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)

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

Operational team
Valeria Betancourt (APC)
Alan Finlay (APC)
Maja Romano (APC)

Project coordination team
Valeria Betancourt (APC)
Cathy Chen (APC)
Flavia Fascendini (APC)
Alan Finlay (APC)
Leila Nachawati (APC)
Lori Nordstrom (APC)
Maja Romano (APC)

Project coordinator
Maja Romano (APC)

Editor
Alan Finlay (APC)

Assistant editor and proofreading
Lori Nordstrom (APC)

Assistant proofreader
Drew McKevitt

Publication production support
Cathy Chen (APC)

Graphic design
Monocromo

Cover illustration
Matías Bervejillo

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

Global Information Society Watch 2021-2022 web and e-book
ISBN 978-92-95113-52-7
APC-202211-CIPP-R-EN-DIGITAL-342

Table of contents

Preface

Valeria Betancourt (APC)

Several of the fundamental notions we took for granted as civil society activists have been transformed by the COVID-19 pandemic. One of the most profound, for me, is our sense of time. It has changed substantially, and we now live oscillating between the dizzying sense of it passing rapidly and having to contend with the feeling that it has been suspended. What impact does this have on the pace of the social changes that we, as civil society organisations and networks, want to be part of?

The pandemic, which hit us in different ways in both the online and offline spheres, has also brought us face to face with the tensions between the connected and the unconnected, the individual and the collective, between the contingent and the predictable, between the rigid and the flexible, between the continuous and the conjunctural, the ephemeral and the permanent, and between the local and the global.

The impacts of digitalisation on the dynamics of our contexts have become more palpable, as well as the ways those impacts relate to old and emerging structural challenges. The weight of physical boundaries and awareness of the limits of the physical space we inhabit were heightened. We were connected in a digital space but were demobilised and disconnected on other levels, a tension tearing at the social tissue that we took for granted.

The relationship between the local and the global, which has historically driven and guided the work of the Association for Progressive Communications (APC), has taken on even greater significance. But if that is the case, what does it mean for our advocacy at both local and global levels? What does this mean for us as a network, as an actor seeking to produce substantial transformations at all levels? Did other forms of collaboration and connection emerge in the peripheries during the pandemic?

These changes have been exacerbated by current overlapping global crises: setbacks in democratic values; the weakening of democratic institutions; the multiplication of anti-rights forces; the rise of authoritarianism; the flourishing of stigmatising narratives; the deterioration of the role of states in the provision of public services; the deprioritisation of sustainable development objectives; and, in general, the shrinking of the civic space.

What does this all imply for strengthening our advocacy in the midst of an intensified sense of fragility and volatility when, paradoxically, everything we do and don' t do will have a decisive bearing on the future? What does this mean in terms of collective action, of activism, of the movements we work with and are part of and the way in which we set goals?

There are no simple answers to these questions.

The pandemic made inequality, discrimination, exclusion and structural inequity more palpable, and rather than stagnating in indignation, it reactivated a sense of rebellion and contestation. The strength and sharpness with which we connect social justice, gender justice, environmental justice, economic justice and racial justice with the potentials and limitations of digital technologies is undeniable. Using this intersectional lens, we need to document and build our own narratives about the challenges that we face related to the impacts of the pandemic and reflect on how our advocacy priorities as well as the ways we do advocacy are changing and keep being modified and adjusted.

At APC we have strengthened capacity to design and implement collective and contextual community responses to the multiple challenges and crises that we face, while having a greater awareness of the kind of global responses that should be prioritised, based on shared but differentiated responsibilities.

We are in a tremendously complex historical moment in which, possibly, the most important anchor of meaning continues to be, for our network and organisation, and for social movements, the commitment to a common horizon of dignity and justice – a horizon in which digital technologies and an open, decentralised, free internet allow us to sustain other ways of life that are compatible with the collective well-being and well-being of our planet.

GISWatch 2021-2022 focuses on responses to some of the fundamental questions brought by the pandemic to inform civil society's advocacy around digital technology issues and their potential to shape future horizons. As illustrated on our cover, a sustained struggle will be necessary in the years ahead, but not only in the public spaces. A nuanced approach to advocacy will be essential to open multiple ways to bring about positive change.

We hope that this edition ignites renewed energy to reshape the sense of "us" going forward towards reinventing the social contract, recognising and embracing our diversity, our multi-referential identities, our complementarities; and contributes to finding effective ways to think and act beyond all the crises and contingencies that surround us at the moment as actors of change in the digital environment.

Introduction

Valeria Betancourt and Alan Finlay
Association for Progressive Communications (APC)

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

Thematic reports

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

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

networks and our advocacy partner in Zimbabwe, 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.

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

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

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.

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.

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

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%A30-de-dados-em-meio-ao-avan%C3%A70-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.

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 gov-

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

ernments 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.

Big data, big tech, big problems: Time to look beyond

Paz Peña[1]
https://pazpena.com

Introduction

We hardly talk about the internet anymore. Instead, we talk about platforms: tweeting, googling, and so on, with almost all our social interactions mediated by technologies. Not only do we no longer talk about the internet, but we have also adopted the intentionally empty concepts with which dominant companies seek to naturalise their extractive interactions: "sharing economy", "communities", "likes", and a long etcetera that even includes the idea of "platforms". On this, Ben Tarnoff indicates that the positioning of the word "platform" has been strategic for big tech, as it projects an aura of openness and neutrality, hiding its control over our digital life and its active role in managing those spaces.[2]

But beyond the convenience it has for big tech, what does the concept of platformisation refer to? First of all, it is a type of business model, increasingly predominant, in which a technological infrastructure is designed as an essential mechanism for extracting and using data. And it is the latter that is essential, driving these companies and giving them their edge over competitors. In other words, datafication underpins platformisation. As data becomes a central resource for technology and non-technology sectors of the economy, companies in various sectors must quickly develop ways to obtain and aggregate this information.[3]

But not all companies using this logic are equally powerful. For example, in recent years, dominant companies from the global North, particularly from Silicon Valley (the companies we mostly refer to when we say "big tech"), have cultivated an advantageous position as a result of their unusual appetite for data, which they must obtain in various forms and using multiple methods (including the purchase of promising start-ups).

For this reason, these "platforms" have the characteristics of both companies and marketplaces. That is to say, on the one hand, they offer various products and services, and on the other, they are constituted as markets for economic exchange. As intermediaries, specifically, platforms connect and define relationships between entities in the multilateral markets they host, while their pursuit of network effects (i.e. the more users use a platform, the more valuable that platform becomes) ends in a "virtuous circle" that leads to winner-take-all monopolies.[4]

In this sense, for many, platformisation signals a broader shift in capitalism: one where the entire economy shifts from a market-based economy to one based on the advantageous conditions that platforms can impose in digital markets. Moreover, the platforms' management of user interactions and relationships in these markets is automated by data-driven algorithms designed for economic gain, and which are structured through technical interfaces and private terms of service, implying a highly politically and culturally advantageous position.

In addition, this unusual appetite for data has led these companies to seek out unregulated and under-regulated areas for extracting personal data. As a result, many researchers claim that we are facing a kind of digital colonialism, in which these companies build communication infrastructures, such as social media platforms and network connectivity, with the express purpose of harvesting

1 Paz Peña is an independent consultant at the intersection of technology, feminism and social justice. She is the coordinator of the Latin American Institute of Terraforming, where she researches the relationship between digital technology and the climate and ecological crisis.

2 Tarnoff, B. (2022, 16 June). 'Wallets and eyeballs': how eBay turned the internet into a marketplace. *The Guardian*. https://www.theguardian.com/technology/2022/jun/16/wallets-and-eyeballs-how-ebay-turned-the-internet-into-a-marketplace

3 Srnicek, N. (2017). The challenges of platform capitalism: Understanding the logic of a new business model. *Juncture, 23*(4), 254-257. https://doi.org/10.1111/newe.12023

4 Srnicek, N. (2017). Ibid.

data, making profits, and storing the data as raw material for predictive analytics. As Danielle Coleman[5] concludes, this allows them to accrue profits from revenue derived from rent (in the form of intellectual property or access to infrastructure) and surveillance (in the form of "Big Data"). It also allows them to control the flow of information, social activities, and various other political, social, economic and even military functions mediated by their technologies.

The eruption of the pandemic

The pandemic has deepened the warnings that were already being made by academia and civil society. For Gavrilenko and Markeeva,[6] the forced digitisation of the past two years has revealed at least three key issues that should make us reflect deeply: the economic and ideological power of platforms, their capability of changing markets and influencing political institutions, and their increasing control over people's lives.

For these researchers, thanks to the pandemic, it is now much clearer that the primary vector of competition in platformisation is not so much control of resources as control of access to them. In other words, big tech is not merely a "service provider": far from neutrality, in many cases, the platforms are significant players in their own markets. The authors also point out how, due to the pandemic, political institutions have been influenced by the platforms' ideology (which has also been referred to as the "Californian" or "Silicon Valley" ideology), and which has been adopted without question by economic elites in many countries. This ideology is nothing more than a form of libertarian thinking that, behind the common façade of "efficient technical solutions", seeks to reduce costs and subordinate social policy to the requirements of labour flexibility and competitiveness, among others.

This relates to a development that is, in my opinion, more disturbing than the privatisation of digital spaces: that the state and platforms are forming a new consensus in the division of power and control over everyday life, testing all the various ways of expanding the aggregation of personal information to do this. In the context of developing solutions to prevent a pandemic, these actions are necessary and justified, say Gavrilenko and Markeeva, but they warn that it is essential to create conditions for the post-pandemic world to consider the opinions and interests of citizens, traditional businesses, and public organisations.

Is it too complex or too late?

In this context, perhaps it is time to take a critical look at the prevention and mitigation mechanisms that have so far been promoted as public policy as a counterweight to the platforms. One should look, for example, at the role that more liberal interpretations of human rights have played in strengthening the power of these platforms. Rights such as freedom of expression have been co-opted by these companies for the almost non-existent intervention in their algorithms and terms of service as if they were neutral spaces where their profit interests were the equitable measure for all societies. Privacy and personal data protection, for their part, falter in the face of covert surveillance for commercial and political purposes that would seem to be an acceptable trade-off in societies exhausted under capitalist production. And even when the personal data legal frameworks of powerful local or regional contexts seem to work – as in the case of the General Data Protection Regulation (GDPR) in the European Union, which served as a shield of protection from WhatsApp's change in terms of service in 2021 – this has only shifted personal data extractivism to confines with less protection and, above all, less power to stand up against big tech.[7]

Several authors have asked whether antitrust law can go deep enough to address the challenges posed by platformisation. For example, for Pawel Popiel,[8] economic regulation and the separation of business lines are key ways of doing this. However, to address the real challenges of digitisation and platformisation, these policies cannot act in silos; and they must be accompanied by the promotion of alternatives to dominant platforms through subsidies, as this type of stimulus, which includes models of public ownership and governance, is essential to attaining benefits of scale. For Michael Kwet,[9] antitrust reform, which is presented as a solution by countries in the global North with the

5 Coleman, D. (2019). Digital Colonialism: The 21st Century Scramble for Africa through the Extraction and Control of User Data and the Limitations of Data Protection Laws. *Michigan Journal of Race and Law, 24*(2). https://repository.law.umich.edu/mjrl/vol24/iss2/6

6 Gavrilenko, O., & Markeeva, A. (2020). Digital Colonization: Development of Digital Platforms in the Context of a Pandemic. *Postmodern Openings, 11*(1Sup2), 65-73. https://doi.org/10.18662/po/11.1sup2/141

7 Kilic, B., & Crabbe-Field, S. (2021, 14 May). You should be worried about how much info WhatsApp shares with Facebook. *The Guardian*. https://www.theguardian.com/commentisfree/2021/may/14/you-should-be-worried-about-how-much-info-whatsapp-shares-with-facebook

8 Popiel, P. (2022). Regulating datafication and platformization: Policy silos and tradeoffs in international platform inquiries. *Policy & Internet, 14*(1), 28-46. https://doi.org/10.1002/poi3.283

9 Kwet, M. (2022, 31 May). Digital Ecosocialism: Breaking the power of Big Tech. *TNI*. https://longreads.tni.org/digital-ecosocialism

desire to take care of their own colonial domains, is particularly problematic because it assumes that the problem of the digital economy is simply the size and "unfair practices" of large companies and not digital capitalism itself. The author reminds us that antitrust laws only work for those players who can compete, so there is little that legislative reform can do for the global South to stem the ongoing dominance of big tech platforms.

Along these lines, it has also been explored how data portability and interoperability measures can foster competition both within and across digital platforms, as they can address barriers to market entry arising from network effects and foster innovation. However, as an Organisation for Economic Co-operation and Development (OECD) report acknowledges,[10] these measures are not suited to all circumstances. For example, where a dominant digital platform faces no rivals (including potential entrants with sufficient capacity to compete), these measures may be more appropriate in promoting competition in related and complementary markets than allowing competitors to the leading platform to emerge.

Many of these approaches lack a real geopolitical approach. It is not about the dominance of only a handful of ultra-powerful companies but also that they count on the protection of their governments that, in alliance, seek the economic supremacy of their countries. As Renata Avila[11] points out, such countries and companies have three elements that most developing nations and even middle-income countries lack: advanced capital and intellectual resources, a domestic and international legal architecture in their favour, and the current patent and intellectual property system that artificially restricts knowledge sharing and innovation.

In this context, for many authors, the response to platformisation should not only rely on individual or coordinated legal reactions but also on the impulse that governments should give to digital sovereignty, consisting of locally designing and producing the next generation of technologies that have values, behaviours and social dynamics different from those that dominate big tech. However, this discussion is similar to those occurring in Latin America regarding the exploitation of natural resources by foreign mining mega-companies: for many, a way out of this exploitation is nationalisation, which is a pale answer to ending extractivism because it now will be exercised by the state. In fact, many of the state funds for new technologies seek to find the new "local unicorn" that will finally make real the promise of building the local Silicon Valley.

Peak data

Perhaps, as in mining, the strategy should vary and, instead, work on building critical reflection on data extractivism that will put an end to the idea that personal data can be produced and exploited at almost no cost. While it is possible to increase these costs through legislation, big tech is today in such an advantageous position with the amount of information it handles that it can dictate the price: one need only recall Google's promise to end third-party cookies by 2023.[12] In this problematic context, perhaps it is time to look at Geert Lovink's proposal,[13] which states that it is only a matter of time before this super-maximisation of data flows reaches its peak, whether due to technical issues or not. Following the definition of peak oil, Lovink believes that peak data will be the moment when the maximum rate of extractivism is reached, and thus, the platform logic implodes:

> Peak data is related to the distinct concept of data depletion when the moral cost of "surveillance capitalism" outweighs the economic benefit for the few and society as a whole starts to decline because of an excess of social disparity. Once the peak is reached, the presumption that the better the information, the better the decision-making process can no longer be maintained.

The idea of peak data also seems interesting not in the sense of believing that data is a finite natural resource like oil (on the contrary, it is infinite and intentionally produced by humans), but in the more recent context of understanding the idea of "peak oil": it is not caused by resource depletion (along the lines of the highly debatable Malthusian idea of overpopulation) but produced by the drop in demand for oil due to the imperative to end the use of fossil fuels because of the planetary climate and ecological crisis.

10 OECD Competition Committee. (2021). *Data Portability, Interoperability and Digital Platform Competition*. OECD. https://www.oecd.org/daf/competition/data-portability-interoperability-and-digital-platform-competition-2021.pdf

11 Ávila, R. (2018). ¿Soberanía digital o colonialismo digital? *Sur, 27*. https://sur.conectas.org/es/soberania-digital-o-colonialismo-digital

12 Rus, D. (2022, 30 June). Google Analytics 4: Moving Into A New Era Of Data Tracking. *Forbes*. https://www.forbes.com/sites/forbestechcouncil/2022/06/30/google-analytics-4-moving-into-a-new-era-of-data-tracking/?sh=7158dacb18a3

13 Lovink, G. (2022, 7 April). Proposition on Peak Data. *Institute of Network Cultures*. https://networkcultures.org/geert/2022/04/07/proposition-on-peak-data

In a concrete sense, perhaps it is precisely this crisis – the most crucial challenge in the history of humankind – that will help to reach peak data in the sense that, as the 2022 Intergovernmental Panel on Climate Change (IPCC) mitigation report says,[14] the only way we can be sure that digitalisation will not contribute to increasing energy use in various industries is if it is decoupled from increased consumption. If, so far, platformisation has been primarily driven by datafication for consumer profiling, the data peak is already near, and governments and different stakeholders must urgently design and deploy a different kind of digitalisation if we want to stay within the 1.5°C targets. In this framework, it is not so far-fetched for the digital rights community to look closely at how the climate and ecological crisis can be vital to understanding the new possibilities for ending the dominance of big data and big tech. The bad news, of course, is that the latter is already deploying investments to show themselves as the "green way" out of the crisis.[15] If the fossil fuel kings fall, others are running after that throne. Let's not let them.

14 Peña, P. (2022, 10 April). That technological future does not exist. *Latin American Institute of Terraforming*. https://terraforminglatam.net/that-technological-future-does-not-exist

15 Brigham, K. (2022, 28 June). Why Big Tech is pouring money into carbon removal. *CNBC*. https://www.cnbc.com/2022/06/28/why-companies-like-stripe-meta-and-alphabet-are-behind-carbon-removal.html

The rights approach: Pushing back against opaque public-private partnerships

Gayatri Khandhadai
Business and Human Rights Resource Centre
https://www.business-humanrights.org/en

Private-public partnerships

Public-private partnerships (PPPs) across a range of sectors, including digital and information and communications technology (ICT), offered important solutions to an impossible situation created by the COVID-19 pandemic. PPPs were lauded for playing a pioneering role in combating the coronavirus.[1] States were swift to adopt digital solutions to support lives and for governance during this period, as well as to help ease challenges created by prolonged lockdowns. As a result, there was significant demand for ICT infrastructure in these fields.[2]

Typically, PPPs offering digital-based solutions and support during the pandemic included the development and deployment of contact tracing apps, vaccine enrolment and management platforms, and health information dissemination partnerships. While the benefits of such partnerships seemed obvious, several civil society actors warned of pitfalls.

Concerns centred around privacy, data protection and security measures that govern digital platforms, particularly for those who communicate with the expectation that their data be held securely from third parties.[3] We also witnessed the large-scale spread of misinformation on social media platforms and messaging applications.[4] Coordinated campaigns were carried out on these platforms to push harmful narratives targeting racial groups[5] and minority communities for spreading the virus.[6] While platforms stated that they were putting in place policies to take down content or harmful "fake news" about coronavirus and vaccines,[7] implementation varied depending on the context. Above all else, the aggressive use of digital technologies to manage the pandemic further widened the digital divide, impacting the lives of millions of people who either do not have any access to the internet or do not have proper access that is affordable and accessible.[8] Enshrining platforms and technology-driven "solutions" at the centre of our pandemic response ceded authority to define the values at stake, and

1 Davis, A. M., Engkvist, O., Fairclough, R. J., Feierberg, I., Freeman, A., & Iyer, P. (2021). Public-Private Partnerships: Compound and Data Sharing in Drug Discovery and Development. *SLAS Discovery: Advancing Life Sciences R & D*, 26(5), 604-619. https://doi.org/10.1177/2472555220982268

2 Grover, S., Rahemtulla, H., & Gin, C. (2020, 29 May). Managing Public-Private Partnerships for a Post-Pandemic Recovery. *Asian Development Blog*. https://blogs.adb.org/blog/managing-public-private-partnerships-post-pandemic-recovery

3 Various. (2020, 21 April). Joint civil society open letter to the UN on public-private partnerships. *APC*. https://www.apc.org/en/pubs/joint-civil-society-open-letter-un-public-private-partnerships

4 Volkmer, I. (2021). *Social media & COVID-19: A global study of digital crisis interaction among Gen Z and Millennials*. Wunderman Thompson, University of Melbourne, Pollfish & World Health Organization. https://www.who.int/news-room/feature-stories/detail/social-media-covid-19-a-global-study-of-digital-crisis-interaction-among-gen-z-and-millennials

5 Dubey, A. D. (2020). The Resurgence of Cyber Racism During the COVID-19 Pandemic and its Aftereffects: Analysis of Sentiments and Emotions in Tweets. *JMIR Public Health and Surveillance, 6*(4). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7596656

6 Murthy, L. (2020). *The Contagion of Hate in India*. APC. https://www.apc.org/en/pubs/contagion-hate-india

7 See, for example: Hern, A. (2020, 19 March). Twitter to remove harmful fake news about coronavirus. *The Guardian*. https://www.theguardian.com/world/2020/mar/19/twitter-to-remove-harmful-fake-news-about-coronavirus

8 Holmes, H. & Burgess, G. (n/d). "Pay the wi-fi or feed the children": Coronavirus has intensified the UK's digital divide. *University of Cambridge*. https://www.cam.ac.uk/stories/digitaldivide

deepened pre-existing patterns of inequality in society.[9]

Despite these challenges, governments invested large amounts of money in procuring private sector technology and building PPPs to deliver digital solutions to the pandemic.[10] The allocation of budgets relating to digital transformation has since risen in many countries.

Information pertaining to PPPs and processes governing them is often hard to find since they typically require exclusive contracts. Even prior to the pandemic, civil society groups and digital rights defenders had to grapple with the "black box" phenomenon where public knowledge about the ways in which technologies or tech-based companies function act as a barrier to mitigating or addressing human rights violations.[11] Another point to note about the state-company nexus is that there is often a lack of clarity regarding the types of data that governments and the companies they work with have access to, along with a lack of transparency of ongoing impact assessments, including those for data protection.[12] The Global Network Initiative has also reported government efforts to acquire "direct access" to user data in ways that remove intermediaries' awareness of and opportunities to object to or be transparent about this access.[13]

Looking to the UNGPs

Given that regulatory systems governing these partnerships and the ICT sector are vastly different across jurisdictions, the UN Guiding Principles on Business and Human Rights[14] (UNGPs) offer a principled and pragmatic approach for ensuring that technological advances are grounded in respect and dignity for all and that their governance is rooted in rights. The UNGPs mandate that the state has the responsibility to protect our rights, that companies have a responsibility to respect our rights, and that we must have access to remedy.

Principles four to six of the UNGPs cover a range of policy areas relating to the "state-business nexus". This includes financial and other support provided by states to companies, the privatisation of services that may impact human rights enjoyment, and public procurement. Irrespective of the kinds of contracts that states may hold with private actors, they cannot outsource the responsibility to protect human rights. Therefore, states must put in place adequate oversight mechanisms and policies or regulations for accountability. Where states financially support, contract with or procure from technology companies, they should actively use that opportunity to ensure that the companies they work with respect human rights.[15]

Another key recommendation in the UNGPs relates to due diligence. While the conduct of human rights and environmental due diligence (HREDD) in itself may not remedy harms caused by technology, it is critical in understanding risks and devising mitigation strategies or solutions. Given the close relationship that states have developed with technology-based companies and the ever-growing procurement of technology, states must conduct proper assessments before formalising partnerships and require companies to conduct thorough HREDD as a prerequisite for contracts.

PPPs with tech-based companies are fast evolving into opaque bilateral relationships. Even in instances where tech-based companies are willing to use HREDD, ongoing challenges,

9 Cohen, J. E., Hartzog, W., & Moy, L. (2020, 17 June). The dangers of tech-driven solutions to COVID-19. *Brookings Tech Stream*. https://www.brookings.edu/techstream/the-dangers-of-tech-driven-solutions-to-covid-19

10 Fiscal responses of most states included digital-related expenditure, as seen in: https://www.imf.org/en/Topics/imf-and-covid19/Policy-Responses-to-COVID-19

11 United Nations Human Rights Office of the High Commissioner. (2021). *B-Tech: Bridging Governance Gaps in the Age of Technology – Key Characteristics of the State Duty to Protect*. https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/b-tech-foundational-paper-state-duty-to-protect.pdf

12 Phu, S. (2021). *Empowering human rights in the State-business nexus: Digital technologies and human rights due diligence*. United Nations Human Rights Office of the High Commissioner. https://www.ohchr.org/sites/default/files/2022-01/Blog_post_GNI_Blog.pdf

13 https://globalnetworkinitiative.org/defining-direct-access-2

14 United Nations. (2011). *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*. https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf

15 United Nations Human Rights Office of the High Commissioner. (2021). Op. cit.

including confidentiality, hinder the development of best practices around HREDD when it comes to sensitive business decisions that involve states as customers or partners.[16] The public – and more specifically digital rights defenders – are left out of these discussions and, as a result, important perspectives are lost.

States using technology and tech-based companies have lost significant public trust in the face of never-ending rights violations. To regain some social licence to operate, companies must engage with civil society actors and affected communities in the HREDD process and states must ensure that an inclusive environment is fostered.

Way forward

The pandemic and the immeasurable loss we suffered have taught us critical lessons for the future. For civil society, the agenda for accountability hinges on eroding the opacity of PPPs and ensuring that our voices are heard. States and the private sector need to know and show that they are committed to processes and safeguards against digital authoritarianism and abuse.

States should commit to guaranteeing access and accessibility to all people, and this promise must be accompanied by sufficient allocation of resources to build the necessary infrastructure and promote community-led solutions to access. This is the stepping stone for a people-centred digital transformation, one that will pave the way for meaningful and rights-based PPPs.

The primary responsibility for protecting our rights rests with the state, and this means that PPPs that the state wishes to enter into need analysis, consultation and oversight. Adequate and predictable accountability mechanisms stemming from regulation and policy, especially in areas relating to data protection and intermediary liability, are necessary for accountability.

PPPs using digital technologies must begin with thorough HREDD and be subjected to audits as needed. Grievance mechanisms in companies that are a part of these undertakings are critical for the relationship they have with the community. Periodic assessments and adjustments are possible only if communities impacted by these operations and civil society have a seat at the table. Stakeholder engagement in PPPs across their life cycle should be mandatory.

For meaningful engagement to take place, information and data about these PPPs and operations are central. The state and companies involved would need to proactively make information available, including information relating to the contracts that bound the parties together.

We are witnessing ongoing efforts from Europe[17] to Japan[18] in the enactment of policies and regulations on HREDD. For civil society and internet users, this is a critical moment to ensure that these policies meet our aspirations and pave the way for an era of accountability in the tech sector.

16 Phu, S. (2021). Op. cit.

17 Khandhadai, G. (2022). *Buffering rights: How Europe's new due diligence regulation can help reverse tech rights risks*. Business and Human Rights Resource Centre. https://www.business-humanrights.org/en/from-us/briefings/buffering-rights-how-europes-new-due-diligence-regulation-can-help-reverse-tech-rights-risks

18 Nikkei Asia. (2022, 15 February). Japan: Govt. to set human rights due diligence guidelines for companies, hoping to close gaps with US and European countries. *Business and Human Rights Resource Centre*. https://www.business-humanrights.org/en/latest-news/japan-govt-to-set-human-rights-due-diligence-guidelines-for-companies-hoping-to-close-gaps-with-us-and-european-countries

Global digital labour platforms offer a mirage of inclusive development in Africa

Kelle Howson
Research ICT Africa; Fairwork, Oxford Internet Institute
https://researchictafrica.net; https://fair.work

Introduction

We have seen a sudden shift in public attitudes towards Uber's business strategies around the world, following widespread coverage of the "Uber Files" – more than 124,000 leaked internal company documents – in July 2022.[1] The documents span a period from 2013 to 2017, and contain extensive details of Uber's aggressive and often illegal expansion.[2] Much of this pertains to the company's strategy of forcing its way into markets including in Africa, and taking advantage of local conditions to exploit workers and pressure regulators. While Uber spokespeople have claimed that the company has changed under new leadership,[3] the digital labour platform model continues to grow in Africa, and its consequences for workers have been laid bare especially in the wake of the COVID-19 pandemic.

While the Uber Files paint a shocking picture for the general public, they contain few revelations for platform workers in Africa, and for those of us who research digital labour platforms in the region. In fact, the leak described with startling accuracy the practices that workers and researchers have long been trying to draw attention to.

In many respects, Uber has been the most successful at instituting these practices, but they are by no means unique to the company, and instead typify the model of digital labour platforms more broadly, including across the ride-hailing, food, last-mile delivery, and domestic services sectors. Hallmarks of the digital labour platform model include digital intermediation of on-demand services, evasion of labour protections, algorithmic management techniques, and piece-rate payment (or payment per "gig").

Many of the practices described in the Uber Files have been honed in African markets in particular.[4] This is due to a variety of structural features that digital labour companies have been able to exploit. These include high levels of unemployment and informality, policies attempting to facilitate digital development, existing social inequities, and legacies of imperialism and colonisation. In these environments, Uber and other global digital labour platforms have deployed monopolistic strategies of rent seeking, regulatory evasion, and data extractivism.

Contrary to the platform narrative of creating decent, flexible work in places where it is desperately needed, these strategies have at their heart the exploitation of precarious workers and accumulation of value offshore. During COVID-19, African platform workers have consequently been exposed to disproportionately high levels of risk.[5] This includes the risk of exposure to the virus in the course of their work. This risk was heightened by platform workers' lack of access to the social safety nets which protected other workers during lockdowns – such as sick leave provisions, or unemployment benefits such as South Africa's Unemployment Insurance Fund. Because platform workers are not classified by platforms as employees, they often fall outside statutory protections.

Yet the pandemic has also shown how successful digital labour platforms have been at interweaving themselves into vital public services and infrastructure, and filling institutional voids in developing

1 International Consortium of Investigative Journalists. (2022). *The Uber Files*. https://www.icij.org/investigations/uber-files

2 Deck, A. (2022, 18 July). "We're just fucking illegal": Uber Files reveal a pattern of shady behavior around the world. *Rest of World*. https://restofworld.org/2022/uber-files-rest-of-world

3 International Consortium of Investigative Journalists. (2022, 10 July). Statement from Uber spokesperson on the Uber Files. https://www.icij.org/investigations/uber-files/statement-uber

4 MacMillan, D. (2022, 11 July). Uber promised South Africans better lives but knew drivers risked debt and danger. *Washington Post*. https://www.washingtonpost.com/business/2022/07/11/uber-driver-south-africa-attacks

5 Howson, K., et al. (2021, 1 July). Stripping back the mask: Working conditions on digital labour platforms during the COVID-19 pandemic. *International Labour Review*. https://doi.org/10.1111/ilr.12222

countries.[6] This report discusses the underlying context of digitalisation in Africa, what the Uber Files reveal about digital labour platform strategies in this context, and how these strategies have impacted workers – particularly in the pandemic. While the discussion is specific to Africa, similar phenomena, although shaped by local conditions, are no doubt evident in other parts of the world.

High hopes for the Fourth Industrial Revolution

Uber and other global digital labour platforms have been supported to expand in African markets in part by development policies which aim to embrace technological advancement to address challenges of low growth and high unemployment. In the global South, the "Fourth Industrial Revolution", or "4IR", is seen by many policy makers as an important opportunity for job and economic growth,[7] and an alternative way to catch up to more advanced economies, amidst trends towards deindustrialisation.[8] 4IR refers to the idea that digitalisation will fundamentally transform production relations.

4IR policy discourse suggests that developing economies can harness this shift to drive productivity and growth, by specialising in information and communications technologies (ICTs) and digital commodities and services, and fostering tech entrepreneurs and startups. The African Union, as well as African governments, have placed heavy emphasis on the potential of the 4IR to create opportunities for young unemployed people across the region.[9] As the COVID-19 pandemic has disrupted industries and employment relations, calls for the creation of enabling regulatory environments for digital development have been amplified.[10] These calls were already gaining ground throughout the 2010s, and had evolved in step with the growth of the global tech sector.

An African Union Specialized Technical Committee Ministerial Meeting on the theme "Leveraging the 4th Industrial Revolution to Address Youth Unemployment in Africa" was set to be held in Accra, Ghana, in March 2020, and later postponed because of the onset of the pandemic. In the lead-up, a media release said that "the continent, if it prepares itself through adequate policies and readiness of the private sector, could enormously benefit through industrial development, digitalization and greater integration, which in turn would result in greater opportunities for our growing youthful populations."[11]

The accompanying concept note anticipates that the growth of the global tech sector will present risks, complexities and uncertainties for the African region, but makes no mention of the need to protect workers' rights or vulnerable social groups in the context of digitalisation. Instead, it adopts a neoliberal line, advocating for private sector-led development, and the removal of regulatory barriers to business.[12] It sees the ideal role of government regulation as "facilitat[ing] the digital era to grow rapidly", as opposed to "slow[ing] down the successful adaptation of new technologies in production."

These priorities have been echoed by various African leaders, including Rwanda's Minister of Information Communication Technology and Innovation Paula Ingabire when, in partnership with the World Economic Forum, she launched a centre for technological innovation and artificial intelligence (AI), called the "Centre for the Fourth Industrial Revolution".[13] South Africa's President Cyril Ramaphosa also established a Presidential Commission on harnessing 4IR.[14]

But, with the Uber Files coming as the latest in a succession of stories of platform power being exercised unchecked on the African continent,[15] the utopian veneer of digital efficiency and empowerment that accompanies digital labour platforms may be starting to fade. Other recent exposés of platform practices include Time Magazine's reporting in 2022 on the exploitation of platform workers moderating

6 Heeks, R., et al. (2021). Digital platforms and institutional voids in developing countries: The case of ride-hailing markets. *World Development*, *145*. https://doi.org/10.1016/j.worlddev.2021.105528

7 African Development Bank Group. (2019). *Fourth Industrial Revolution in Africa: Study on unlocking the potential of the fourth industrial revolution in Africa*. https://www.technopolis-group.com/wp-content/uploads/2020/02/Potential-of-the-fourth-industrial-revolution-in-Africa.pdf

8 Naudé, W. (2017). *Entrepreneurship, Education and the Fourth Industrial Revolution in Africa.* IZA Institute of Labor Economics. https://www.iza.org/publications/dp/10855/entrepreneurship-education-and-the-fourth-industrial-revolution-in-africa .

9 African Union. (2020, 26 February). The 4th industrial Revolution, a watershed moment for Africa's development. https://au.int/fr/node/38163

10 Nachit, H., & Belhcen, L. (2020). *Digital Transformation in Times of Covid-19 Pandemic: The Case of Morocco.* SSRN. https://dx.doi.org/10.2139/ssrn.3645084

11 African Union. (2020, 26 February). Op. cit.

12 African Union Specialized Technical Committee on Finance, Monetary Affairs, Economic Planning and Integration. (2020). *Leveraging the 4th Industrial Revolution to Address Youth Unemployment in Africa.* https://au.int/sites/default/files/newsevents/conceptnotes/38223-cn-2020_4th_stc_concept_note_-_eng.pdf

13 Indebele, L. (2020, 6 April). Rwanda launches centre dedicated to artificial intelligence. *News24*. https://www.news24.com/news24/africa/news/rwanda-becomes-first-african-country-to-launch-centre-dedicated-to-artificial-intelligence-20220406

14 The Presidency (Republic of South Africa). (2019, 9 April). President appoints Commission on Fourth Industrial Revolution. https://www.thepresidency.gov.za/press-statements/president-appoints-commission-fourth-industrial-revolution

15 International Consortium of Investigative Journalists. (2022). Op. cit.

content for Facebook in Kenya,[16] as well as reporting from media organisation Rest of World on the pressures that digital platform workers in Africa have been exposed to during the pandemic.[17] Rather than triggering a virtuous cycle of economic empowerment and innovation, it seems increasingly clear that these companies have used their digital tools to extract rents from African service and transport sectors and exploit workers without giving much back in return.

The platform model: Management at arm's length

The recent reports and leaks have called into question narratives of 4IR-driven development and technological solutionism in the global South. While initiatives such as Rwanda's centre for technological innovation envision local digital innovation as a driver of future growth, in reality, ownership and profit in the tech sector are highly concentrated in existing centres of wealth and power – notably California in the United States.[18] This follows long-established geographical patterns of global capitalism.[19] The Uber Files call attention to the arm's length, disembedded management model instituted by digital labour platforms,[20] alongside the general absence of the platform companies from policy and labour relations dialogue, and from civic life in general, despite their enormous influence.

The Uber Files show how the company leveraged extremely high levels of unemployment in African countries to rapidly enrol an oversupply of workers, capture transport markets, and then raise prices.[21] South Africa, for instance, has an unemployment rate of over 40% (including discouraged work seekers).[22] In this desperate context, Uber lured thousands of drivers with attractive subsidies, and once the platform had enrolled enough users to secure a monopoly while ensuring that labour supply vastly outstripped demand, it undercut drivers – upping its commission and eroding pay to the extent that South African cities became the company's most lucrative markets outside the US.[23] More recently, the company has introduced cut-price services in African markets (for instance, Uber Chap Chap in Kenya, Uber Go in South Africa), forcing drivers of older or smaller cars onto these poorer-paying services. In many cases this has left drivers struggling to meet their obligations under car rental or financing arrangements.[24]

Uber contracts drivers from a limited liability company registered in the Netherlands (Uber B.V.), and classifies them as "independent contractors". This has ensured their workers have little recourse to local judicial or statutory labour protections. In countries with high levels of informality, where the majority of workers are not formal employees with protections such as minimum wage, sick and maternity leave, income insurance, and due process for dismissal, these arrangements have been justified as a step up from the status quo.[25]

However, they have forcibly closed off avenues for improvement in labour standards and collective bargaining, and aimed to normalise and legitimise precarious informal labour relations as standard. A case brought against Uber by a group of drivers challenging what they saw as employment misclassification was dismissed by the South African Labour Court because the drivers were contracted by a company in the Netherlands. The court said they could not dispute their contracts in South Africa.[26]

These strategies of regulatory evasion are reflected throughout the Uber Files. Uber's rapid expansionism, enabled by advancements in computing capabilities and connectivity infrastructure, allowed the company to insert itself into local transport systems so quickly and decisively – ignoring local civic processes, social dialogue and regulation – that by the time its influence became clear, it was extremely difficult to regulate. Then, when it did eventually become subject to regulatory pressure, it unleashed massive corporate lobbying efforts to deflect such pressure, and in some cases attempted to rewrite laws in its favour.[27] When Nigerian authorities tried to address Uber's tax evasion, the Uber Files show

16 Periggo, B. (2022, 17 February). Inside Facebook's African Sweatshop. *Time*. https://time.com/6147458/facebook-africa-content-moderation-employee-treatment

17 Mwareya, R., Bhat, A., & Relmucao, J. J. (2022, 17 June). Rising food and fuel costs are making gig work unsustainable. *Rest of World*. https://restofworld.org/2022/rising-fuel-food-costs-gig-workers

18 Rani, U., et al. (2021). *World Employment and Social Outlook 2021: The role of digital labour platforms in transforming the world of work*. International Labour Organization.

19 Howson, K., et al. (2021, 28 December). Driving the digital value network: Economic geographies of global platform capitalism. *Global Networks*. https://doi.org/10.1111/glob.12358

20 Wood, A. J., Graham, M., Lehdonvirta, V., & Hjorth, I. (2019). Networked but Commodified: The (dis)embeddedness of digital labour in the gig economy. *Sociology*, *53*(5), 931-950. https://doi.org/10.1177/0038038519828906

21 MacMillan, D. (2022, 11 July). Op. cit.

22 Statistics South Africa. (2022). *Quarterly Labour Force Survey: Quarter 1, 2022*.

23 Ibid.

24 Howson, K., et al. (2021, 28 December). Op. cit.

25 Pollio, A. (2019). Forefronts of the sharing economy: Uber in Cape Town. *International Journal of Urban and Regional Research*, *43*(4), 760-775. https://doi.org/10.1111/1468-2427.12788

26 MacMillan, D. (2022, 11 July). Op. cit.

27 Davies, H., Goodley, S., Lawrence, F., Lewis, P., & O'Carroll, L. (2022, 11 July). Uber broke laws, duped police and secretly lobbied governments, leak reveals. *The Guardian*. https://www.theguardian.com/news/2022/jul/10/uber-files-leak-reveals-global-lobbying-campaign

that the company deflected by offering to help the government collect tax from its drivers.[28]

Meanwhile, despite the high commissions that the platform companies take from each transaction, their operating costs are miniscule. They tend to own very little, if any, physical assets in the places they operate, such as cars, buildings and mobile connectivity infrastructure.[29] They are not subject to many taxi and transport regulations and they also do not contribute directly to road maintenance. If they decided to exit African markets, they could do so with very little cost or difficulty – and this dynamic gives them significant leverage over regulators.[30]

Worker resistance against algorithmic control and poor pay

Even though platform workers are nominally independent, in reality they are subject to methods of digital control which reduce their agency and institute a relationship of subordination with platform companies. Drivers on Uber, or similar platforms such as Bolt and DiDi, don't set their rate, and as gig workers they have no way of knowing what they might earn in a day (especially if the platform gives customers unexpected discounts and incentives).[31] They are surveilled and disciplined by platforms, including through ratings systems. They can have their accounts blocked or terminated instantly and without recourse, losing access to their livelihood – and many do.

As fuel prices and platform fees increase, most drivers have little choice but to work for longer and longer hours, competing with other drivers for relatively inelastic demand from passengers. For women workers who carry a higher burden of unpaid care and domestic work, this pressure to work longer hours is even less tenable, making it more difficult to compete with their male counterparts. Women are often attracted to platform work because they need flexibility. Yet this is often revealed not to be the reality. Research ICT Africa's recent research on working conditions in the South African platform economy uncovered marked gender inequities within and between sectors.[32]

But workers face high barriers to holding platforms accountable in court. In many places they are not easily able to form or be represented by traditional unions, typically only available to employees. Often the platforms' methods of digital management atomise workers, cast them into competition, and make it difficult for them to meet and build solidarity. Nevertheless, ride-hailing drivers and food couriers have organised through social media and WhatsApp groups, which are used for sharing information and mutual support.[33]

Numerous strikes and protests have taken place against platform practices across African cities since the onset of COVID-19. Many of these have focused on issues of safety and security stemming from the pandemic, but the majority have focused on cost pressures in light of pandemic-driven inflation, rising fuel prices, and depressed demand. Striking workers have highlighted the platforms' rising commissions and lack of local accountability.

In 2021, Uber and Bolt drivers in Kenya and Nigeria protested the platforms' commissions amid COVID-related inflationary pressures and the rising cost of fuel.[34] In South Africa, drivers working on Uber, Bolt, InDriver and DiDi brought services to a near standstill during a three-day strike in major cities in South Africa from 22 to 24 March 2022.[35] The organisers – a group called Unity in Diversity – mobilised drivers for an app "switch-off". This was accompanied by protests calling for fair remuneration and better security. In Egypt, food couriers held a two-day strike in April 2022 to demand higher wages in light of inflation.[36]

Conclusion

Experience since the pandemic is increasingly revealing that the entry of digital labour platforms into African markets has not spurred inclusive digital transformation and the creation of sustainable livelihoods, as anticipated by 4IR-friendly policies. Instead, global platforms have entered African economies as rent seekers, deriving profit from (largely already existing) service sectors like transport and

28 Deck, A. (2022, 18 July). Op. cit.

29 Srnicek, N. (2016). *Platform Capitalism*. Polity Press.

30 Graham, M. (2020). Regulate, replicate, and resist – the conjunctural geographies of platform urbanism. *Urban Geography*, *41*(3), 453-457. https://doi.org/10.1080/02723638.2020.1717028

31 Fairwork. (2021). *Fairwork Kenya Ratings 2021: Labour Standards in the Gig Economy*. https://fair.work/wp-content/uploads/sites/131/2021/12/Fairwork-Kenya-2021-Report.pdf

32 Ahmed, S., Chinembiri, T., Moyo, M., & Gillwald, A. (2021). *Future of Work in the global South (FOWIGS): Digital Labour, New Opportunities and Challenges*. Research ICT Africa. https://researchictafrica.net/publication/future-of-work-in-the-global-south-fowigs-digital-labour-new-opportunities-and-challenges

33 Harrisburg, K., & Asher-Schapiro, A. (2021, 14 April). Risks for South Africa's food couriers surge during the pandemic. *Thomson Reuters Foundation*. https://longreads.trust.org/item/South-Africa-delivery-drivers-risk-lives

34 Prinsloo, O., Alake, T., & Genga, B. (2021, 19 April). Uber and Bolt drivers in Nigeria and Kenya protest over rising costs. *Business Live*. https://www.businesslive.co.za/bd/companies/2021-04-19-uber-and-bolt-drivers-in-nigeria-and-kenya-protest-over-rising-costs

35 Howson, K. (2022, 1 April). Digital facade shields e-hailing companies from accountability to drivers or passengers. *Research ICT Africa*. https://researchictafrica.net/2022/04/01/digital-facade-shields-e-hailing-companies-from-accountability-to-drivers-or-passengers

36 AFP. (2022, 24 April). Egypt gig economy workers face rough ride. *France 24*. https://www.france24.com/en/live-news/20220424-egypt-gig-economy-workers-face-rough-ride

domestic work, while adding little real value to local economies. As revealed in the Uber Files, platforms like Uber have adopted a strategy of monopolistic expansion, aided by venture capital injections, which has left little room for local innovators or startups to gain a foothold.

The key lesson from the experience of African platform workers during the pandemic, reinforced by the Uber Files, must be that inclusive growth does not automatically flow from digitalisation. Digitally driven development must be sensitive to local needs and context, include the participation of all stakeholders, and make a contribution to tackling Africa's long-term challenges. Platforms can and should be accountable to workers' demands for fairer pay, contracts and conditions. But ultimately, many are able to avoid responsibility due to a lack of enforcement and responsive regulation from governments, which have been keen to attract tech company investment.

Recent months have seen increasing inflationary pressures, mounting worker victories and platform regulation in the global North, growing worker resistance in the global South, and a new sensitivity to the importance of sectors such as delivery and transport to overall social and economic resilience to crises. The future of digital labour platforms seems uncertain – but it is possible that growing pressure in the global North could spur platforms to turn even more to permissive regulatory environments in the global South, and exert added pressure against regulation. Removing regulatory barriers to their expansion in Africa is the pathway to digital imperialism, not inclusive development. Instead, appropriate regulation of digital labour platforms in the post-pandemic world must aim to protect workers, local stakeholders and vulnerable social groups first.

This article includes some text originally published on the Research ICT Africa Blog in April 2022. See: https://researchictafrica.net/2022/04/01/digital-facade-shields-e-hailing-companies-from-accountability-to-drivers-or-passengers

Advocacy in times of TRIPS waiver

Deepika Yadav
Digital Trade Alliance[1]
yadavdeepika@gmail.com; https://twitter.com/deepika_yadav

Introduction

COVID-19, the novel coronavirus first discovered in December 2019 in Wuhan, China, is an extremely contagious virus which spread at an unimaginable rate. On 11 March 2020[2] the World Health Organization (WHO) declared it a pandemic. Suddenly, we had to adapt to new ways of living, working and socialising. Governments, scientists and pharma companies raced towards developing vaccines. Pharma companies like Pfizer, AstraZeneca, Moderna and Johnson & Johnson[3] were able to develop vaccines at a speed never witnessed before.[4] There was a sense of relief that soon everyone would be vaccinated and the world would go back to being normal. However, that expectation was far away from the reality of what ensued.

Vaccine and medical product shortages

The enormity of what followed can only be captured in terms such as "vaccine apartheid", "vaccine nationalism" and "vaccine inequality". We saw a gap in access to vaccines between the countries in the global North and global South,[5] and the stockpiling of vaccines by Canada, the EU and the US[6] while the marginalised population of the world either had no access or could only get them at prices much higher than those in the developed world.[7] We saw people living in the global North getting booster shots and those living in middle- and low-income countries not even receiving their first one.[8] At the date of writing this, only 19% of Africa[9] is vaccinated while 68% of the US population is fully vaccinated.[10]

This is a narrative of broken promises. At the start of the pandemic the global North promised "universal, common good"[11] vaccines to the world. They pledged donations to COVAX, a facility set up to promote the equitable distribution of vaccines.[12] However, COVAX failed because developed countries did not keep their promise.

The problem was not limited to vaccines alone. Since the beginning of the pandemic, we witnessed supply chain problems: there were acute shortages of medicines, testing kits,[13] N95 masks, PPE kits, ventilators and other medical products. As more deadly COVID waves ravaged the world, citizens in developing countries also faced the problem of corrupt

1 Deepika Yadav is a consultant and coordinator for the Digital Trade Alliance at Public Citizen.

2 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

3 Chen, E. (2020, 30 July). Drugmakers Race to Build Covid-19 Vaccine Supply Chains. *Wall Street Journal.* https://www.wsj.com/articles/drugmakers-race-to-build-covid-19-vaccine-supply-chains-11596101586

4 Santos Rutschman, A. (2020). *The Mosaic of Coronavirus Vaccine Development: Systemic Failures in Vaccine Innovation*. Saint Louis University School of Law. https://scholarship.law.slu.edu/cgi/viewcontent.cgi?article=1330&context=faculty

5 Pfeiffer, J. (2020, 10 March). A Global Day of Action to End Vaccine Apartheid. *University of Washington Department of Global Health*. https://globalhealth.washington.edu/news/2022/03/10/global-day-action-end-vaccine-apartheid

6 Nyabola, N. (2020, 22 March). Poor countries are paying more for the doses that remain after rich countries have had their fill. *The Nation*. https://www.thenation.com/article/world/coronavirus-vaccine-justice

7 Ibid.

8 Bajaj, S., Maki, L., & Stanford, F. C. (2022). Vaccine apartheid: global cooperation and equity. *The Lancet*, *399*(10334), 1452-1453. https://www.thelancet.com/journals/lancet/article/PIIS0140-6736(22)00328-2/fulltext

9 WHO. (2022, 24 June). Delivering progress in Africa's COVID-19 vaccination drive. *ReliefWeb*. https://reliefweb.int/report/world/delivering-progress-africas-covid-19-vaccination-drive

10 Based on the figures published at that time by the Google News COVID-19 tracker. https://news.google.com/covid19/map?hl=en-US&mid=%2Fm%2Fo9c7w0&state=7&gl=US&ceid=US%3Aen

11 European Commission. (2020, 24 April). Von der Leyen announces Global Response and calls for united world front against coronavirus. https://ec.europa.eu/commission/presscorner/detail/en/ac_20_749

12 WHO. (2022, 24 June). Op. cit.

13 Tomlinson, C. (2020, 5 May). COVID-19: Behind SA's shortages of test materials. *Spotlight*. https://www.spotlightnsp.co.za/2020/05/05/covid-19-behind-sas-shortages-of-test-materials

black-market practices[14] because of acute shortages of medicines and medical products. Advocates wrote letters[15] to companies to raise issues of shortages faced by middle- and low income-countries. There was an urgent need to scale up manufacturing of medical products and vaccines. As the pandemic progressed, countries in the EU and the US and India put export restrictions in place to meet their own domestic needs.[16] This directly impacted nations dependent on them for medical supplies.

How did IP become a problem?

The only solution to this public health crisis was to rapidly scale up manufacturing, which could only be achieved by technology transfers and sharing know-how. During World War II, the need for penicillin for injured soldiers was met only because the proprietor, Oxford University, decided to waive its intellectual property (IP) rights and share the know-how.[17] COVID-19 called for a similar human rights-based response. However, the IP owners refused to share their knowledge.

Civil society organisations (CSOs) demanded action to create patent pools for tech transfer and sharing know-how to scale up production to meet any shortages.[18] In May 2020, the WHO set up the COVID-19 Technology Access Pool (C-TAP)[19] as a "single global platform" to share IP and data using voluntary licensing for those scaling up production of COVID-19 vaccines and medical products. The forum was set up with much anticipation that it would act as an enabler to overcome global shortages. However, the pool remained relatively empty[20] for a long time. It took almost two years for the first tech transfer to take place.[21] C-TAP was welcomed with a cold shoulder by global pharmaceutical companies[22] as they did not want to give up their monopoly. Instead, they opted for bilateral agreements with restrictive clauses that limited scaling up production. Almost 250 advocacy groups raised concerns in a letter to the director-general of the World Trade Organization (WTO)[23] on how these exclusive agreements with only certain manufacturers in developing countries created artificial shortages. For example, Gilead entered into an exclusive agreement to produce Remdesivir with five manufacturers that were allowed to cater to a limited number of countries, leaving almost 70 countries to purchase the same medicine from Gilead at much higher prices.[24]

It is a lie when the pharma companies insist that IP is not a barrier. The truth is that they did not want to part with their knowledge. There are numerous examples which prove that IP rights have created barriers in producing and accessing vaccines and medical products.[25] While Pfizer excluded Latin American countries from its deal with C-TAP,[26] a recent study revealed that BioNTech is trying to stop an mRNA[27] vaccine hub in South Africa from using the mRNA technology, claiming it will "infringe on patents." This hub aims to scale up its capacity to 60% by 2040.[28] The same study has identified 120 manufacturers across the world that have the capacity to produce the mRNA vaccine.[29] It is proof against the long-standing argument by pharmaceutical companies that the global South lacks the capacity to manufacture mRNA vaccines. Advocacy groups[30] have written letters to the US and German governments to take action to ensure that tech transfer takes place with these manufacturers.

14 Mander, H. (2022, 2 June). Harsh Mander: How some exploited India's Covid-19 crisis to make money. *Scroll.in*. https://scroll.in/article/1023156/harsh-mander-how-some-exploited-indias-covid-19-crisis-to-make-money

15 See, for example: https://www.tbonline.info/media/uploads/documents/open_letter_to_cepheid_covid-19_test_supply_and_prices_2-25-2021.pdf

16 Human Rights Watch. (2021, 3 June). Seven Reasons the EU is Wrong to Oppose the TRIPS Waiver. https://www.hrw.org/news/2021/06/03/seven-reasons-eu-wrong-oppose-trips-waiver

17 Garrison, C. (2021). *Ensuring that intellectual property rights aren't a barrier to scaling-up: the remarkable example of penicillin production in the United States during World War II*. Medicines Law & Policy. https://medicineslawandpolicy.org/wp-content/uploads/2021/04/Ensuring-IP-rights-arent-a-barrier-to-scaling-up-the-example-of-penicillin.pdf

18 Tomlinson, C. (2020, 5 May). Op. cit.

19 https://www.who.int/initiatives/covid-19-technology-access-pool

20 Garrison, C. (2021). Op. cit.

21 Mara, K. (2022, 15 February). With technology transfer, 120 companies in low- and middle-income countries could manufacture mRNA vaccines. *Medicines Law & Policy*. https://medicineslawandpolicy.org/2022/02/with-technology-transfer-120-companies-in-low-and-middle-income-countries-could-manufacture-mrna-vaccines

22 Baumgaertner, E. (2021, 30 April). Vaccine companies and the U.S. government snubbed WHO initiative to scale up global manufacturing. *Los Angeles Times*. https://www.latimes.com/world-nation/story/2021-04-30/vaccine-companies-and-the-u-s-government-snubbed-who-initiative-to-scale-up-global-manufacturing

23 The text of the letter, sent on 13 April 2021, is available here: https://www.twn.my/title2/intellectual_property/trips_waiver_proposal/CSOLetter_Dr.%20Ngozi.pdf

24 Maybarduk, P. (2020, 12 May). Remdesivir Should Be in the Public Domain; Gilead's Licensing Deal Picks Winners and Losers. *Public Citizen*. https://www.citizen.org/news/remdesivir-should-be-in-the-public-domain-gileads-licensing-deal-picks-winners-and-losers

25 Human Rights Watch. (2021, 3 June). Op. cit.

26 MSF. (2022, 8 March). Latin America: How patents and licensing hinder access to COVID-19 treatments. https://msfaccess.org/latin-america-how-patents-and-licensing-hinder-access-covid-19-treatments

27 A vaccine that uses a copy of the messenger RNA (mRNA) molecule to produce an immune response.

28 Mara, K. (2022, 15 February). Op. cit.

29 Ibid.

30 Human Rights Watch. (2021, 15 December). Experts Identify 100 Plus Firms to Make Covid-19 mRNA Vaccines. https://www.hrw.org/news/2021/12/15/experts-identify-100-plus-firms-make-covid-19-mrna-vaccines

The current pandemic has revealed at every step that IP rights are barriers. If manufacturers in countries like India, South Africa, Bangladesh and Egypt were allowed access to technologies and know-how, their manufacturing capacity could have been easily, efficiently and effectively scaled up to meet the global needs at affordable and equitable prices. We could have probably averted the heartbreaking Delta wave in India and Latin America.

What is the TRIPS waiver and why was it needed?

On 2 October 2020, India and South Africa together presented a proposal to the WTO called the Trade-Related Aspects of Intellectual Property Rights (TRIPS) waiver. The waiver asked that all IP rights for technologies that are important to develop vaccines, medicine, equipment and kits be waived until "the majority of the world's population has developed immunity."[31] The proposed waiver aimed to overcome the restrictive global IP rules to help countries enter tech transfer partnerships and export medical products without fear of sanctions or trade disputes[32] to scale up and help produce "second-generation" vaccines against emerging variants.[33]

Australia, Canada, the EU, Japan and the US opposed the waiver, standing their ground that existing TRIPS flexibilities were sufficient to overcome the IP issues.[34] The proposal quickly gathered support from many developing countries, advocacy groups and CSOs, as well as organisations like the WHO and UNAIDS.[35] Those advocating for the waiver knew that for it to be approved, the global North had to be on board. From here on began months of hard work and advocacy campaigning. CSOs started raising their voices and making fierce efforts to be heard by developed countries. CSOs from developing countries, and international, regional and domestic advocacy groups from the global South, sent letters to call on the US president and leaders of the developed world to support the waiver. A global advocacy movement grew. There were open letters and petitions, including from the South African Anglican Archbishop of Cape Town, Thabo Makgoba,[36] in support of the TRIPS waiver, and petitions to the US president and administrators by Health Gap, The Delhi Network of Positive People,[37] Amnesty International USA[38] and Partners in Health,[39] to name a few. The pharma lobby was not far behind as they also sent a letter to US administrators not to back the waiver. The pharma lobby criticised the waiver as vague, broad and a tool to weaken IP rights.

On 5 May 2021, in an extraordinary move, the US announced[40] its support for the TRIPS waiver for vaccines "in service of ending this pandemic" after months of opposing it. It was a big moment in the world of access to medicine advocacy and it played a critical role. Had the advocates not worked hard, rallied politicians, and built global campaigns, this would not have happened. However, the US did not deliver on the leadership, giving the EU an opportunity to block any progress on the waiver.[41] In June 2021 they put forward their own "counter proposal"[42] covering only patents but excluding other IP rights (copyright, trade secrets, regulatory data and biologics) and promoting the use of compulsory licensing and voluntary licensing.[43] It was old wine in a new bottle. Compulsory licensing is a complicated process which comes with its share of pre- and post-approval requirements which are time consuming, cumbersome and often export restricting. Compulsory licensing can be an effective tool if the

31 Council for Trade-Related Aspects of Intellectual Property Rights. (2020, 2 October). Waiver from certain provisions of the TRIPS Agreement for the prevention, containment and treatment of COVID-19 - Communication from India and South Africa (IP/C/W/669). https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/IP/C/W669.pdf&Open=True

32 Human Rights Watch. (2021, 3 June). Op. cit.

33 Johns Hopkins Bloomberg School of Public Health. (2021, 10 May). WTO TRIPS Waiver for COVID-19 Vaccines: A Q&A with Anthony D. So, MD, MPA. https://publichealth.jhu.edu/2021/wto-trips-waiver-for-covid-19-vaccines

34 Inside U.S. Trade. (2021, 17 February). Civil society groups push Biden, other leaders to back TRIPS waiver. https://insidetrade.com/trade/civil-society-groups-push-biden-other-leaders-back-trips-waiver

35 UNAIDS. (2020, 15 October). UNAIDS supports a temporary WTO waiver from certain obligations of the TRIPS Agreement in relation to the prevention, containment and treatment of COVID-19. https://www.unaids.org/en/resources/presscentre/pressreleaseandstatementarchive/2020/october/20201015_waiver-obligations-trips-agreement-covid19

36 The text of the letter, sent 6 April 2022, is available here: https://healthjusticeinitiative.org.za/wp-content/uploads/2022/03/Letter-to-the-Prime-Minister-of-India-from-Makabo-Mazzucato-Medhora-Reddy-Stiglitz-Valodia.pdf

37 Don't Trade Our Lives Away. (2021, 2 February). The Delhi Network of Positive People write to 18 Ambassadors calling for supporting the COVID-19 waiver at the WTO. https://donttradeourlivesaway.wordpress.com/2021/02/02/the-delhi-network-of-positive-people-write-to-18-ambassadors-calling-for-supporting-the-covid-19-waiver-at-the-wto

38 Amnesty International USA. (2021, 26 February). Amnesty International USA and Hundreds of US Civil Society Organizations Urge Pres. Biden to Support COVID-19 WTO Waiver to Boost Vaccines, Treatments Worldwide. https://www.amnestyusa.org/our-work/government-relations/advocacy/amnestyinternationalusa-and-400-ngos-call-on-biden-to-support-covid19-wto-trips-waiver

39 Partners in Health. (2021, 4 May). Petition: U.S. Must Support Patent Waiver for COVID-19 Vaccines. https://www.pih.org/article/petition-us-must-support-patent-waiver-covid-19-vaccines

40 Tai, K. (2021, 5 May). Statement from Ambassador Katherine Tai on the Covid-19 Trips Waiver. *Office of the United States Trade Representative*. https://ustr.gov/about-us/policy-offices/press-office/press-releases/2021/may/statement-ambassador-katherine-tai-covid-19-trips-waiver

41 Public Citizen. (2021, 23 November). How the Vaccine Rich Get Richer. https://www.citizen.org/article/how-the-vaccine-rich-get-richer

42 European Union. (2021, 4 June). Communication from the European Union to the Council for TRIPS. https://trade.ec.europa.eu/doclib/docs/2021/june/tradoc_159606.pdf

43 Ibid.

existing rules and regulations are simplified. Advocacy groups across the globe staged protests[44] and delivered petitions to the Biden administration for them to get back in the game and not back down on the waiver. However, developed countries refused to give in and this resulted in a revised TRIPS waiver far away from what was proposed.[45]

During the 12th WTO Ministerial Conference (WTO MC-12) negotiations, advocacy groups led a vocal campaign to call out countries blocking the waiver. On 15 June 2022, around 223 CSOs sent a letter to the trade ministers at the WTO to reject the revised proposal.[46] CSOs, advocacy groups and academics across the globe pleaded to heads of states to not to agree to the revised waiver.[47] However, after two years of intense battle, on 20 June 2022 the WTO reached a ministerial decision on the waiver.[48] The final text is very different from the original proposed waiver. It only covers vaccines and is limited to patent. We would not have reached this stage if the IP was open for use.

Open knowledge

Open knowledge is "any content, information or data that people are free to use, re-use and redistribute without any legal, technological or social restriction."[49] It leads to swift, efficient and collaborative policy decisions. As an umbrella term, open knowledge encompasses open science, open data and open source software, and open education such as MOOCs, among other forms of "free-to-use" knowledge that are available to people. Open licences are a tool to achieve open knowledge.

Open licences used by inventors, researchers and institutions lead to the dissemination of their work to the public by overcoming restrictive IP barriers[50] and help to optimise public funding.[51] One example of open licensing is Creative Commons, created as a response to a US copyright case that extended the monopoly power of the creator.[52] These licences are now extensively used by research institutions, CSOs and government-run agencies.[53] Creative Commons has been driving awareness around the lack of effectiveness of voluntary licensing in disseminating knowledge and is actively promoting a mindset of "progressive copyright law" through national and global awareness.[54]

Over the years we have witnessed growing advocacy for open knowledge. The Open Knowledge Network, Public Domain and the Comprehensive Knowledge Archive Network (CKAN) are a few examples[55] of open sources which share knowledge.

There exist many new advocacy opportunities to embrace when it comes to open knowledge and open licensing. However, in the context of the current geopolitical struggle around vaccine advocacy, TRIPS waiver-like advocacy may not work in the context of open knowledge. The vaccine advocacy occurred against the background of a grave global health crisis which had both social and economic impacts. In the case of open knowledge, the gravity of the situation does exist, but it is not backed by COVID-19-like time-sensitive circumstances. This works against advocates for open knowledge. Does this mean we should give up? No. A realistic assessment of potential impediments is required.

Roadblocks to an open system

The advocacy will not easy because:

First, many advocates suggest that a global agreement on open knowledge is the need of the hour.[56] Even UNESCO, during the 41st session of its General Conference in November 2021, recommended having an internationally regulated national legal instrument in place to promote open science.[57] Any negotiations and debates to make a binding instrument a reality necessitate a collective will from the global North and global South to agree on IP and transfer issues.[58] However, the negation of the

44 See, for example: https://rethinktrade.org/toolkit/nov-30-photo-page-for-press

45 Green, A. (2022, 17 March). TRIPs waiver compromise draws mixed response. *Devex*. https://www.devex.com/news/trips-waiver-compromise-draws-mixed-response-102860

46 MSF. (2022, 15 June). Open CSO letter to WTO Trade Ministers: Do not accept the current draft, demand a real waiver. https://msfaccess.org/open-cso-letter-wto-trade-ministers-do-not-accept-current-draft-demand-real-waiver

47 Chintan, R. (2022, 28 June). India- South Africa TRIPS proposal dies at WTO. *NewsClick*. https://www.newsclick.in/India-South-Africa-TRIPS-Waiver-Proposal-Dies-WTO

48 WTO Ministerial Conference. (2022, 17 June). Draft Ministerial Decision on the TRIPs Agreement. WT/MIN(22)/W/15/Rev.2. https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/MIN22/W15R2.pdf&Open=True

49 https://okfn.org/opendata

50 https://creativecommons.org/about/program-areas/policy-advocacy-copyright-reform

51 Ibid.

52 https://certificates.creativecommons.org/cccertedu/chapter/1-1-the-story-of-creative-commons

53 https://creativecommons.org/about/program-areas/policy-advocacy-copyright-reform

54 https://creativecommons.org/about/program-areas/policy-advocacy-copyright-reform/reform

55 Pollock, R., & Walsh, J. (2012). Open Knowledge: Promises and Challenges. In M. Dulong de Rosnay & J. C. De Martin (Eds.), *The Digital Public Domain: Foundations for an Open Culture.* Open Book Publishers. http://books.openedition.org/obp/550

56 Parker, A. (2021, 7 June). Open Science and Intellectual Property: Using Open Licenses to Open Your Science. *Wilson Center*. https://www.wilsoncenter.org/blog-post/open-science-and-intellectual-property-using-open-licenses-open-your-science

57 https://en.unesco.org/science-sustainable-future/open-science/recommendation

58 Montgomery, L., et al. (2019). Action. *Works in Progress*. https://wip.mitpress.mit.edu/pub/oki-ch10

TRIPS waiver does not leave much to hope for, as we can expect protests and blockades from developed countries and industries.

Second, when it comes to open data advocacy, there will be resistance from big tech giants backed by developed countries who would not want to lose their monopoly over revenue-generating big data or aggregated data. A prime example of such solidarity is the 24-year-old moratorium on custom duties in electronic transmission[59] because of US lobbying, despite South Africa and India's protest at the WTO.

Third, there are legitimate issues of cross-border data flow, consumer privacy and national security. Most countries, both in the global North and global South, lack a robust regulatory framework to protect consumer data. There is no legally binding international treaty to manage international data flow.

Fourth, we must realise that in this globalised world, knowledge becomes truly open when it is free, diverse and inclusive. Advocacy needs to be built beyond the issue of IP barriers. It must focus on making research accessible in every "voice and language" to make it truly open.[60]

Fifth, negotiation processes at the multilateral level are often slow. For example, the definition of "Traditional Cultural Expressions" has been under debate at the World Intellectual Property Organization (WIPO) for many years now, yet there is no common ground to agree on because the developed and developing countries fail to reach a commonly agreed definition every year.[61]

Yes, there are opportunities. There is an urgent need to build advocacy on inclusion. In a world which is getting smaller and smaller because of the internet, open knowledge must be based on the principles of inclusion, diversity and non-discrimination. There is a need to build advocacy around promoting these principles.

Another area which has gained immense relevance is open data. First, there is a need to generate awareness around how open data should be collected for it to be inclusive. Second, data is reusable. The same data sets can be used for different purposes resulting in meaningful outputs. The application of AI and big data analysis poses a threat to individual privacy, because it de-anonymises anonymous data. The need to build awareness around these issues cannot be overlooked. In the case of open software there is a need to focus on how to make open software better and improve its quality.

However, for open knowledge, any advocacy has to address issues which are multi-sectoral and require a focus on both national and international level advocacy. Advocacy needs to be realistic and consistent. There will be periods of quiet and periods where it has to be vociferous. This makes the advocacy terrain incredibly complex for civil society organisations, which require advocacy specialists, global partnerships and alliances with governments and sympathetic voices in the private sector to create an effective movement. This renewed debate on IP is a golden opportunity to reinvigorate advocacy around open knowledge. There are many lessons from the TRIPS waiver and the most important one is to not be threatened by the limitations of licensing and super profits.

59 Banga, R. (2022, 8 June). Why Removing WTO Moratorium on E-Commerce Will Aid Developing World's Post-COVID Recovery. *The Wire*. https://thewire.in/economy/why-removing-wto-moratorium-on-e-commerce-will-aid-developing-worlds-post-covid-recovery

60 Montgomery, L., & Neylon, C. (2018, 17 September). In a globalised and networked world, what is the unique value a university can bring? Introducing Open Knowledge Institutions. *LSE Impact Blog*. https://blogs.lse.ac.uk/impactofsocialsciences/2018/09/17/in-a-globalised-and-networked-world-what-is-the-unique-value-a-university-can-bring-introducing-open-knowledge-institutions

61 Forum on Indian Traditional Medicine. (2019). *Protection of Traditional Cultural Expressions in India*. https://fitm.ris.org.in/node/990

Documenting and navigating emerging trends for digital rights funding

Natalia Tariq
Association for Progressive Communications (APC)
www.apc.org

Introduction

In the wake of the COVID-19 pandemic, there have been widespread implications for every aspect of development.[1] The economic downturn has accelerated and global debt has surged,[2] hitting already poor and vulnerable people hard, while partly changing the profile of global poverty by creating millions of "new poor".[3] According to the *Poverty and Shared Prosperity Report 2020*, "COVID-19 and its associated economic crisis, compounded by the effects of armed conflict and climate change, are reversing hard-won gains in poverty reduction and shared prosperity."[4] The pandemic has also revealed and exacerbated the digital and gender divides as "power imbalances are made more evident and starker, disproportionately affecting groups that suffer multiple, intersectional forms of discrimination."[5]

The economic downturn because of COVID-19 – which came against the backdrop of already existing pressures to urgently address climate change, besides other ongoing regional and country conflicts, tensions and human rights abuses – has been made worse by the Russian war in Ukraine and political tensions between major players that have resulted from this. When the conflict in Ukraine began, the demands on funders to meet the humanitarian and refugee crisis overwhelmed aid budgets. However, unlike in the case of COVID-19, where an increase in overall contributions by donors in response to the pandemic came at the expense of other humanitarian needs,[6] high-income states were urged to not divert funds from existing programmes but to set aside additional funds for the conflict.[7] To what extent bilateral donors have been able to do this has varied, and competing aid priorities have in some cases led to funding being diverted or delayed to other programme areas, including funding for human rights and digital rights elsewhere.

While these global crises have stressed funding budgets, the pandemic has also created opportunities for civil society to build horizontal relationships with donors, opening the space for authentic and transparent conversations. Donors have shown a willingness to be caring, agile and innovative in their funding approach, and this transformational shift in the funder-grantee relationship dynamic is continuing well into the "post-shock" era of COVID-19.

Competing funding priorities and implications for human rights funding

Our interviews with representatives from the European Union (EU), the Swedish International Development Cooperation Agency (Sida), the UK Government's Foreign, Commonwealth and Development Office (FCDO) and the International Development Research Centre (IDRC) revealed that while these organisations have directed funding towards COVID-19 and the humanitarian crisis in Europe, this has not been at the cost of funding available for other human rights work. At a global

1 Blake, P., & Wadhwa, D. (2020, 14 December). 2020 year in review: The impact of COVID-19 in 12 charts. *World Bank Blogs*. https://blogs.worldbank.org/voices/2020-year-review-impact-covid-19-12-charts

2 Gold, S. (2022, 2 August). How the debt crisis imperils development – and why it's getting worse. *Devex*. https://www.devex.com/news/how-the-debt-crisis-imperils-development-and-why-it-s-getting-worse-103700

3 Nguyen, M. C., Yoshida, N., Wu, H., & Narayan, A. (2020). *Profiles of the new poor due to the COVID-19 pandemic*. World Bank. https://thedocs.worldbank.org/en/doc/767501596721696943-0090022020/original/ProfilesofthenewpoorduetotheCOVID19pandemic.pdf

4 World Bank. (2020). *Poverty and Shared Prosperity 2020: Reversals of Fortune*. https://www.worldbank.org/en/publication/poverty-and-shared-prosperity

5 Association for Progressive Communications. (2020). *Closer than ever: Keeping our movements connected and inclusive – APC's response to the COVID-19 pandemic*. https://www.apc.org/sites/default/files/closerthanever_pp.pdf

6 Igoe, M. (2021, 23 June). Devex Newswire: How COVID-19 broke humanitarian funding. *Devex*. https://www.devex.com/news/devex-newswire-how-covid-19-broke-humanitarian-funding-100206

7 Gold, S. (2022, 8 March). Devex Newswire: How Russia's war in Ukraine will affect the world's poorest. *Devex*. https://www.devex.com/news/devex-newswire-how-russia-s-war-in-ukraine-will-affect-the-world-s-poorest-102810

level, the EU has a separate envelope of funding to meet the needs of immediate crises, which is being used to provide assistance in Ukraine, and so there have not been any major cuts for human rights support elsewhere.[8] The situation is similar in the case of other bilateral funders we interviewed; however, even though the funding has not been permanently redirected from other human rights work, there have been delays in funding available due to the competing emergency priorities of the Ukrainian conflict and COVID-19. These delays have created a situation of uncertainty for civil society groups working in the digital rights space, particularly those in the global South who are heavily reliant on direct support from government donors or indirect support through international NGO subgranting programmes.

Funding of digital rights remains central to donor concerns

The pandemic has highlighted the importance of digital rights and access, and, among other issues, donors are prioritising working on issues of digital inclusion, literacy and security. This includes a new wave of funders who did not previously support digital rights initiatives as well as those who have increased and expanded their existing digital rights portfolios.[9] Oak Foundation, for instance, under its broader umbrella of the International Human Rights Programme, is in particular looking at human rights abuses online, such as digital surveillance, censorship and information controls.[10]

The pandemic has led to a common understanding among donors that equitable and affordable internet connectivity has been and is critical to access relevant information, health and education services, to sustain economies through virtual work, for civil society and social movements to sustain themselves, and for people to communicate and stay connected.[11] The role of digital technologies has also been central to many donors' response to the pandemic. For instance, the FCDO's Digital Development has relied on digital solutions for provision of emergency relief and services like health and education, in creating opportunities for work and learning online, and also to build long-term resilience to the pandemic and future crises.[12]

At the same time, the challenges of digital rights, exacerbated during COVID-19 as the "responses by some governments to the pandemic revealed fault lines that challenge the democratic foundations of societies,"[13] have remained a priority. According to an IDRC senior programme officer, "digital rights will only become more important because we don't have good fixes for the challenges we are facing like gender misinformation, cybersecurity surveillance, digital subversion, all of which are critically important issues and speak to the convergence of online and offline rights."[14] The IDRC invested a lot of funding in research from the global South around the short- and long-term impacts of COVID-19,[15] the results of which indicate how the digital rights agenda remains of critical importance to the organisation.

There is also a shift in the wider funder community to integrate the digital in all aspects of their programming in a more holistic and strategic manner that explores ways of supporting a diverse convening of civil society actors to come up with collective and innovative solutions to an increasingly complex digital landscape and ecosystem. Whether this means an increase in the amount of funding available for digital rights work is yet to be seen, but there is no doubt that there will be a continued commitment to this field, even if the funding has different emphases.

Moving towards embedding a politics of care in funding approaches

Adapting to working in the context of COVID-19 and extremely precarious economic and political situations across the globe has presented civil society organisations as well as donors with unprecedented challenges. Increased stress levels and online fatigue have been widely reported by organisations, and donors have undertaken various strategies to respond. Donors and their grantees have had to navigate shifting conditions together, such as transitioning activities and operations online, realigning project deliverables and adjusting timelines.

All donors we interviewed acknowledged the complications, trauma and burnout associated with working during the pandemic and implemented strategies aimed at minimising these stresses. Sida, for instance, has relied on open dialogues with its grantees to understand their challenges and provide support accordingly. For example, Sida found that grantees in the Middle East and North Africa experienced difficulties in transitioning their interventions

8 Renuka Srinivasan, Senior Project Manager, Delegation of the European Union to India, personal communication, 14 July 2022.

9 Alberto Cerda Silva, Global Program Officer for Internet Rights and Access, Ford Foundation, personal communication, 13 July 2022.

10 Oak Foundation. (2022, 6 April). Digital space: The frontier of civic repression and activism. https://oakfnd.org/access-now-citizen-lab-digital-space-the-frontier-of-civic-repression-and-activism

11 Alessandra Lustrati, Head of Digital Development, UK Government's Foreign, Commonwealth & Development Office (FCDO), personal communication, 1 August 2022.

12 Ibid.

13 Association for Progressive Communications. (2020). Op. cit.

14 Ruhiya Seward, personal communication, 21 July 2022.

15 IDRC. (2022, 7 March). Two years into the COVID-19 pandemic: Insights from IDRC research partners. https://www.idrc.ca/en/research-in-action/two-years-covid-19-pandemic-insights-idrc-research-partners

online due to the complexity of their contextual environments and lack of viable connectivity and infrastructure support.[16] Sida provided these organisations more flexibility around altering their activities and providing extensions for project and reporting timelines.

Some donors have even gone a step further and have started providing financial support and set up well-being funds for civil society organisations to centre care in their practices. An example of this is the Care Fund that has been set up under Oak Foundation's Issues Affecting Women Programme,[17] which is specifically intended to support small, time-limited projects on self or collective care for its grantee partners. Other donors, such as Global Fund for Women, are taking into consideration the cost implications of remote work and participation in online convenings (such as increased data and connectivity costs, software and hardware costs, and costs of arranging for alternative family care).

Core, flexible funding prioritised to build resilience for future crises

During the pandemic, many donors switched to providing core funding to their grantees so that they had the flexibility and resources to adjust to the new realities they were faced with.[18] Others, like Ford Foundation, who were already implementing a general support grant-making approach,[19] did not have to adjust their strategies, but it became clear that it was precisely this kind of support that civil society organisations needed most. An evaluation report of the Ford Foundation's BUILD Programme[20] corroborated that, particularly in unpredictable and challenging contexts, "strengthening institutions and networks leads to improved programming and impact – that is, to an increased number of programs and/or improvements in their quality, strategic relevance and adaptability."

There is an effort on the part of funders like the Ford Foundation to do further advocacy in wider funding circles to encourage donors to move in the direction of flexible, general support grant making. This is necessary to ensure that social justice organisations can be more resilient and impactful so they can seize opportunities and take on further challenges.

16 Fredrik Westerholm, personal communication, 1 August 2022.

17 https://oakfnd.org/programmes/issues-affecting-women

18 Katarína Bartovicova, European Digital Rights initiative (EDRi), personal communication, 28 June 2022.

19 https://www.fordfoundation.org/work/our-grants/building-institutions-and-networks

20 Bisiaux, R., Dwyer-Voss, R., Bangser, M., Morales, S., Boateng, A., & Poli, F. (2022). *Final Report: BUILD Developmental Evaluation*. NIRAS. https://www.fordfoundation.org/media/7095/build-evaluation-final-report.pdf

Donors exploring the intersections of technology with human rights, gender and environmental justice in their programming

Donors funding human rights initiatives are now looking more closely at the interconnections of technology with the fields they fund. The importance of the digital as a cross-cutting theme, and as an enabler of all other rights, has become more apparent as a result of the pandemic. Technology has had a profound impact on international development and humanitarian aid programmes. The application of digital innovations and the responsible use of data were key to successful responses to COVID-19. We also saw how the impacts of the crisis were not uniform, and the challenges of the virus have exacerbated longstanding inequities and decades of discriminatory practices, leading to unequal trajectories.[21]

According to the Ford Foundation,[22] exploring the intersections of gender, human rights, civic engagement, racial justice, environmental sustainability and technology has become key to its programmes having meaningful impact. It commissioned research in collaboration with Ariadne and the Mozilla Foundation that APC was involved in, and which centred around the intersection of digital rights with environmental and climate justice.[23] The research's primary audiences are grant makers and practitioners working in or adjacent to the digital rights sector interested in understanding how to centre environmental and climate justice in their work, or environmental justice funders who want to integrate digital technologies in their work. Going forward, funders in the digital rights space, as well as those working on other human rights and social justice issues, are looking to craft grant-making strategies that advance work on issues that converge with digital rights and make more space for intersectional agendas.

Shifting modalities of how resources for digital rights are channelled

While having to navigate COVID-19, civil society groups have continued to have to face multiple other unrelated challenges. According to the *2022 State of*

21 UN Women. (2020, 1 July). Intersectional feminism: What it means and why it matters right now. https://www.unwomen.org/en/news/stories/2020/6/explainer-intersectional-feminism-what-it-means-and-why-it-matters

22 Alberto Cerda Silva, personal communication, 13 July 2022.

23 Kazansky, B., Karak, M., Perosa, T., Tsui, Q., Baker, S., & The Engine Room. (2022). *At the confluence of digital rights and climate & environmental justice: A landscape review*. https://engn.it/climatejusticedigitalrights; Association for Progressive Communications. (2022). *At the Interstice of digital rights and environmental justice: Four issue briefs to inform funding*. https://www.apc.org/en/node/38149

Civil Society Report from CIVICUS,[24] we are living in "a world characterised by crisis and volatility, where regressive forces are mobilising a fierce backlash, but where dogged civil society mobilisation is still winning vital battles." With anti-rights movements and repressive governments on the rise, the civic space for civil society, particularly groups that are working on human rights, is shrinking. States are passing legislation, such as the Foreign Contribution Regulation Act (FCRA)[25] in India, which is targeting NGOs and giving government tighter control and scrutiny over the receipt and utilisation of foreign funds by NGOs.

Even the EU is finding it difficult to support grassroots organisations in the country as sub-granting to smaller and informal groups has become impossible (the FCRA requires every person or NGO seeking to receive foreign donations to be registered under the Act and to not transfer the funds to another NGO).[26] This means that they no longer have the kind of outreach they had before, as they can only work through larger NGOs that have FCRA registration and the capacity to meet the eligibility requirements of the EU's funding calls. One way that the EU is planning to get around this situation is by channelling funding through international NGOs who do not face FCRA restrictions and can make sub-grants. This funding strategy, however, defeats the donor's own ethos to build capacity and resourcing of local civil society groups. It also perpetuates the problematic power relations between civil society in the global North and global South. International NGOs are mostly headquartered in developed countries, and their agendas are not necessarily the same as those of NGOs from the global South. "The world of NGOs is not a network of equals but is based on a hierarchical power structure,"[27] and these problematic power relations are perpetuated when funding to civil society groups in the global South is channelled through NGOs from the global North.

In this context, the role of intermediaries with strong global South connections has become key.

The FCDO sees organisations like APC, with a wide membership network and ability to reach grassroots organisations, playing a crucial role as conduits of these funds.[28] A representative stated that the FCDO has a preference for working with such organisations as opposed to large contractors and consultancies that are from the global North, as this brings value for money and long-term sustainability to their programming. Sida added that it was necessary for funders to be innovative in how they disburse their funding so it can reach less visible players.[29] This includes exploring mini-grants, intermediaries and diverse funding platforms.

Going forward

Even though the pandemic has highlighted the significance of funding digital rights work, there is still a knowledge gap around these issues among donors, particularly those who are not directly supporting this field or have several other competing priorities. The lack of face-to-face meetings and convenings during the pandemic has also meant fewer spaces for donors to connect with and learn about the work of civil society groups working on digital rights. As the opportunities for in-person convenings increase, there is a need for digital rights organisations to keep the important role of the digital "simmering and alive"[30] in donor circles by continuing to raise awareness and influence the debate on digital development so that funding programmes reflect the needs and priorities on ground. The FCDO representative highlighted the key role of meeting and sharing resources and research with donors on the impact of digital technologies on important and emerging issues.[31] She said that the FCDO did not support community networks up until a few years ago, when they were made aware of community networks by APC at various international platforms. Now it is a key part of their programming.

Donors themselves also have a responsibility to share their knowledge and learnings with each other, as better donor coordination could go a long way in encouraging collaboration and streamlining efforts, providing the needed funding opportunities for the digital sector, which has multiple gaps and challenges and is evolving very quickly.

24 Firmin, A., Pousadela, I. M., & Tiwana, M. (2022). *2022 State of Civil Society Report*. CIVICUS. https://www.civicus.org/documents/reports-and-publications/SOCS/2022/CIVICUS2022SOCSReport.pdf

25 Tiwary, D. (2022, 14 July). Explained: What is FCRA, the law related to NGO funding? *The Indian Express*. https://indianexpress.com/article/explained/everyday-explainers/what-is-fcra-ngo-funding-mha-explained-8026895

26 Renuka Srinivasan, personal communication, 14 July 2022.

27 Sorj, B. (2015). *Civil Societies North South Relations: NGOs and Dependency*. The Edelstein Centre for Social Research. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.521.7257&rep=rep1&type=pdf

28 Alessandra Lustrati, personal communication, 1 August 2022.

29 Fredrik Westerholm, personal communication, 1 August 2022.

30 Renuka Srinivasan, personal communication, 14 July 2022.

31 Alessandra Lustrati, personal communication, 1 August 2022.

Organising for sustainable connectivity: Centring communities in crisis

Shawna Finnegan and APC Environmental Sustainability Working Group
Association for Progressive Communications (APC)

Introduction

COVID-19, like many crises, has revealed foundational flaws in our global systems of governance. In the West, the governments of wealthier countries have hoarded vaccines, refused to waive intellectual property rights, enforced unjust travel bans, and failed to fund resilient public health care. In many other regions of the world, governments are unable to protect and defend rights, are under-resourced and overwhelmed by debt, and are systemically bound[1] to the logics of colonial extractivism.[2]

For many people living with the realities of crisis on a daily basis, the systems that govern our world have largely failed, and governments have not lived up to their responsibilities as duty bearers. Instead, our collective planetary resilience increasingly relies on community-led action and solidarity.[3]

In crises, safe and resilient communications infrastructure becomes ever more critical for communities to respond effectively and collectively care for each other, ourselves and the planet. Communities currently living with climate catastrophe cannot afford to wait for external actors to bring about meaningful and sustainable connectivity; they must be able to connect themselves.[4]

This report explores historical, ongoing and emerging work across the APC network to organise for meaningful and sustainable connectivity, centring communities in crisis. APC values and uplifts the power of connected communities working through decentralised action – it is at this level that the core of a sustainable response to any future crisis such as COVID-19 needs to be built.

Feminist, circular and community-led: APC perspectives on sustainable connectivity

APC's strategic priority to contribute to environmental justice and preservation of the earth[5] emphasises the need to address the negative environmental impacts of digital infrastructure, while also supporting the strategic use of digital technologies for environmental monitoring. These twin challenges are framed by APC's commitment to working towards a feminist internet[6] "in which women and people of diverse sexualities and genders are able to access and enjoy a free and open internet to exercise agency and autonomy, build collective power, strengthen movements, and transform power relations for gender and sexual justice."

Over the past three years, APC's Environmental Sustainability Working Group has engaged our network in the discourse of environmental justice, advocated for internet governance actors to address the environmental impacts of the internet,[7] developed an evolving guide to a circular economy of digital devices,[8] supported the ongoing development of a feminist principle of the internet on the environment,[9] and implemented a pilot grant using

1 Schalk, O. (2022, 4 July). Documents show how Ottawa intervened in Tanzania to benefit Canadian mining firms. *Canadian Dimension*. https://canadiandimension.com/articles/view/documents-show-how-ottawa-intervened-in-tanzania-to-benefit-canadian-mining-firm

2 Niang, A. (2019, 17 August). The colonial origins of extractivism in Africa. *Al Jazeera*. https://www.aljazeera.com/opinions/2019/8/17/the-colonial-origins-of-extractivism-in-africa

3 Carstensen, N., Mudhar, M, & Schurmann Munksgaard, F. (2021). 'Let communities do their work': the role of mutual aid and self-help groups in the Covid-19 pandemic response. *Disasters, 45*(Suppl 1). https://doi.org/10.1111/disa.12515

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

5 https://www.apc.org/en/strategicpriorities2020_2023#6

6 https://www.apc.org/en/strategicpriorities2020_2023#3

7 https://www.intgovforum.org/multilingual/content/igf-2020-pre-event-32-environmental-justice-and-an-anti-extractive-internet-impacting-policy

8 https://circulartech.apc.org

9 Radloff, J. (2022, 2 September). Towards a new feminist principle of the internet on the environment: Two new publications now available in English. *APC*. https://www.apc.org/en/news/towards-new-feminist-principle-internet-environment-two-new-publications-now-available-english

participatory approaches to project design, facilitation and assessment.

As we move forward, APC's collective action for environmental justice and preservation of the earth is grounded by the local action of members, partners, allies and staff, and ongoing insight into the possibilities for feminist, circular and community-led connectivity that serves environmental justice.

Africa

In Africa, where meaningful connectivity is an ongoing struggle for many communities, APC members have taken diverse approaches in response to the twin challenges of digital exclusion and environmental injustice.

Arid Lands Information Network (ALIN) was first conceived in 1987 at a cross-regional workshop in Benin to facilitate an exchange of ideas to improve agricultural practices in regions experiencing water scarcity. Over the past 30 years it has evolved from a project of Oxfam in Senegal to a regional network headquartered in Kenya. In 2007, ALIN began a new project to set up community Maarifa Centres (Knowledge Centres) with information and communications technology (ICT) equipment and training programmes designed to ensure that all community members can access the information, skills and technologies that they need.[10]

In Cameroon, PROTEGE QV has been working since 1995 to promote and support individual and collective initiatives to protect the environment and improve the well-being of communities. PROTEGE QV has implemented projects to support, inform and empower local communities in response to changing climates, including designing and developing more efficient cookstoves and developing resource kits that can be used by community radios in Cameroon.[11]

In Nigeria, APC members are working with communities to use technology strategically for environmental sustainability and address the environmental impacts of e-waste. The Centre for Information Technology and Development (CITAD) joined the APC Environmental Sustainability Working Group in 2019 and has been an active contributor to the APC guide to a circular economy of digital devices. CITAD has emphasised the need for regional action in response to the illegal import of e-waste into Africa, and in 2021, CITAD developed a case study on mobile repair in Nigeria.[12]

In rural communities of Nigeria, Fantsuam Foundation has implemented several environmental initiatives, using repaired and recycled computers and renewable energy sources, and supporting knowledge exchange for climate adaptation and food security.[13]

In 2022, the Media Awareness and Justice Initiative (MAJI) officially joined the APC network as an organisational member, operating in the Niger Delta region. MAJI's Soot Mapping project[14] aims to support a sustainable community network through the use of citizen science methodologies and free/libre open source software technology to address air pollution in the region.[15]

In Mankosi, in the Eastern Cape of South Africa, APC member Zenzeleni Networks is operating a Solar Learning Lab with the help of Computer Aid, an APC member located in the UK. Computer Aid first launched the Solar Learning Lab initiative in 2011. The joint project between Zenzeleni Networks and Computer Aid includes a documented process to learn and evaluate the outcomes of deploying solar-powered learning lab infrastructure with community networks.[16]

Asia

In Asia, where communities are already experiencing some of the worst effects of the climate catastrophe, and where e-waste is growing faster than in any other region worldwide, APC members are nurturing partnerships and coalitions to foster meaningful connectivity and climate adaptation.

Digital Empowerment Foundation (DEF), based in India, has long focused on grounded action for digital inclusion and environmental sustainability. In 2009, DEF and APC developed a baseline study of e-waste in India, analysing global, regional and national policy contexts. The report also explored civil

10 APCNews. (2009, 10 June). "Cybercafé in a container": Rural Kenya's mobile internet stations. *APC*. https://www.apc.org/en/news/cybercafe-container-rural-kenyas-mobile-internet-s

11 https://www.apc.org/en/greenit_apc_initiatives#mozTocId622594

12 Ya'u, Y. Z. (2021). GSM Repairers Association: Building capacity and creating opportunities for mobile repairers in Nigeria. In A. Finlay (Ed.), *A guide to the circular economy of digital devices*. APC. https://circulartech.apc.org/books/a-guide-to-the-circular-economy-of-digital-devices/page/case-study-gsm-repairers-association-building-capacity-and-creating-opportunities-for-mobile-repairers-in-nigeria

13 https://www.apc.org/en/greenit_apc_initiatives#mozTocId622594

14 https://datacab.org/soot-mapping-project

15 Prado, D. (2022, 13 September). Seeding change: Communities mobilise open data to challenge oil industry pollution in Nigeria. *APC*. https://www.apc.org/en/node/38246

16 Espinosa, A. (2021). Computer Aid's Solar Learning Lab: Sustainable, scalable and adaptable to local needs. In A. Finlay (Ed.), *A guide to the circular economy of digital devices*. APC. https://circulartech.apc.org/books/a-guide-to-the-circular-economy-of-digital-devices/page/case-study-computer-aids-solar-learning-lab-sustainable-scalable-and-adaptable-to-local-needs

society initiatives to address e-waste, and highlighted the need for multistakeholder engagement and networking. In 2020-2021, DEF co-led the development of APC's guide to a circular economy of digital devices, contributing case studies and policy analysis from the region.[17]

From Taiwan, Open Culture Foundation (OCF) is collaborating with groups around the world to help local communities install and operate open source environmental sensors. OCF launched Civic Sense[18] in 2021 and is collaborating with several APC members in the project, including MAJI in Nigeria and the Society for the Promotion of Alternative Computing and Employment, Kerala (SPACE Kerala) in India. SPACE Kerala is working to improve water quality monitoring in the Nallathanni River in Munnar, partnering with the local community to operate and maintain water boxes provided through the OCF Civic Sense project.[19]

In Bangladesh, APC members have developed research and undertaken advocacy to address the impacts of electronic waste. In 2021, Voices for Interactive Choice and Empowerment (VOICE) convened an event in Dhaka to discuss e-waste management and environmental sustainability in Bangladesh, bringing together government representatives, leaders of environmental movements, NGOs, teachers and journalists. Speakers at the event emphasised the need for collaboration and public-private partnerships to support repair, recycling and e-waste management.[20]

The Americas

In Latin America and the Caribbean, social movements and community-led resistance to extractive practices are grounding the work of the APC network to support meaningful and sustainable connectivity.

In the Amazon rainforest, many communities cannot rely on broadband or even mobile internet access to communicate across distances. As illegal logging, deforestation and mining threaten ecosystems, these communities must find ways to communicate safely in order to monitor and defend the forest against extractivism.[21] Recognising this need, APC member Rhizomatica is working with isolated communities in Latin America to set up digital communication systems based on high frequency (HF) shortwave radio. The High-frequency Emergency and Rural Multimedia Exchange System (HERMES) developed by Rhizomatica is capable of connecting communities across hundreds of kilometres, creating secure exchange points to send and receive information.[22]

In Central America, Sulá Batsú is supporting women leaders engaging in sustainable entrepreneurship, building digital business models "that are not predatory and extractivist."[23] Sulá Batsú has offered workshops on e-waste, extraction of minerals and energy consumption for digital technologies, and facilitated ongoing conversations to support women entrepreneurs to actively engage with these issues and address emerging threats and challenges.

In Colombia, Colnodo has emphasised environmental sustainability as a cross-cutting priority since its foundation, and for more than 20 years it has operated the Red de Desarrollo Sostenible (Sustainable Development Network), originally an initiative of the United Nations Development Programme (UNDP) and the Colombian Ministry of Environment. Colnodo has also been involved in coordinating the publication of environmental data with the Environmental Observatory for Bogotá and the Bogotá River. In addition, Colnodo actively participated in the development of APC's guide to a circular economy of digital devices and contributed a case study that explores the management of e-waste in Colombia through the Computadores para Educar (Computers for Schools) initiative.[24]

Nodo TAU, based in Rosario in Argentina, has worked to repair and reuse donated computers for almost 20 years as part of their commitment to digital inclusion. In 2003, Nodo TAU began working with local organisations to set up a network of

17 Kazi, S., & Pratap, T. (2021). Transitioning to the circular economy in the South Asia region: A phased policy approach for Bangladesh, India, Sri Lanka and Pakistan. In A. Finlay (Ed.), *A guide to the circular economy of digital devices*. APC. https://circulartech.apc.org/books/a-guide-to-the-circular-economy-of-digital-devices/page/case-study-transitioning-to-the-circular-economy-in-the-south-asia-region-a-phased-policy-approach-for-bangladesh-india-sri-lanka-and-pakistan

18 https://ocf.tw/en/p/civicsense

19 Ibid.

20 Staravis. (2021, 6 July). Demand for implementation of e-waste management rules in Bangladesh. *VOICE*. https://voicebd.org/2021/07/06/demand-for-implementation-of-e-waste-management-rules-in-bangladesh

21 Bloom, P., & Brock, N. (2020). Digital communications to build autonomy and combat ecocide. In A. Finlay (Ed.), *Global Information Society Watch 2020: Technology, the environment and a sustainable world*. APC. https://www.giswatch.org/index.php/node/6227

22 Romano, M. (2022, 11 August). Seeding change: Rhizomatica's high frequency radio showcases the power of communication in remote regions of the Amazon. *APC*. https://www.apc.org/en/node/38186

23 APCNews. (2022). Seeding change: Environmental sustainability and the need to strengthen female leadership. *APC*. https://www.apc.org/en/node/37911

24 Casasbuenas, J. (2021). Computadores para Educar: Ensuring circularity through managing e-waste properly in a computers-for-schools initiative. In A. Finlay (Ed.), *A guide to the circular economy of digital devices*. APC. https://circulartech.apc.org/books/a-guide-to-the-circular-economy-of-digital-devices/page/case-study-computadores-para-educar-ensuring-circularity-through-managing-e-waste-properly-in-a-computers-for-schools-initiative

telecentres, using donated computer equipment. As the project developed, Nodo TAU began to receive large donations of computers that could not be repaired, and in 2008 they joined a project to set up an e-waste management plant in Rosario.[25] In 2021, Colnodo and Nodo TAU collaborated to develop an online Moodle course in Spanish on ICTs and the environment, and are preparing to expand the course in the future.[26]

In Brazil, APC member Intervozes is working with Coordenação Nacional de Comunidades Negras Rurais Quilombolas (CONAQ) and Movimento de Mulheres Trabalhadoras Rurais do Nordeste (MMTR-NE) to build solidarity networks through collective mapping and conceptualising of ICTs by quilombola and rural communities in northeastern Brazil. Intervozes is also working with Indigenous communities in the Guarani territories in São Paulo to build protocols for internet use and improve access.[27] In other regions of the country, another APC member in Brazil, Nupef, is partnering with local communities to design and deploy community-based internet infrastructure and community networks that help these communities defend their territories against extractivism and fight for their rights.[28]

Europe

In Europe, where internet penetration is among the highest on the planet, and where the European Union is seen as a leader in legislative and regulatory responses to environmental harm, the APC network is working with local communities to repair and transform infrastructure to work for the planet.

In Catalunya, APC member Pangea is harnessing the power of networked action through eReuse.org, a project and community that promotes and facilitates local autonomous open platforms to repair, refurbish and reuse electronics.[29] The eReuse initiative first began in 2013, launching a campaign for computer donations in 2015. Since then, the eReuse network has processed more than 10,000 computers, which has benefited families, schools, public facilities and NGOs, and supported local social inclusion and participation.

In Eastern Europe, BlueLink Foundation has continued to focus on climate and environmental issues in the region, including projects to improve communication and learning between journalists and scientists and fostering policy change to bring Bulgarian legislation in line with European climate legislation. In 2021, BlueLink joined APC staff and consultants in the development of four issues briefs on climate justice and digital rights,[30] including a brief exploring the interplay between environmental and internet governance, inspired by BlueLink's experience with regional bodies and policy processes.

In the UK, APC founding member GreenNet[31] has increasingly focused on reducing the environmental harms of internet service provision, responding to growing requests for environmentally conscious web design.

Cross-cutting priorities for technology and the planet

APC's Environmental Sustainability Working Group has identified four cross-cutting priorities for sustainable connectivity:

1. Centering the sovereignty and rights of Indigenous peoples and traditional communities

Indigenous peoples and traditional communities have the right to make decisions about if and how ICTs are used in their communities, and to defend against ICT development that threatens their rights and the rights of nature. APC supports Indigenous data sovereignty – the rights of Indigenous people to govern the collection, ownership and application of data.

2. Supporting digital safety and care, rooted in communities of practice

Holistic digital safety and care are growing priorities for environmental justice movements. The

25 Roveri, F. (2021). Planta de Gestión de Residuos Informáticos: The long and challenging road in setting up an e-waste recycling plant in Argentina. In A. Finlay (Ed.), *A guide to the circular economy of digital devices*. APC. https://circulartech.apc.org/books/a-guide-to-the-circular-economy-of-digital-devices/page/case-study-planta-de-gestion-de-residuos-informaticos-the-long-and-challenging-road-in-setting-up-an-e-waste-recycling-plant-in-argentina

26 Red de Desarrollo Sostenible. (2021, 19 February). Usando las Tecnologías de Información y Comunicación – TIC para el cuidado ambiental. https://rds.org.co/es/novedades/usando-las-tecnologias-de-informacion-y-comunicacion-tic-para-el-cuidado-ambiental-2

27 Intervozes, CONAQ, & MMTR/NE. (2021, 5 October). Lived experience and connection: Networks of knowledge produced by Black and rural women through the Territórios Livres, Tecnologias Livres project. *APC*. https://www.apc.org/en/news/lived-experience-and-connection-networks-knowledge-produced-black-and-rural-women-through

28 APCNews. (2021). Seeding change: Nupef works with community networks to support the right to communication of traditional communities in Brazil. *APC*. https://www.apc.org/en/node/37531

29 Navarro, L. (2021). eReuse: Building reuse circuits for social inclusion. In A. Finlay (Ed.), *A guide to the circular economy of digital devices*. APC. https://circulartech.apc.org/books/a-guide-to-the-circular-economy-of-digital-devices/page/case-study-ereuse-building-reuse-circuits-for-social-inclusion

30 APC. (2022). *At the interstice of digital rights and environmental justice: Four issue briefs to inform funding*. Ford Foundation, Ariadne and Mozilla Foundation. https://www.apc.org/en/node/38149

31 https://www.greennet.org.uk

global pandemic has forced many community organisers to adapt to working with and through digital technologies, often with little support for secure communications. APC's research suggests many environmental organisations and movements do not have digital safety policies and practices in place.

3. Integrating work towards social and economic justice and digital inclusion

The APC network supports initiatives to repair, refurbish and redistribute digital devices, working closely with community networks and local social enterprises for digital inclusion. At the same time, APC is working with partners to understand the impacts of extractivism and manufacturing on the health of ecosystems and human labour.

4. Working against environmental injustice in the governance of digital technologies

Individuals and communities that are affected by racism, exclusion, discrimination and inequality are disproportionately impacted by ecosystem degradation, pollution and disaster. APC centres these voices and experiences in our research and advocacy, and supports APC members working with communities to provide meaningful and sustainable connectivity.

Conclusion

The COVID-19 pandemic has exposed stark realities in the failures of governments and corporations to prevent, address and remedy the violation of human rights and the rights of nature.[32] In our global information society, meaningful connectivity continues to be an enormous challenge for many communities, and demands for "transition minerals" and "green technologies" pose huge risks for our already fragile ecosystems. The APC Environmental Sustainability Working Group acknowledges that there is no one-size-fits-all solution for building a sustainable internet. We are committed to centring communities in crisis and organising through joint action and learning for sustainable connectivity in all its complexity.

32 Office of the High Commissioner for Human Rights. (2022, 23 March). COVID-19 and human rights https://www.ohchr.org/en/stories/2020/03/covid-19-and-human-rights

A feminist backpack for crises: Care-fullness, messiness and responsive knowledge

Nyx McLean, in conversation with Jennifer Radloff, Namita Aavriti and Smita V.
Association for Progressive Communications (APC)
www.apc.org

Introduction

"The world is suddenly and radically changed,"[1] the Association for Progressive Communications Women's Rights Programme (APC WRP) wrote in April 2020 in an open letter to their friends and partners. COVID-19 and responses to the pandemic asked that people move online, and with this came an intensification around issues that had already had the attention of feminists and digital rights activists. Some of these issues included online gender-based violence, other forms of online violence, data extraction and surveillance.

This conversation with APC WRP team members Jennifer Radloff, Namita Aavriti and Smita V.[2] is supplemented by observations from the Feminist Internet Research Network (FIRN) meta-research project[3] that APC coordinated, and is only a glance at their experience of the pandemic, new concerns and priorities that emerged, the lessons they learned from the pandemic, and what they would like to take forward in a feminist backpack for future work and moments of crisis.

Online versus offline

The move to online had an impact on organising, network building, how we think about community and belonging, our sense of embodiment, how we think about participation, and how we think about and activate care. Some projects had to be put on hold as a result of the pandemic, while others which had primarily been offline had to do a hard pivot to online.

Smita, who had joined the APC WRP in March 2021, spoke about how they had started work on a new project, and the impact the pandemic had on initiating this project. For instance, they shared that it took longer to establish relationships online in contrast to "the connection that physical space builds." Online connection, Smita said, "is very different," and the absence of physical space can "cause very subtle delays and impacts in building networks." It is "knowledge that you can only gain when you experience it for yourself and when your body experiences it." Embodiment is a challenge to movement building in the digital age or during moments of crisis when movements must move online.

The embodiment of space continued to emerge in our conversation as critical to establishing connections. Namita shared her experience of how the move from offline to online "worked really well with groups that were connected beforehand because [...] 'We've met you, and I've seen you in a physical space, I have a connection with you,'" whereas "with new people, I was never quite sure it was working." Here this is speaking to how the online appeared to work better with people who had already established a connection offline in face-to-face meetings because of what an embodied physical space provides, whereas for those who had not met previously, the move to online created a challenge.[4]

The offline-online binary also had an impact on teaching people how to use technology. Smita flagged how when one is working with people "who are very new to technology [...] there is a very strong value-add that happens when you teach them how to use [it] in person." There is a link between teaching in person, and "the confidence they get in how they relate to the devices, and this takes more time online," they explained.

1 APC Women's Rights Programme. (2020, 23 April). An open letter to friends and partners. *GenderIT.org*. https://genderit.org/resources/open-letter-friends-and-partners

2 The WRP team members will be referred to by their first names throughout this report.

3 McLean, N. (2022a). *Feminist Internet Research Network: Meta-research project report*. Association for Progressive Communications. https://www.apc.org/en/node/38022

4 This is supported by research work such as, for example: Dijkstra, K., & Post, L. (2015). Mechanisms of embodiment. *Frontiers in Psychology, 6*. https://doi.org/10.3389/fpsyg.2015.01525

"Any delay which happens in building this confidence around technology directly means that certain communities get left behind," they added. This is another challenge to address when people are expected to move online during moments of crisis.[5]

The means to connect was not available to everyone due to the enormous digital and resource divides in the world, which continue to disadvantage and grow worse in the global South.[6] Not everyone had the means to connect online, but some donors responded to the pandemic by expanding the budget to include covering tech needs such as "infrastructure, devices and access," as Jennifer shared. One response was to "build packages of laptops and devices to send [to people struggling to get online] so they could participate fully," she explained. "The reality of what COVID and the lockdown were showing is that you can't participate if you don't have devices," Jennifer stressed. Here we see the emergence of another priority: the need to understand tech and infrastructure needs in order to ensure greater participation online.

Access and barriers to use

Many people were excluded and left out with the move to online. As Smita put it, "Anything and everything related to COVID [was] suddenly online." Even though there were expectations that people move online, "there were [few] provisions made for actually allowing for free internet, free data," they added.

Another example of barriers to use came from Jennifer, who shared how she noticed that older people were "completely helpless without a smartphone and completely locked out of systems," such as when they wanted to get vaccinated. Health care workers such as nurses also "couldn't work the software that they needed to use in order to track everything." This raised concerns around technology and intergenerational conversations, and how the technology used and adopted without training harmed those who were "really good" at their jobs.

This barrier to access, especially for those with little to no knowledge of technologies, showed an absence of care in response to the pandemic, and this is something that is needed in response to future moments of crisis – care-full[7] consideration around technology that is used, access to technology, and training for better use of the technology. This is also a call for greater reflexivity and consideration about our privilege, positionality and power when we propose solutions to moments of crisis.

Surveillance

COVID-19 saw an increase the development of apps in response to the pandemic and in attempts to contain its spread. Many of these apps were flagged for issues around "data collection, transparency of the data collected and the data stored," Smita shared. There was also "no actual evidence of any of these apps actually working in controlling the infection rate," they said. What these apps did do was raise concerns around surveillance and how data is being used.[8] The APC WRP in their open letter drew attention to "surveillance and [the] expansion of state power" during the pandemic.[9]

Namita spoke of an "uptick in surveillance generally," how apartments and gated communities were using "complex software that tracks people," and how access to homes and places of work "was so much more controlled" during the pandemic. Because of the pandemic, she said, there were "new pieces of software that were floated around as solutions, all of which, frankly, look bad." An increase in surveillance during a moment of crisis may not see surveillance levels return to pre-crisis levels.[10] We need to be critical of increases in surveillance and question how data extracted during a crisis like COVID-19 is being stored and used, and how the data will be destroyed afterwards, if at all.

Feminist infrastructures

In addition to questioning how our data gets used, we need to question the kind of technology we use, and to challenge our preconceptions of this technology.[11] Jennifer was critical of what she called "the ownership and control of the existing northern male,

5 Research has documented this in relation to online learning and shown that in-person availability of a trainer removed many of the barriers to learning such as timely feedback, support services, understanding instructions. See, for example: Marcial, D. E., Caballero, R. D. B., Rendal, J. B., & Patrimonio, G. A. (2015). "I am offline": measuring barriers to open online learning in the Philippines. *Інформаційні технології і засоби навчання*, *45*, 1, 28-41.

6 Power, T. (2020). *The gender digital divide and COVID-19: Towards feminist internet regulations in southern Africa*. APC. https://www.apc.org/en/node/36718; Ragnedda, M., & Gladkova, A. (2020). *Digital Inequalities in the Global South*. Springer International Publishing; United Nations. (2021, 27 April). With Almost Half of World's Population Still Offline, Digital Divide Risks Becoming 'New Face of Inequality', Deputy Secretary-General Warns General Assembly. https://press.un.org/en/2021/dsgsm1579.doc.htm

7 A deliberate choice to write as "care-full" instead of "careful".

8 van Zyl, I., & McLean, N. (2021). The Ethical Implications of Digital Contact Tracing For LGBTQIA+ Communities. *Proceedings of the 1st Virtual Conference on Implications of Information and Digital Technologies for Development*. https://www.mn.uio.no/ifi/english/research/groups/is/ifip-94/proceedings-virtual-conference-2021/all-papers/zylmclean.pdf

9 APC Women's Rights Programme. (2020, 23 April). Op. cit.

10 van Zyl, I., & McLean, N. (2021). Op. cit.

11 Lim, S. (2022, 7 March). Misogyny as a commodity in digital spaces. *GenderIT.org*. https://genderit.org/articles/misogyny-commodity-digital-spaces; Sanjuan Mejia, L. (2020, 12 November). Feminists are building their own technology to organise but where are funders? *GenderIT.org*. https://www.genderit.org/feminist-talk/feminists-are-building-their-own-technology-organise-where-are-funders-o

white infrastructure." She proposed that we look to "alternative structures" like "feminist infrastructures" instead of relying on the Googles and Zooms of the world. During the pandemic there were instances of violence experienced in spaces such as Zoom. Namita said that the pandemic was "definitely a turning point [...] in the sense of taking [online violence] far more seriously." Jennifer shared that in response to instances of violence, APC shaped their approaches by focusing on online digital safety training, and more awareness of data extraction, of surveillance, and of misinformation and disinformation. In addition to this, Jennifer said that it was important to "question the systems and the politics and the power and the privilege underneath it." It is critical that we continue to critique, challenge and interrogate the power that informs the technologies we use.

There is a need for feminist infrastructures which are "shareable with partners and comrades," Smita said. It is important, they said, to give consideration to "how accessible the software is, especially when working with partners who have low connectivity [or] restrictions on data." Care is something that emerged from our conversation, as well as in the FIRN project. Care needs to be prioritised going forward, whether in moments of crisis or not. Namita shared that care needs to be extended beyond the self and there "needs to be a movement to collective forms of care in a more serious way."

From these lessons we gave consideration to a feminist backpack for future work and future moments of crisis.

A feminist backpack for future work and moments of crisis

In concluding our conversation, Jennifer, Namita, Smita and I imagined what we would need to carry with us from our experience of the pandemic, and the work in APC WRP and on FIRN, that could serve our future work and help us respond to moments of crisis. We decided to think of it as a backpack in which to carry the tools, resources and values with us. In this backpack we have placed: care – self and collective; digital safety; listening and exchange of experiences; embracing messiness; responsive knowledge; and reflexivity.

Care – self and collective

Care emerged as a central theme. We see this in multiple responses from APC and partners.[12] As Namita discussed earlier, it is important that we give consideration not only to care as it relates to the individual self, but also to what it means for the collective. As Jennifer shared, it is also important to "reimagin[e] what it looks like when it is an online space."

Digital safety

We all added digital safety to our backpack, because it was apparent in our discussions around online violence and its consequences for vulnerable groups that there is a need for better digital safety and training in this area. Previous conversations with FIRN partners saw digital safety as an aspect of care for ourselves as digital rights defenders, activists and researchers, as well as for our research partners, project participants and communities.

Listening and exchange of experiences

Jennifer added "storytelling and listening" to our backpack. She shared that during the pandemic she found that it "was really important being part of APC and listening to what people were going through in different contexts," and that it was critical to find "ways of exchange, of understanding, of knowledge, of strategies, of tactics."

Embracing messiness

What we called "messiness" emerged from this conversation and also conversations with partners[13] during the FIRN project. Messiness asks that we learn, as Jennifer shared, "to sit with discomfort, face it, confront it, and even if you don't have the words, just to try." Smita added that messiness was about letting go of rigid ways of doing things, and to "allow for fluidity and dynamicness in movement building, in digital security, in workshops."

Responsive knowledge

Responsive knowledge building, and "making" and "sharing", was added to our backpack. GenderIT.org[14] was given as an example of "responsive knowledge" because, as Jennifer said, it produces "that kind of knowledge from contextual knowledge that comes out quickly and can be discussed and archived and made real." Namita referred to this approach of knowledge building, making and sharing as "knowledge that is not straightjacketed." It is important that the knowledge we produce and share is responsive and accessible to as many as possible.

12 APC Women's Rights Programme. (2020, 23 April). Op. cit.; Association for Progressive Communications. (2020). *Closer than ever: Keeping our movements connected and inclusive – APC's response to the COVID-19 pandemic*. https://www.apc.org/sites/default/files/closerthanever_pp.pdf; Transfeminist Network of Digital Care. (2022). *Digital care for feminist activists*. APC. https://www.apc.org/en/digital-care-feminist-activists;

13 McLean, N. (2022a). Op. cit.; McLean, N. (2022b). Feminist internet research is messy. In Aavriti, N., Hussen, T. S., & Fossatti, M. (Eds), *Feminist by Design: APRIA Journal Issue 4*. https://apria.artez.nl/feminist-internet-research-is-messy

14 https://genderit.org

Reflexivity

The final item to be added to our backpack was that of reflexivity. Reflexivity emerged out of this conversation and the conversations with FIRN partners. Reflexivity creates space for us to consider our current contexts, our experiences, and how we can imagine things differently. It is exceptionally useful as a way forward in terms of movement building, creating safe spaces and holding space. It is a useful tool for learning and adapting to moments of change and crisis.

Conclusion

The COVID-19 pandemic was a moment of crisis that asked a great deal of all of us. It was a moment of learning, of leaning into the uncomfortable, and hopefully rethinking and reimagining the way that we work, live and respond to each other and ourselves. The conversation above is in no way exhaustive – but it is a glimpse into new challenges, concerns, priorities, lessons learned and approaches, such as those found in the feminist backpack. We live in a world that faces numerous challenges such as structural inequalities, moments of crisis, and those ongoing, such as the climate crisis. We need to give consideration to the work we do, the tools we use, and how we can be responsive from a space of care and safety that ensures that nobody is left out.

Internet governance of the future

Anriette Esterhuysen[1] and Wim Degezelle[2]

The past

Twenty years ago, at the start of the preparatory process for the World Summit on the Information Society (WSIS), the internet – a "network of networks" – and internet governance were still abstract and largely unknown concepts to many delegates. In response, at the end of the first phase of the WSIS, the UN Secretary-General mandated a multistakeholder Working Group on Internet Governance (WGIG)[3] to investigate, define and make proposals on the governance of the internet to inform negotiations at the second and final phase of the WSIS in Tunis in 2005. The WGIG's working definition for internet governance was formally adopted in Tunis:

> Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.[4]

This definition, along with the affirmation in the Tunis Agenda (the final WSIS output document) that "the management of the Internet encompasses both technical and public policy issues and should involve all stakeholders and relevant intergovernmental and international organizations,"[5] and the formation of the Internet Governance Forum (IGF),[6] promised a dynamic and inclusive future for internet governance.

David Souter recently described this period as a time when internet governance was "bright and shiny", when "new technologies and new ways of governing technologies suggested that there might be ways of changing how public policy gets made – not least by bringing more diversity into decision-making through multistakeholder participation."[7] It presented an opportunity for civil society actors to be part of evolving a new, fairer, global governance model at a time when there were wider calls in the UN for more inclusive and accountable global governance.[8] In its statement at the conclusion of the WSIS process, civil society expressed support for the idea of the IGF, committed to participate in it, but reiterated its view that "the forum should be more than a place for dialogue" and "should also provide expert analysis, trend monitoring, and capacity building, including in close collaboration with external partners in the research community."[9]

Civil society organisations have since participated actively in the IGF and in other post-WSIS global, regional and national policy processes.[10] They collaborated with institutions from other stakeholder groups to produce multiple internet governance frameworks, norms, principles and guidelines. Examples include the Brazilian Principles for the Governance and Use of the Internet,[11] the Necessary

1 Anriette Esterhuysen is an APC associate and a senior advisor on internet governance.

2 Wim Degezelle is an internet policy analyst and consultant.

3 Working Group on Internet Governance. (2005). *The Working Group on Internet Governance: Background Report.* https://www.itu.int/net/wsis/wgig/docs/wgig-background-report.pdf

4 Tunis Agenda, paragraph 34. https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html

5 Ibid., paragraph 35.

6 The Tunis Agenda, in article 72, asked the UN Secretary General to convene a forum for multistakeholder dialogue, called the Internet Governance Forum. https://www.intgovforum.org

7 Souter, D. (2022, 21 June). Inside the Digital Society: Does internet governance require a reboot? *APC.* https://www.apc.org/en/blog/inside-digital-society-does-internet-governance-require-reboot

8 For example, at the UN World Summit on Sustainable Development (Johannesburg, August 2002), the failure of global financial, trade and environmental governance to effectively manage the uneven effects of globalisation featured prominently. The outcome document emphasised the need for all levels of policy formulation and decision making to be inclusive of developing country voices and also called for strengthened partnerships with civil society. Johannesburg Declaration on Sustainable Development, 2002, paragraph 26. https://www.un.org/esa/sustdev/documents/WSSD_POI_PD/English/POI_PD.htm

9 Various. (2005). *"Much more could have been achieved": Civil Society Statement on the World Summit on the Information Society.* https://waccglobal.org/wp-content/uploads/2020/07/Much-more-could-have-been-achieved.pdf

10 For example, the regional WSIS action plans in Africa and Latin America and the Caribbean.

11 Developed by the Brazilian Internet Steering Committee in 2009. https://www.cgi.br/principles

and Proportionate Principles on the Application of Human Rights to Communications Surveillance,[12] the Charter of Human Rights and Principles for the Internet,[13] the African Declaration on Internet Rights and Freedoms,[14] the Manila Principles on Intermediary Liability[15] and the Feminist Principles of the Internet.[16] The Code of Good Practice on Information, Participation and Transparency in Internet Governance[17] was developed by APC with the Council of Europe and the United Nations Economic Commission for Europe, and civil society contributed to the milestone Human Rights Council resolution of 2012 that affirmed that human rights that apply in the "offline world" also apply online.[18]

Civil society invested time and resources in the IGF's Multistakeholder Advisory Group (MAG), in IGF intersessional work (Dynamic Coalitions and Best Practice Forums) and, in 2011 at the Nairobi IGF, initiated the "day zero" tradition of having linked events on the day before the official IGF programme. Several of the national, regional and youth IGFs (NRIs) that emerged from 2008 onwards were initiated by civil society groups and contributed to them building closer relationships with national governments and regional intergovernmental institutions.

This WSIS- and IGF-inspired multistakeholder public policy engagement "bubble" reached a peak in 2014 with the NETmundial,[19] a response to the shock of the Snowden revelations and the controversy around the Internet Assigned Numbers Authority (IANA) transition. It was hosted and organised by the then left-leaning government of Brazil with the technical community, in close collaboration with civil society, governments and the academic and business sectors. The resulting NETmundial Multistakeholder Statement[20] was drafted collaboratively, with all interest groups having to compromise to some extent. Several civil society actors were not fully happy with the NETmundial process and outcome documents, which they felt favoured the "core interests of the most resourceful parties, which, at the global level, are often the US and big business."[21] However, the vast majority accepted the outcome and celebrated its strong commitment to the internet as a global public resource that should be managed accordingly, and to the emphasis given to openness, transparency, inclusion and human rights.

To date, NETmundial remains the largest and most inclusive multistakeholder process for distilling principles for internet governance. Its innovative process enabled collective and transparent drafting, with contributions from 1,480 stakeholders from 97 countries collected via an online platform, followed by face-to-face negotiation and consensus building.

Sadly, and despite receiving widespread endorsement, the NETmundial principles were never systematically promoted, "socialised" and legitimated by the stakeholders that negotiated them. Nor did they move from the multistakeholder into the multilateral space – in fact, some UN member states actively opposed formal recognition of the NETmundial principles in UN forums.[22] The work of consolidating principles for governing the internet – once a core theme at the IGF – came to a halt.

NETmundial did have impact. The IANA transition, one of the most controversial internet governance processes of the post-WSIS era, benefited from both the NETmundial process – which outlined a roadmap for the transition – and the IGF, as a platform for providing broader, and global South, engagement. NETmundial also proves that collective multistakeholder drafting of text is possible, even if not easy.

But would the NETmundial principles, if they had been globally socialised and adopted by both multilateral and multistakeholder decision-making forums, have enabled a more coherent public interest and human rights-centred approach to internet governance? Would this have helped harmonise the spate of national-level internet-related regulation that has emerged in the last few years, and as such, safeguarded the internet as a global public resource from fragmentation produced by the actions of internet companies and national governments? Would current efforts to regulate corporate behaviour on the internet have been more global and cooperative, as opposed to fragmented along geopolitical, regional or national lines? Perhaps or perhaps not;

12 Developed by the Electronic Frontier Foundation and a coalition of NGOs in 2013-2014. https://necessaryandproportionate.org/principles

13 Developed by the IGF Internet Rights and Principles Dynamic Coalition in 2011. https://internetrightsandprinciples.org/charter

14 Drafted in 2014 as a Pan-African initiative to promote human rights standards and principles of openness in internet policy formulation and implementation on the continent. https://africaninternetrights.org

15 Developed through an open, collaborative process conducted by a broad coalition of civil society groups and experts from around the world in 2015. https://manilaprinciples.org/index.html

16 Originally drafted in 2014 at the first Imagine a Feminist Internet in Malaysia, organised by APC. https://feministinternet.org

17 https://www.apc.org/en/projects/code-good-practice-information-participation-and-t

18 "The promotion, protection and enjoyment of human rights on the Internet", A/HRC/RES/20/8, resolution adopted by the UN Human Rights Council on 16 July 2012. https://digitallibrary.un.org/record/731540?ln=en

19 https://netmundial.br

20 https://netmundial.br/netmundial-multistakeholder-statement

21 Just Net Coalition. (2014, 5 May). The JNC Response to the NETmundial Outcome Document. *ALAI*. https://www.alai.info/85299-2

22 Evident in, for example, discussions at the UN Commission on Science and Technology for Development (CSTD) on WSIS follow-up and the resulting Economic and Social Council (ECOSOC) resolution in 2015.

but having some soft law instruments that expanded on the WSIS principles would definitely have provided – at least in the context of UN processes – a more focused and potentially influential global approach to discussing solutions to emerging internet-related policy and regulation challenges.

The present

Today, internet-related issues are priorities on many policy agendas. Having grown from 1.1 billion users in 2005 to more than four billion users today,[23] the internet is at the centre of a process of digitalisation that is transforming the workplace, social and political processes, business and trade, as well as people's personal lives, a transformation accelerated by COVID-19.

However, several of the challenges that were on the table during the WSIS remain unresolved. For example, access to the internet remains unequal, between and within countries and regions. The availability and affordability of infrastructure and devices, local content in local languages, and the human capacity needed to reap the benefits of using the internet are "old challenges". On the other end of the spectrum, many new challenges have emerged and are emerging from hyper connectivity and the resulting dependence on internet-based systems and services. With new opportunities come new threats and risks. Datafication, surveillance-based business models, artificial intelligence, machine learning and automated decision making, cybercrime, mis- and disinformation and harmful content create a whole new range of challenges and policy questions.

Internet governance is no longer a stand-alone discipline but has become part of broader "digital governance" and "digital transformation". The range of internet-related policy and regulation issues continues to expand, cross borders, and intersect with other spheres. Linked to this is a proliferation of venues. Some are new, such as the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes,[24] but many pre-date internet governance, for example, national legislatures, telecoms regulatory bodies, trade organisations, competition commissions and human rights institutions. What is new is that they have to give serious attention to internet-related aspects of their areas of work. This constitutes a challenge in its own right, particularly for civil society organisations who lack the human and financial resources required to follow all these processes effectively.

COVID-19

The early 2020s will always be associated with the COVID-19 pandemic, a global crisis which affected almost everyone everywhere, in developed and developing countries. The severity of the pandemic's impact depended on multiple factors, but four of these are worth noting, because they contain lessons learned that are also relevant to internet governance. They are equitable and sustainable development; publicness (as in resilient public infrastructure and services); coordinated collaboration; and trust and human rights.

First, **equitable and sustainable development**. As the World Health Organization (WHO) recently put it:

> The pandemic has laid bare the social fractures in our societies and it is no longer possible to ignore the fact that many people are struggling to live a decent and dignified life and are unable to meet essential needs for safe and secure shelter, food, fuel and income. The coexistence of material deprivation and discrimination by gender, race and religion have emerged in the risks of infection, excess loss of life, and growing poverty and poor health faced by ethnic minorities, women, informal workers, and the poor and vulnerable.[25]

Digital equity proved to be vital for accessing information, education and culture, for staying in touch with friends and family, and for people to be able to continue working to earn a living. Access to the internet and the ability to use it in a meaningful way[26] softened the social, psychological and economic impact of lockdowns and quarantine, and the impact of *not* having access became starkly visible, which highlighted the need for digital inclusion.

But achieving equitable and sustainable digital development is not easy. As the extent and sophistication of internet-based transactions and applications increase, those without the needed devices, bandwidth and skills tend to fall even further behind, and the digital inequality actually

23 According to data from the International Telecommunication Union (ITU), 50% of the world population (around four billion people) used the internet at the end of 2019. Other sources, such as Internet World Stats, put the mid-2021 figure at well over 4.5 billion. ITU. (2020). *Measuring digital development: Facts and figures 2020*. https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2020.pdf

24 https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

25 WHO. (2022, 7 July). WHO encourages stakeholders to embed health equity in COVID-19 recovery plans. https://www.who.int/europe/news/item/07-07-2022-who-encourages-stakeholders-to-embed-health-equity-in-covid-19-recovery-plans

26 Which in turn relates to issues such as skills, affordability, quality of broadband internet connectivity, etc.

increases. In addition, increased digitalisation, once seen as a more sustainable alternative to industrialisation, has become a contributor to climate change, pollution and habitat destruction through massive energy use, electronic waste and its dependency on rare minerals, the mining of which has fuelled conflict and damage to sensitive ecosystems (e.g. the sea bed). Internet and digital governance, policy and regulation need to consider the impact of innovation and growth on people, communities, biodiversity and the natural environment.

Second, and linked to equitable and sustainable development, is **"publicness"** and resilient public services and infrastructure. Under-investment in resilient public health systems[27] left national and global health authorities struggling to respond effectively to the crisis. Once vaccines became available, the ability of health services to manage the vaccination supply chain, from procuring vaccines, to communicating with the public, to storing, delivering and administering vaccinations, impacted on economic recovery and a return to normal life. Dependency on the internet during the pandemic revealed under-investment in internet infrastructure and services. Many people did not have reliable broadband access, particularly in rural areas. Despite being a priority since the WSIS, enabling policy and regulation to expedite universal access are still not in place in many parts of the world. While some countries approach access to the internet as essential, and even as a right, others have introduced new barriers, for example, through taxation of social media and voice over IP (VoIP) service or through internet shutdowns.

Much internet infrastructure is built and maintained by the private sector and the technical community, which is a characteristic of internet infrastructure, and a primary reason for its governance being multistakeholder. However, this does not, and should not, negate the need for such infrastructure to be incentivised and regulated in the public interest and for the internet to be understood and protected as a commons or public good.

Third, **coordinated collaboration**. Around the world, the effort to address the pandemic and prevent it from getting worse was marred by insufficient international and multistakeholder coordination and collaboration. The already insufficient resources (and capability) of the WHO were exacerbated by the United States' withdrawal of support (since reversed by President Biden) and former President Trump's consistent public attacks on the institution and its leadership.[28] Even the expansive regulatory machinery of the European Union could not produce clear and coordinated responses on vaccine approvals, lockdowns or travel restrictions.[29] With respect to vaccine development, the complexity resulting from so much COVID-19-related research and development being led by the private sector had not been anticipated. When it was most needed, there was simply not enough active coordination or collaboration between public and private health and pharmaceutical authorities and regulators. Neither government nor business seemed to engage the media and civil society sufficiently, and they rarely presented common positions. This created a climate of uncertainty, prone to mis- and disinformation and an overall trust deficit, which made responding to the pandemic more difficult.

Effective internet governance also relies on cross-border multistakeholder and multilateral collaboration. This too lacks a clear and coordinated commitment by both public and private sector actors to protecting and governing the internet as a global commons or public good. Increasingly, people's use of the internet – and access to news and information – takes place through privately owned, commercial platforms. As pandemic-related panic set in, mis- and disinformation were spread on social media.[30] The response from platforms was delayed at best, and often inadequate. From states it was often rushed and overly aggressive. Several used the pandemic to justify legislation that criminalised COVID mis- and disinformation online, using vague definitions that endangered freedom of expression, particularly people's freedom to challenge state responses to the crisis.[31]

27 In general, but with multiple issues that relate to internet governance challenges, such as connectivity to exchange data and information between public health institutions, collect data, adequately inform and sensitise the general public, manage vaccination campaigns, etc.

28 KFF. (2022, 19 May). The U.S. Government and the World Health Organization. https://www.kff.org/coronavirus-covid-19/fact-sheet/the-u-s-government-and-the-world-health-organization

29 Springall, J. (2022, 5 March). How will we ever overcome the confusion and complexity of COVID-19 travel? *Euronews*. https://www.euronews.com/travel/2022/03/05/how-will-we-ever-overcome-the-confusion-and-complexity-of-covid-19-travel

30 https://www.poynter.org/ifcn-covid-19-misinformation

31 Fish Hodgson, T., Farise, K., & Mavedzenge, J. (2020, 5 April). Southern Africa has cracked down on fake news, but may have gone too far. *Mail & Guardian*. https://mg.co.za/analysis/2020-04-05-southern-africa-has-cracked-down-on-fake-news-but-may-have-gone-too-far; Dushyant, & Manzar, O. (Eds.) (2020). *The New Normal: How to Survive a New World Order*. Digital Empowerment Foundation. https://www.defindia.org/wp-content/uploads/2021/02/The-New-Normal-Full-Book-by-DEF.pdf

This brings us to the fourth factor, **trust and human rights**. Many governments underestimated the importance of building trust through strengthening their own public information and communication systems. Trust was further undermined by rushed COVID contact-tracing solutions, which in some cases were introduced without data protection frameworks being in place and were rolled out in a manner that could be described as "surveillance by stealth". What data was collected, where and how long it was stored, and how it was processed and used were often unclear, including who had access to the data or with whom data and results were shared.[32]

The trust deficit during the pandemic existed at multiple levels, between countries, between citizens and states, between private and public health care entities, and between consumers and corporations. Trust is intrinsically linked to human rights. One of the most profound characteristics of the human rights framework that has evolved over the last 75 years is that it puts individuals at its centre, not citizens. As duty bearers for upholding and promoting human rights, all states have the responsibility to do so for all of humanity, not just for their citizens. One can argue that one of the weaknesses in the global response to COVID-19 was that it followed national, citizen-oriented lines, rather than being rooted in international collaboration aimed at protecting and supporting humanity at large. Internet governance too needs to be grounded in international human rights laws and standards as a means of avoiding harms, exclusion and fragmentation.

Internet governance of the future

The future of internet governance is often presented in binary terms,[33] a trend reinforced by the conflict in Ukraine, and described recently by Alex Klimburg and others as two alternate futures:

> In the best case, the world can hope for a bright, stable digital future, with different parts of cyberspace working in tandem and available globally, and where international cooperation makes it increasingly safe and secure. The alternate vision is bleaker: a "splinternet" of competing internets and walled gardens, where cybercrime is rife, and the calamitous threat of civilization-crashing cyberwar is ever-present.[34]

The problem with binary views of the future of the internet is two-fold. First, they overlook the diverse reality that characterises how people today (can) use and experience the internet. The idealised "free and open internet" has never existed for people who have no access or intermittent, poor quality access, for people who have to spend more than 20% of their monthly household income for broadband, or who live in countries where the government shuts down the internet unilaterally. Second, binary rhetoric to describe the future of the internet, particularly when repeatedly expressed by government representatives in international forums, could become self-fulfilling prophecies contributing to and accelerating the very polarisation they predict. Jason Pielemeier and Chris Riley point this out in their critique of a recent report by the US Council on Foreign Relations[35] that declared the era of the global internet as being over:

> The internet is a network of networks, and despite the advanced information controls imposed in some jurisdictions, its technical design – including the critical Internet Protocol and Border Gateway Protocol – [is] designed to maintain interconnection above all else. Separating countries into friends and enemies also, ironically, buttresses the long-standing goals of China, Russia, Iran, and other authoritarian regimes to center internet governance in "cyber sovereignty" rather than internationally protected human rights.[36]

32 The WHO published an excellent set of guidelines on contact tracing in February 2021. These guidelines emphasise the human component of contact tracing, warn of risks to individual privacy and security, and state very clearly that it is not necessarily the most appropriate response: "Contact tracing efforts need to be balanced against other resource requirements, and the impact of contact tracing should be assessed relative to other health interventions. Planning for contact tracing includes ensuring that the costs of setting up and maintaining an effective system are secured and that the social and economic consequences of quarantine are addressed for affected individuals." WHO. (2021, 1 February). Contact tracing in the context of COVID-19: Interim guidance. https://apps.who.int/iris/bitstream/handle/10665/339128/WHO-2019-nCoV-Contact_Tracing-2021.1-eng.pdf

33 At the 2018 IGF held in Paris, at UNESCO, President Macron posited the idea of the "internet of California", self-regulated by companies against the "internet of China", controlled by government. He proposed a middle way where governments work with other stakeholders to regulate the internet "properly". See: https://www.intgovforum.org/multilingual/content/igf-2018-speech-by-french-president-emmanuel-macron

34 Klimburg, A., Perucica, N., & Dobrygowski, D. (2022, 24 May). How to safeguard the internet after the war in Ukraine. *World Economic Forum*. https://www.weforum.org/agenda/2022/05/safeguarding-the-internet-post-ukraine

35 Segal, A., Goldstein, G. M., & Schmemann, A. (2022). *Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet*. Council on Foreign Relations. https://www.cfr.org/report/confronting-reality-in-cyberspace/download/pdf/2022-07/CFR_TFR80_Cyberspace_Full_SinglePages_06212022_Final.pdf

36 Pielemeier, J., & Riley, C. (2022, 1 September). In Defense of the Global, Open Internet. *Lawfare*. https://www.lawfareblog.com/defense-global-open-internet-o

They continue:

> In a moment of historic expansion of internet connectivity, most governments around the world still haven't firmly established their position on the spectrum between an authoritarian and freedom-centric approach to internet governance. If the United States, in particular, portrays the future of the internet as inevitably isolationist, it is as likely to push governments *toward* authoritarian models as it is to incentivize governments away from them.[37]

Is there a way forward for internet governance that avoids binary thinking and reaffirms the internet as an interconnected, interoperable network and, ultimately, a global public resource? Is there a role for the IGF, which will be convening for the 17th time this year?

The IGF is being questioned for not effectively producing outcomes that feed into policy processes. This critique, while not entirely without merit, has unfortunately resulted in undervaluing the IGF's long-term impact as a platform for networking, learning, and open dialogue and debate. The reality is that in a world where many governments have never given full support to the idea of multistakeholder global governance, and many more have inconsistent human rights records, the IGF succeeded as an inclusive and open forum covering all aspects of internet governance, including human rights and the multistakeholder approach.

Critiques of the IGF, particularly by states, can also be seen as a reflection of a nascent shift away from mainstreamed and substantive commitments to establishing global, cooperative, inclusive, multistakeholder internet governance. Governments that were foremost among those that championed inclusive, multistakeholder, human rights-oriented internet governance now seem to advance an "us against them" approach in relation to "non-like-minded" states, rather than systematically joining forces with civil society and other non-state actors to seek common ground and strive for cooperation.

Conclusions and call to action

There are no shortcuts to achieving the inclusive, people-centred, human rights-oriented information society that civil society organisations have envisaged since the WSIS. Realising this vision requires a holistic approach that considers the factors discussed above: equitable and sustainable development, the publicness of the internet, coordinated collaboration, and trust and human rights. To do so, civil society should take stock, analyse and prioritise, and do so collaboratively – within civil society, but also with other sectors/stakeholder groups.

Take stock and prioritise. Assessing progress, success and setbacks of the last 20 years is a good basis for civil society from the global South and North to collaborate and plan future action. The Global Digital Compact, the Summit of the Future, cybersecurity processes and WSIS+20 are opportunities. The diversity within civil society might not allow achieving complete consensus about everything, but that should not matter. Gathering together to assess the past, share perspectives and look at the main developments in different policy spaces that affect internet governance will provide building blocks for this holistic view and approach. There are bound to be areas of commonality that can underpin some form of collective input into formal policy processes.

Invest in, and demand, inclusive multilateral and multistakeholder governance processes. In 2003 civil society proposed that "[p]rocedurally, decision-making processes must be based on such values as inclusive participation, transparency, and democratic accountability."[38] These words are still relevant today across the board of multilateral, multistakeholder, and national or industry-level internet-related policy and regulatory processes. Division within civil society on whether it should support the multistakeholder approach or not has been unproductive. What matters is how transparent, inclusive, participative and accountable any policy process is. Lack of transparency and accountability can hide and enable capture by vested corporate or national interests. The multistakeholder approach is not a substitute for effective multilateral governance. We need both multistakeholder and multilateral processes, and both need to be more effective and inclusive. Sadly, the recently published draft modalities for the upcoming Summit of the Future,[39] a multilateral process that claims it will facilitate multistakeholder input, suggests that opportunity for non-state actor engagement will be limited and constrained. Civil society's only way of working around that is to work collaboratively, particularly during the preparation for the Summit.

37 Ibid.

38 WSIS Civil Society Plenary. (2003). *"Shaping Information Societies for Human Needs": Civil Society Declaration to the World Summit on the Information Society*. https://www.itu.int/net/wsis/docs/geneva/civil-society-declaration.pdf

39 United Nations General Assembly. (2022, 7 September). Draft resolution submitted by the President of the General Assembly: Modalities for the Summit of the Future. A/76/L.87. https://daccess-ods.un.org/access.nsf/Get?OpenAgent&DS=A/76/L.87&Lang=E 2022. https://daccess-ods.un.org/tmp/2137181.31184578.html

Challenge fragmentation of the internet *and* of internet governance. Internet-related regulation is here to stay, whether it is intended to reduce online harm, regulate corporate behaviour, hold platforms accountable for disseminating false information, or combat cybercrime. Walled gardens, national firewalls, censorship, surveillance, shutdowns and the exploitation of personal data are all part of today's internet and go against the ideal of one unfragmented internet. At the same time, faith in the value of open and inclusive dialogue, and in the IGF as a platform to facilitate such a dialogue, seems to be in decline, fuelled by "new cold war" discourse. But this does not need to be the case. The open internet's core protocols continue to enable interoperability and interconnection to all those who have access to it. Civil society can counter fragmentation of the internet and of internet governance by advocating for and participating in collaborative coordination, and policy and regulation that harmonise across borders, building on common existing international norms and principles (spanning the fields of human rights, social justice, peace and sustainable development) as a foundation.

Reuse, mix and remix. When it comes to formulating positions, principles and norms, there is a vast body of work already done by civil society itself, as well as by other stakeholder groups, such as the UN First Committee's Group of Governmental Experts' norms on responsible state behaviour in cyberspace. Adapting to context changes and being agile is crucial in the digital space, but it is not necessary to go back to the drawing board empty handed. The statements and principles cited above, along with tools such as UNESCO's Internet Universality Indicators,[40] are all valuable. So are ones not yet mentioned such as the Just Net Coalition's Delhi Declaration,[41] or the Communication Rights in the Information Society (CRIS) Campaign's handbook on assessing communication rights,[42] more recent norms and guidelines focused on platform governance or human-centric cybersecurity, or the human rights-based approach (HRBA). The HRBA is not just about human rights and building trust. It is an approach that builds on the norms and principles outlined in the Universal Declaration of Human Rights, and the subsequent legally binding UN treaties, but it also challenges unequal power relations and social exclusion. Many governments are familiar with this approach through the EU Consensus on Development agreement[43] and the UN Common Understanding of the HRBA.[44] This means that civil society has a common language to draw on when using the HRBA in internet policy processes. Its core elements are captured by the acronym PLANET: participation; links to human rights obligations; accountability; non-discrimination; empowerment and capacity development; and transparency. Sida recently published two helpful guides to using this approach in digitalisation and internet policy and development.[45]

Find and mind the gap. Assessing past work is also a way of identifying gaps. For example, early civil society documents, and the NETmundial statement, refer to the internet as a public resource, or a public good. The Global Commission on the Stability of Cyberspace proposed the norm to protect the public core of the internet.[46] The UN Secretary-General highlights the need for digital public goods in his *Our Common Agenda* report.[47] But no one has explored systematically what the normative implications of approaching the internet itself as a commons would be for policy and regulation. Civil society should consider whether there are pivotal shifts needed to redirect the trajectory of internet governance away from becoming contested terrain between states and corporations, and help it move towards protecting the internet as a global public good or commons, to be governed in the public interest based on international human rights norms. In this context, civil society could consider and propose possible instruments, for example a UN-based framework agreement that captures the WSIS principles in a way that can be used to hold states accountable for upholding them. Gaps can also be more specific, and addressed as such – for example, norms for online advertising and content moderation during elections to enhance trust and prevent manipulation and that can be used to hold companies and political parties accountable.

40 https://www.unesco.org/en/communication-information/internet-governance/internet-universality-indicators

41 https://justnetcoalition.org/delhi-declaration

42 CRIS Campaign. (2005). *Assessing Communication Rights: A Handbook*. https://archive.ccrvoices.org/cdn.agilitycms.com/centre-for-communication-rights/Images/Articles/pdf/cris-manual-en.pdf

43 https://international-partnerships.ec.europa.eu/policies/european-development-policy/european-consensus-development_en

44 UN Sustainable Development Group. (2003). *The Human Rights Based Approach to Development Cooperation: Towards a Common Understanding Among UN Agencies*. https://unsdg.un.org/resources/human-rights-based-approach-development-coordination

45 Sida. (2022). *Human Rights Based Approach and Digitalisation*. https://cdn.sida.se/app/uploads/2022/05/03092839/10205933_Sida_TN_HRBA_Digitalisation_webb.pdf; Sida. (2022). *HRBA and a Free, Open and Secure Internet*. https://cdn.sida.se/app/uploads/2022/05/03093124/10205933_Sida_TN_HRBA_Secure_Internet_webb.pdf

46 https://hcss.nl/gcsc-norms

47 https://www.un.org/en/common-agenda

Context matters. For civil society, an equitable, inclusive public and human rights-oriented internet is not an isolated goal. As civil society engages in internet governance of the future, it must stay aware and engaged with working for social and economic justice, gender equality, peace and environmental sustainability – locally and globally. David Souter recently pointed out:

> Technology's development's not independent of what's happening in the wider world around it. External circumstances – individual events, changes in the way we live, trends in geopolitics – affect digital development just as much as digital development affects the wider world.[48]

Staying connected to the "wider" world means, for example, being connected to local issues and contexts, networking with communities and community-based organisations, and interacting with national, regional and local government. It means working collaboratively but also being constructively critical, by asking questions rather than making assumptions; by listening to people who are affected directly by issues discussed in policy spaces; by building alternative solutions and working in partnership; by caring for our planet and all lives; and by carefully evaluating – and acting on – the impact of digitalisation on the environment as well as how digitalisation can help to mitigate climate change and manage its effects.

48 Souter, D. (2022, 20 July). Inside the Digital Society: What impact has COVID had in practice? *APC*. https://www.apc.org/en/blog/inside-digital-society-what-impact-has-covid-had-practice

Country and regional reports

ARGENTINA

INTERNET RIGHTS IN A PANDEMIC: HOW CIVIL SOCIETY ORGANISATIONS ADVOCATED FOR RIGHTS AND BETTER POLICIES

Nodo TAU
María Florencia Roveri
https://tau.org.ar

Introduction

The beginning of the pandemic found Argentina with a new, progressive government, committed to expanding rights. It took on the health crisis with pre-emptive measures aimed at protecting the public's health, access to education and the economy.

Internet access was also addressed in several policies – mainly in terms of connectivity, but also in relation to access to equipment – as was access to public information and freedom of expression, including the problem of "fake news". Digital resources aimed at controlling the circulation of people during lockdown and policies on diagnosing COVID-19, monitoring and, more recently, vaccination, were also put in place, some of which raised the challenge of processing personal information using the necessary privacy safeguards.

In this context, organisations and actors that, from different perspectives, address access to technologies and the internet, found themselves confronted by a scenario where internet rights were more visible than ever before. Their challenge was to broaden and deepen a rights-based approach in policies related to information and communications technologies (ICTs).

This report discusses the challenges of internet access, freedom of expression and privacy that were foregrounded during the pandemic, and how civil society organisations addressed the challenges.

Context

On 3 March 2020, the first case of COVID-19 was registered in Argentina. Seventeen days later, the Argentine government decreed mandatory preventive social isolation throughout the country.[1] In the field of health, Argentina played an active role in developing containment policies, strengthening infrastructure, and setting scientific and research policies in place. In the economic field, the government launched an Emergency Family Income and Emergency Assistance for Work and Production Fund, and prohibited lay-offs, evictions and cuts in public services.[2]

The mandatory isolation period was prolonged in Argentina, catalysing the need to be online, especially for education and work. This motivated a series of policies and regulatory measures to meet the demands for access to technology and connectivity. These measures highlighted actual conditions of access in a context in which numerous aspects of daily life are dependent on having a telephone or a computer and an internet connection.

These are some percentages that show the increase in internet access over the past two years:

- In March 2020, fixed internet penetration was 63 per 100 people, with 108% in the City of Buenos Aires (meaning there are more connections than homes). Nine provinces in the country were below 50% penetration.[3]
- At the end of 2020, Argentina reached a year-on-year variation of 8.9%. Over the previous five years this had been an average of 2.8% per year.
- The increase in internet consumption was 50% from December 2019 to December 2020. From April 2020 to May 2020 alone it was 10%.
- In the first half of 2021, only 14 out of 100 households had an internet connection through fibre-optic cables. In Uruguay this figure exceeded 78%, in Brazil 56% and Chile 49%. However, in the last quarter of 2021, official statistics indicate that 65% of households have access to computers, with 40% using them.[4]

These numbers evidence a context of growing internet access, with large variations in relation to geography, the type of devices with which the internet is accessed, and the quality of connectivity. The problems that threaten access are the lack of equipment available in homes, the availability of services,

1 Decreto 297/2020. https://www.boletinoficial.gob.ar/detalleAviso/primera/227042/20200320

2 https://www.argentina.gob.ar/economia/medidas-economicas-COVID19

3 Cámara Argentina de Internet. (2021, 10 June). CABASE Internet Index. Segundo semestre de 2020. https://www.cabase.org.ar/el-32-de-los-hogares-de-argentina-hoy-no-cuenta-con-conectividad-fija-a-internet

4 Instituto Nacional de Estadística y Censos. (2022). *Accesos a internet. Cuarto trimestre de 2021.* https://www.indec.gob.ar/uploads/informesdeprensa/internet_03_22F82A81E9B8.pdf

and the costs of a monopolised and concentrated market.

On 21 August 2020, the national government issued Decree 690[5] which refers to "ICT services and access to telecommunications networks as essential public services." The telecoms regulator, ENACOM, established minimum benefits and costs for each service and a prohibition on rates increases, among other policies. However, in June 2021, the courts repealed the decree at the request of the economic groups that monopolise the internet, telephony and TV markets, who argued that these regulations would produce "irreparable damage to the economy of the companies."[6]

In the educational field, several policies addressed access. The government responded to the request for educational content from ministerial portals under zero-rating policies. At the same time, the Ministry of Education developed a programme called "Seguimos Educando" ("We Continue Educating")[7] with content for television, radio, and digital and paper booklets, which were distributed throughout the country. This programme was nevertheless criticised for being inaccessible to the most excluded sectors. In popular[8] territories there were social initiatives to support education, mediated by ICTs, such as broadcasting lessons on community radio or using community networks.[9]

In relation to access to devices, with the help of organisations, schools promoted the repair of equipment used in Conectar Igualdad, a programme for distributing netbooks to schools that had ended.[10] In 2021, the government also launched a new equipment distribution programme called Juana Manso. However organisations criticised the involvement of Microsoft in the new programme, given that Conectar Igualdad had been explicitly committed to free software.[11]

5 Decreto 690/2020. http://servicios.infoleg.gob.ar/infolegInternet/anexos/340000-344999/341372/norma.htm

6 Moreno, A. (2021, 14 August). Argentina en disputa por servicios esenciales. *Radio Gráfica*. https://radiografica.org.ar/2021/08/14/argentina-en-disputa-por-servicios-esenciales-2

7 https://www.educ.ar/recursos/151358/serie-seguimos-educando-cuadernos-para-estudiantes

8 The word "popular" as used in this report refers to communities that lack basic services but also have a certain level of organisation. They could also be referred to as "precarious" or "poor" communities, but "popular" connotes a level of organisation, and a local culture.

9 Ciarniello, M. C. (2020, 12 May). Educación popular para el cambio social. *EnREDando*. https://www.enredando.org.ar/2020/05/12/un-medio-esencial

10 Stoianovich, M. (2021, 10 April). Recuperar y reparar igualdad. *EnREDando*. https://www.enredando.org.ar/2021/04/10/recuperar-y-reparar-igualdad

11 García Alfaro, J. (2022, 22 January). La mano invisible de Microsoft. *Redacción Rosario*. https://redaccionrosario.com/2022/01/22/la-mano-invisible-de-microsoft

Expanding rights and improving policies

Access and the social appropriation of technologies

The lack of access to connectivity, most evident in the pandemic, affects geographically and socially marginalised communities in particular. To address these inequalities, ENACOM developed two public policies:

- The "Connectivity Programme for Popular Neighbourhoods"[12] was created in September 2020 with the aim of promoting access to networks for the inhabitants of settlements registered in the National Registry of Popular Neighbourhoods in the Process of Urban Integration (RENABAP). Since 2017, RENABAP has been used to inform public policies, and now connectivity had been added to its focus areas.
- The "Roberto Arias Programme",[13] launched in June 2021, was aimed at meeting the connectivity needs of rural and Indigenous communities, and promoted self-management through community networks. The programme was named in homage to an icon of community communication.

ENACOM enabled "non-refundable contributions" (or funding) for these programmes, using resources from the Universal Service Trust Fund, which financed connectivity projects, if approved, in their entirety. Before that, ENACOM framed community networks as "those composed of infrastructure managed by their own users or by non-profit entities in populations of no more than 5,000 inhabitants".[14] These programmes expand the framework that regulates community networks in the country.

Both policies are recognised as being created through dialogue between ENACOM, universities and civil society organisations that had already been providing access to marginalised communities.

The community networks movement in Argentina has developed tools and methodologies for expanding community networks, such as the production of the LibreRouter[15] and the development of community training methodologies – efforts that have made some community networks in the country worldwide pioneers. The organisation AlterMundi is a good example. It promoted the Roberto Arias Programme, supporting organisations and sharing community

12 https://www.enacom.gob.ar/programa-barrios-populares_p4615#contenedorSite

13 https://www.enacom.gob.ar/redes-comunitarias-roberto-arias_p5049

14 Resolución 4958/2018. http://servicios.infoleg.gob.ar/infolegInternet/anexos/310000-314999/313590/norma.htm

15 https://librerouter.org

network experiences during the pandemic.[16] A member of AlterMundi, Jessica Giudice, pointed out that during the pandemic, "people continued to have a strong need for connectivity, and because of the fact that the state took too long to provide efficient and long-lasting options, the Popular Neighbourhoods and Roberto Arias Programmes were born."

Other organisations develop initiatives in this field, like the Popular Communication Roundtable of Salta and Jujuy, in the north of the country, and an organisation called Atalaya, which worked in precarious neighbourhoods, known as "villas", in Buenos Aires, in the areas of education and the social appropriation of the technologies, and also ran a community network in Villa 20. Another initiative that should be highlighted in this context is the Diploma in Social Appropriation of Technologies offered by the Faculty of Social Sciences of the National University of Buenos Aires with the participation of the Ministry of Social Development. Although the diploma was designed before the pandemic, it had its first cohort of students in 2021.

The diploma includes a module dedicated to community networks that specifically addressed the Roberto Arias Programme and its technical aspects. For Mariela Baladrón, researcher, university professor and director of the diploma, "the richness of this diploma lies in the search for the construction of collective knowledge, located and entangled between people with common interests and diverse perspectives and trajectories."

Manuela Gonzales Ursi is both a professor in the diploma programme and a member of the organisation Atalaya. She said:

> The pandemic made visible the consequences of the digital divide in access to basic rights. The isolation had a major impact in poor neighbourhoods and exposed the lack of public policies, deficiencies in infrastructure, lack of water and, of course [...] the lack of connectivity, which became essential in this context, mainly to sustain schooling. This made it possible for our demands to be reflected in public policies.

Manuela points out that the development of the ENACOM programmes is an example of this influence, and that the political will of the government to carry the programmes forward was essential. She explained:

> As a non-profit civil association, we do not have the necessary capital to make the investments in infrastructure that are required, hence the importance of having public financing programmes.

Both 2020 and 2021 saw the growth of Atalaya's community network in Buenos Aires. According to Manuela:

> The urgency was that families needed to count on the service. With a contribution from the Ministry of Productive Development, the organisation was able to scale up the network to 650 homes. The discussion regarding the internet as an essential service also revalued our experiences in developing community connectivity. Clearly, the judgment against the decree [preventing an increase in internet service fees] shows that the correlation of forces continues to be unfavourable.

Regarding the ENACOM programmes, Manuela points out that "although there are elements of the programmes that should be modified, they meant a great advance for the extension of community networks," which she defines as "fundamental actors in the universalisation of technological appropriation of communities." To sustain and extend them, she said, "it is essential that there are market regulation policies."[17]

Freedom of expression and access to information

The COVID-19 "infodemic" also spread in Argentina. To mitigate it, the state news agency Télam launched an information-checking platform called Confiar ("Trust") to deal with false information about the coronavirus. The government also made agreements with search engines and social networks to rank official information on their platforms.

On 8 April 2020, the Minister of Security announced that it was carrying out "cyber patrolling" of information publicly available on social networks to monitor "social humour".[18] Experts from local and international organisations pointed out that this action "violates the presumption of innocence, breaks

16 Muller, A. (2021, 17 June). Programa Roberto Arias. Una puerta que abre la conectividad comunitaria en la Argentina. *AlterMundi*. https://altermundi.net/2021/06/17/programa-roberto-arias

17 Baladrón, M. (2021). Fondos del Servicio Universal para redes comunitarias urbanas y rurales. Los programas Barrios Populares y Roberto Arias en Argentina. In Instituto de Estudios de América Latina y el Caribe, *V Jornadas Internacionales de Estudios de América Latina y el Caribe. Escenario regional de ofensiva capitalista y rebeliones populares*. http://iealc.sociales.uba.ar/wp-content/uploads/sites/57/2022/04/JORNADAS-IEALC-2021.pdf; Baladrón, M. (2021). Universal Service Funds for Urban and Rural Community Networks: The Barrios Populares and Roberto Arias Programs in Argentina. In L. Belli & S. Hadzic, S. (Eds.), *Community Networks: Towards sustainable funding models.* FGV Direito Rio. ttps://www.intgovforum.org/en/filedepot_download/92/20438

18 Página/12. (2020, 18 April). El "ciberpatrullaje" en la mira de los organismos. *Página/12*. https://www.pagina12.com.ar/260497-el-ciberpatrullaje-en-la-mira-de-los-organismos

the expectation of privacy and turns the security forces into observers of public discourse," in this way "attacking freedom of expression, promoting self-censorship, and reducing citizen participation."

A report that compares measures taken in Argentina, Brazil and Mexico[19] says that fact-checking initiatives, together with the measures adopted by social media platforms to reduce the massive spread of misinformation and disinformation, contributed to the public being able to access reliable information about COVID-19, and are therefore progressive in terms of human rights. On the other hand, the measures to promote self-censorship and the "excessive" use of artificial intelligence for the moderation of content by platforms at a global level are regressive in terms of rights.

Personal data and rights

The Argentine government created the Cuidar ("Care") application to regulate the movement of people during isolation measures, and to guarantee access to health, including diagnosis and vaccination. Cuidar advises on symptoms, provides assistance and recommendations, and is linked to the certificates people need to circulate in public. In the current stage of the pandemic, the application is used to issue vaccination certificates, which also enable people to circulate in public spaces. Another application that was extensively used during the pandemic is MI Argentina, which was launched as a "citizen digital profile" – an identification system linked to a citizen management portal.

Before the pandemic, there were questions regarding the implementation of biometric identification systems and access to social security information for political use. These included the dangers associated with the use of artificial intelligence in facial recognition technologies (in the subway in Buenos Aires, for example) and the use of social data in the application of social policies (as exposed in the province of Salta in which a birth control plan stigmatised young women through social profiling). This challenge became more visible in the context of the health crisis.

The government recognised that "given the sensitivity of the data on the Cuidar system and the recommendations of the WHO [World Health Organization] and PAHO [Pan American Health Organization], the platforms were improved with contributions made by the health sector, the scientific field, civil society organisations, human rights organisations and experts in information technology." These contributions had implications in terms of the mandatory use of the platforms, data proportionality, privacy, identification, geolocation, transparency of the source code and data processing at the end of the pandemic.[20]

More recently, a group of internet rights organisations released an open letter to the executive and legislative branches of government, addressing them on the dangers related to the violation of personal data and the risks associated with personal data.[21] The open letter mentioned a series of worrying aspects such as cases where sensitive information was leaked, the lack of direction in the law enforcement authority, and the judicial persecution of those who had reported vulnerabilities in some computer systems. The Personal Data Protection Law in Argentina was pioneering when it was created in 2000, but, as the letter pointed out, that was "before the internet became a massive tool for large-scale data processing." Currently it is considered one of the most outdated in the region.

"What happened to our data in 2020 is an abrupt acceleration of a process that turns people's daily lives more and more towards digitisation," Beatriz Busaniche, from the Vía Libre Foundation, noted.[22] "Many situations that in other contexts would have raised a reaction [...] in this context became a strategy for dealing with a critical situation."

Beatriz said that epidemiological surveillance is a necessity in any pandemic. However, she noted:

> The big difference is that, in this pandemic, there are a series of technological devices that enable [surveillance] in a much more invasive and efficient way. That is where this tension between epidemiological surveillance, public health measures and the momentary suspension of certain rights comes into play.

Conclusion

In the current context of the health crisis, technologies were resorted to for connectivity, for sustaining the online contact that isolation demanded, and also

19 Bizberge, A., & Segura, M. S. (2020). Los derechos digitales durante la pandemia COVID-19 en Argentina, Brasil y México. *Revista de Comunicación, 19*(2), 61-85. https://revistadecomunicacion.com/article/view/1939/1583

20 Portal Argentina. (2020, 19 September). Cuidar: cuidado y transparencia de un trabajo en sociedad. https://www.argentina.gob.ar/noticias/cuidar-cuidado-y-transparencia-de-un-trabajo-en-sociedad

21 Access Now, et al. (2022, 28 January). Organizaciones de la sociedad civil solicitan la suspensión del desarrollo e implementación de tecnologías de procesamiento masivo de datos personales en Argentina. *Access Now*. https://www.accessnow.org/solicitud-suspension-tecnologias-procesamiento-masivo-datos-personales-argentina

22 Martínez, C. R. (2021, 14 January). Beatriz Busaniche, activista digital: "Lo que pasó con nuestros datos en 2020 es casi una masacre". *elDiarioAR*. https://www.eldiarioar.com/sociedad/beatriz-busaniche-activista-digital-paso-datos-masacre_128_6747272.html

for control. The latter was promoted mainly through health policies, and affected rights, but was necessary for the epidemiological surveillance required to address the pandemic, even though the extent of their impact on rights needs to be debated.

The actions that took place during the pandemic highlight the importance of the participation of civil society organisations that work not only on the realisation of rights associated with access, but guarantee that the use of technologies is carried out in a way that respects rights. They are necessary to help point out when policies may result in the violation of rights in ways that may not be immediately obvious.

In the case of Argentina, the participation of civil society is evident with the policies promoting internet access. Organisations pointed out the lack of access in communities and the concentration of the market that results in unattainable prices for large sectors of the population. Both the decree and the ENACOM programmes responded not only to the experience and input of these organisations, but also created a situation where the organisations will continue to monitor the programmes. The Roberto Arias Programme was a result of the tenacity of social organisations committed to expanding internet access in communities, while questioning the prevailing model of access. It creates a model that respects and responds to the needs of communities. The advocacy work of these organisations managed to define and promote community networks and at the same time consolidate and articulate the need for community access with other actors. The pandemic, which made this need more visible and essential, found Argentina with a government that listened, and with a regulatory authority willing to address the challenge.

The development of government platforms – some implemented for the pandemic, others earlier, but whose use was extended in this context – also had the watchful eye of the organisations who kept a check on the violations of rights that can occur when these technologies are used. The perspectives of these organisations not only influenced the government and public sphere, but also the academic and technical fields.

Although the group of organisations engaged in internet rights is heterogeneous, it is consolidated and includes different successful advocacy experiences. Working together, they managed to make their demands heard, influence the promotion of public policies, and improve existing ones.

In these contexts in which measures are urgent, the urgency leaves fertile ground for hasty decisions without a proper consideration of rights. Even regressive proposals that respond to the specific interest of institutions or business can be created. But they are also contexts in which collective work that draws on the accumulated experience of different actors can respond to fresh opportunities.

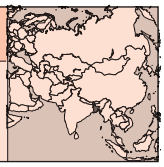
Action steps

The following steps are necessary in Argentina:

- Create awareness of the impact of the violation of rights that technology implies and strengthen awareness of the dangers and possible solutions to this problem.
- Strengthen mechanisms that assess rights in the implementation of policies, involving people who have the technical, social and rights knowledge to do so.
- Demand regulatory measures that encourage equal access for all, taking into account the fact that various actors offering access in the private sector are reluctant to modify their business models to achieve this.
- Demand transparency from the government and from the private sector in the development and implementation of technologies that involve the processing of personal data.
- Create awareness campaigns so that citizens understand how data collection works and can then use software, applications and platforms in an informed way.

BANGLADESH

A "LEARNING LOSS": ONLINE EDUCATION DURING THE PANDEMIC IN BANGLADESH



Bytesforall Bangladesh
Partha Sarker and Munir Hasan
http://www.bytesforall.org

Introduction

Although the right to education is not a fundamental right contained in the Bangladeshi constitution,[1] Article 17 of the constitution states clearly that the state shall adopt effective measures for the purpose of:

- Establishing a uniform, mass-oriented and universal system of education and extending free and compulsory education to all children to such a stage as may be determined by law.
- Relating education to the needs of society and producing properly trained and motivated citizens to serve those needs.
- Removing illiteracy within such time as may be determined by law.

The government provides elementary education free of charge in public schools, available to all at the age of six. Secondary education is not totally free; students still have to pay tuition fees, but usually receive stipends and subsidies to cover different costs.

With the onset of the COVID-19 pandemic, the government decided to close all educational institutions including primary and secondary schools for all in-person classes starting from 18 March 2020. After nearly 18 months of closure, the schools first partially opened on 11 September 2021. But the schools closed again until they fully re-opened on 1 March 2022. More than 36 million students (including 17 million in primary education) and one million teachers could not attend 120,000 primary and secondary schools during that period of time.[2] UNESCO suggests that it was one of the most restrictive school closures in the world.[3]

The government did put alternative education streams in place. It ran online classes via Facebook Live, Zoom and the Ministry of Education website.[4] A YouTube channel – Amar Ghore, Amar School[5] (My School is at My Home) – was also developed, and "Parliament TV" and radio were used to air recorded classes for students through an initiative called Ghore Boshe Shikhi (Let's Learn at Home).

However, the school closure and long absence of in-person classes changed the entire landscape of learning in Bangladesh. The new phenomenon of online classes introduced the old debate of the digital divide and connectivity gap. Existing inequalities in terms of access to information and communications technology (ICT) infrastructure, connectivity, content and opportunities exposed the impossibility of learning outcomes for many poorer communities in the country. The digital divide translated into a learning divide.

Context

Bangladesh is a success story in terms of providing access to primary and secondary level education, particularly for female students. The country's net enrolment rate at the primary school level increased from 80% in 2000 to 98% in 2015,[6] and 120% in 2020.[7] This rate can exceed 100% due to the inclusion of over-aged and under-aged students because of early or late school entrance and grade repetition. Secondary school net enrolment was around 74% in 2020,[8] up from 54% in 2015 and 45% in 2000.[9] These are all pre-pandemic figures – but with the pandemic the situation changed a lot.

As the schools went online, access to the internet, computers and electricity became all too real a question. Some pre-pandemic data on accessibility and

1 http://bdlaws.minlaw.gov.bd/act-367.html

2 Uddin, M. (2020, 13 June). Effects of the pandemic on the education sector in Bangladesh. *The Financial Express*. https://www.thefinancialexpress.com.bd/views/effects-of-the-pandemic-on-the-education-sector-in-bangladesh-1592061447; see also: https://a2i.gov.bd/publication/teachers-portal

3 https://covid19.uis.unesco.org/global-monitoring-school-closures-covid19/country-dashboard

4 http://digitalcontent.ictd.gov.bd/index.php/site/index

5 https://www.youtube.com/watch?v=ly88k5t6Wjw&list=PLoijsUvO6bOXsEkuj8EH-wniEHomrd6Ps

6 World Bank. (2016, 13 October). Ensuring Education for All Bangladeshis. https://www.worldbank.org/en/results/2016/10/07/ensuring-education-for-all-bangladeshis

7 http://uis.unesco.org/en/country/bd

8 Ibid.

9 Arribas Layton, L., et al. (2021, 8 July). How to provide opportunities for all? From girls' education to women's labor force participation in Bangladesh. *World Bank Blogs*. https://blogs.worldbank.org/education/how-provide-opportunities-all-girls-education-womens-labor-force-participation-bangladesh

connectivity will probably be helpful in this regard. A 2019 survey[10] from the Bangladesh Bureau of Statistics (BBS) suggests that only 37.6% of households in the country have access to the internet. This data also has a socioeconomic perspective. According to the BBS, only 8.7% of the poorest 20% of households in Bangladesh have internet access at home, compared with 75.3% of the richest 20% of households. The same report also found that only 5.6% of households in Bangladesh have a computer.[11]

Online education requires uninterrupted high-speed internet or broadband connection. In Bangladesh, the average internet speed is 5 Mbps, which is one of the lowest in South Asia.[12] In many rural households there is only one mobile phone, which the families were unable to dedicate to children's remote learning or online education. Television is an important tool for remote learning. However, the same BBS report[13] suggests that nationally, only 51% of households own televisions. Out of that, only 4.8% of the poorest 20% of households have a television compared to 90.2% of the richest 20% of households.

To reflect the constitutional guarantee at all levels of education, Bangladesh formulated its National Education Policy in 2010.[14] The primary objectives of this policy are directed toward the cultivation of human values and seeking ways through which citizens can be groomed to become leaders in pro-people development programmes and other initiatives geared towards the progress of the society. The education policy also attached importance to ICTs along with STEM (science, technology, engineering and maths) to build up "digital Bangladesh" and a knowledge-based society.

The Ministry of Education (MoE) in Bangladesh first thought and strategised about using ICTs in education in 2012 through the Master Plan for Information and Communication Technology in Education (2012-2021).[15] The plan was expected to result in education for all, an improvement in the standard of education, a skilled workforce, and the eradication of the digital divide and discrimination. One of the objectives of the use of ICTs in education was to make education services accessible "at the doorsteps" of people – an objective which was tested during the pandemic.

A review on the implementation of the Master Plan in 2019[16] (prior to the pandemic) shows that some progress had been made in enhancing the teaching and learning environment by using ICTs in classrooms (the aim was one laptop and one projector per classroom) and getting teachers to co-create and share digital content via the teachers' portal managed by the Ministry of Education.[17] But as the review suggests, many schools were still lagging in acquiring devices and connectivity. In semi-urban and rural areas in particular, learners and teachers were still facing significant challenges due to limited infrastructure, and when ICT facilities existed, inadequate internet connectivity meant they could not be properly used.

This baseline information was important to understand the context of education when the pandemic hit hard in Bangladesh and the schools were closed. During the pandemic, the MoE's teachers' portal had to be repurposed. Teachers were encouraged to be "ICT for education ambassadors" and to initiate and facilitate online classes, collaborating on and co-creating content. More than 100,000 classes have been added to the teachers' portal for online delivery.[18]

Inequalities in the time of the school closure

The pandemic-related lockdown probably had the toughest impact in the education sector of Bangladesh. When the primary and secondary schools were first closed for in-person classes, millions of students and parents were clueless about their next course of action. Eventually, the schools were closed for such a long time that Sheldon Yett, the UNICEF representative to Bangladesh, emphasised that "schools should be among the last institutions to close, and among the first to reopen, as we put in measures to tackle infection waves."[19]

This long closure coupled with a lack of access to internet connectivity not only created a learning divide, but also a learning loss. For example, in three rounds of COVID-19 follow-up surveys, studies by

10 Bangladesh Bureau of Statistics. (2019). *Bangladesh Multiple Indicator Cluster Survey 2019: Key Findings*. http://bbs.portal.gov.bd/sites/default/files/files/bbs.portal.gov.bd/page/b343a8b4_956b_45ca_872f_4cf9b2f1a6e0/37817b8e25d0d6c1f442e294921ff85e.pdf

11 Uddin, M. (2020, 13 June). Op. cit.

12 Prothom Alo. (2018, 24 April). Internet speed is slowest in Bangladesh. *Prothom Alo*. https://en.prothomalo.com/science-technology/Internet-speed-is-slowest-in-Bangladesh

13 Bangladesh Bureau of Statistics. (2019). Op. cit.

14 https://reliefweb.int/report/bangladesh/national-education-policy-2010-enbn

15 https://planipolis.iiep.unesco.org/sites/default/files/ressources/bangladesh_master_plan_ict.pdf

16 Ministry of Education. (2019). *Master Plan for ICT in Education in Bangladesh (2012-2021): Progress Review Report 2019*. https://unesdoc.unesco.org/ark:/48223/pf0000372984/PDF/372984eng.pdf.multi

17 http://www.teachers.gov.bd

18 Ibid.

19 UNICEF Bangladesh. (2022, 24 January). COVID-19: Scale of education loss 'nearly insurmountable', warns UNICEF. https://www.unicef.org/bangladesh/en/press-releases/covid-19-scale-education-loss-nearly-insurmountable-warns-unicef

the Population Council[20] suggested that one third of girls or less (21%, 16% and 34% in round 1, round 2 and round 3, respectively) followed televised classes. Time spent studying declined drastically: while pre-pandemic average study time was seven to eight hours per day, this declined to two hours per day during COVID-19-related school closures.

Numeracy and literacy scores have declined significantly. The World Bank identifies this learning loss as learning poverty, which is defined as a lack of ability to read and understand a simple story at 10 years of age. Prior to the pandemic, this learning poverty was 56% in Bangladesh, but after the long school closure and non-functional and poorly designed remote learning, this rate may have gone up to 70%.[21]

Another World Bank study[22] shows that the disruptions have already led to a decline in student learning and retention. Bangladesh's learning adjusted years of schooling (LAYS) are expected to fall from 6.0 years in 2019 to 5.3 years in 2021,[23] costing the Bangladesh economy between USD 67 billion and USD 114 billion in GDP (based on January 2021 estimates).

In May 2020, the MoE prepared a COVID-19 Response and Recovery Plan[24] for primary and secondary education, which also identified learning loss, inequality of learning, an increase in dropout rates, etc. as some of the possible consequences of a long school closure. The report took into cognisance that only 44% of 5-11-year-old children in rural areas and 6% of children belonging to the poorest wealth quintile have a television at home. Similarly, only 3% of rural 5-11-year-old children and close to 0% in the poorest wealth quintile have a computer at home. Regarding the internet, only 30% of 5-11-year-olds in rural areas have internet access and just 7% in the poorest wealth quintile – generally, through mobile phones.

Another study conducted by the BRAC Institute of Governance and Development at the beginning of the pandemic (June 2020) showed that "the study time at home actually went down from usual during the school closure. This means the learning loss has been greater than what it should be because of the school closure."[25] It also showed that only 25% of rural children with access to the television followed the classes. Use of the internet in learning was almost non-existent among the students surveyed.

The long interruption of in-person classes in the schools and the delivery of education through online means had some other serious socioeconomic consequences.

Many child rights advocates opined that tens of thousands of students across the country did not return to classes after the schools were reopened.[26] The majority, they say, are boys ages 12 and above, who during the interim were pushed into full-time work. This was also echoed by Tomoo Hozumi, UNICEF representative in Bangladesh, who stated in 2021: "With school closures in place since March 2020 and poverty levels rising amidst the pandemic, UNICEF is concerned that growing numbers of children are being pushed into child labour."[27] This is happening because household incomes across the country plunged by an average of 23% during the first 18 months of the pandemic and families were using all means possible to survive.[28]

This same reason also forced many families to arrange early marriage for their girl children, who otherwise could be going to school. One survey[29] conducted by the non-profit Manusher Jonno Foundation recorded almost 14,000 underage marriages across one-third of the country during the first six months of lockdown, with half of the girls aged 13 to 15.

In pre-pandemic times, in the 104 most poverty-prone areas in Bangladesh, the government with assistance from the World Food Programme (WFP) used to run different school feeding programmes to reach nearly three million children.[30] With the closure of the schools, the feeding programme also stopped, creating a further risk of poverty,

20 Amin, S., Hossain, M. I., & Ainul, S. (2021). *Learning Loss Among Adolescent Girls During the COVID-19 Pandemic in Rural Bangladesh.* Population Council. https://www.popcouncil.org/uploads/pdfs/2021SBSR_LearningLossBangladesh.pdf

21 Ahmed, M. (2022, 13 February). Learning loss from Covid-19: Can a generational threat be averted? *The Daily Star*. https://www.thedailystar.net/recovering-covid-reinventing-our-future/blueprint-brighter-tomorrow/news/learning-loss-covid-19-2960811

22 World Bank. (2021, 18 April). Keeping Bangladesh's Students Learning During the COVID-19 Pandemic. https://www.worldbank.org/en/results/2021/04/18/keeping-bangladesh-s-students-learning-during-the-covid-19-pandemic

23 Ibid.

24 Ministry of Primary and Mass Education. (2020). *COVID-19 Response and Recovery Plan: Education Sector.* https://planipolis.iiep.unesco.org/sites/default/files/ressources/bangladesh_moe_covid_19_response_and_recovery_plan.pdf

25 BRAC Institute of Governance and Development. (2020). *Coronavirus Outbreak, Schooling and Learning: Study on Secondary School Students in Bangladesh*. https://bigd.bracu.ac.bd/study/coronavirus-outbreak-schooling-and-learning-study-on-secondary-school-students-in-bangladesh

26 Redfern, C., & Ahsan, A. (2022, 26 April). Tens of Thousands of Boys in Bangladesh Were Forced into Work During the Pandemic. Now School Is Resuming Without Them. *TIME*. https://time.com/6170432/bangladesh-child-labor-pandemic/

27 UNICEF Bangladesh. (2021, 11 June). Child labour rises to 160 million – first increase in two decades. https://www.unicef.org/bangladesh/en/press-releases/child-labour-rises-160-million-first-increase-two-decades

28 BRAC Institute of Governance and Development. (2022). *PPRC-BIGD COVID-19 Livelihoods & Recovery Panel Survey*. https://bigd.bracu.ac.bd/study/rapid-survey-on-immediate-economic-vulnerabilities-created-by-covid-19-and-the-coping-mechanisms-of-poor-and-marginal-people/

29 Redfern, C., & Ahsan, A. (2022, 26 April). Op. cit.

30 Uddin, M. (2020, 13 June). Op. cit.

malnutrition and illness. Although the WFP later found a way around this by creating a take-home food rationing programme, not all children were covered or reached through this programme.

Conclusion

Despite the fact that online education due to the school closure created a learning divide, and had other socioeconomic consequences in Bangladesh, the hybrid model of education (i.e. a mix of online and offline education) is here to stay. The fact that Bangladesh could not ensure access to many rural and remote families does not mean that the idea of online education is to blame. However, Bangladesh was less prepared in terms of its delivery of infrastructure than it should have been.

The Master Plan for ICT in Education[31] developed by the MoE has identified issues related to digital content development, introducing ICTs as a subject or topic in education, and the development of teaching-learning materials, but talks less about delivery mechanisms. Most of the infrastructure was centred around schools or teacher training institutes. Many schools have multimedia classrooms, and teachers could collaborate on, prepare and share digital content using the teachers' portal. But for a disaster like the lockdown, what was required was individual access to affordable devices and connectivity.

The National Broadband Policy 2009,[32] updated in 2018, had a vision to connect all areas with high-speed broadband internet and provide broadband for all with affordable internet and devices. The pandemic has however exposed the reality of the access divide and the importance of the internet in the case of learning and education. Any new tariff structure for broadband should therefore keep in mind the needs and affordability of these tariffs for students.

In the context of Bangladesh, schools are not merely education institutes – they are local-level establishments that make broader socioeconomic contributions. The fact that school closure led to an increased drop-out rate, child labour, child marriage, malnutrition, etc. proves that the individual level of access to social services needs to be enhanced as much as access to education.

Action steps

Civil society in Bangladesh still does not have a total picture of the learning loss and possible long-term impact of online education due to the school closures. Research needs to be done by collating and reviewing disparate research pieces on the topic, by interviewing relevant stakeholders, and conducting a survey with the students and teachers directly affected by the closures.

Civil society also needs to see what policy interventions can be brought to address the needs of broadband connectivity, digital content, learning resources, and capacity building, among others. Policy advocacy could involve a campaign built on evidence-based research, including collecting best practices from other countries.

Policy options should explore the potential of broadband service providers and mobile phone companies creating separate tariff layers for students and for educational purposes, as well as the potential of government support or subsidies in this regard.

31 Ministry of Education. (2019). Op. cit.

32 http://old.btrc.gov.bd/national-broadband-policy

BENIN

FROM E-SERVICES TO E-DEMOCRACY: STRENGTHENING PUBLIC PARTICIPATION AND RIGHTS IN BENIN

Sênoudé Pacôme Tomètissi
tometissi@gmail.com

Introduction

In 2020, instead of lockdowns, Benin opted for sanitary cordons around the regions affected by the virus, allowing the free movement of people within the restricted area. This was done alongside measures such as promoting hygiene, social distancing, and the shutting down of non-essential services. Despite this "softer" approach to containing the virus, the measures nevertheless appeared to increase the use and reach of the internet during the first years of the pandemic.

While the number of internet and social media users increased between 2020 and 2021 – the latter almost doubling – there were also indications that the government's online public services were more widely used.

The government's flagship projects on e-governance, e-education and e-commerce, initiated before the coronavirus pandemic, were instrumental in making these public services available. By 2020 an impressive number of online services were already offered by the government,[1] in particular through its online administration project called Smart Gouv.

With evidence of the success of these services during the early stages of the pandemic, one of the key policy questions for decision makers now is how to capitalise on their use as a basis for the consolidation of democracy. This not only through finding shortcuts to reducing inequalities by providing access to technology and enabling the right to information, but also by encouraging popular participation in the formulation of public policies and developing mobilisation strategies around electoral processes. In the wake of the successful organisation of an e-voting process to elect trade union representation in January 2021, the potential for wide-reaching changes feels stronger now than it has ever before.

The political will and the necessary mobilisation of resources to design and implement, as far as possible, a system of direct democracy online, while institutionalising e-voting in parallel,[2] would be an invaluable opportunity for the country to meet its human rights targets, while keeping pace with the rapid technological changes taking place across the world.

The state of democracy in Benin

The Republic of Benin (formerly the Republic of Dahomey) gained international sovereignty on 1 August 1960. From 1960 to 1989, the country experienced a turbulent constitutional and political evolution. Following a deep economic and socio-political crisis, the country organised a national conference to define a new type of government. The *Conference des Forces Vives de la Nation* ran from 19 to 28 February 1990, opening a new era of political liberalism.[3] Political leaders participated in the conference, paving the way for democratic elections and political change not only in Benin, but also in most other countries in Sub-Saharan Africa.[4]

Afrobarometer, a pan-African non-partisan research network on democracy, governance and related issues in Africa, noted that almost three-fourths of people in Benin prefer democracy to other types of governments.[5] However, Benin's democracy remains on shaky ground.

While from 1990 to 2021 Benin held seven presidential and eight legislative elections in addition to a referendum in 1990, in 2019 violence erupted in the country, particularly during the legislative election process in which the opposition was not able

1 See, for example: https://www.service-public.bj and https://numerique.gouv.bj/reformes/les-projets#

2 ''Päivärinta, T., & Sæbø, Ø. (2006). Models of E-Democracy. *Communications of the Association for Information Systems*, *17*. https://doi.org/10.17705/1CAIS.01737; Freeman, J., & Quirke, S. (2013). Understanding E-Democracy Government-Led Initiatives for Democratic Reform. *JeDEM - EJournal of EDemocracy and Open Government, 5*(2), 141-154. https://doi.org/10.29379/jedem.v5i2.221; Blumler, J. G., & Coleman, S. (2001). *Realising Democracy Online: A Civic Commons in Cyberspace*. IPPR/Citizens Online. http://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/3240/blumler.pdf

3 Heilbrunn, J. R. (1993). Social Origins of National Conferences in Benin and Togo. *The Journal of Modern African Studies, 31*(2), 277-299. https://www.academia.edu/7503344/Social_Origins_of_National_Conferences_in_Benin_and_Togo?from=cover_page

4 Amuwo, K. (2003). The State and the Politics of Democratic Consolidation in Benin 1990-1999. In J. O. Ihonvbere & J. M. Mbaku (Eds.), *Political Liberalizations and Democratization in Africa. Lessons from Country Experiences.* Praeger.

5 Scheller, C., & Lazar, M. (2019). *Is Benin's democracy living up to its reputation?* Afrobarometer. https://www.afrobarometer.org/sites/default/files/publications/Dispatches/ab_r7_dispatchno321_is_benins_democracy_living_up_to_its_reputation.pdf

to take part due to new electoral rules. There was also political unrest in 2021 during the presidential election process and several politicians close to the opposition were arrested.

In March 2020, in its concluding observations on Benin's third periodic report, the UN's Committee on Economic, Social and Cultural Rights highlighted that one of the strategic axes of the government's action programme for 2016-2021 aimed to strengthen fundamental social services and social protection. However, the Committee also recommended that Benin review the legal provisions relating to gatherings and the dissemination of false information in order to allow human rights defenders to work freely and without fear.

In this context, voter turnout appears to be dwindling. Turnout in the legislative elections in 2019 was only 27.1% compared to 65.9% in 2015,[6] while 50.17% of voters cast their ballot for the presidential elections in 2021, compared to 66.13% in 2016.[7]

Beyond e-government: Using ICT projects to consolidate democracy

The fast-tracking of e-government projects like Smart Gouv during the first year of the COVID-19 pandemic has created the necessary momentum to capitalise on the potential of strengthening a participatory democracy in Benin through institutionalising online democratic participation. There are several levers to this that need to be supported by civil society. These include: the promotion of affordable and meaningful internet access; the ongoing provision of government services and access to information online, particularly with the view of strengthening transparency and accountability; the strengthening of the independence of a free and fair media, especially online; the practical application of e-voting to motivate an interest in democratic participation, especially among the youth, while also aiming at increasing voter turnout; and advocacy campaigns that encourage the government to not resort to internet shutdowns as a mechanism of control.

Affordable internet access

When it comes to internet affordability, a recent UNESCO report ranks Benin among the top 10 countries of Africa.[8] However, in November 2021 during a press briefing, the NGO *La Voix des Consommateurs* asked for a reduction in the cost of internet data in Benin while denouncing the poor quality of mobile network services.[9] For mobile data, the cost of 1.5 GB is about USD 4.[10]

The number of internet users (+18%) and of social media users (+45%) increased in Benin between 2020 and 2021 while there were 10.27 million mobile connections in Benin in January 2021 (+3.8%).[11] There is, however, no known data that shows an increase in internet use due to the virus.

The provision of e-government services

Smart Gouv is one of the six flagship projects of the government's digital strategy. It aims to promote good governance and the transparent management of public resources, and was implemented from 2016 to 2021 with the support of the Estonian e-Governance Academy. Given it was only completed the year the pandemic hit,[12] its practical effectiveness had not yet been tested when it was needed the most. However, the usefulness of the project to the public became evident in the first year of the virus.

Smart Gouv gives people access to hundreds of official documents and services online, including criminal records, and facilities to pay taxes and for electricity. The benefits of the project are demonstrable, as in this example:

> To apply for a position in the civil service, Delali[13] needed to get her criminal record, one of the documents required in the application process. As she was born in Malanville in the north of Benin, Delali, who now lives in Cotonou, had to travel to Malanville, 732 km away, to get her criminal record. Like her, each of the 63,700 candidates whose applications were accepted and who competed in November 2017 for one of the 326 positions at the Ministry of Economy had to go and get their criminal record where they were born. And, like them, all applicants to public administration positions have to provide a criminal record. With the Smart Gouv,

6 https://www.jeuneafrique.com/770256/politique/legislatives-au-benin-un-taux-de-participation-de-27-selon-la-cour-constitutionnelle

7 https://www.jeuneafrique.com/1154144/politique/benin-patrice-talon-reelu-des-le-premier-tour-selon-la-commission-electorale

8 Kiyindou, A. (2020). *Evaluation du développement de l' Internet au Bénin: utilisation des indicateurs ROAM-X de l' universalité de l' Internet de l' UNESCO*. https://unesdoc.unesco.org/ark:/48223/pf0000374577

9 https://www.beninwebtv.com/benin-la-voix-des-consommateurs-milite-pour-la-reduction-du-cout-de-linternet

10 https://www.mtn.bj/particuliers/internet/forfaits-volumes/data-volumes

11 https://www.datareportal.com/reports/digital-2021-benin. The report states that its statistics on social media users should not be equated with unique users.

12 Lani, M. (2021). Case study: Benin and Estonia's e-government partnership. In OECD. (2021). *Development Co-operation Report 2021: Shaping a Just Digital Transformation*. https://doi.org/10.1787/37ad9025-en

13 Delali is an imagined character who is nevertheless representative of an everyday experience.

the criminal record is obtained online. This is a great relief for all candidates in all competitions for civil service positions.

From July 2020 to August 2021 – roughly the first year and a half of the pandemic – more than 100,000 criminal records were issued in this way.

Benin's digital strategy aims to create digital services platforms for accelerating growth and social inclusion in the country. By doing so, it aims to offer better access to information and knowledge, catalyse the economic development of all sectors of activity, and improve the transparency of governance and the efficiency of administration centred on the citizen. For example, the implementation of the personal identification number has facilitated access to social protection and has simplified administrative procedures.[14]

Several agencies have been created for the implementation of the digital strategy, in particular to prepare and monitor national digital policies. Among other government agencies, there is the Digital Development Agency, responsible for high-speed and very high-speed infrastructure; the Information Services and Systems Agency, which is in charge of the execution of the flagship projects including Smart Gouv, and the implementation of the national information systems master plan; and the National Agency for the Identification of Persons, which is responsible for operationalising the biometric database and storing personal identification numbers in a database.

Several other institutions help coordinate the regulation and monitoring of specific digital operations: the Regulatory Authority for Electronic Communications, the Personal Data Protection Authority, the National Agency for the Safety of Information Systems, the Central Office for Combating Cybercrimes, and the Authority for Audiovisual and Communication.

COVID-19 accelerated the implementation of dozens of electronic government services, such as applying for visas and tax clearance certificates, through this digital strategy. This is an important step towards meeting citizens' rights through providing access to information and key public services online.[15] These initiatives have also been set up to encourage transparency and fight corruption. For example, the launch of a digital platform for submitting CVs for senior positions in public expenditure in the country aims to increase the transparency in the appointment processes in public administration, allowing citizens to follow the nomination processes.[16]

Strengthening of a free media

The digital economy is a key aspect of democracy. The Digital Code in Benin provides a framework for the regulation of the digital economy with rules on cybersecurity, digital infrastructure development, and affordable internet access.[17] There are, however, several aspects that need to be improved.

For example, several local and international civil society groups and the UN Economic, Social and Cultural Rights Committee called on the government to revise its digital code to better protect human rights, especially those related to freedom of expression and surveillance.[18]

The Union of Media Professionals in Benin, the largest association of journalists in the country, organised a workshop for media professionals, lawyers and activists in August 2020 to discuss the digital code and send comments to the government and the parliament. The union has asked for an amendment to the code because of several provisions deemed restrictive to the freedom of the media and expression.[19]

On 28 April 2019, the day of the legislative elections in Benin, social networks, including messaging applications for Facebook, Twitter, WhatsApp and Telegram, were blocked. Following this there was a total internet shutdown throughout the country. Benin civil society groups and several international human rights organisations including Amnesty International, Internet Without Borders and Internet Society Benin condemned the internet shutdown and the blocking of social networks.

In April 2021, before the presidential election, a coalition of civil society organisations including Internet Society Benin launched a digital campaign to draw the attention of decision makers and other public institutions to the serious consequences of an internet shutdown on the economy and education, and specifically on the digital sector.

The Internet Governance Forum (IGF) Benin, one of the civil society organisations that carry the voice of consumers, organises annual national forums on the governance of the internet for

14 https://numerique.gouv.bj/images/DPS.pdf

15 https://www.service-public.bj

16 https://www.fichiernational.gouv.bj/#

17 https://www.afapdp.org/wp-content/uploads/2018/06/Benin-Loi-2017-20-Portant-code-du-numerique-en-Republique-du-Benin.pdf

18 Jarroux, P., & Tama, B. C. (2020). Benin. In A. K. Awedoba, B. Kamski, A. Mehler, & D. Sebudubudu (Eds.), *Africa Yearbook Volume 16*. Brill.

19 http://www.ortb.bj/infos-une/medias-lupmb-lance-la-reflexion-pour-une-relecture-du-code-du-numerique

stakeholders. The eighth edition of its forum (in 2019) was devoted to human rights, in particular digital rights and their importance in our societies. The aim was to underline the responsibilities of government authorities in providing unrestricted access to the internet for all, while supporting the formulation of public policies likely to make it more accessible, more affordable and more available in terms of digital infrastructure and data quality. The forum was also an opportunity to encourage telecommunications service providers to adopt policies that address online disinformation and misinformation or "fake news".[20]

The establishment of the Media Development Support Fund (FADEM) in accordance with article 39 of the Information and Communication Code allows the government to set up an institutional framework to support media freedom.[21] This fund is an opportunity to support online media that promote fair information and strengthen democracy and human rights. In such a context, the government's commitment to promote digital content is also an opportunity to promote citizen-led participatory documentary film-making that highlights economic, social and cultural rights.

However, this needs to happen with other changes in the media freedoms context.

Currently, although senior positions in public media are shortlisted by the Authority for Audiovisual and Communication, the public media are still under the supervision of the government and managers are nominated by the head of state during a cabinet meeting. In January 2022, the Authority of Audiovisual and Communication authorised 59 online media operators in Benin.[22] The release of the list came after the suspension in 2020 of all online media by the Authority, many of whom had been publishing without a licence.

Participatory democracy and e-voting

Beyond the protection of digital rights and the improvement of people's access to technology (including their technological capabilities), the potential exists to simultaneously develop agendas that will help shape an effective online democracy in Benin. Such an option would increase transparency, openness and people's participation in credible public processes.[23]

There are a few examples of participatory citizen initiatives in Benin. The most well-known is the Programme on Citizen Participation in Public Policy Development in Benin (PartiCiP), implemented in all 77 municipalities in the country by the NGOs Alcrer and Social Watch Benin. The programme has set up Citizen's Participation Units at the local level in order to strengthen a culture of citizen involvement in their own development, and the implementation and monitoring of public policies that take into account the aspirations of grassroots populations and organisations. PartiCiP activities include information sessions, radios programmes, village assemblies and hearings on public accountability.[24]

By taking this initiative online, through electronic platforms, social networks and mobile applications, it will become possible to establish an online democracy, in particular if digital infrastructures and the technological capabilities of vulnerable groups are ensured.

This idea is not far-fetched. On 24 January 2021, the country's electoral commission organised elections to designate the most representative trade union federations in Benin. As announced by the cabinet one month earlier, the vote was to be held electronically. All public administration workers and those in the private sector affiliated with the National Social Security Agency voted online. Connectivity points were made available to workers throughout the country in order to facilitate voting for those who did not have digital devices such as smartphones, tablets or computers.[25] Implementing an e-voting system might increase the participation of young people in the legislative and presidential elections.

20 https://fgi.bj/wp-content/uploads/2019/08/Rapport-de-la-8eme-Edition-du-Forum-pour-la-Gouvernance-d%e2%80%99internet-au-Benin-2.pdf

21 https://www.gouv.bj/actualite/786/financement-secteur-medias-benin-ministre-orounla-concerte-avec-odem-fadem

22 https://www.matinlibre.com/wp-content/uploads/2022/01/Dec-N%C2%B022-003-HAAC-du-19-janvier-2022-portant-selection-requerant.pdf; https://www.voaafrique.com/a/les-journalistes-contre-la-suspension-des-médias-en-ligne-au-bénin/5511719.html

23 Freeman, J., & Quirke, S. (2013). Op. cit.; Clift, S. (2003). *E-Democracy, E-Governance and Public Net-Work*. Publicus. Net. http://www.opensourcejahrbuch.de/download/jb2004/chapter_04/IV-5-Clift.pdf; Coleman, S., & Gøtze, J. (2001). *Bowling Together: Online Public Engagement in Policy Deliberation*. Hansard Society. https://www.academia.edu/26878057/Bowling_together_Online_public_engagement_in_policy_deliberation?from=cover_page; Chadwick, A. (2003). Bringing e-democracy back in: Why it matters for future research on e-governance. *Social Science Computer Review*, *21*(4), 443-455. https://www.dhi.ac.uk/san/waysofbeing/data/citizenship-robson-chadwick-2003a.pdf; Djengue, S. (2021). Enjeux et opportunités de la révolution du numérique : comment rattraper sans coup férir le retard au Benin? In A. Schott & L. Vieira (Eds.), *Territoires intelligents et sociétés apprenantes : XVe Conférence Internationale EUTIC Dakar*. http://www.conference-eutic.org/wp-content/uploads/2021/11/Actes-2019-Eutic-A1-A3.pdf#page=57

24 https://rsr.akvo.org/en/project/6521/#updates

25 http://www.faapa.info/blog/societe-les-elections-professionnelles-du-dimanche-se-feront-par-voie-electronique-declare-fred-whannou

Conclusion

The election of Benin to the UN Human Rights Council despite criticism in October 2021 is an opportunity to push for a stronger democracy and for the greater protection of people's rights.[26] With the dozens of online services already available, and an increase in the use of these services during COVID-19, the country has the opportunity to use technology as a strategy to strengthen governance. Digital strategies such as online voting have already proved effective, while grassroots citizen initiatives could be digitised. The media also has a role to play here in representing the voices and the aspirations of ordinary people, so that a real direct participatory democracy can be built.[27] This will take the political will of all stakeholders involved, and research-based advocacy from civil society to push for these changes, taking into cognisance both the potential and limitations of e-democracy in a country like Benin. Anti-democratic measures such as internet shutdowns need to be kept in check, and the success of online measures that seek to promote transparency in the government sector monitored. This requires new advocacy and monitoring strategies by civil society, based on a broader vision of establishing a workable e-democracy framework as a foundation for participatory democracy in the country.

Action steps

In order to build on the current momentum in accessing government services online, and the culture of transparency being promoted in the e-government programme, there are several areas of engagement where civil society could place its energy and advocacy efforts:

- Reduce internet costs while maintaining quality. The high cost of data is an obstacle to promoting e-citizenship. For the trade union elections mentioned above, voting was entirely online. However, in several localities dozens of people could not vote for lack of internet access or because of its cost.
- Amend some of the provisions of the Digital Code. The Digital Code is an excellent tool for addressing key issues in the sector. All stakeholders unanimously welcomed it when it was passed in parliament, especially with respect to its mechanisms to address cybercrime. However, there are several aspects that need to be revised to protect freedom of expression, and which are critical to an e-democracy agenda. These include articles that criminalise the publication of false information and those that relate to online media offences.
- Use the Media Development Support Fund to support online media that promote fair information, and that aim to strengthen democracy and human rights. Key media platforms in this respect include Banouto.bj and www.crystal-news.net.
- Strengthen the Authority of Audiovisual and Communication as an institution for protecting and regulating the media, while limiting the government's influence on the governance and content of public media. A more independent authority is needed to promote access to fair news coverage and information in line with the political, social and cultural diversity of the country.
- Institutionalise e-voting in order to increase voter turnout. Combining online ballots and physical voting can help reach a larger audience and increase people's interest in public processes and democracy.
- Investigate the possibility and potential of taking grassroots participatory initiatives online.
- Support the civil society advocacy agenda against internet shutdowns. These are fundamentally anti-democratic, weaken the potential impact of the current e-government agenda, and would work against building any long-term, participatory e-democracy in the country.

26 https://www.un.org/en/ga/76/meetings/elections/hrc.shtml

27 Albert, I. O. (2009). Whose E-Governance?: A Critique of Online Citizen Engagement in Africa. *International Journal of eBusiness and eGovernment Studies*, *1*(1), 27-40. https://dergipark.org.tr/en/download/article-file/257094

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.

BRAZIL

NEW PATHWAYS FOR ADVOCACY ON PERSONAL DATA FOLLOWING A SUPREME COURT RULING DURING COVID-19

Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec)
André Ramiro and Mariana Canto[1]
https://ip.rec.br

Introduction

The pandemic was considered a watershed in terms of how countries view the use of surveillance technologies and personal data. In Brazil, it was no different. Amidst a variety of privacy-unfriendly solutions intended to mitigate the spread of COVID-19 in the country, a Presidential Executive Provisional Measure (MP 954/2020) mandated Brazilian telecom companies to share personal data of more than 200 million users with the Brazilian Institute of Geography and Statistics (IBGE, a government entity responsible for census research) "for statistical purposes". The MP ended up being halted in the Brazilian Supreme Court, resulting in a landmark ruling, according to which data protection was considered an autonomous fundamental right. As a result, the ruling paved the way for the recent promulgation of a constitutional amendment that effectively included the fundamental right to data protection in the constitution. Therefore, our main goal is to present how this decision has been a cornerstone for civil society organisations (CSOs) in their opposition to personal data-related abuses. The report will show how CSOs have been exploring the Supreme Court's precedent to conduct campaigns, litigation, research and advocacy work in the promotion of digital rights.[2]

Pandemic surveillance adds to the techno-authoritarianism

Due to the COVID denialist movement and the lack of centralised leadership by President Jair Bolsonaro in relation to policies aimed at mitigating the pandemic, including social distancing, the numbers of COVID-19 cases in Brazil reached tragic levels.[3] Therefore, in order to minimise the effects of the pandemic, technological solutions – often controversial, disproportionate and unnecessary – have been adopted by Brazilian states and municipalities. As a result, we had the proliferation of dozens of contact-tracing applications and other technological solutions that did not have any transparency regarding the collection and processing of data.[4]

The justification for collecting huge amounts of personal data – that it was necessary to contain the pandemic – was not an exclusive agenda of the private sector. MP 954/2020 instituted by Bolsonaro provided for the sharing of user data by telecommunications service providers with the IBGE, "to support official statistical production during the coronavirus pandemic."[5] The MP required telephone companies to provide IBGE with a list of the names, telephone numbers and addresses of their customers, whether individuals or legal entities. The shared data, according to the text, would be used to produce official statistics through remote household interviews.

It is important, however, to point out that this situation is considered concerning in the context of the growth of what we call "techno-authoritarianism" in Brazil. The practice is carried out through proposals and actions that expand the access of the state to sensitive data of citizens without clear justification, proper guarantees, and safeguards. These include projects such as the multi-biometric database that was the result of Decree No. 10,046 (on creating a Citizen Base Register) and the various proposals to

1 Both directors of the Law and Technology Research Institute of Recife (IP.rec).

2 Our thanks to Bianca Kremer (Coding Rights), Bruno Bioni (Data Privacy Brasil), Luã Fergus (Idec), and Veridiana Alimonti (Electronic Frontier Foundation) for their contributions to our research on how the changing interpretation of the data protection regime in Brazil has been or will be used by CSOs in their work to promote digital rights.

3 Simões, E. (2021, 22 June). Brazil passes half a million COVID-19 deaths, experts warn of worse ahead. *Reuters*. https://www.reuters.com/world/americas/brazil-set-pass-half-million-covid-19-deaths-2021-06-19

4 Ramiro, A., & Canto, M. (2022). Rastros Urbanos e a Covid-19: Economia, Políticas de Vigilância e Tecnologias de Monitoramento. In J. Reia & L. Belli (Eds.), *Smart Cities no Brasil: regulação, tecnologia e direitos*. FGV Direito Rio. https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/31403/o.%20MIOLO_Smartcities.pdf?sequence=1&isAllowed=y

5 Agência Senado. (2020, 17 August). Perde eficácia MP que obrigava operadoras a compartilhar dados com o IBGE. https://www12.senado.leg.br/noticias/materias/2020/08/17/perde-eficacia-mp-que-obrigava-operadoras-a-compartilhar-dados-com-o-ibge

amend the Civil Rights Framework for the Internet.[6] Furthermore, in November 2021, Rio de Janeiro city councillor Carlos Bolsonaro – the son of Bolsonaro – began negotiations with representatives of the companies DarkMatter, Polus Tech and NSO Group for the acquisition of spyware programmes from these companies. Also in 2021, the president's son intervened in a tender by the Ministry of Justice in order to purchase Pegasus spyware. The attempt failed, however, after the Federal Audit Court suspended the bidding process.[7]

Fortunately, as previously mentioned, the Brazilian Supreme Court decided against the MP and data sharing with IBGE, recognising – in a historic decision – that the protection of personal data was an autonomous fundamental right. This precedent represents a major step forward in relation to principles that guide the protection of personal data and creates instruments to combat techno-authoritarianism, a serious threat to human and fundamental rights and inconsistent with the rule of law in Brazil.[8]

The origins of a new fundamental right

The federal government's data-sharing proposal between IBGE and telecom companies tried to justify itself based on the necessity to conduct interviews for the National Household Sample Survey at the height of the pandemic. The alleged trade-off between data protection on one side – historically seen as an individual right – and public security or public health on the other, has been used as a typical justification for mass surveillance and social control around the world, diminishing collective data privacy in the name of a "greater good".

It is essential to put the Supreme Court's decision into perspective: before the shift in the interpretation, the previous laws were sectorial. For instance, the Brazilian Consumers' Code protected data subjects in consumer relations; the Civil Rights Framework for the Internet protected personal data, mainly regarding relations with service and internet providers; the Statute for Children and Adolescents protected its specific public, and so on. Even with a modern general regulation such as the Brazilian General Data Protection Law (LGPD), problematic areas related to the collection of personal data were left aside, such as public security, criminal investigations and national security. As a result, the LGPD has not been enough to address, by itself, crucial problems such as biometric surveillance, access to encrypted communications, or government hacking activities.

So, the IBGE case gave the Supreme Court an opportunity to update privacy legislation and bring it in line with the Brazilian Federal Constitution of 1988. With a majority of 10 votes to one,[9] the decision effectively revoked MP 954/2020's effects, given that, among other reasons, the MP was (1) too broad and vague, (2) lacked clarity in its purpose and, therefore, (3) failed to justify the necessity of the mass data sharing.[10] It also did not provide the due process needed to safeguard the set of data – in terms of technical security as well as in administrative protocols for processing the data – and it was not proportional, given that the IBGE's National Household Sample Survey programme worked literally with samples, making it unnecessary to gain access to all the databases of telecom service providers.

The court found that the right to privacy and data protection – already granted in the constitution, but mostly referred to as "confidential data" and privacy of telecommunications – should also cover "informational self-determination", adopting an autonomous right to data protection beyond the spheres of telecommunications or private data. It was argued that the right to data protection was a fundamental part of the individual's dignity and that the value of personal data escapes the public/private dichotomy, i.e. all personal data, held by public or private entities, should be subjected to constitutional protection. Finally, at least two *amici curiae* were proposed within the Supreme Court case, sustaining that the autonomous right to data protection instrumentalised a series of other liberties, as a pillar of the collective social contract, and therefore, the MP was highly disproportionate.[11]

The shift in the interpretation in the judicial branch paved the way to the Constitutional

6 Coalizão Direitos na Rede. (2019, 16 October). Nota da Coalizão Direitos na Rede sobre o Decreto nº 10.046/2019. https://direitosnarede.org.br/2019/10/16/nota-da-coalizao-direitos-na-rede-sobre-o-decreto-no-100462019/

7 Business and Human Rights Resource Centre. (2021, 8 June). Brazil: Million-dollar negotiation for the Pegasus espionage programme, developed by the NSO Group, excluded official government investigation bodies that would directly benefit from the tool. https://www.business-humanrights.org/en/latest-news/brazil-million-dollar-negotiation-for-the-pegasus-espionage-programme-developed-by-the-nso-group-excluded-official-government-investigation-bodies-that-would-directly-benefit-from-the-tool

8 Coalizão Direitos na Rede. (2021, 19 August). #16 Tecnoautoritarismo (podcast). https://direitosnarede.org.br/podcast/16-tecnoautoritarismo

9 Poder 360 (2020, 7 May). STF derruba MP que compartilhava dados telefônicos com IBGE. https://www.poder360.com.br/justica/stf-forma-maioria-para-suspender-mp-que-compartilha-dados-telefonicos-com-ibge

10 The World Health Organization's International Health Regulations (2005), adopted by Brazil, also prevent unnecessary personal data from being processed beyond the minimum necessary to address a risk to public health.

11 Namely, the Research Association Data Privacy Brasil (see: https://www.dataprivacybr.org/wp-content/uploads/2020/05/dpbrr_roteiro_sustentacao_stf_english_final.pdf) and the Laboratory of Public Policy and Internet (LAPIN), both Brazilian organisations.

Amendment No. 115/2022, recently enacted by the Brazilian Senate,[12] and effectively elevating the right to data protection to the Brazilian Federal Constitution (Article 5º, LXXIX).

According to civil society representatives, activists and policy analysts, this opened an avenue to strengthen digital rights in Brazil. As mentioned before, the previous data protection framework had limitations that left crucial advocacy work without concrete solutions, such as in the areas of public security and criminal investigations, as well as loopholes allowing abusive surveillance programmes. However, now, with the change in the legal landscape, civil society organisations could count on a powerful advocacy tool.

The dawn of a new front in digital rights advocacy

Protected by the constitution, safeguarding personal data is now a government obligation at the national and local levels. The government needs to proactively ensure the protection of personal data for the entire population, not only by avoiding unauthorised use of citizens' data, but also by promoting institutional means to continuously improve the protection of personal data. This includes education of the public, the empowerment of oversight and ombudsperson's entities such as data protection authorities,[13] public campaigns, and a broad range of incentives that promote data protection in the processing of public and private personal data. At the same time, the public sector can also be held accountable for any collective damage to Brazilians regarding personal data abuse.

At first, civil society might benefit from this scenario by demanding, for instance, that public actors reveal the amount of public resources spent in a specific year regarding the protection of citizens' personal data, as well as how the resources were spent, and who any monies were paid to. This will be very valuable in helping to understand the extent to which it has been a priority agenda. Additionally, with the new fundamental right status, data protection can be the basis for judicial actions filed directly to the Supreme Court – for instance, through Request for Non-Compliance with Basic Constitutional Principles and Direct Action of Unconstitutionality actions, whose decisions have binding effects nationwide. These are considered key opportunities for civil society to engage in judicial actions as *amici curiae* and to mobilise public opinion when landmark data protection cases are being heard at the Supreme Court.

Cases at the centre of the digital rights debate in Brazil will also be directly affected by the new constitutional landscape, such as the massive federal data-sharing programmes. In 2019, the Citizen's Basic Register (*Cadastro Base do Cidadão*) was created by presidential decree, and has been referred to as a massive "data collection and surveillance infrastructure".[14] According to the programme, multiple biographic, social and other sensitive citizen data (including biometrics of the palm, retina, face and voice, as well as gait recognition) is being shared among public entities "in order to improve the offering of public services." Another case is the sharing of Brazilians' driver's licence numbers between the Federal Data Processing Service and the Brazilian Intelligence Agency, the central domestic surveillance entity in the country.[15] As these programmes have not proven necessary and proportionate, they have been challenged at the Supreme Court[16] – and now these challenges have gained a new context that favours them based on the fundamental right to data protection.

Equally urgent is the resolution of data protection parameters regarding private messaging services. Since 2020, for instance, traceability provisions for the mass sharing of private communications within end-to-end encrypted platforms are seen as a possible solution to the dissemination of disinformation in Brazil (through Bill No. 2630/20, the "Fake News Law"). Although facing strong opposition from digital rights groups,[17] the measure is perceived by some as "justified" as it would be used in prosecution, which is considered a loophole in the prior legal regime. Now that this enforcement would be subject to the constitutional right to data protection, and considering that the proposed legislation violates the "necessity" principle in data protection guidelines – according to which only the minimum of data should

12 Autoridade Nacional de Proteção de Dados. (2022, 10 February). Proteção de Dados Pessoais agora é um direito fundamental. *Governo do Brasil*. https://www.gov.br/anpd/pt-br/protecao-de-dados-pessoais-agora-e-um-direito-fundamental

13 In Brazil, the National Data Protection Authority (ANPD) was established just recently, in 2020.

14 Kemeny, R. (2020, 19 August). Brazil is sliding into techno-authoritarianism. *MIT Technology Review*. https://www.technologyreview.com/2020/08/19/1007094/brazil-bolsonaro-data-privacy-cadastro-base

15 Dias, T., & Martins, R. M. (2020, 6 June). Documentos vazados mostram que Abin pediu ao Serpro dados e fotos de todas as CNHs do país. *The Intercept Brasil*. https://theintercept.com/2020/06/06/abin-carteira-motorista-serpro-vigilancia

16 Carneiro, L. O. (2020, 16 June). PSB aciona STF contra compartilhamento de dados da CNH entre Serpro e Abin. *JOTA*. https://www.jota.info/stf/do-supremo/psb-aciona-stf-contra-compartilhamento-de-dados-da-cnh-entre-serpro-e-abin-16062020

17 Ramiro, A., Saraiva, R., & Fernandes, A. (2021, 15 September). Os novos mitos da eficácia da rastreabilidade contra a desinformação. *ConJur*. https://www.conjur.com.br/2021-set-15/opiniao-novos-mitos-rastreabilidade-desinformacao

be processed – civil society organisations will have a stronger base for conducting advocacy and litigation against message monitoring of this nature and for protecting end-to-end encryption in general.[18]

In the field of criminal prosecution and investigation, the Brazilian Congress has been discussing the Reform of the Criminal Procedures Code, which has introduced, in its first draft, broad authorisations to law enforcement to use remote and on-device hacking technologies, including brute force tools to exploit digital security and spyware. Beyond the legislative debate, the providers of hacking tools – such as Cellebrite[19] and Verint[20] – have a very close relationship with Brazilian law enforcement. As mentioned, most recently, it was also disclosed that the son of President Jair Bolsonaro, Carlos Bolsonaro, tried to purchase hacking tools from companies such as the NSO Group and DarkMatter[21] in order to surveil political opponents. Furthermore, the government's acquisition of software that does broad data gathering from open sources (also known as "open-source intelligence" or OSINT) is being reported and questioned by civil society organisations for the lack of clarity and legality in its uses, as well as its threat to democratic values in the country.[22] Due to the potential of these tools to be extremely invasive to individuals, the government's predilection for surveillance can be challenged on constitutional grounds and should be overseen by data protection authorities and digital rights organisations.

This demonstrates the need to bring the discipline of data protection closer to the practice of law enforcement in Brazil. Not coincidentally, in 2021 the Draft Bill on Data Protection Law for Criminal Investigation and Public Security (the "LGPD Penal Law") was introduced, building a specific data protection system by regulating limits and permissions on the processing of personal data within the field of law enforcement.[23] Although it did not gain much traction last year, the shift in the legal framework creates a pathway for civil society advocacy pushing for the enactment of the law in the Brazilian Congress.

Conclusion

It seems that the Supreme Court's decision introduced not only a new fundamental right but a new interpretation regarding the importance of the right to privacy and data protection for Brazilian citizens. The right to data protection is no longer just an individual right, related to the use and collection of data – on the contrary, it has become a matter related to collective and social well-being, along with human dignity. Although we still need specific laws for the use of certain technologies for law enforcement purposes, the recognition of the fundamental right is essential for the prevention of abusive surveillance measures within the scope of public safety, such as the use of mass surveillance for political persecution, as well as the use of specific technologies such as facial recognition and tools used to bypass the security of encrypted devices and services. As stated by some of the people interviewed for this report, with the approval of the constitutional amendment, the judicial branch has become a lifeline in a Brazil that is currently subject to a less progressive legislature and an institutionally weak and authoritarian administration.

Moreover, this new fundamental right alongside existing data protection legislation creates an important cornerstone for demanding greater transparency and mechanisms for evaluating and monitoring the processing of data by public and private agents. It can also be said that there is a great "revisional movement" in relation to certain previously approved abusive and invasive laws from a privacy perspective. From now on, civil society is able to use this precedent in order to consolidate legal grounds so that they can be used in strategic litigation actions. Therefore, it will be possible to challenge data protection-unfriendly laws that need to be re-evaluated now and possibly declared as unconstitutional since they violate a fundamental right granted in our constitution.

Because of this, we are witnessing a change that seems very promising. The possibility that organised

18 Aleixo, G., et al. (2019, 30 May). The Encryption Debate in Brazil. *Carnegie Endowment for International Peace*. https://carnegieendowment.org/2019/05/30/encryption-debate-in-brazil-pub-79219

19 Ventura, F. (2021, 8 April). Polícia usa Cellebrite para resgatar provas apagadas de celular no caso Henry Borel. *Tecnoblog*. https://tecnoblog.net/noticias/2021/04/08/policia-usa-cellebrite-para-resgatar-provas-apagadas-de-celular-no-caso-henry-borel

20 Braga, A. (2020, 3 October). Governo do AM comprou o mesmo equipamento de espionagem israelense apreendido pela PF no Pará. *D24am*. https://d24am.com/artigos/alex-braga/governo-do-am-comprou-o-mesmo-equipamento-de-espionagem-israelense-apreendido-pela-pf-no-para

21 Chade, J., & Valença, L. (2021, 18 January). Cobiçado pelo 'gabinete do ódio', sistema DarkMatter é usado por ditaduras. *UOL Notícias*. https://noticias.uol.com.br/politica/ultimas-noticias/2022/01/18/darkmatter-foi-usado-para-investigar-jornalista-saudita-morto-em-consulado.htm

22 Conectas. (2021, 9 August). Entidades questionam no TCU contratação de software de espionagem. https://www.conectas.org/noticias/entidades-questionam-no-tcu-contratacao-de-software-de-espionagem

23 Consultor Jurídico. (2020, 31 October). Anteprojeto de lei disciplina proteção de dados em investigações criminais. https://www.conjur.com.br/2020-out-31/anteprojeto-disciplina-protecao-dados-investigacoes-criminais

civil society can demand a greater commitment by the state in terms of its duties and the protection of citizens is a light at the end of a presently frightful moment in Brazil.

Action steps

The following actions are necessary in Brazil:

- Civil cociety should invest in creating a movement for the "constitutionalisation" of demands on data protection, i.e. actions aimed at questioning, based on the fundamental right of data protection, the constitutionality of certain policies and laws.
- Problems related to obtaining user consent and current abusive data-sharing practices between government agencies and private entities should be brought to light, as a way of promoting transparency and accountability in the government's obligation to protect citizens' data.
- Campaigns and other initiatives can be carried out by civil society in the field of public security, criminal prosecution and national defence based on this new fundamental right, including creating pressure for more detailed and specific regulations.
- Civil society must be attentive, always seeking "strategic litigation" – i.e. assisting public prosecutors in collective actions and/or participating in judicial processes of public interest as *amicus curiae* – because otherwise, Brazilian courts can endorse negative practices and give them an even greater degree of legitimacy.

CAMEROON

THE COVID-19 PANDEMIC AND ACCESS TO EDUCATION IN CAMEROON

PROTEGE QV
Serge Daho, Avis Momeni and Emmanuel Bikobo
www.protegeqv.org

Introduction

Cameroon is a lower-middle-income country located in the West Central African region, and is bordered by six countries including Chad, Nigeria and Gabon.

Faced with the outbreak of the coronavirus pandemic, the government of this country of more than 25 million inhabitants[1] spread over 475,000 square kilometres implemented several measures to contain the virus. These included social distancing and the use of electronic communications and digital tools for education and distance learning. This, together with e-working, lead to an increase in the use of information and communications technologies (ICTs) in the country.

In the context of a surge in demand for the internet, this report discusses how a reliance on the internet impacted the right to education in Cameroon during the pandemic. It also suggests recommendations to help civil society use the internet effectively, and to advocate for digital rights.

Background

Cameroon, like many states in the world, was not spared by the COVID-19 pandemic. In the face of what then appeared to be a global health crisis, the government adopted 13 measures to prevent the spread of the virus in the country, which entered into effect on 18 March 2020.[2] Later on, five additional measures still aimed at curbing the pandemic were taken by the government.[3] These governmental actions ranged from the closure of all public and private school facilities from nursery to higher education, to the prohibition of gatherings of more than 50 people. The measures changed people's lifestyles deeply, and rapidly increased internet usage for social interaction, e-working, information sharing and online studies. However, internet usage in Cameroon is hindered by limited internet access,[4] costly internet data, poor connectivity, underserved rural areas and poor internet speeds.

According to the Inclusive Internet Index 2020,[5] the country was ranked 102nd overall out of the 105 countries assessed (and tied for 13th place among 30 Sub-Saharan African countries). This means that the increased use of the internet in areas such as education or for distance work as advocated by the public authorities was not possible for most.

Accessing the internet: An uphill task for many Cameroonians during COVID-19

According to the African Declaration on Internet Rights and Freedoms, "Access to the internet should be available and affordable to all persons in Africa without discrimination on any ground."[6] The government's efforts in Cameroon to curb the COVID-19 pandemic created a range of knock-on consequences for the ICT sector, and its infrastructures and services, as access to the internet became both a key channel for authorities seeking to manage the crisis, and for citizens seeking to accommodate its exigencies.[7]

There are legal provisions relating to the right to access electronic communications, notably Law

1 https://www.worldbank.org/en/country/cameroon/overview#1

2 https://www.spm.gov.cm/site/?q=en/content/government-response-strategy-coronavirus-pandemic-covid-19

3 Emmanuel. (2020, 13 April). Fight against coronavirus: Government takes additional measures. *Cameroon Tribune*. https://www.cameroon-tribune.cm/article.html/31736/en.html/fight-against-coronavirus-government-takes

4 "In January 2020, 7.8 million people were connected to the internet in Cameroon, according to a report published by Hootsuite and We Are Social, two organisations that monitor internet and social media feed. With that number of users, the internet penetration rate reached 30% in the country in January 2020." Business in Cameroon. (2020, 24 February). Cameroon: Internet penetration rate up 30% YoY in Jan 2020, with the addition of 570,000 news users. https://www.businessincameroon.com/economy/2402-10003-cameroon-internet-penetration-rate-up-30-yoy-in-jan-2020-with-the-addition-of-570-000-news-users

5 The Inclusive Internet Index, commissioned by Facebook and developed by The Economist Intelligence Unit, seeks to measure the extent to which the internet is not only accessible and affordable, but also relevant to all, allowing usage that enables positive social and economic outcomes at the individual and group level. https://theinclusiveinternet.eiu.com/explore/countries/performance/overall?highlighted=CM&year=2020

6 The African Declaration on Internet Rights and Freedoms is a Pan-African initiative to promote human rights standards and principles of openness in internet policy formulation and implementation on the continent. For more information, see: https://africaninternetrights.org/en/declaration

7 Lewis, C. (2020). Digital divisions: COVID-19 policy and practice and the digital divide in Africa. In African Declaration on Internet Rights and Freedoms Coalition, *The impact of COVID-19 on digital rights in Africa*. https://africaninternetrights.org/en/node/2553

N°2010/013 of 21 December 2010 governing electronic communications, which states in its article 4 that "everyone has the right to benefit from electronic communications services, irrespective of his or her geographical location within the national territory." Further on, article 28 (para 1) requires "Cameroon's telecommunications operators to provide communications services of good quality, at affordable rates and in an uninterrupted manner."

Moreover, Law N°2015/006 of 20 April 2015 amending and supplementing certain provisions of Law N°2010/013 of 21 December 2010 establishes the Universal Service Access Fund (in section 34), whose resources are intended *inter alia* for "the development of electronic communications throughout the national territory." The ultimate aim of the Fund is to ensure equal, good-quality and affordable access to services.

However, a survey commissioned by the Alliance for Affordable Internet[8] in 2014 ranked Cameroon 40th out of 46 emerging and developing nations surveyed in terms of internet access costs, with an overall score of 17.1 (out of a possible 100). At that time, the country's failure to launch an internet exchange point (IXP) and its failure to use the WACS and ACE[9] submarine cables were blamed.[10]

To date, the same is true: the cost of internet access, as evidenced by a recent study commissioned by Facebook,[11] is still high despite the head of state's commitment when he said in 2015 that his government would give the ICT sector "all the attention it deserves."[12]

Notwithstanding incentives for widespread access to internet services, both access to and affordability of the internet remain a real challenge in Cameroon for poor communities in rural areas as well as in some disadvantaged urban areas. This was particularly the case during the coronavirus pandemic, hampering a shift to e-learning, even though this was a government-led initiative.

E-learning as a display of Cameroon's unpreparedness to face one of the COVID-19 consequences

To ward off the spectre of a "blank year" and to ensure the continuity of education in Cameroon, the government responded to the pandemic by implementing various distance-learning programmes on radio, television and using the internet. With regard to primary schools, a solution called *"l'école à la télé"* (school on TV) was launched by the Ministries of Basic Education and Secondary Education with CRTV, the state-owned radio and television broadcaster, as a technical partner. This distance-learning programme ran from 6 April 2020 until 31 May 2020, with courses broadcast on TV in both French and English. This helped to ease learning from home for more than 7.2 million pupils and students affected by the closure of schools and universities due to the pandemic.[13]

At the higher education level, the minister reminded the heads of public and private universities, during a meeting held on 20 March 2020,[14] of the urgency of an appropriate and concerted response so that the academic year could be continued. Among the measures adopted were the use of institutional digital platforms that were already accessible to students for online teaching and the use of social networks.

Reactions from students, teachers and education stakeholders pointed to a lack of preparedness and readiness among all stakeholders, including the government and private education providers, as well as the students themselves. Teachers and staff interviewed pointed to a lack of computer knowledge and training opportunities as a setback to an effective COVID-19 digital learning response.[15] Most teachers lacked the necessary skills, and needed to be trained in e-learning and on the use digital learning systems. In most schools in the country, the only teachers who can boast knowledge in using ICTs are computer science teachers and other teachers who teach technical subjects.[16] The same applies to

8 https://a4ai.org

9 The West Africa Cable System (WACS) is a submarine communications cable linking South Africa with the United Kingdom along the west coast of Africa, while the Africa Coast to Europe (ACE) optical fibre submarine cable system serves 24 countries on the west coast of Africa and Europe. See: https://en.wikipedia.org/wiki/West_Africa_Cable_System and https://en.wikipedia.org/wiki/Africa_Coast_to_Europe_(cable_system)

10 Owono, J., & Blanc, F. (2014). *Internet and broadband in Cameroon: Barriers to affordable access.* Alliance for Affordable Internet. https://a4ai.org/a4ai-releases-cameroon-case-study

11 Ibid.

12 Excerpt from the Head of State's Message to the Nation, 31 December 2015. https://www.prc.cm/en/news/speeches-of-the-president/1612-head-of-state-s-message-to-the-nation

13 Actu Cameroun. (2020, 23 April). Cameroun/E-learning : la difficile épreuve de l'enseignement à distance. https://actucameroun.com/2020/04/23/cameroun-e-learning-la-difficile-epreuve-de-lenseignement-a-distance

14 Siyam, S., Momeni, A., Daho, S., Amahata, L., & Bikobo, E. (2020). *Le respect des droits numériques dans le contexte de la COVID 19 au Cameroun.* African Declaration on Internet Rights and Freedoms Coalition. https://www.apc.org/sites/default/files/Rapport-de-recherche_Respect-des-droits-numeriques.pdf

15 Ajebe Akame, G., Bates Anoma, R. A., & Crockett, J. (2021). *Cameroon's COVID-19 Pandemic Education Response and the Shift to Distance/Digital Learning.* Solidarity and Development Initiative. https://reliefweb.int/sites/reliefweb.int/files/resources/Cameroon%E2%80%99s%20COVID-19%20pandemic%20education%20response%20and%20the%20shift%20to%20distance-digital%20learning%2C%20November%202021.pdf

16 Siyam, S., Momeni, A., Daho, S., Amahata, L., & Bikobo, E. (2020). Op. cit.

students, with many unable to use a computer, let alone meeting the challenge of providing them with the necessary devices for distance learning.

Alongside this, internet services are not evenly distributed throughout the country, a problem compounded by multiple power failures and limited access to electricity. Similarly, even the CRTV signal is not available throughout the national territory, meaning that some pupils without internet access could not even benefit from the *l'école à la télé* initiative.[17]

Conclusion

The COVID-19 pandemic has sounded a wake-up call on how critical internet access has become to our daily lives. With social distancing measures in force across the world at the time of writing, we are now living online (to keep in touch with our families and friends, to work or learn from home).

Through measures limiting physical contact, the government has opened up the road to the widespread take-up of ICTs. This has resulted in numerous actors in the private and non-profit sectors setting up initiatives using the internet for online learning, online work and citizen training.

Unfortunately, physical isolation has starkly exposed the digital divide across the national territory. People in poorer areas of the country and those in remote and rural areas were not able to get online. This inequality had many consequences. For instance, without internet access or computers, and most of the time without electricity, many citizens fell behind in their education.

The COVID-19 pandemic has shown how citizens become vulnerable when governments do not protect and promote human rights in the online environment. Since many have turned to the internet to reach out, the issue of digital rights has become foregrounded. This is exacerbated by the fact that during the pandemic, civil society has faced several constraints on its ability to carry out its work as a result of lockdowns, distancing and quarantine measures.

Action steps

The pandemic has exposed barriers to internet access in Cameroon (poor infrastructures, constant power failures, high data costs, lack of adequate access devices, etc.). While these barriers existed before, the pandemic has demonstrated the direct consequences of the lack of access, particularly in the education sector. This has potentially compromised the right to education for many citizens.

To allow civil society organisations to efficiently address this issue, in the context of a growing number of people moving online, the following action steps are recommended:

- Civil society organisations should collaborate, share their skills and upskill in order to be more efficient online and reach both a local and international audience. Voices are more powerful when they are put together.
- Investigate better ways to campaign online, including by learning about successful cases elsewhere in the world. For example, organisations could use a "smart switch" to reach intended audiences through online campaigns simply by using a hashtag.[18] Online petitions as well as crowdsourced social media campaigns would also be effective. However, the possibilities and limitations of these sorts of campaigning tools need to be understood.
- Humanise digital communications as much as possible for online events. The message is as powerful as the messenger.[19]
- Build the capacities of both civil society organisations and citizens on cybersecurity issues and on the use of personal data.
- Inform citizens of their rights online and develop the necessary capacity to protect and promote these rights.

17 Journal du Cameroun (2014, 19 March). Le signal de la CRTV disponible dans deux localités de l'Est. https://www.journalducameroun.com/le-signal-de-la-crtv-disponible-dans-deux-localites-de-lest

18 Bowater, D. (2020, 23 March). How to advocate effectively in the age of COVID-19. *Devex*. https://www.devex.com/news/opinion-how-to-advocate-effectively-in-the-age-of-covid-19-96812

19 Ibid.

CANADA

THE NEED FOR A BROAD-BASED DIGITAL RIGHTS MOVEMENT IN CANADA

eQualitie
Michel Lambert
https://equalit.ie

Introduction

On 8 February 2022, almost two years into the pandemic, two important political events happened in Canada. For the first time, a member of the federal parliament, Joel Lightbound, who is also from Prime Minister Justin Trudeau's Liberal Party of Canada, spoke out publicly on the government's COVID-19 policies, saying they had become "politicised" and "divisive". His political future was at stake for a few weeks.

The same day, as infection rates from the fifth wave appeared to be declining in his province, the premier of Quebec, François Legault, declared that most restrictions would be removed within the following month. However, two major policies would remain in effect: the vaccine passport – an application on mobile phones necessary for every individual to have access to stores and services – and the state of emergency which allows the government to run affairs without using the usual political institutions.

These two separate events demonstrate how the federal and provincial governments have kept tight control over the management and messaging of the COVID-19 pandemic, and wish to carry on doing so, including by disallowing debates on their policies and stifling any divergent viewpoints.

Signs that the government wants more control

Vaccine passports

In Quebec, where 81% of the population has received two vaccines already, and where this rate is still growing daily, insisting on the vaccine passport is inexplicable other than by the government's interest in continuing to track people. The Quebec National Institute for Public Health in Quebec (*Institut national de santé publique du Québec*) has even recently admitted that they have no proof of the efficiency of the passport. Many technical weaknesses with the passport application have also been exposed. As of January 2022, more than 150 investigations into fake passports were opened, with guilty people facing fraud charges and up to five years in prison.

Mass surveillance

In December 2021, the Canadian public health agency admitted to having tracked 33 million mobile devices during the lockdown that year. To do so, they awarded a contract to the Telus Data for Good programme,[1] a programme launched by the Telus telecommunications company, claiming to help "solve pressing societal issues in ways that preserve privacy and build trust." The irony of that situation has made the public realise that there are few regulations that act as safeguards in protecting privacy in Canada. As a result, local NGOs have started to request that the government introduce new laws that would create rules around how public bodies report on the collection and use of sensitive personal information, and provide oversight from an independent third party, like the Office of the Privacy Commissioner of Canada.

New laws to control Canadians – and no law to protect them

At the federal level, while disinformation and misinformation existed before COVID-19, the pandemic has spawned two ambitious and very dangerous draft laws looking at controlling what is accessible to Canadians over the internet from almost all online services, as well as controlling what Canadians publish online.

In November 2020, the government introduced Bill C-10, followed in June 2021 by Bill C-36.

Bill C-10, called the "censorship bill" by many, was initially presented as a way of generating new taxes for streaming services. It was rapidly sent to the senate after a gag order was placed on the committee studying it. Instead of simply taxing streaming services, critics found that the bill would amend the Canadian Broadcasting Act and grant utterly inappropriate power to one institution, the Canadian Radio-television and Telecommunications Commission (CRTC). It would have the power to decide which audiovisual content is available on the internet. The bill's adoption was delayed because of the Canadian elections in September 2021. It was, however, reintroduced as Bill C-11 in February 2022.

Despite government promises of a less aggressive version, the second version of the bill still gives

1 https://www.telus.com/en/about/privacy/data-for-good

a limitless reach to the CRTC's jurisdictional power over audiovisual services on the internet. An internal memo from the government[2] identified a wide range of sites and services, including video streaming, podcast apps, audiobooks, home workout apps and adult and sport websites potentially covered by the legislation. Michael Geist, a well-known researcher from the University of Ottawa, believes that this may result in many services choosing to block the Canadian market[3] entirely.

Bill C-36 was presented in June 2021 to fight online hate speech. It would have amended the Canadian Criminal Code, the Youth Criminal Justice Act and the Canadian Human Rights Act to allow individuals or groups to file hate speech complaints with the Canadian Human Rights Commission. Critics said it was fraught with problems and risked hampering freedom of speech on top of being difficult to enforce.

Between July and September 2021, the Canadian Heritage Ministry consulted interested parties on the proposed bill. While the majority of respondents consulted during this process confirmed the need to take action on the problem of hate speech, they also identified several overarching concerns, including those related to freedom of expression, privacy rights, the impact of the proposal on certain marginalised groups, and compliance with the Canadian Charter of Rights and Freedoms.[4]

Civil society has caught "long COVID"

These threats to civil freedoms coming from the national and provincial level have seriously affected political life in Canada, and particularly in provinces like Quebec. Mainstream media have completely abdicated their role of being a watchdog to power, and have reduced themselves to just being transmission channels for government decisions on the pandemic. Journalists who dared to question those policies were fired. The most recent example is Francine Pelletier, a well-known journalist from the newspaper *Le Devoir* in Montreal who dared to write an article questioning the government's policy of prioritising vaccination over other possible interventions in its strategy for combatting the virus in January 2022. She was fired a week later.

As governments are managing the pandemic outside of the normal institutions and parameters, political parties have been reduced to observers, hardly criticising the footnotes from government policies that are introduced.

Maybe most of all, civil society organisations have slowly slipped into a state of dormancy – a kind of long COVID. As many of the global campaigns and movements – against climate change, racism, gender-based violence, war and others – were suddenly paused due to the pandemic, many local organisations lost contact with a global perspective. They were trapped into managing immediate difficulties, including financial difficulties, and were struggling to maintain democratic structures online and to reflect and act on pressing political issues. Added to this is the absence of a substantial, critical and alternative vision that is not aligned with the idea that the virus is a conspiracy and that it does not exist. Civil society had its TINA[5] – or "there is no alternative" – moment. This has resulted in a real inability to debate alternative political perspectives from a factual point of view, and to create alternative, meaningful strategies that safeguard human rights.

The future of digital rights advocacy

Canadian digital rights advocacy can be defined in many ways, but in particular by the obvious characteristic that there are far fewer actors in the actual movement than the number of people and organisations that really should be concerned by the development of such a broad-scope tool as the internet. This might be explained by the fact that the Canadian Internet Governance Forum (IGF) process is very young (it was first funded in 2019) and fragmented (a Quebec Provincial IGF also exists, but the two processes are still not formally connected), and possibly by a certain conviction held by many that the internet in Canada is "safe and secure", here to stay, relatively easy to access, and somehow self-managed. In comparison to other human rights movements in Canada, digital rights organisations can be quite specialised, not always successfully connecting with the "offline" rights movements or any other civil society group concerned about the internet.

It is also fair to say that the digital rights organisations could be better connected to each other, learn more from each others' work, and cooperate more on campaigns. While Canadian community-based campaigns working on many issues are often federated in associations, giving weight to their advocacy,

2 https://fr.scribd.com/document/508665790/A-2020-00498-Heritage-c10-Digital-Exclusion

3 Geist, M. (2022, 9 February). Bill C-11's Foundational Faults, Part One: The Nearly Unlimited Global Reach of CRTC Jurisdiction Over Internet Audio-Visual Services. https://www.michaelgeist.ca/2022/02/bill-c-11s-foundational-faults-part-one-the-nearly-unlimited-global-reach-of-crtc-jurisdiction-over-internet-audio-visual-services

4 https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/what-we-heard.html

5 TINA was a slogan often used by the Conservative British prime minister Margaret Thatcher. It was used to signify Thatcher's claim that the market economy is the only system that works, and that there was nothing to debate.

this is not the case in the field of digital rights. For instance, when ethical hackers easily infiltrated the COVID vaccination app in Quebec, and pointed out the app's weaknesses to the government, they were immediately labelled as anti-government and threatened with judicial proceedings, but hardly any organisation stood up to support them.

Digital rights organisations are probably not spending enough of their resources on educating other organisations or their constituents about the importance and challenges of digital rights. A study[6] by Lab-Delta, a Montreal-based group doing research on technology and activism, concluded after interviewing university students that even when people assume and pretend that they understand digital rights issues, the majority of them do not. This lack of understanding of the issues is one reason why it is difficult to connect digital rights movements meaningfully to other societal concerns, and also shows the huge need to educate the public on digital rights issues.

However, there is only so much digital rights organisations can do. Their resources are limited, and most of them are currently spent on engaging the government on policy and legislation, as was clear from the last two roundtables held at the Canadian IGF. While there were many recommendations, they were all directed at what the government should do.

Conclusion

I would argue that there has been more of a pause than a real shift in digital rights advocacy in Canada as a result of the pandemic. Central issues facing the movement, namely the lack of networking inside and outside the movement, and the lack of public education, were realities prior to March 2020, and are likely to persist in the near future.

Even the two new federal laws, C-11 and C-36, were already planned, at least as far as government intentions go, as early as 2019. The scope they initially chose to give to these bills was boosted by the sudden need to counter COVID disinformation, which was not expected, but a mandate letter to the Canadian Heritage Minister in December 2019[7] already mentioned the government's plans to create new regulations for social media platforms, requiring them and internet service providers (ISPs) to remove "illegal content", including hate speech.

The rights movement – including the digital rights movement – responded to these and forced revisions which show the capacities of these movements, and the responsiveness of the government. It can be expected that further adjustments will occur in future versions of the laws, but nobody knows exactly how flexible the government will finally be.

Two issues can, nevertheless, be considered new issues:

- A vaccine passport, falling under the jurisdiction of each of the country's ten provinces. The passports were originally created to encourage people to get vaccinated, but since Canada now has one of the highest levels of vaccination in the world, their utility has become highly questionable. In Quebec, the government also decided to create an app to replace a paper document, making the passport available only to mobile phone owners. Furthermore, each province has its own system, creating a completely disorganised patchwork of systems.
- The Canadian government showing its willingness to track millions of mobile devices during lockdowns to "analyse" people's movement, without there being any real public protection in the current legislation.

What is also clearly necessary is that digital rights organisations need to challenge their advocacy silos, and begin to build broader advocacy movements that include other actors, including at the community level. This is all the more important given that the restrictions contemplated and enacted by the government are cross-cutting and have implications for everyone in the country.

What is interesting is that when movements confront the government on issues like hate speech, often activists tend to focus the discussion on legislation. But involving others with fresh approaches in the discussions might well open them up to new ideas. An advocacy approach countering hate speech could for instance also involve proactive strategies using education – formal and informal – as well as supporting interventions by community-based organisations. Digital literacy training, so that the public can recognise when content is abusive, is also essential. After all, instead of overly restrictive legislation, in 2019, the UN Special Rapporteur on the right to freedom of opinion and expression encouraged states to explore alternative ways to combat hate speech, including creating platforms for dialogue.[8]

6 Couture, S., et al. (2021). *Stratégies d' engagement pour et par le numérique*. Lab-Delta. https://www.labdelta.ca/publications/strategies-dengagement-pour-et-par-le-numerique

7 https://pm.gc.ca/en/mandate-letters/2019/12/13/archived-minister-canadian-heritage-mandate-letter

8 UN Office on Genocide Prevention and the Responsibility to Protect. (2020). *United Nations Strategy and Plan of Action on Hate Speech: Detailed Guidance on Implementation for United Nations Field Presences*. https://www.un.org/en/genocideprevention/documents/UN%20Strategy%20and%20PoA%20on%20Hate%20Speech_Guidance%20on%20Addressing%20in%20field.pdf

Action steps

Specifically, movements should:

- Force governments to revoke vaccine passports in every province.
- Lobby the federal government for a law to be adopted aimed at creating rules around how public bodies report on the collection and use of sensitive personal information, and provide oversight from an independent third party, like the Office of the Privacy Commissioner of Canada.
- Work towards creating a pan-Canadian network on digital security. The global IGF may be held in Canada in 2024, and this might help to facilitate such a process.
- Connect more with offline movements to avoid solely techno-centric or legislative answers to issues.

On the C11 and C36 bills, movements should advocate for the government to:

- Reaffirm its commitment to net neutrality and the principles of the open internet.
- Reflect on enforcing existing laws to keep big tech companies in check and ensure they are held responsible for the harms occurring on their platforms.
- Define clearly several key terms and concepts before regulating big tech.[9]
- Provide narrower, clearer definitions of the illegal and harmful content addressed by the pending legislation.
- Acknowledge that using automated decision making to flag and remove content should be avoided, as it will lead to legitimate content being censored.
- Acknowledge that automated systems that send user data to law enforcement agencies should also be avoided.
- Acknowledge that there are other avenues to deal with online harms, and explore these before resorting to removing content, such as digital literacy, understanding better the impact of paid-for content on hate speech, as well as the role of competition law in this regard, and more control for users over the algorithms used in their content feeds.[10]

9 Several key terms and concepts are mentioned in the laws that need better definition, such as "CanCon" (Canadian content), "discoverability", "social media services", and the delineation between companies' services and the companies themselves.

10 This last point was raised at the Canadian IGF, where one participant suggested that giving more algorithmic choice or control over algorithms to parents could provide for a better online experience for their children.

COLOMBIA

DIGITAL ADAPTATION UNDER COVID-19 – ONLY A REALITY FOR A FEW

Colnodo
Marcya Hernández
https://www.colnodo.apc.org/

Introduction

Two years after the dynamics of public and private organisations around the world began to be transformed by the health emergency caused by COVID-19, it is of great importance to review the implications of these new circumstances for civil society organisations (CSOs) in Colombia.

How did the prevention measures adopted during the past two years affect the development of programmes and projects? How were digital solutions incorporated into the new dynamics of organisations? And what were the implications of these changes for what we call the "integral security" of communities – or the context and capacity of communities to enact their rights both online and offline? These are some of the questions that guided the conversation with CSOs and allowed an understanding of the main challenges they face in the midst of such a particular and unexpected context.

The impact of COVID-19 was felt globally, and the world of work was no exception. However, for organisations that run social and humanitarian projects in different regions of the country, the preventive isolation measures and the cancellation of face-to-face events meant great changes in their internal dynamics, in the methods of interacting with communities, and in the perception of the privacy of their information. This had implications for the integral security of children, young people, and leaders and activists working for the defence of human rights.

CSOs in Colombia: Diverse contexts and particular challenges

In order to understand what COVID-19 has meant for CSOs in Colombia, we approached people from different organisations[1] that ran social, educational, economic, food and humanitarian assistance projects in different regions of the country, including in urban and rural areas, and in ethnic communities. Many of these projects relied on the participation of communities themselves. The organisations explained the immense difficulties they faced when they started the confinement measures in March 2020 and the changes they implemented to continue their institutional programmes so that they could fulfil the objectives of their projects.

Waiting time, uncertainty and internal adjustments

The organisations experienced the arrival of COVID-19 in Colombia and the beginning of preventive isolation in a very similar way: a completely unexpected situation that, in principle, forced the vast majority of people to work remotely, and which required the optimisation of digital tools, particularly tools for communication and interaction, to maintain team dynamics.

What began as a temporary contingency measure became a permanent dynamic in a new institutional context that implied fundamental changes. The waiting period to return to "normality" became a time of uncertainty and constant questioning; a time characterised by profound reflections, adjustments and structural transformations that allowed the entities to continue implementing their programmes and projects within the framework of a new reality.

That first few months of the pandemic resulted in an unprecedented effort by the CSOs to adapt to the sudden change. It demonstrated their strength and social commitment to keep the projects going and to propose alternatives in the development of activities that prioritised face-to-face activities and in which human contact was fundamental for the achievement of project objectives.

For many organisations that have lived through these past two years between uncertainty and opportunity, ICTs have allowed them to digitise training, participation and advocacy processes. This has

1 Persons interviewed: Sandra Saenz Sotomonte, member of the coordinating team of the Women's Network for Economic Empowerment in the Province of Vélez, department of Santander; Liliana García, coordinator of the project "Response to the emergency situation and the disproportionate impacts of the pandemic on women's lives" carried out by the Lutheran World Federation in partnership with UN Women and the UN Central Emergency Response Fund (CERF), in the department of Chocó; Lucy Cardona, lawyer and project coordinator for the AVP Foundation for Social Development; Genith Quitiaquez, a representative of the Pastos Indigenous community in the department of Nariño (during the two years of the pandemic she served as governor of the Gran Tescual Indigenous Reservation, one of the Pastos people's 25 reservations); and Luisa Fernanda González, vice president of the Schools of Peace Foundation, in charge of pedagogy and knowledge management, and a member of the Women and Peace Summit movement.

involved improving skills in the use of technological tools and also being more aware of the risks to which they are exposed in the digital world.

For example, for organisations like the Women's Network for Economic Empowerment in the province of Vélez, which runs the Escuela de Formación por el Derecho de las Mujeres a la Ciudad y el Territorio y las Escuelas de Paz (Training School for Women's Rights to the City and Territory and the Schools of Peace), digital tools allowed them to advance in the development of educational programmes. They managed to decentralise and expand the participation of people in different parts of the country, and also to optimise the reuse of resources such as time and travelling costs needed for face-to-face meetings that were usually held in capital cities.

In this sense, CSOs have valued the workshops and advice they have received from Colnodo during this time on digital security issues, with the purpose of guiding them to safeguard their privacy and protect their personal and institutional information. They have also had the opportunity to share this knowledge with children, young people and community leaders, promoting good practices in using the internet.

However, this process of redesigning projects highlighted a great paradox of the digital era. For some organisations this time meant a learning experience; for others, the reality of lack and precariousness. The experiences were as gratifying for some as they were devastating for others.

For some organisations, remote interaction was insufficient because the reality of the communities essentially requires direct face-to-face work. This includes, for example, organisations working on food security, basic sanitation, or attending to violence and psychosocial support in communities that have historically experienced state abandonment. In these communities, the precariousness of living conditions is enormous and, of course, technological devices are very scarce and internet connectivity is deficient.

For organisations working in these communities, remote work within the organisations was a minor change compared to the greater challenge of implementing activities remotely with the communities in the different regions of the country.

Challenges faced by communities

Talking about integral security in the framework of rights implies reviewing the particular conditions of communities and their capacity to exercise autonomy to guarantee their well-being or a good life, both in the physical and digital environment.

While a situation like COVID-19 puts food security at risk, especially in cities that depend to a large extent on centralised distribution channels, the pandemic and the measures implemented to deal with it affected the daily life of communities, their social and family ties, their productive activity, their economic income and, of course, their physical and mental health. In contexts of precariousness and exclusion these effects were undoubtedly much stronger.

For organisations that experience a reality of deprivation and exclusion, the main digital rights that are violated are not having access to technological devices, quality connectivity and training opportunities. Although this does not seem to be a high priority when compared to fundamental rights related to the guarantee of life, such as access to food, drinking water, health care and the prevention of physical or emotional violence, the fact is that the appropriation of ICTs can facilitate access to other rights.

In this regard, the pandemic forced the redesign of projects and budgets by CSOs so that they included the purchase of tablets, payments for connectivity services, and even allocations for transportation, so that people could travel to places with a better internet signal and thus connect to virtual sessions run by various initiatives. This was an important effort on the part of the CSOs, as these expenses were not initially budgeted for in their projects.

A great example of the capacity for adaptation and appropriation of technologies happened in the Resguardo Indígena Gran Tescual (Gran Tescual Indigenous Reservation), which is located in the south of the country and is home to the Pastos Indigenous people. The project team managed to implement a virtual training strategy aimed at the more technically skilled people in the communities, who received technical training from experts who could not travel to the territory due to isolation measures. This knowledge was then shared with families in the region through in-person visits, strengthening community ties.

However, under COVID-19 preventive measures, CSOs also saw setbacks in some of the processes that were being developed in communities. An example of this is the strengthening of criminal paramilitary gangs in the department of Chocó in the west of Colombia. Here the presence of humanitarian organisations implementing initiatives with the community had been respected, but unfortunately the preventive isolation limited their institutional presence in the region and made it possible for the armed groups to occupy or make their presence felt again in the territory.

Violence against children and women increased, given that they had to be confined under the same roof with their abusers, isolated from their wider family or community support network, and subjected to the conditions laid down by the breadwinner. It is important to mention that women were the first to lose their jobs: for the October-December quarter in 2020, unemployment among women reached 18.7%, compared

to 10.2% for men. And it is also women who dedicate more hours to household chores and unpaid care activities – an average of 28.4 hours per week, while men only dedicate 12.3 hours to these tasks.[2]

In communities that did have connectivity, many expressed fear of the risks posed by the uncontrolled use of digital tools by children and young people in particular. This includes the personal and family information that they may share with strangers, the sharing of intimate images and the consequences that this entails, cyber-dependence, social isolation, loneliness and mental health problems. All of these are situations that concern CSOs and they consider that they deserve to be addressed. Some educational initiatives have been launched by CSOs in this regard, especially including families and groups of young women. However, this concern requires further consideration and advice from expert organisations.

It is also evident that due to the scarcity of resources and the barriers to accessing virtual education, many young people abandoned their studies in the department of Nariño, also in the west of the country, and bordering Ecuador. Instead they dedicated themselves to collecting coca leaves to contribute to the economic support of their families. As Genith Quitiaquez, a member of the Indigenous Pastos community, put it, "We can no longer recover these young people."

Conclusion

Dealing with the impact of the health emergency caused by COVID-19 has been a very demanding and exhausting task for CSOs. It has implied profound transformations both in their internal dynamics and in their outreach to communities. This is a learning path that is just beginning, and relies on an openness to change and redesigning work models that strategically combine face-to-face and virtual activities, and which include training to strengthen digital skills, to prevent risks, and on the responsible use of ICTs in communities. This also involves consideration of better ways for people in the regions to access devices and connect to the internet.

It is necessary to listen to the demand for face-to-face activities in particular contexts. In projects related to food security, basic sanitation, violence and psychosocial support, and especially in ethnic and peasant communities, it is very important to prioritise face-to-face activities that ensure a differential[3] and gender approach. In addition, for the privacy of information and security of leaders and activists, it is preferable to address sensitive issues in person and not through digital media.

With respect to virtual activities, it is essential to explore new digital tools, innovative methodologies and participatory dynamics that make these spaces much more enjoyable and attractive to those who are not familiar with information and communications technologies (ICTs).

For CSO management teams, it is necessary to establish a relationship of active listening with professionals working in the territories, and to design strategies for fluid communication that allow for a focus more on the quality of the processes involving the communities and less on administrative protocols. It is also important to implement an ethical concept of care that takes into account their well-being in relation to the risks they experience in the territories.

Finally, it is important to mention that the level of understanding and flexibility that donors show in a contingency situation is key to allowing CSOs to propose viable alternatives in the redesign of their activities, so that the objectives of their projects and the requirements of the communities are met. Exerting too much pressure to achieve goals within specific time frames, without taking into account the context, generates emotional exhaustion and frustration in project teams and can also affect the quality of the process.

Action steps

The following considerations are suggested for organisations that are launching digital projects in Colombia, particularly in disadvantaged communities:

- Include a training component in basic digital skills in the design of the projects for those who require it.
- Share best practices in the responsible use of ICTs and tools for risk prevention in digital spaces.
- Include solutions for access to technological devices and/or internet connectivity for people facing these as barriers to getting online.
- Strategically and creatively propose virtual and face-to-face methodologies according to the realistic potential of the communities to participate, taking into account the nuances of their context.
- Consider the concept of care as a cross-cutting ethical framework for all of an organisation's processes. This should include communication, safety, physical and emotional well-being and care of the communities where work is being done.

2 Departamento Administrativo Nacional de Estadística (DANE), 2021.

3 The differential approach identifies the diverse conceptions, meanings and logics of life and collective and personal thinking shared by people in order to enhance differential actions that materialise the effective enjoyment of their rights. It makes it possible to understand and make visible the dynamics of discrimination and social exclusion, so that from there, actions for transformation to equity and human development can be established.

CONGO, DEMOCRATIC REPUBLIC OF

CIVIC SPACE ONLINE DURING AND AFTER THE PANDEMIC

Bingwa Civic Tech Lab
Providence Baraka
www.bingwa-civictech.org

Introduction

The advent of the coronavirus pandemic has brought different challenges in almost all aspects of the daily lives of citizens around the world and has deepened inequalities in many developing countries.

The measures taken by governments to stop or reduce the spread of the COVID-19 pandemic, such as limiting the movement of individuals, social distancing and travel restrictions, quickly revealed the need to migrate different social dynamics to online platforms in order to ensure continuity. In many African countries, this negatively affected areas that were already struggling and unequal relative to countries in the global North, including in employment, education, health and transport.

Internet access statistics for the Democratic Republic of Congo (DRC) show a marked increase in access in the first year of the pandemic. However, this potential for Congolese citizens to realise their rights online was to a large extent limited by the opportunistic actions of the government, which introduced a new mobile tax, as well as by an increase in gender-based violence online. Both of these narrowed the civic space online.

Civil society organisations nevertheless saw an opportunity to use online platforms to campaign against the new government tax laws, and to raise awareness against online gender-based violence.

An increase in internet access during COVID-19

The DRC is a Central African country with nearly 90.9 million inhabitants, with an estimated internet penetration rate of nearly 23.2% in the first quarter of 2021.[1] In 2019, the country had around 16.35 million internet users on different devices, which represented a 19% penetration rate out of a population of around 88.18 million.[2] This increase of around four percentage points can at least in part be explained by the COVID-19 pandemic that forced many people online, whether to work or to stay in contact with the people they care about around the world.

Despite this, internet access remains a luxury in the DRC – it is one of the most expensive countries in the world to be connected to the internet.[3]

The introduction of a new mobile tax

Digital rights issues – including access, the inclusion of local and marginalised communities in policy making, and censorship – have often been at the centre of advocacy activities of civil society organisations in the country. For example, over the past 10 years, under Framework Law No. 013-2002 of 16 October 2002 governing telecommunications,[4] the country has drawn the attention of activists, both locally and globally, who have pointed to human rights violations enabled by the law. Through this law, authorities have strategically put in place mechanisms to stifle public protests and criticism of the ruling powers by shutting down the internet, including messaging services, and filtering the internet.[5]

This concern with digital rights continued under the "new normal".

In September 2020, while the world was suffering the negative effects of the pandemic, the government, through the Minister of Posts, Telecommunications and New Information and Communication Technologies, announced the establishment of the Mobile Device Registry (RAM).[6] This introduced a mobile device tax (known as the "RAM tax"), under which users of telecommunications services pay between USD 0.17 for a 2G device and USD 1.17 for 3G/4G/+ devices once a month over six months. According to the DataReportal website, the

1 Kemp, S. (2021, 11 February). Digital 2021: The Democratic Republic of the Congo. *DataReportal*. https://datareportal.com/reports/digital-2021-democratic-republic-of-the-congo?rq=congo

2 Kemp, S. (2020, 17 February). Digital 2020: The Democratic Republic of the Congo. *DataReportal*. https://datareportal.com/reports/digital-2020-democratic-republic-of-the-congo

3 https://a4ai.org/mobile-broadband-pricing-usd-2019q2

4 http://www.leganet.cd/Legislation/Droit%20economique/telecommunication/LC.013.2002.16.10.2002.htm

5 Dahir, A. L. (2018, 24 January). There's a decades-old law threatening digital freedom in DR Congo. *Quartz*. https://qz.com/africa/1187727/the-dr-congo-is-using-a-decades-old-law-to-shut-down-the-internet

6 Actualite.cd. (2020, 24 September). RDC: lancement à Kinshasa du Registre des Appareils Mobiles. https://actualite.cd/2020/09/24/rdc-lancement-kinshasa-du-registre-des-appareils-mobiles

number of mobile connections in the DRC increased by nearly one million between 2019 and 2020.[7] However, civil society organisations have expressed concern that this trend will be reversed due to the introduction of the new tax.[8]

Communities were nevertheless quick to exploit some of the means available online to deepen the advocacy already initiated to counter this decision, which weighed heavily on a poor population whose living conditions had been aggravated by the effects of COVID-19.[9]

Twitter spaces played an important role in this process, which brought citizens together, and also saw the participation of several influential figures in the country, including national deputies and Congolese civil society leaders.

An increase in gender-based violence

While the pandemic has meant that many new people are now connected, and many are what we could call "overly connected", this has not been without consequences for new infringements of human rights. In particular, civil society organisations have noted an increase in gender-based violence on the internet, accentuated by the fact that the internet is the new meeting place for many people.

Barely a day goes by in the DRC without a young woman falling victim to sexual or sexist violence perpetrated online. Lacking access to quality education – which may at least offer some context and defence against these assaults – for the most part Congolese women and girls are paying a heavy price socially, but also in their professional capacities as academics, journalists or politicians, among others.[10]

In order to curb, or even stop, the rise of gender-based violence online, civil society organisations including Si Jeunesse Savait, SEFEPADI, BloGoma, Jeunialissime, Oasis and Cuso International initiated the #TechSansViolences ("tech without violence") campaign. #TechSansViolences is an awareness campaign against gender-based violence online, with the aim of alerting internet users, Congolese authorities and the community, and more particularly women, girls and sexual minorities, of the harmful effects of sexual and gender-based violence perpetrated through information and communications technology (ICT) tools.[11] For almost a month, from 22 February to 20 March 2021, the campaign was conducted on the various social media platforms, mainly on Twitter, using the campaign's hashtag.

Conclusion

Online civic space during and after the worst of the pandemic is being pushed both ways. In this sense, it can be said to be both narrowing and expanding.

The internet has played a very important role during the pandemic by mitigating many of its effects through substitution, or taking some processes and services online. However, the government has worked against this by introducing a controversial tax on mobile devices, the main way that Congolese citizens access the internet. At the same time, as more people have come online through necessity in the DRC, there has been an increase in gender-based violence online. These two factors, alongside the high cost of data for the average Congolese citizen, have limited the potential for citizens to properly realise their rights online, including access to information, education and work. Civil society has nevertheless capitalised on an increase in access by Congolese citizens to launch two important advocacy campaigns using social media.

Apart from revealing the resilience of the internet as a critical communications tool, the COVID-19 pandemic has shaped the way civil society organisations conduct their advocacy work around issues related to digital technologies, including digital rights. While the use of social media for campaigning in the DRC is not a new phenomenon, as more people come online, it has grown in prominence as a potentially effective tool for advocacy. That platforms such as Twitter are becoming more useful to the Congolese is suggested by citizen initiatives that have emerged, including SpacesRDC,[12] which provides Twitter users with a weekly calendar for meetings (#TwitterSpaceRDC), to help them align events in the DRC alongside different topics.

At the same time, the new mobile tax introduced by the government during COVID-19 does not necessarily introduce a new focus of resistance – even though advocacy is necessary to push for the law's revision. The government has long been inclined to limit the use of the internet in various ways, and taxing mobile access is just a new way in which this is being done. However, it does suggest an intensification of government limitations, which need to be

7 Kemp, S. (2020, 17 February). Op. cit.

8 Rudi International. (2020, 18 September). Rudi International se joint à d'autres voix pour dire non à la taxe sur les téléphones mobiles en RDC. https://rudiinternational.org/2020/09/18/rudi-international-se-joint-a-dautres-voix-pour-dire-non-a-la-taxe-sur-les-telephones-mobiles-en-rdc

9 Ibid.

10 SOFEPADI. (n/d). Communiqué de lancement de la campagne #TechSansViolences. https://www.sofepadirdc.org/communique-de-lancement-de-la-campagne-techsansviolences

11 Cuso International. (2021, 8 October). Congolese women strengthen their digital skills to fight online violence. https://cusointernational.org/stories/congolese-women-strengthen-their-digital-skills-to-fight-online-violence

12 https://twitter.com/SpacesRDC

addressed by civil society if the internet is to enable the rights of ordinary Congolese.

Action steps

These recommendations draw on the input from different stakeholders involved in digital and human rights in the DRC:

- Civil society should realise both the potential and limitations of the internet as an advocacy tool. Given less than 25% of the population has access to the internet in the DRC, advocacy activities in this regard are only likely to impact most on those already online. In terms of pushing for legislative change, the internet can be a useful tool given that many parliamentarians and prominent civil society organisations are online. Similarly, on internet-specific issues, such as online gender-based violence, social media campaigns are appropriate. However, the limited civic space allowed by the internet needs to be kept in mind when using the internet for broad-based campaigns in the DRC.
- Develop policies conducive to the promotion of internet access and the accessibility of ICTs. Policy revision is necessary in the DRC so that rights-based policy decisions are made that support the affordable take-up of the internet, and in the absence of restrictive regulations such as additional taxation or forms of censorship.
- Immediately revise Law No. 013-2002 to bring it in line with international norms on freedom of expression and association, as well as with government commitments in this regard.
- Through multistakeholder deliberations, revise the Mobile Device Registry (RAM) law, so that unfair taxes do not limit the take-up of the internet by ordinary Congolese who do not have the resources to do so. Encourage the government not to see the internet as a tax resource that cripples its ability to enable the rights of people in the DRC.
- Push for a dramatic lowering in data costs. Through campaigns and multistakeholder discussions, continue to advocate for data costs to come down in the DRC.
- Strengthen the participation of civil society organisations in multistakeholder forums such as the Internet Governance Forum, as a way to build both the capacity and the influence of civil society organisations concerned with digital rights.

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.

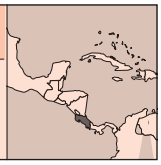
20 Sabbe, B. (2022, 1 February). Grievances, Governance and Gold in the Eastern DRC. *IPIS*. https://ipisresearch.be/weekly-briefing/ipis-briefing-december-2021-january-2022-grievances-governance-and-gold-in-the-eastern-drc

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.

COSTA RICA

ROBOTICS AND AI DURING THE PANDEMIC: THE FUTURE OF AUTOMATED JOBS IN COSTA RICA



Technische Universität München
Yawri Carr

Introduction

Many countries are turning into highly technology-driven and digitised societies due to the COVID-19 pandemic. While Costa Rica is no exception, it raises the issue of how robots and artificial intelligence (AI) are being used in a way that will impact on the future of work.

This shift to automated processes and autonomous systems is being experienced more and more in our daily lives. Intelligent systems are making decisions for us and shaping the way society interacts with and perceives technology.

Although there have been various debates recently on violations of digital rights, many in civil society are still concerned about the lack of recognition of certain fundamental rights nationally, and also in the regional human rights tribunal. Moreover, the shift to a future of automated and autonomous systems also affects how digital rights advocacy should act, and the issues that should be considered important. In this sense, these new challenges require collective action, including the development and revision of public policy and laws, and the strengthening of institutions.

From tourism and agriculture to a future built on automation and autonomous systems

Costa Rica is a country located in Central America that bases its economic activities mainly on tourism, agriculture (coffee, pineapples and bananas) and some industrial activity that includes the manufacturing of computer chips.[1] It is a country with just over five million people,[2] with one of the highest levels of internet coverage in Latin America.[3]

Costa Rica is still considered one of the most solid democracies in the Americas.[4] In the 1990s it was even recognised as one of the most just and equal countries, with one with the highest levels of human development globally.[5] Nevertheless, over the years, concerns have been raised over the country's steady increase in socioeconomic inequalities. By 2018 Costa Rica was considered the eighth most unequal country in the region – and by 2020, due to the COVID-19 pandemic, this inequality had worsened.[6]

The internet has played a fundamental role in activities such as remote work and education, but it is not the only technology used during these difficult times: the use of automation as well as AI has also been growing around the world.[7]

One definition of automation – written in the middle of the 20th century – defines it as the "mechanical combination of numerous operations while adding controls in order to automatically generate a product."[8] Since then the use of the term "output" has been preferred over "product", but it is nevertheless important to establish that unlike AI, automation does not imply "intelligence", but is about executing an operation automatically.[9]

Costa Rica's first signs of automation impacting on the kinds of work available for people could be seen in simple ways such as the progressive automation of the job of a security guard in a parking lot. Nowadays, in many shopping centres, machines and booms control the entry and exit of cars from parking lots and no human operator is required to do this.

1 Rodríguez, Ó. (2021, 22 July). Demanda global de 'chips' impulsa a Intel a doblar su apuesta por Costa Rica. *El Economista*. https://www.eleconomista.net/tendencias/Demanda-global-de-chips-impulsa-a-Intel-a-doblar-su-apuesta-por-Costa-Rica-20210722-0020.html

2 https://datos.bancomundial.org/indicator/SP.POP.TOTL?end=2020&locations=CR&start=2020

3 Rojas, E., Poveda, L., & Grimblatt, N. (2016). *Estado de la banda ancha en América Latina y el Caribe 2016*. CEPAL. https://www.cepal.org/es/publicaciones/40528-estado-la-banda-ancha-america-latina-caribe-2016

4 OEA. (2022, 8 February). *Misión de la OEA saluda al pueblo costarricense tras la exitosa jornada electoral del 6 de febrero*. https://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-005%2F22

5 Programa de las Naciones Unidas para el Desarrollo. (1991). *Desarrollo Humano Informe 1991*. https://hdr.undp.org/sites/default/files/hdr_1991_es_completo_nostats.pdf

6 Muñoz, D. (2022, 23 February). Costa Rica avanza sin freno hacia una sociedad cada vez más desigual. *Semanario Universidad*. https://semanariouniversidad.com/pais/costa-rica-avanza-sin-freno-hacia-una-sociedad-cada-vez-mas-desigual

7 Chamola, V., Hassija, V., Gupta, V., & Guizani, M. (2020). A Comprehensive Review of the COVID-19 Pandemic and the Role of IoT, Drones, AI, Blockchain, and 5G in Managing Its Impact. *IEEE Access, 8*, 90225-90265. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9086010

8 Harrington, D. F. (1958). Automation's Impact on Industrial Safety. *Cleveland State Law Review, 7*(2).

9 Defense Science Board. (2016). *Summer Study on Autonomy.* Office of the Under Secretary of Defense for Acquisition, Technology and Logistics. https://www.hsdl.org/?view&did=794641

Automation eventually expanded into our notion of "autonomous systems". Different to the phenomenon of automation, an autonomous system does not just work with minimum or no human intervention, but also possess what we might call cognitive capacities, such as "intelligence" through the use of AI, and an "orientation" towards a goal, that are essential to the autonomy of the system.[10]

But what makes AI-driven technology different from other technologies that could put human rights at risk? AI has some features that more traditional technologies do not. There is, for example, its level of autonomy, requiring less and less human intervention. It can be unpredictable, because it is uncertain what action a machine collecting and processing data will take. Finally, there is a lack of transparency, as a person cannot clearly know why a specific decision or action was taken.

During the COVID-19 pandemic, countries such as China used autonomous systems extensively in the form of AI to detect possible new infections, and robots for medical care and for disinfection.[11] As discussed below, similar developments have been seen in Costa Rica.

According to the Inter-American Development Bank, 68% of jobs in Costa Rica could be replaced by robots.[12] Robotics is considered the most important trend within the life science and manufacturing sectors in Costa Rica, and 64% of companies in the country say that they will adopt robotics processes in their enterprises.[13] The country has the potential to grow this field even more. By 2019, the number of graduated professionals on mechanical and electrical engineering rose to 700.[14]

The rise of autonomous systems during the pandemic

Different to highly automated countries such as Japan, Germany and China,[15] Costa Rica does not have a solid foundation of using robots or AI as workers. However, Costa Rica is deploying the technologies rapidly, mainly motivated by the critical necessities brought on by the coronavirus. Therefore, the ways Costa Rica has been introducing automation and autonomous systems in the context of COVID-19, how this has impacted current employment opportunities and will impact the future of work, how this will introduce inequalities, and the role of digital rights and civil society advocacy in this context are critical questions.

In light of the many deaths of health care personnel due to COVID-19 and their huge risk of exposure to the virus on a daily basis,[16] one of the first measures implemented in Costa Rica was telemedicine in various forms.[17] For instance, it was used in the country for several applications: advising on medical procedures, collecting medical data, and even remote medical examinations.[18] Robots were also used for disinfecting hospitals,[19] as well as for security.[20]

Robots play increasingly more decisive roles in society, including when the cognitive capacities of autonomous systems are put to work in critical moments of health care in which lives are at stake. Last year, Costa Rica became the first Central American country using a robot to guide doctors in a knee-replacement operation.[21] The doctors said that in highly complex surgeries such as this, the robot was able to work with more precision, resulting in a quicker recovery for the patient.[22] The use of AI in health care, as suggested, is already taking place. There are algorithms that interpret data through sensors and produce health diaries for patients in Costa Rica,[23] with doctors notified about changes in the data.[24] There is also a robot that prepares

10 Roff, H. M. (2019). Artificial Intelligence: Power to the People. *Ethics & International Affairs, 33*(2), 127-140. https://doi.org/10.1017/S0892679419000121

11 Toh, M., & Wang, S. (2020, 24 February). Drones. Disinfecting robots. Supercomputers. The coronavirus outbreak is a test for China's tech industry. *CNN*. https://edition.cnn.com/2020/02/23/tech/china-tech-coronavirus-outbreak/index.html.

12 Ripani, L., Kugler, A., Kugler, M., Soler, N., & Rodrigo, R. (2020). *El Futuro del Trabajo en América Latina y el Caribe: ¿ Cuál es el impacto de la automatización en el empleo y los salarios?, p. 13*. Banco Interamericano de Desarrollo. https://doi.org/10.18235/0002960

13 https://www.cinde.org/es/tecnologias/robotica#hero

14 Ibid.

15 International Federation of Robotics. (2021, 27 January). Robot Race: The World's Top 10 automated countries. https://ifr.org/ifr-press-releases/news/robot-race-the-worlds-top-10-automated-countries

16 ElPais.cr. (2020, 23 October). Costa Rica reporta 13 fallecimientos por Covid-19 entre personal médico de la CCSS. *ElPais.cr*. https://www.elpais.cr/2020/10/23/costa-rica-reporta-13-fallecimientos-por-covid-19-entre-personal-medico-de-la-ccss

17 CAF et al. (2020). *Las oportunidades de la digitalización en América Latina frente al COVID-19*. CAF & United Nations. https://repositorio.cepal.org/bitstream/handle/11362/45360/4/OportDigitalizaCovid-19_es.pdf

18 PAHO. (2020). *Asegurando la continuidad del tratamiento de pacientes crónicos en tiempos de pandemia: Telesalud en Costa Rica*. https://www.paho.org/es/historias/asegurando-continuidad-tratamiento-pacientes-cronicos-tiempos-pandemia-telesalud-costa

19 Rodríguez, I. (2021, 12 February). Llega a Costa Rica robot que promete 'destruir' virus causante de covid-19. *La Nación*. https://www.nacion.com/ciencia/salud/llega-a-costa-rica-robot-que-promete-destruir/N2ECJVF67NADTN46TVGVXF42QQ/story

20 Ibid.

21 de la Cruz, A. (2021, 18 June). Robot asiste a ortopedistas en cirugía de reemplazo de rodilla. *CCSS Noticias*. https://www.ccss.sa.cr/noticias/salud_noticia?robot-asiste-a-ortopedistas-en-cirugia-de-reemplazo-de-rodilla

22 Jerez, M. (2021, 18 June). Robot guía a médicos en cirugía de rodilla: CCSS es pionera en Centroamérica. *AM Prensa*. https://amprensa.com/2021/06/video-robot-guia-a-medicos-en-cirugia-de-rodilla-ccss-es-pionera-en-centroamerica

23 https://www.cinde.org/es/tecnologias/ia-machine-learning

24 Ibid.

your medical prescriptions in less than one minute, including how and when the medicine should be taken, increasing efficiency, reducing costs, and avoiding human flaws. These are just examples of the current, emerging narrative about automated and autonomous systems working in health care in the country.[25]

Rising inequalities and human rights at stake

Automation has also been introduced into tourism, one of the most important economic activities in Costa Rica. Some of the most tangible cases can be seen in the Chorotega region, where many of the most visited beaches and resorts are located.[26] This region suffered hugely due to the pandemic, going from the second most prosperous region in 2019 to the second poorest by 2020, which means that poverty increased by 52%.[27] Nowadays, lots of hotels do not need personnel at reception, because there is an automated machine process that registers guests.[28]

While automation and autonomous systems provide advantages such as not getting infected by diseases nor needing social security, three of four jobs in Latin America could be replaced by robots.[29] Nonetheless, since human personnel in the region is cheap, it could still be better for some to stick with cheap human labour than to buy expensive robots.[30] People under poverty have been the most affected, as they cannot work from home nor do they have the necessary education to work on new technological innovations.[31]

However, technological advancements cannot and should not be stopped. The negative impacts of the pandemic could also be more serious if we did not have access to the internet and other technologies that have helped us in numerous ways. Nevertheless, risks to human rights are latent, meaning responsible innovation research is necessary. The most significant question for an already unequal country is how to advance technological development while leaving no one behind.

25 La Republica. (2020, 17 November). Meditek pone a disposición robots para potenciar las farmacias inteligentes en Costa Rica. *La Republica*. https://www.larepublica.net/noticia/meditek-pone-a-disposicion-robots-para-potenciar-las-farmacias-inteligentes-en-costa-rica

26 Fernández Aráuz, A. (2021). *Desempleo, pobreza y desigualdad en Costa Rica durante la pandemia por el COVID-19: Consideraciones para una recuperación resiliente*. Konrad-Adenauer-Stiftung. https://www.kas.de/es/web/costa-rica/einzeltitel/-/content/desempleo-pobreza-y-desigualdad-en-costa-rica-durante-la-pandemia-por-el-covid-19

27 Ibid.

28 Ibid.

29 Ibid.

30 Ibid.

31 Lustig, N., & Tommasi, M. (2020). El COVID-19 y la protección social de los grupos pobres y vulnerables en América Latina: un marco conceptual. *Revista CEPAL, 132*, 283-295.

The role of civil society

In terms of legislation, the country presents several challenges that need to be tackled in order to manage science and technology responsibly. AI, robotics and other autonomous systems use large amounts of data in order to work.[32] Given all the recent developments, civil society priorities in Costa Rica should shift to address the new challenges and in a way that addresses the shifting relationship between technology and society. The country still lacks the policy, legal and practical mechanisms that are required in order to tackle the challenges that these new technologies introduce.

There is a need to advocate for an AI strategy in the country. The AI strategy recently approved in Brazil[33] provides a good model that might be suitable for Costa Rica. Brazil's strategy is principle-based and risk-based regulation. Applying a similar one in Costa Rica would help the country contextualise the implementation of the technologies in a concrete way, establishing directly responsibilities, including who will coordinate their implementation, what goals need to be meet, and how long it should take to accomplish a goal, with details such as how implementation will happen, and the financial costs.

Further, in a datafied society, other policies should be taken into consideration. Even though access to public information is contemplated under articles 11, 27 and 30 of the Costa Rican constitution,[34] civil society has revealed that institutions do not comply with information requested.[35] The lack of a specific law on access to information has made it very hard for transparency and accountability, because there was not a legitimate procedure to follow when asking for relevant public information, nor a body that ensured it. Therefore, civil society has demanded a law for accessing public information, not just creating the legal framework for institutions to do this as the constitution already establishes, but actually making it mandatory, with sanctions to those public officials who deny information requests.[36] It was not until May 2022 that the first law

32 https://www.sas.com/es_cl/insights/analytics/what-is-artificial-intelligence.html

33 Ministério da Ciência, Tecnologia, Inovações e Comunicações. (2021). *Estrategia Brasileira de Inteligencia Artificial*. https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ebia-diagramacao_4-979_2021.pdf

34 http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=871

35 Abriendo Datos, et al. (2021, 28 September). Bicentenario sin derecho pleno de acceso a la información. *Delfino*. https://delfino.cr/2021/09/bicentenario-sin-derecho-pleno-de-acceso-a-la-informacion

36 Ibid.

of this kind was approved in Costa Rica.[37] Nevertheless, the law is still the subject of discussion within civil society, as it still does not establish an explicit obligation for the exercise of the right to access information, beside others. From now on, the role of civil society will be to keep on demanding this, as well as becoming very vigilant about the law's application, because it is fundamental for a transparent and accountable deployment of robotics and AI.

Finally, the data protection agency in the country is also very weak. It only responded to one of 236 complaints received in 2020.[38] At the same time, there is not a law against discrimination in the country that could also tackle biases that technologies generate. In telemedicine, data security and confidentiality in information systems must also be widely improved.[39]

Conclusions

This report shows a country that once was really prosperous and that had really strong institutions that were guided by the rule of law and that protected the digital rights of its citizens extensively, despite the absence of the laws mentioned above. However, Costa Rica has been experiencing alarming levels of increasing inequality that should really worry its citizens.

In a country in which automation and autonomous systems are a new concept, but where their use is growing in many fields of the working environment, it is fundamental that civil society organises to understand these new challenges and to advocate for possible solutions. It is also necessary that opportunities are created for all stakeholders to understand and prepare for this changing and dynamic field, including policy makers, business leaders and academics. Costa Rica still has to face many challenges in order to take advantage of the opportunities offered by telemedicine and other new technological processes. To advance in these areas it is necessary to strengthen training and administrative processes, and build capacity in the use of robotics and information technology. It should not just be about providing access to the internet and new technologies, nor creating education and training plans for professionals and users. Capacity building should instead be an integral process that unpacks the relationship between the deployment of technology and its impacts and consequences on society. A better understanding among stakeholders when addressing the needs of the country's AI-driven future would make debates and discussions more meaningful.

Building private-public alliances to deal with this future is also fundamental. Businesses, entrepreneurs and academics are advancing quickly in terms of developing innovations, but the public arena is staying behind, not seeming to understand what is going on.

At the same time, the development and review of laws, as well as the reform of institutions, such as the data protection agency that has not been efficient nor protective of citizen rights, needs to happen urgently. The future of work must be responsibly built.

Action steps

The following action steps are proposed:

- Organise meetings with different stakeholders for advocating the creation of a principles-based AI strategy.
- Monitor the needed reform of the data protection agency so that it is efficient and attends to every complaint effectively.
- Increase transparency and accountability through the new law on access to public information, explicitly including the obligation to do so, so that it is effective in practice.
- Approve a non-discrimination law that can also deal with biases produced by new technologies using AI, as well as those biases that affect the dynamics of workers and their recruitment.
- Provide training for people whose jobs are being automated or are likely to be in the future, so that they can build their capacity to be employable in the new market.

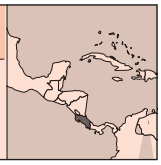
37 Madrigal, L. M. (2022, 27 April). Nueva ley de acceso a información pública reduce a la mitad plazo de respuesta de instituciones públicas. *Delfino*. https://delfino.cr/2022/04/nueva-ley-de-acceso-a-informacion-publica-reduce-a-la-mitad-plazo-de-respuesta-de-instituciones-publicas

38 Ruiz, G. (2021, 12 May). Prodhab tarda de diez meses a un año en resolver denuncias. *CRHoy.com*. https://www.crhoy.com/nacionales/miercoles-prodhab-tarda-de-diez-meses-a-un-ano-en-resolver-denuncias

39 Valerio, M. (2020, 14 September). Costarricenses podrán conocer más acerca de la telemedicina y sus beneficios. *SINART Costa Rica Medios*. https://costaricamedios.cr/2020/09/14/costarricenses-podran-conocer-mas-acerca-de-la-telemedicina-y-sus-beneficios

COSTA RICA

"WE ALL PREFER TO SEE EACH OTHER IN PERSON": GIRLS, THE PANDEMIC AND DIGITAL TECHNOLOGIES



Cooperativa Sulá Batsú
Kemly Camacho
https://www.sulabatsu.com

Introduction

This report is a summary of the progress of research carried out by the Sulá Batsú Cooperative in Costa Rica and Central America on girls, the pandemic and digital technologies. Since 2013, the Cooperative has been working on foregrounding the concerns and proposals of girls aged 10 to 18 years in the Central American region within the broader process of the social appropriation of digital tools.

Context

The State of Education of Costa Rica in 2021 report[1] classifies the last four years as an "educational blackout". This is not only due to the consequences of the pandemic on preschool, primary and secondary education, but also because prior to the health crisis, the deprioritisation of quality education implied a substantive setback in the educational process for many young people, to the point that Costa Rica became a regional example of stagnating educational standards.

This same report shows that half of the students in the country during the pandemic did not have the opportunity to adequately receive an online or hybrid education as a result of connectivity problems (either a lack of access or poor signal quality) or because their families did not have access to digital devices.

This situation aggravates the exclusion of young people with fewer resources, since private education continued to develop over this same period, widening the conditions of inequality for the new generations. This occurred despite the principle of universalisation and compulsory education that is established in the country's constitution. In Costa Rica, eight out of 10 boys and girls complete primary education, only 60% complete secondary education, and only 8% complete higher education.

We have, at the Cooperative, been interested in how this context affects girls, and in this report we discuss the concerns and proposals for a more meaningful use of the internet in the country that they themselves have raised.

Before detailing the results of this qualitative work and with the purpose of giving a little more context, some relevant characteristics of girls from six to 12 years old in Costa Rica are presented in Table 1.

TABLE 1.
General characteristics of girls aged 6 to 12 in Costa Rica

Characteristic	Percentage of girls aged 6 to 12
Are studying	98.6%
Have social security insurance	92%
Live in urban areas	71%
Have functional difficulties	19,2%
Are physically punished	50%
Have parents or guardians who consider it correct to physically punish their daughters	24%
Do unpaid chores at home (28 hours per month)	71.4%
Do paid chores for the family	5%
Poor and very poor households with at least one girl	48.7%
No one takes care of them	1.4%

Source: INEC, 2018-2022

1 https://programatic-as.com/la-voz-de-las-chicas-del-centro-de-america

From these data, it should be noted that the majority of girls are enrolled in the school and college system, but a majority must dedicate a significant part of their time to housework. In addition, many girls live in conditions of poverty and extreme poverty, and at least half receive physical punishment as a form of discipline.

The role of the internet for girls during the pandemic

We conducted a series of open interviews with 10 girls – five from rural areas and five from urban areas – in relation to the role of the internet in their lives during this period of "educational blackout". The girls were all aged 10 to 12 years old. This work has been complemented by a discussion of two case studies that are part of a series of case studies on the use of the internet for the development of activities outside the school environment by young people.

In this report, the anonymity of the girls is maintained. To this end, profiles are established based on the common elements that have emerged from the analysis of the conversations. These have been written from the voice and perspective of the girls.

Profile built from interviews with urban girls

We had a short interruption of classes for a few weeks, but later everything was reorganised and we began to receive virtual classes. At first it was very strange to get used to this new way of having lessons. However, very quickly we began to see it as normal.

Even other activities in which we participated such as sports, arts, languages, began to be done virtually. We left off a lot of these extra activities because they weren't pretty online. But we made new friends on the internet during the pandemic because after school – for fun – we stayed playing in groups of four or five.

We can say that there was a difference within the class depending on the internet because some had a poorer connection and therefore could not do the same activities as the rest, both in class and outside of it.

In addition to playing, we did extra activities that we liked, such as taking online courses to learn new things according to the tastes of each one. We still like to take these courses.

We used the internet much more intensively during the pandemic than before, but we have decreased its use again now that we are back in person because we have less time to use the internet. We all feel more comfortable with face-to-face interaction than virtual because we have more direct contact.

Boys use the internet more than us even now that we're back in school. They use black humour a lot – it's very rude to relate to – and they build jokes with digital tools, like rude memes. They are also more interested in online sports than we are.

We don't like this kind of humour so much, or video games. We use more WhatsApp to talk to each other. When we were younger, we wanted to be YouTubers; now we are more interested in TikTok.

The internet seems to me to be very important for life because of the information part, but it worries me because of the addictive issue. We all know that there is that danger, but we like it a lot. I try to do other things outside of the connection to avoid addiction.

After the pandemic, the class became much more aggressive, especially the boys who became more violent. They fight constantly, and it's becoming second nature. We also notice that the children in the smaller classes are also more aggressive than before the pandemic. We believe that it is because of the content they see on the internet, especially video games and videos in general.

Profile built from interviews with rural girls

We take most of the classes through guides that we receive and send over the internet. We studied like this during the pandemic because the internet connection was not good in the places where we live and we had classmates who did not have internet. We connected once or twice a week, but it was very difficult because there were many differences between the classes and it became very complicated. We also used it to do our own research and complement the studies when we had a connection.

The biggest issue was access and signal quality, even more so than whether or not we had a device. Even if it was with the mobile phones of our fathers or mothers, we communicated by WhatsApp. We made many efforts to connect, such as walking to look for a signal wherever it was, borrowing a signal from neighbours, buying a plan when possible. Teachers also made many efforts – for example, some made individual calls to follow up with students who were unable to connect.

We noticed that the boys tried to connect to the classes less than the girls. We always made more effort to comply. They lost interest faster whether or not they had connectivity. But all of us prefer face-to-face classes much more.

For fun, we use the internet sometimes when we can, but mainly to do things by ourselves, such as play games or watch a video or listen to music, but not to do things together.

During the pandemic, we were able to do a lot of things outside – we weren't as cooped up. For example, going to the river, helping my grandmother with the gardens, helping with the animals, working in

the fields with my family, going to visit close family, playing with my brothers, sisters, cousins. We didn' t feel very isolated because we could do things outside. We believe that we learned a lot by doing these things and that we do less when going to school, because we have less time there. We interacted with many people from the same family.

The internet made a difference between those of us who could connect and those of us who couldn' t. We believe that it is our right to have access to the internet no matter where we live. We should all be able to study quietly with connectivity.

Two case studies on the appropriation of the internet by girls and young women in the pandemic

In addition to the analysis of the role of the internet in the educational process of girls, case studies on internet use for self-organisation by girls and young women during the pandemic were also developed. Two of these cases studies were developed in Nicaragua and Guatemala, with both processes supported by our Sulá Batsú Cooperative. For the development of the case studies, a review of digital resources was made and a public forum was held with the participation of the young female leaders.

Case 1: Colectivo Tonantzin, Nicaragua

This is a group of girls and adolescents (10 to 18 years old) that emerged from a training programme in the safe use of digital technologies led by Sulá Batsú for Central America. They belong to an art group dedicated to engraving. During the pandemic, their families saw job opportunities greatly reduced with the economic consequences that this implies.

They decided to organise themselves to sell their prints digitally. They carried out various online sales campaigns and managed not only to generate their own income for the group and their families, but also to position themselves nationally and internationally as artists. With this leap through using the internet, they strengthened themselves as organised young women and consolidated the organisation of their collective.

"Belonging to the collective and having managed to sell our art nationally and internationally through the internet and help our families has allowed us to strengthen ourselves as young women and believe in ourselves," said Julieth Valle, a member of Colectivo Tonantzin, in an interview.

Case 2: Colectivo Bats, Guatemala

Colectivo Bats is a group of mostly young women, aged 12 to 19, led by one of our female leaders from Guatemala. The group has the motto "We are and we have the strength of the volcanoes." The collective is dedicated to social and community work using street art and popular sports.

They indicated that online social networking is useful for them because it allows the work they do to be seen. "We are the leaders, but we don't always have money. We use social networks to generate our resources from the dissemination of our work. We create contacts and alliances little by little, and we get them to support the work we do," said Ester Salazar, a member of the collective.

During the pandemic, they used the internet to encourage people to help create "dignified packages" that were used to support families in greatest difficulty in Jocotenango, where they work. "Through this campaign we managed to distribute packages to many families. We collected things and distributed them with our bicycles," Salazar said.

"Thanks to this process we were able to break stereotypes about everything that young women can do when we organise ourselves and use the internet to do things that come from our hearts. We work against stereotypes and against the system. It also helped us to work collectively," she said.

Conclusions

It is urgent to listen to girls and young women. They have particular situations determined by their age and gender that are decisive for the construction of local actions and the definition of public policies. It is urgent to build proposals based on their conditions, always listening to their voices and building processes with them, where they are truly involved.

It was already known that the difference in quality internet access was substantial between rural girls and urban girls. This was confirmed once again in the profiles that we developed through our work. However, it is important to appreciate the different strategies used by rural and urban girls to deal with the pandemic.

Urban girls turned to the internet to get through the pandemic, not only studying with greater ease online, but also getting together to play games with their friends and taking extra courses available online on topics that interested them. Several extra class activities that they organised also took place online.

Rural girls were less confined and many of their activities were able to continue in open spaces. They learned new things through their family interactions and being outside. Despite the fact that they were not able to complete their formal education in good conditions – and despite the multiple efforts of their teachers – they did not stop learning. These learnings that took place in their rural environments, and through interacting with their families and other children close to them in the communities, are not

properly acknowledged as part of their education over the past two years.

It is also very important to acknowledge the innovative social uses of digital technologies by girls and young women, as briefly described in the two case studies presented. As shown, girls and young women launched exceptional initiatives using the internet. It is necessary to encourage these uses: the internet allowed them to organise, empower themselves and support their families and communities. The encouragement of these uses of digital tools should be part of the educational processes of girls.

Girls identified differentiated uses of digital technologies compared to boys, both in rural and urban areas. It is urgent to pay attention to these differences, analyse them and determine if any interventions are necessary to ensure that young people's interaction with the internet is healthy and productive.

Recommendations and action steps

It is essential to give girls a voice in the construction of digital strategies so that they can influence the exercise of digital rights.

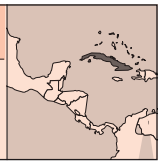
During the pandemic they have lived in and transformed their digital world based on their age, where they live, and gender. These experiences should not be underestimated in the construction of educational policies, and other policies impacting on children's rights and community actions. Contact with digital technologies and the differences that this produced in their lives has not left them indifferent to the potential of these technologies to bring about change.

From their point of view, girls and boys have different uses of digital technologies. They link an increase in aggressiveness among their peers with access to digital technologies and the internet and how it is used. It is essential to analyse this perception in greater depth so that it can inform public and educational decisions.

Our Cooperative will continue working with the girls, especially in relation to their use of the internet, to 1) position their voice, 2) strengthen them, and 3) encourage initiatives where they can support themselves, their families and communities, because this potential interests them very much.

CUBA

INTERNET ACCESS AS A NEW ENGINE FOR SOCIAL MOBILISATION IN CUBA



RedesAyuda
David Aragort
https://redesayuda.org/

Introduction

In recent years, Cuba has experienced a progressive expansion of internet access among its citizens, partially motivated by economic reasons. However, the connection with the rest of the world has caused deep changes in society, and has presented a great challenge for its rulers, who have historically relied on censorship and isolation to maintain control and power. With greater access to information, people have been able to question the "truth" transmitted by the country's traditional media and have also been able to compare their living conditions to those found in other countries.

For this reason, the regime has tried to control the activities of its citizens on the internet through blocking, filtering, throttling, new laws and threats. These, however, have not been enough to stop civil society organisations from connecting with a large diaspora that seeks political changes and an expansion of civil rights and liberties in the country, turning the internet into one of the main triggers of the biggest demonstrations that the country has seen in recent decades.

The ground is now laid for a new era of activism on securing the right to internet access in the country, largely due to the pro-democracy demonstrations that occurred during the COVID-19 pandemic, calling for humanitarian aid to enter the country, and for regime change.

Internet access in Cuba: A story that has just begun

Public access to the internet in Cuba is a relatively recent phenomenon. It was not until 2013 that the country had access to high-speed internet through the submarine cable ALBA-1,[1] which allows download speeds up to 3,000 times faster than those that had been available until then.[2] The commissioning of ALBA-1 prompted the Cuban regime to open more than 100 internet cafés owned by the state, charging the equivalent of USD 4.5 per hour for using the internet[3] – an extremely high price considering the average monthly salary in Cuba.

In 2015, as a result of the rapprochement between the government of Barack Obama and the Cuban regime, and the latter's promises to improve internet access for citizens, the decision was made to temporarily reduce prices in these internet cafés by more than 50%.[4] While this was a significant improvement, it was still prohibitive for most Cubans. That same year, the regime announced its plans to establish 35 Wi-Fi hotspots in public spaces on the island.[5] In 2016, a spokesperson for the Empresa de Telecomunicaciones de Cuba (ETECSA), the state company that maintains the monopoly of telecommunications in the country, announced plans to bring broadband internet to homes and businesses.[6]

The most significant step came in 2018, when ETECSA began offering its users internet connections on their mobile phones through a 3G network, even though this service continued to be prohibitive for most of the country's inhabitants, as mobile data packages were priced at USD 7 for 600 MB and USD 30 for 4 GB.[7] In 2019, another step in favour of internet access was taken through the legalisation of private Wi-Fi networks. However, the owners of these networks are not able to sell access to them, maintaining ETECSA's telecommunications monopoly on the island.[8] That same year, ETECSA began to operate its 4G/LTE network.[9]

1 https://www.submarinecablemap.com/submarine-cable/alba-1

2 Frank, M. (2013, 22 January). Cuba's mystery fiber-optic Internet cable stirs to life. *Reuters*. https://www.reuters.com/article/us-cuba-internet-idUSBRE90L13020130122

3 Oppmann, P. (2013, 6 August). Internet access now a reality for some Cubans, but not cheap at $4.50 an hour. *CNN*. https://edition.cnn.com/2013/08/05/world/americas/cuba-online-access

4 Associated Press. (2015, 18 February). Cuba Cuts the Price of Internet Access. *NBC News*. https://www.nbcnews.com/news/world/cuba-cuts-price-internet-access-n308591

5 Trotta, D. (2015, 18 June). Cuba to create first Wi-Fi signals for the public at large. *Reuters*. https://www.reuters.com/article/cuba-internet-idINKBN0OY2EY20150618

6 Weissenstein, M. (2016, 1 February). Cuba says it will launch broadband home internet project. *Associated Press*. https://apnews.com/article/8d87e43964ab46d197289b257fbd3ff9

7 Reid, D. (2018, 5 December). Cuba to roll out mobile internet for the first time. *CNBC*. https://www.cnbc.com/2018/12/05/cuba-to-roll-out-mobile-internet-for-the-first-time.html

8 Marsh, S. (2019, 29 May). Cuba legalizes private Wi-Fi networks in bid to boost connectivity. *Reuters*. https://www.reuters.com/article/us-cuba-internet/cuba-legalizes-private-wi-fi-networks-in-bid-to-boost-connectivity-idUSKCN1SZ2UD

9 Cubadebate. (2019, 14 October). Cuba avanza en la habilitación de la tecnología 4G/LTE. *Cubadebate*. http://www.cubadebate.cu/noticias/2019/10/14/cuba-avanza-en-la-habilitacion-de-la-tecnologia-4g-lte

A joint investigation between the organisations CONNECTAS and YucaByte argued that one of the main reasons why the Cuban regime has been so interested in increasing internet access is economic, since revenues from exports of "telecommunications, transmission and supply of information" are among the main three categories of services exports in the country, being only surpassed by those related to "social services and human health"[10] and "accommodation, supply of food and beverages". This can be explained in part by the migration of approximately 14% of the country's total population, who, in order to keep in communication with their relatives, must send mobile top-ups from abroad to the state telecommunications monopoly ETECSA.[11]

Censored almost from its inception

In addition to access barriers related to infrastructure and connectivity, the internet in Cuba has been partially censored since its inception – a reality that is not limited to the internet, since almost all the traditional media are controlled by the state.[12]

It is known that since at least 2016, ETECSA has been filtering text messages that contain some keywords that are uncomfortable for the regime, such as "freedom" or "human rights".[13] In 2017, an investigation revealed that access to at least 41 websites was being blocked from the Wi-Fi hotspots that Cuba had installed in certain public spaces. These blocks were mainly aimed at independent media outlets and pro-democracy and human rights websites.[14] Two years later, during the 2019 constitutional referendum, several websites belonging to independent media outlets were blocked. In this case, the evidence showed that the techniques used to block the websites were more sophisticated than those documented years before.[15]

In 2019, the regime also approved Decree Law 370, which was criticised by many civil society organisations for representing a threat to freedoms on the internet.[16] That same year, the European Parliament adopted a resolution in which it "calls on the Cuban Government to stop imposing online censorship and to stop blocking internet sites and restricting access to information."[17]

Pandemic, repression and social media as a tool

The advances in internet connectivity in Cuba occurred before the arrival of the COVID-19 pandemic. This meant that during the quarantine, Cubans had some means to stay connected that they did not have previously. However, this caused the regime to increase its efforts to try to silence dissenting voices on digital platforms, both through the temporary interruption of internet service to certain individuals and through harassment and arbitrary arrests.[18] The internet nevertheless also allowed civil society organisations and activists to show the reality of the country and express their discontent despite not being able to leave their homes. An example of this was the case of Denis Solís, a rapper and member of the San Isidro Movement who, days before being arbitrarily arrested and imprisoned, broadcast the moment in which an official harassed him inside his residence live on his Facebook account.[19]

The San Isidro Movement is a group of Cuban artists and intellectuals who fight for an expansion of civil rights and liberties in Cuba. Days after Solís' arrest, several members of the group decided to start a hunger and thirst strike at its headquarters in Havana to demand the release of their colleague, but the strike ended on the night of 26 November 2020, when state security forces raided the headquarters and arrested them.[20] While this was happening, ETECSA partially blocked access to some social media platforms and instant messaging applications such as Twitter, YouTube and WhatsApp. Just a few days later, a new partial

10 For example, in the past Venezuela and Cuba had an agreement where Venezuela had to pay with oil for the services of Cuban doctors sent there.

11 Borrero Batista, D. (2022, 2 February). ETECSA, el negocio cubano inmune al embargo. *CONNECTAS*. https://www.connectas.org/etecsa-negocio-cubano-inmune-al-embargo

12 BBC News. (2018, 13 March). Cuba profile - Media. *BBC*. https://www.bbc.com/news/world-latin-america-19578348

13 Frank, M. (2016, 5 September). Cuba government filtering mobile text messages, dissidents say. *Reuters*. https://www.reuters.com/article/us-cuba-censorship-idUSKCN11B265

14 Xynou, M., Filastò, A., & Basso, S. (2017). *Measuring Internet Censorship in Cuba's ParkNets*. OONI. https://ooni.org/post/cuba-internet-censorship-2017

15 Pérez Pujol, E., Filastò, A., & Xynou, M. (2019, 26 February). Cuba blocks independent media amid 2019 constitutional referendum. *OONI*. https://ooni.org/post/cuba-referendum

16 Access Now. (2020, 17 June). Statement: International support for the petition to declare Decree-Law 370 unconstitutional in Cuba. https://www.accessnow.org/statement-international-support-for-the-petition-to-declare-decree-law-370-unconstitutional-in-cuba; Reporters Without Borders. (2020, 6 May). Cuba and its Decree Law 370: annihilating freedom of expression on the Internet. https://rsf.org/en/news/cuba-and-its-decree-law-370-annihilating-freedom-expression-internet

17 European Parliament. (2019, 28 November). Resolution (EU) 2019/2929 of 28 November 2019 on Cuba, the case of José Daniel Ferrer. https://www.europarl.europa.eu/doceo/document/TA-9-2019-0073_EN.pdf

18 Mattiace, T. (2020, 19 October). Cuba's Government Targets Social Media Influencers. *Human Rights Watch*. https://www.hrw.org/news/2020/10/19/cubas-government-targets-social-media-influencers

19 https://www.facebook.com/denis.solisgonzalez.5/videos/790464094872551

20 BBC. (2020, 27 November). Cuban police raid HQ of dissident San Isidro Movement. *BBC*. https://www.bbc.com/news/world-latin-america-55098876

blocking of Twitter and Facebook was reported, coinciding with calls for demonstrations on the occasion of Human Rights Day.[21]

A month earlier, international organisations had made a public call to ETECSA and asked the company to guarantee internet access on the island, as well as to be transparent and explicit about the reasons behind the apparent blocking of Telegram and some virtual private network (VPN) services, and to fix any disruptions that could be affecting the quality of service.[22] However, over the following months, there was an increase in reports of selective cuts of mobile phone and internet services for journalists and activists.[23] This practice has apparently been increasing because, unlike the blocking of websites, it is harder to verify and has less collateral impact on the public in general.

2021, a turning point

The expansion of internet access made it possible to connect activists in Cuba with those who have had to go into exile. This was evidenced by the #SOSCuba campaign, which sought to pressure the Cuban regime into allowing humanitarian aid into the country amid the health crisis that the province of Matanzas was going through due to the high increase in COVID-19 cases. As in many other provinces, its health care centres had collapsed and there was a shortage of medicines, food and hygiene products.[24]

But the health crisis caused by the pandemic is not the only reason why discontent with the regime has increased. According to the director of YucaByte, Norges Rodríguez, because the expansion of internet access has meant that people who previously did not have access to alternative sources of information now have it, many citizens have begun to realise that the regime is largely to blame for the deep economic crisis that has been exacerbated by the pandemic, rather than an "external enemy", as the authorities claim.[25]

In February 2021, the song "*Patria y Vida*" (Homeland and Life) was released, which featured internationally recognised Cuban artists and one of the members of the San Isidro Movement, Maykel Osorbo. It quickly went viral inside and outside of Cuba, becoming an anthem for the fight for human rights and freedom in the country. The song won two Latin Grammy Awards, including Song of the Year;[26] but while it was reaping this success, Osorbo was serving six months in prison after being arrested in May 2021, accused of "resistance" and "contempt".[27]

Opposition political activist Manuel Cuesta Morúa believes that one of the reasons why the repression against Osorbo and others like him was so strong is because "they brought together [people from the] younger sectors and from the culture sector, where symbols, [a] new language and images are created that drive the intellectual debate of ideas."[28] Although there are no figures on the distribution of internet use by age groups in Cuba, in 2021 people between 18 and 34 years old made up more than half of adult internet users globally.[29] This means it is likely that young people are also the most active on the internet in Cuba.

Before the demonstrations of July 2021, there were at least two internet disruptions in Cuba in the same year. The first of them was partial and occurred on 27 January 2021,[30] coinciding with a demonstration called by a group of artists and journalists outside the Cuban Ministry of Culture,[31] while the second took place on 12 February 2021 and, according to ETECSA, was due to a "technical interruption" that affected not only access to the internet but all of the country's international communications services.[32]

Knowing the history of internet censorship in Cuba, it is not surprising that when thousands of citizens took to the streets across the country to

21 NetBlocks. (2020, 30 November). Social media disrupted in Cuba amid protests for artistic freedom. https://netblocks.org/reports/social-media-disrupted-in-cuba-amid-protests-for-artistic-freedom-aAwrqa8M

22 Access Now. (2020, 5 November). Telegram blocked in Cuba? Civil society demands answers. https://www.accessnow.org/telegram-blocked-in-cuba-civil-society-demands-answers

23 Committee to Protect Journalists. (2021, 4 March). Staff of Cuban press freedom group ICLEP lose internet service, fear targeted disruption. https://cpj.org/?p=86767

24 EFE. (2021, 10 July). Crece la campaña para pedir un corredor humanitario de ayuda a Cuba. *EFE*. https://www.efe.com/efe/america/sociedad/crece-la-campana-para-pedir-un-corredor-humanitario-de-ayuda-a-cuba/20000013-4583410

25 Interview with YucaByte director Norges Rodríguez, 3 February 2022.

26 Reuters. (2021, 19 December). Cuba protest anthem 'Patria y Vida' wins Latin Grammy Song of the Year. *Reuters*. https://www.reuters.com/lifestyle/cuba-protest-anthem-patria-y-vida-wins-latin-grammy-song-year-2021-11-19

27 Al Jazeera. (2021, 3 June). Cuba criticised over rapper jailed for 'resistance'. *Al Jazeera*. https://www.aljazeera.com/news/2021/6/3/cuba-criticised-over-rapper-jailed-for-resistance

28 Interview with the vice president of the Council for the Democratic Transition in Cuba, Manuel Cuesta Morúa, 10 February 2022.

29 https://www.statista.com/statistics/272365/age-distribution-of-internet-users-worldwide

30 Madory, D. [@dougmadory]. (2021, 27 January). According to @Kentikinc data, there was a significant drop in internet traffic from #Cuba today for a little more than two hours [tweet]. *Twitter*. https://twitter.com/DougMadory/status/1354581571840389127

31 Committee to Protect Journalists. (2021, 29 January). Cuban internet access cut amid free expression protest; journalist harassed. https://cpj.org/?p=79558

32 Frank, M. (2021, 12 February). Cuba loses phone, internet connections for about 90 minutes. *Reuters*. https://www.reuters.com/business/media-telecom/cuba-loses-phone-internet-connections-about-90-minutes-2021-02-12

demonstrate on 11 July 2021, the response was to block access to social media platforms and instant messaging applications such as Facebook, Instagram, WhatsApp, Telegram[33] and Signal.[34] However, it also meant that this time Cubans were prepared to circumvent censorship using tools like VPNs. As a result, the government had to completely cut off internet access throughout the country[35] to stop the spread of images and videos of the demonstrations that were being broadcast and shared with the world almost instantly.

While taking this measure, the regime was also calling on its supporters and security forces to confront protesters in the streets,[36] resulting in one person being killed and hundreds more detained.[37] Months later, Cuba acknowledged having detained and prosecuted more than 700 people, including 55 minors.[38]

The disruptions and blockades continued during the following days[39] and evidence was found that ETECSA may have tried to throttle the internet to prevent its effective use in the country.[40] On 15 July 2021, almost a million and a half users from Cuba connected to the Psiphon network,[41] a well-known free VPN provider. In response, ETECSA began filtering SMS containing keywords such as "Psiphon" or "VPN",[42] and that same day the United States government announced that they would evaluate alternatives to try to restore internet access in Cuba.[43]

Less than a month after the demonstrations, the regime approved Decree Law 35, which establishes greater controls over the activities of Cubans on the internet and threatens to further increase censorship and self-censorship in the country.[44] For Cuban journalist Camila Acosta, this legislation is a way of intimidating people and, although to date no case is known in which it has been used, she says that the regime has used other mechanisms to fine citizens for criticism of the government, or even for sharing third-party content that criticises the government on social media.[45]

Looking to the future

Although in 2021 the political change that the citizens of Cuba expected did not occur, the historic demonstrations were a clear example of the potential for transformation and mobilisation that the internet has in society and, therefore, the threat it represents to authoritarianism in Cuba in the long term.

While Venezuela, Myanmar and more recently Kazakhstan have shown that citizen mobilisation is not the only element necessary to achieve a transition to democracy, in Cuba it did at least have some impact.

Days after the demonstrations, the regime announced a temporary lifting of some restrictions related to the amount of food and medicine that travellers entering the country can carry.[46] It also allowed the entry of humanitarian aid, although only from allied countries such as Russia, Mexico and Bolivia.[47]

33 NetBlocks. (2021, 12 July). Social media restricted in Cuba amid widening anti-government protests. https://netblocks.org/reports/social-media-restricted-in-cuba-amid-widening-anti-government-protests-QAdrmwyl

34 Xynou, M., & Filastò, A. (2021, 21 October). How countries attempt to block Signal Private Messenger App around the world. *OONI*. https://ooni.org/post/2021-how-signal-private-messenger-blocked-around-the-world/#cuba

35 Madory, D. (2021, 16 July). Internet Disruptions in Cuba Following Widespread Protests. *Kentik*. https://www.kentik.com/analysis/internet-disruptions-in-cuba-following-widespread-protests

36 Perrett, C. (2021, 12 July). Cuban President Miguel Díaz-Canel called on supporters to fight in the streets as anti-government protests grow. *Business Insider*. https://www.businessinsider.com/cuban-president-fight-in-the-streets-amid-protests-2021-7

37 Phillips, T., & Agustin, E. (2021, 13 July). Cuba protests: one man killed and more than 100 missing in historic unrest. *The Guardian*. https://www.theguardian.com/world/2021/jul/13/cuba-protests-activists-journalists-protesters-detained

38 BBC. (2022, 26 January). Cuba says more than 700 charged over anti-government protests. *BBC*. https://www.bbc.com/news/world-latin-america-60124600

39 Madory, D. (2021, 17 July). Another Internet Disruption in Cuba Following Week of Protests. *Kentik*. https://www.kentik.com/analysis/another-internet-disruption-in-cuba-following-week-of-protests

40 Madory, D. [@dougmadory]. (2021, 4 August). Based on @kentikinc performance measurements to Cuba, there was increased latency and packet loss for three distinct periods in late July [tweet]. *Twitter*. https://twitter.com/DougMadory/status/1423067836826755078

41 Psiphon Inc. [@psiphoninc]. (2021, 16 July). Update: Yesterday 1.389 Million daily unique users accessed the open web from Cuba through the Psiphon Network [tweet]. *Twitter*. https://twitter.com/PsiphonInc/status/1416069807301185537

42 14ymedio. (2021, 15 July). El monopolio cubano Etecsa censura los SMS con las palabras "Psiphon" y "VPN". *14ymedio*. https://www.14ymedio.com/cuba/monopolio-cubano-Etecsa-censura-SMS-Psiphon-VPN_0_3131086865.html

43 Shepardson, D. (2021, 15 July). U.S. reviewing whether it can help restore internet access in Cuba -Biden. *Reuters*. https://www.reuters.com/world/americas/us-reviewing-whether-it-can-help-restore-internet-access-cuba-2021-07-15

44 Marsh, S. (2021, 19 August). New Cuban decree tightens controls on social media, sparking outrage. *Reuters*. https://www.reuters.com/world/americas/new-cuban-decree-tightens-controls-social-media-sparking-outrage-2021-08-18

45 Interview with Cubanet journalist and Havana correspondent for the ABC newspaper Camila Acosta, 7 February 2022.

46 Marsh, S., & Acosta, N. (2021, 15 July). Cuba lifts food, medicine customs restrictions after protests. *Reuters*. https://www.reuters.com/world/americas/cuba-lifts-food-medicine-customs-restrictions-after-protests-2021-07-15

47 Marsh, S. (2021, 30 July). Cuba receives food, medicine donations from allies to ease crisis. *Reuters*. https://www.reuters.com/world/americas/cuba-receives-food-medicine-donations-allies-ease-crisis-2021-07-31

Cuban cyber activism has also not ceased. Proof of this is the call to boycott the San Remo Festival[48] that is being organised by the Cuban regime at the same time that it is carrying out mass trials against hundreds of protesters, and also the international campaign in rejection of these trials.[49]

Action steps

The following action steps need to be taken to support open access to the internet in Cuba:

- Democratic governments of the world must look for ways to encourage the expansion of internet access in Cuba. For example, this can be done through conditioning trade agreements on a real commitment and actions by the Cuban government to provide reliable and quality access to its citizens.
- Civil society organisations outside of Cuba need to help find technical alternatives that allow keeping access to the internet in the event of government censorship such as that seen in July of 2021. In particular, an alternative to the Psiphon network needs to be found so that access is not limited to a single point of access, which could be targeted by ETECSA.
- Donors should support the work of non-profit organisations that monitor internet censorship in Cuba so that evidence of this censorship can be built.
- Digital rights organisations in the region must train grassroots activists and journalists in Cuba to circumvent internet censorship and collect evidence of website and digital platform blocking using open tools like OONI Probe.[50]
- Civil society organisations must continue to pressure multilateral organisations to reject censorship and internet shutdowns as a method of repressing citizens across the world.

48 Deutsche Welle. (2022, 10 January). Controversia política llega al San Remo Music Awards Cuba. *Deutsche Welle*. https://p.dw.com/p/46mcy

49 Kurmanaev, A., & Lopez, O. (2022, 14 January). Mass Trials in Cuba Deepen Its Harshest Crackdown in Decades. *The New York Times*. https://www.nytimes.com/2022/01/14/world/americas/cuba-mass-trials-crackdown.html

50 https://ooni.org

EL SALVADOR

DISINFORMATION DURING THE PANDEMIC: OPPORTUNITIES FOR MEDIA AND INFORMATION LITERACY IN EL SALVADOR

HNL Consultores
José Roberto Amaya Valencia

Introduction

The enormous amount of information produced constantly in the context of the COVID-19 pandemic has travelled both online and through traditional media, similar to a tsunami, with reliable information and disinformation mixed together. The World Health Organization baptised this phenomenon an "infodemic".[1]

To combat disinformation in the long term, the United Nations Educational, Scientific and Cultural Organization (UNESCO) has recommended that states invest in media and information literacy (MIL)[2] programmes so that citizens are able to search, select, evaluate, synthesise and share the information they encounter in a responsible way. In some regions, the involvement of large platforms like Facebook in MIL programmes is evident. However, in other latitudes there is not only state apathy, but private efforts, in most cases, are small initiatives that do not reach the general public, the main target of these efforts.

In El Salvador, there is no specific public policy that involves training or teaching MIL, beyond some references in official documents. In the context of the pandemic, efforts to combat disinformation were few and not necessarily focused on MIL.

Projects that have been deployed to combat the information disorder, such as fact-checking initiatives, are the starting point for implementing MIL training and education on a larger scale, both in the public and private spheres.

However, it is worth reflecting, as a first step, on the real need to bet on MIL training and education as a solution to the circulation of disinformation and misinformation, the difficulties inherent in its implementation at scale, as well as the challenges in promoting MIL training in the Salvadoran context. This report aims to address these questions.

False information in El Salvador during the pandemic

One of the main problems in El Salvador is the absence of a public educational policy on MIL that serves as a transversal axis for other policies. A review of different official study programmes of the Ministry of Education yield few references to MIL – and when references are made they are unclear, and do not allow one to properly evaluate the intention behind the inclusion of MIL in the curriculum.

On the other hand, the government's Digital Agenda El Salvador 2020-2030[3] includes an MIL component, but there are no indications of specific long-term programmes to make it a reality and realise the goals of the agenda. In fact, in some media interviews, the Innovation Secretariat of the Presidency, responsible for developing the Digital Agenda, refers to MIL in extremely limited terms – more about improving "digital skills" and solving the problem of access to digital devices, than about promoting social practices facilitated by reading and writing.[4]

In this context, Salvadorans had to face the avalanche of information that the pandemic brought with it. Contrary to what happened in other countries, in which people returned to television as a trusted medium for reliable information,[5] in El Salvador a recent study showed that social networks remained the main sources of news and information

1 The World Health Organization defines an infodemic as "an overabundance of information – some accurate and some not – that makes it hard for people to find trustworthy sources and reliable guidance when they need it." Pan American Health Organization. (2020). *Understanding the infodemic and misinformation in the fight against COVID-19*. https://iris.paho.org/bitstream/handle/10665.2/52052/Factsheet-infodemic_eng.pdf?sequence=16&isAllowed=y

2 According to the International Federation of Library Associations and Institutions (IFLA), "Media and Information Literacy consists of the knowledge, the attitudes, and the sum of the skills needed to know when and what information is needed; where and how to obtain that information; how to evaluate it critically and organise it once it is found; and how to use it in an ethical way." IFLA. (2011). *IFLA Media and Information Literacy Recommendations*. https://www.ifla.org/wp-content/uploads/2019/05/assets/information-literacy/publications/media-info-lit-recommend-en.pdf

3 https://www.innovacion.gob.sv

4 Parra, R. (2021, 10 July). El Salvador presenta avances de su Agenda Digital 2020-2030. *DPL News*. https://dplnews.com/el-salvador-presenta-avances-de-su-agenda-digital-2020-2030

5 Negredo, S., et al. (2021). Spain. In N. Newman et al. (Eds.), *Digital News Report 2021*. Reuters Institute for the Study of Journalism. https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2021/spain

on the pandemic.[6] Although this study indicates an increase in television consumption during the pandemic – mainly of news – it does not refer to whether this was due to the fact that Salvadorans trusted TV news more.

Salvadorans also had to face a specific distortion of information not found in many countries dealing with the circulation of false information: propaganda.[7] It was this, mainly, that resulted in some digital media developing content where public information that could be accessed at the time was contrasted to the government's narrative on the pandemic. This exercise resulted in evidence of false, misleading or incomplete information provided by the government and circulating on social networks, generally in the form of advertising spots or posts on Twitter.

Currently, digital magazines such as *Factum*[8] and *Gato Encerrado*[9] continue to publish content contrasting the official discourse on different topics that range from politics to health. In addition, a new site[10] has been set up dedicated exclusively to combating disinformation through fact checking, and it also checks government statements on the pandemic, among other issues.

Opportunities for MIL after the pandemic

Disinformation and misinformation are not new phenomena whose appearance can be attributed to the birth and growth of the internet. Their existence and dissemination are also associated with other media such as television, newspapers and radio. False information has also always travelled through communities by word-of-mouth, or through other means.

Studies on the skills that a reader must have to deal with disinformation suggest that they are not new either – although the extent of the information that needs to be processed online has increased, and there are technical tools and an understanding of how the internet works that are necessary to process the circulation of online information. Numerous studies have identified these skills as including choosing precise search terms, selecting relevant results, critically evaluating information, synthesising information from multiple sources, and sharing what is learned in a responsible way.[11]

UNESCO has recommended to states that they invest in MIL programmes to combat disinformation in a lasting way, a recommendation that is consistent with the available evidence[12] and with the recommendations of other organisations.[13] There is, therefore, a preference for educational and training strategies over those that involve legislation that can restrict fundamental rights, such as the right to freedom of expression.

This call should be heeded, in the first instance, by states, which are responsible for ensuring that their citizens enjoy their rights fully, including those that are exercised in the digital environment. The private sector also has a role to play in this, even companies that have been blamed for the circulation of disinformation online. Cases such as Facebook, which has consolidated its MIL programme in Africa,[14] or the DW Academy,[15] which offers MIL programmes in Central America, are examples of how the private sector can become actively involved in this task.

However, improving the public's MIL cannot be done without foundations and only with a short-term goal in mind. Public policies are needed, including in education, that articulate the need for MIL in all areas of training, teaching and learning.

In El Salvador, a review of official educational documents, which include the curricula of different grades in different subjects, especially those related to the study of language and the study of computing, reveal a limited approach to the MIL concept.

6 Carballo, W., & Marroquin, A. (2020). *2020 D.C. Asi dio vuelta el consumo mediático en El Salvador durante la COVID-19*. Escuela de Comunicación Mónica Herrera y Maestría en Gestión Estratégica de la Comunicación, UCA. https://uca.edu.sv/wp-content/uploads/2020/12/investigacion-uca-asi-dio-vuelta-en-consumo-mediatico-en-el-salvador-durante-la-covid-19.pdf

7 https://propaganda.mediaeducationlab.com/learn

8 https://www.revistafactum.com

9 https://gatoencerrado.news

10 https://infodemia.com.sv

11 Walraven, A., Brand-Gruwel, S., & Boshuizen, H. (2009). How students evaluate information and sources when searching the World Wide Web for information. *Computers & Education, 52*(1), 234-246. https://doi.org/10.1016/j.compedu.2008.08.003; Goldman, S. R., et al. (2012). Comprehending and Learning From Internet Sources: Processing Patterns of Better and Poorer Learners. *Reading Research Quarterly, 47*(4), 356-381; Leu, et al. (2013). The New Literacies of Online Research and Comprehension: Assessing and Preparing Students for the 21st Century With Common Core State Standards. In S. B. Neuman & L. B. Gambrell (Eds.), *Quality Reading Instruction in the Age of Common Core Standards*. International Reading Association.

12 Cunliffe-Jones, P., et al. (2021). The State of Media Literacy in Sub-Saharan Africa 2020 and a Theory of Misinformation Literacy. In P. Cunliffe-Jones et al., *Misinformation Policy in Sub-Saharan Africa*. University of Westminster Press.

13 Relatoría Especial para la Libertad de Expresión de la CIDH. (2019). *Guía para garantizar la libertad de expresión frente a la desinformación deliberada en contextos electorales*. Organización de Estados Americanos. https://www.oas.org/es/cidh/expresion/publicaciones/Guia_Desinformacion_VF.pdf

14 Moyo, A. (2020, 17 June). Facebook consolidates digital literacy programmes in Africa. *ITWeb*. https://www.itweb.co.za/content/kYbe9MXDGKPMAWpG

15 Banos Ruiz, I., & Binder, S. (2021, 22 March). Campus AMI, competencias mediáticas en un viaje interactivo. *DW*. https://www.dw.com/en/campus-ami-competencias-medi%C3%A1ticas-en-un-viaje-interactivo/a-56954102

The same happens when reviewing the current government's commitment to digital transformation, in which, as mentioned, reference is made to the concept of digital literacy, but in practice there are few projects that will contribute towards realising this goal, and certainly not in line with a proper definition of MIL.

To develop an efficient and representative public policy, it is necessary to start with a diagnosis of the situation in which the largest number of stakeholders participate. From this a draft policy should be developed which is then sent out for public comment. It is only after this that a policy can be finalised.

In the initial diagnosis, as well as in later stages of execution, it is necessary to identify the difficulties in the implementation of this policy.

One of the main obstacles that can explain the absence of a public policy on MIL in El Salvador is the lack of political will. Without the convergence of different actors involved in the decision-making processes, it will not be possible to develop an effective policy. In this regard, there is little that gives us hope that MIL is being taken seriously in El Salvador, outside of merely discussing the topic.

If the same government uses propaganda as a tool to feed a triumphalist narrative, which does not hold up against journalistic scrutiny; and if access to public information has been limited to the point of putting locks on information in the form of criminal legislation[16] to discourage the use of anonymous sources in journalistic reports critical of the government, it is not possible to remain optimistic.

It is true that the implementation of MIL curricula, whether for training or education, is not only the responsibility of the public sector, nor limited to the school environment. Instead, MIL training includes the collaboration of private entities and is an analytical skill that can be developed at home, work and in the community.

However, the effort of civil society organisations dedicated to strengthening education is essential to a successful MIL programme. Not only because of the financial resources that are necessary for this type of project, but also because of their experience in advocacy on a key issue of public concern, and their ability to forge alliances with other organisations or with companies interested in the implementation of MIL curricula.

Another obstacle is that there is very little academic research on this topic. Little is known about the current MIL competencies of Salvadorans, and how this may differ according to age group, or economic and social circumstances. One of the pillars on which a public policy must rest is the scientific knowledge of the phenomenon in which it is intended to intervene.

A search for material related to the subject returned few results. However, this does not mean that there is no research that has been done, or that there are no professionals with knowledge of the subject or no institutions that are paying attention to the subject. For example, two institutions that are paying attention to MIL are the José Simeón Cañas Central American University (UCA) and the Mónica Herrera School of Communications. However, more is needed, and universities and organisations dedicated to social research should be encouraged to research the topic to produce the scientific evidence to back up any policy that is developed.

The efforts initiated by digital magazines in fact checking the statements of public officials is a first step – and illustrate the need to teach people how to consume, produce and share information in a responsible manner. Although the work is carried out by the journalists or fact checkers, as a short-term action, it is possible to take these initiatives as a starting point from which advocacy work can begin to establish alliances with the large internet platforms that have shown interest in combating disinformation.

Conclusion

The appearance of a new disease that later became a pandemic brought with it the problem of information overload, which exposed a large number of people around the world to the information disorder.

The need to counter disinformation led to a focus of attention on MIL as a long-term intervention that should be instituted by states as a public policy, but that does not exclude the collaboration of multiple stakeholders. Some large technology companies are already implementing MIL projects either through donations, collaborations with civil society organisations and states, as well as through the provision of curricula and other educational resources on the subject.

In El Salvador, a public policy that integrates MIL as a transversal axis to other policies is necessary, and this proposal should come from civil society. However, before this can be done, there is a need for more research on the matter in order to have a scientific basis that allows establishing priority areas for intervention. This work should be carried out by universities and social research centres that have the financial and human resources to carry out the work.

16 Rodríguez, M., & Alas, L. (2021, 9 December). Reformas a la Ley de Delitos Informáticos amenazan al periodismo. *elsalvador.com*. https://www.elsalvador.com/noticias/nacional/asamblea-prensa/907913/2021

On the other hand, the main obstacle to the implementation of a broad-based MIL programme in the country is the lack of political will, which manifests itself in actions that seek to limit access to information that would allow the development of a critical citizenry. This issue conflicts with the objectives of an MIL programme, which precisely seeks to provide citizens with tools that allow them to know, criticise and propose solutions to the problems of their daily life. The government has also shown itself to be an active participant in disinformation through propaganda.

This obstacle, however, should not be insurmountable. Human rights organisations should strengthen their advocacy strategies, which should include multisectoral alliances to implement long-term MIL projects in the country, even if they start with specific or limited research or training objectives.

The renewed interest in MIL in reaction to digital magazines beginning to fact check statements by public officials in El Salvador should be taken advantage of. This interest should become the starting point for efforts to promote and implement MIL programmes. The health crisis that produced other sub-crises, such as the so-called infodemic, must be used to strengthen the interest in developing the tools to consume and produce information in a responsible and ethical manner.

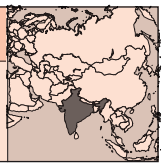
Actions steps

The following steps are proposed to strengthen MIL training and education in El Salvador in the immediate term:

- Increase research on MIL capacities among priority groups, such as rural and marginalised communities and women.
- Establish alliances with large platform intermediaries to secure financial support for the development of multidisciplinary MIL projects.
- Establish a roadmap for the development of a public policy that places MIL on a transversal axis in relation to other policies.

INDIA

THEN AND NOW: NEW POST-PANDEMIC CHALLENGES TO DIGITAL RIGHTS ADVOCACY IN INDIA



Digital Empowerment Foundation and Council for Social and Digital Development
Osama Manzar, Syed S. Kazi and Tuisha Sircar
https://www.defindia.org and https://www.csddindia.in

Introduction

The COVID-19 pandemic has greatly affected civil society – operations were disrupted, new issues emerged, and civic space continued to close.[1] The pandemic brought about travel restrictions, supply and network chain disruptions, and a lack of access to many of the services that civil society organisations (CSOs) offered. Consequently, digital technology emerged as a way for civil society to network, collaborate and engage in their areas of work and on their priorities. Although digital tools reshaped global communications decades ago, lockdown measures strengthened digital adoption among movements, organisations and communities, with many using social media to mobilise people and resources, organise, and engage in advocacy, networking and campaigning to raise concerns and seek support and solutions.[2]

The pandemic also forced organisations in India to reach for fresh ways of understanding, interpreting and dissecting digital rights issues in an attempt to find remedies in a new context. With the acceleration in digital adoption during the pandemic, the issues around which there is a renewed dialogue include the following:

- In a bid to connect and network large-scale civic organisations, grassroots collectives and communities are freshly focusing on digital literacy and access to the internet and technology to limit the risk of excluding people.[3]
- Tech-based CSOs are increasingly becoming cognisant of the massive extraction and collection of data that have reached unprecedented levels, whether through government initiatives in response to the pandemic, or by the private sector through the intensified use of the internet globally.[4]
- With the pandemic stirring the relations between the state and civil society, and more activism going online, further restrictions on digital communications have become a reality.[5]

Besides this framework of changes, there have been other areas of concern for CSOs, including enabling the right to information, addressing disinformation and misinformation, and access to critical public information and government schemes.

In this newfound and accelerated digital space, there are two broad shifts that emerged quite clearly in how CSOs in India changed their ways of working to meet the challenges that they confronted. Firstly, issues emerged around the "why" and "how". Traditional rights advocacy CSOs started revisiting traditional modes of communicating, and are now looking at adapting to digital modes to advocate on rights. Many are now opting to reorient and upgrade their work using digital platforms. And secondly, digital rights and tech-based organisations already engaged in digital advocacy started to refocus on the new challenges of digital rights that were emerging, looking for alternative ways to address these: the "what" and "how". This included transiting to a "super-normal" or higher-level use of digital platforms, resources and tools and alternative ways of networking to engage in advocacy.

This report aims to foreground the above key considerations in India, the world's largest democracy and emerging "digital democratic" country. It

1 Brechenmacher, S., Youngs, R., & Carothers, T. (2020, 21 April). Civil Society and the Coronavirus: Dynamism Despite Disruption. *Carnegie Endowment for International Peace*. https://carnegieendowment.org/2020/04/21/civil-society-and-coronavirus-dynamism-despite-disruption-pub-81592

2 Nampoothiri, N. J., & Artuso, F. (2021). Civil Society's Response to Coronavirus Disease 2019: Patterns from Two Hundred Case Studies of Emergent Agency. *Journal of Creative Communications, 16*(2), 203-212. https://doi.org/10.1177/09732586211015057

3 Allmann, K. (2020, 11 May). Covid-19 is increasing digital inequality: We need human connectivity to close the digital divide. *Medium*. https://medium.com/swlh/covid-19-is-increasing-digital-inequality-but-human-connectivity-is-the-answer-424812acbb65; Reddy A, B., Jose, S., & Vaidehi, R. (2020). Digital Divide in Online Education: Of Access and Inclusivity. *Economic and Political Weekly, 55*(36).

4 Zwitter, A., & Gstrein, O. J. (2020). Big data, privacy and COVID-19 – learning from humanitarian expertise in data protection. *International Journal of Humanitarian Action, 5*(4). https://doi.org/10.1186/s41018-020-00072-6

5 Lindberg, S. I. (Ed.) (2021). *Autocratization Turns Viral: Democracy Report 2021*. University of Gothenburg: V-Dem Institute. https://www.v-dem.net/media/filer_public/c9/3f/c93f8e74-a3fd-4bac-adfd-ee2cfbc0a375/dr_2021.pdf

discusses how digitally-enabled,[6] digital technology and rights-based organisations in the country have revisited their priorities, strategies, means and mediums in a period of accelerated transition to advocate, network and seek solutions to the digital issues that concern millions in an emerging digital society and economy. This report seeks to look at the future of digital rights and other technology-based issues in India, through the lens of the civil society organisations in the tech space, but not limited to this.

To be able to imagine a post-pandemic reality of how CSOs engage in advocacy, it is pertinent to highlight how the COVID-19 pandemic has shaped their advocacy strategies on critical digital rights and tech issues in India, a country marred by various challenges. While for some stakeholders these changing means, methods and approaches to advocacy have the potential for a drastic digital transformation, others hold a more pessimistic perspective, expressing concerns about the challenges that civic actors are facing in the creation of a robust network of digital rights advocates in India. The latter can be highlighted by the fact that since the advent of the digital century, the number of CSOs working on digital rights and tech issues in India has been abysmally low, and few new voices are emerging.

Context: A shifting focus for CSOs

The highly infectious COVID-19 virus, which originated in Wuhan, China, was declared by the World Health Organization (WHO) as a global health emergency on 11 March 2020.[7] The declaration of the pandemic led to the imposition of lockdowns across nations, including India, as a precautionary measure to contain the spread of infection by mandating populations to self-isolate, quarantine and maintain social distancing. Since March 2020, India has seen three waves of exponentially rising cases of the virus, which led to full or partial restrictions on the mobility of people both inter- and intra-states. The restrictions forced organisations and institutions to adapt to the use of digital communications in order to continue their work from remote locations. The large network of CSOs in India advocating on various rights-based issues also developed innovative strategies to continue functioning and provide support to those in need during these dire times.

The advent of the pandemic not only forced CSOs advocating on rights-based issues to adapt to new strategies, but also induced them to shift their advocacy priorities. They tirelessly participated in relief efforts, disseminated critical information necessary to contain panic, and worked with the state's centralised funding mechanism created to combat the pandemic to supplement their work.

The health, education and livelihood sectors promptly adapted to digital strategies. For instance, Smile Foundation[8] launched an initiative called "Shiksha Na Ruke" where they provided underprivileged children access to continuous learning through the provision of electronic devices, trained teachers for virtual teaching, curated educational content suitable for digital platforms, and ensured mental well-being through individual mentoring sessions. In the health sector, the Society for Nutrition, Education and Health Action (SNEHA)[9] has been conducting emotional resilience sessions and counselling through online group calls with adolescents in grassroots communities. They also trained Accredited Social Health Activist (ASHA) workers and hundreds of members of Mahila Arogya Samitis (Women's Health Committees) remotely on preventive measures, proper use of masks, the identification of early symptoms of COVID-19, and how to do referrals to medical practitioners. It has been estimated that nearly three million people were impacted by the outreach of CSOs in India.[10]

The pandemic also forced CSOs working on critical digital rights and tech issues in India to revisit issues such as free speech, digital security, accessibility, internet governance, digital surveillance, data privacy, censorship, and what was termed the "infodemic". The debates around these issues are being juxtaposed and intersected with other social discourses around gender, caste, poverty and the environment.

Our investigation

In line with the substance of the enquiry of this issue of GISWatch, the core question we sought to address in this report was: "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?"

6 Digitally enabled organisations are those that opt to primarily function using digital platforms, tools and resources. Largely, their internal and external communication and advocacy work (research, workshops, meetings, etc.) are done online. Many digital rights organisations had already transitioned to such a mode of working prior to the pandemic. However, the pandemic pushed most organisations to make the transition and develop either fully online or hybrid ways of functioning.

7 Ducharme, J. (2020, 11 March). World Health Organization Declares COVID-19 a 'Pandemic.' Here's What That Means. *TIME*. https://time.com/5791661/who-coronavirus-pandemic-declaration

8 https://www.smilefoundationindia.org/me

9 https://snehamumbai.org/covid-19

10 Participatory Research in Asia & VANI Network. (2020). *Response of Indian Civil Society Towards COVID-19*. https://www.pria.org/knowledge_resource/1594293825_Response%20of%20CSO%20towards%20covid19.pdf

This required a careful analysis of its many layers. For example, in order to arrive at a comparative perspective, it has been necessary to understand the changes that CSOs had to make in their methods, tools and approaches to continue their advocacy work, compared to the pre-pandemic period.

The digital capacities of the organisations was also important, as was the extent of networking and collaboration among CSOs, public agencies and communities, which spoke to the resilience of CSOs during the pandemic.

Lastly, it was necessary to look at the scope of the changes engendered by the pandemic, and the extent to which these changes might impact the functioning and advocacy work of CSOs with respect to digital tech issues in the future.

The following sections are based on research conducted by Digital Empowerment Foundation (DEF) and the Council for Social and Digital Development (CSDD) through both qualitative and quantitative processes. The qualitative data was collected through in-depth interview sessions with five well-known CSOs working on digital rights and other tech-based issues in India. Quantitative data has been used to map the changing advocacy strategies and shifting priority issues of the CSOs. For this, nine organisations were selected. A detailed mapping of their advocacy between March 2020 and December 2021 was conducted by looking at the content on their websites and social media profiles. This considered the focus of their research, workshops, webinars, conferences and discussions, among others. These were then subjected to a cross-tabulation analysis using variables such as the topic and the advocacy methods, its frequency and date.

Filling the gap: CSOs and informal activism during COVID-19

Civil society in India is a vast network of organisations, working upwards from the grassroots level. It is conceptualised as "the sum total of all individual and collective initiatives for common public good."[11] During the pandemic, the most striking trend in civil society has been the spread of informal activism – forms of self-organisation aimed at practical problem solving.[12] On one hand, civil society filled the gap left by the state. On the other hand, informal networks and communities filled the gaps left by some of the larger and more formal CSOs with more rigid bureaucracies.

Technology played a central role in the delivery of various emergency services that were earlier dependent on community mobilisation. For example, Social Media Matters,[13] an organisation primarily working on online safety, disinformation and misinformation, and digital parenting, started a project called "My Pincode" where a few million users in India were reached through 783 Facebook groups. The purpose was to counter the spread of "fake news" about the pandemic, to present real-time updates on the pandemic from the government in simple, accessible language, and to share videos made by volunteers.[14]

During the second wave of the COVID-19 outbreak in India in April 2021, there was an acute shortage of life-saving oxygen, drugs and hospital beds across the nation.[15] Efforts by both government and CSOs had shortcomings given the vastness of the crisis. Consequently, thousands of civilians, especially youth, participated in a voluntary drive of setting up apps to crowdsource aid, delivering key supplies and using social media to direct resources to people in need.[16]

Moving to digital: Minimising the use of resources and maximising reach

For tech-based CSOs, the shift to a digital mode of operating has been relatively easier, despite changes in the mode of communication to phone calls and online meetings. For some organisations, the transition to online work has also allowed them to minimise the use of resources, including financial resources, and maximise reach. For instance, the Software Freedom Law Centre (SFLC), an organisation based out of Delhi, now conducts its digital security training and research on digital platforms using free/libre and open source platforms like Jitsi or BigBlueButton. Like other CSOs, it has started publishing its research reports online, which not only saves resources but also saves time. Before the pandemic, the SFLC ran in-person conferences for policy consultations that required a heavy financial investment. Now its conferences have moved online, which allows them to increase their reach globally.[17]

11 Tandon, R., & Mohanty, R. (2002). *Civil Society and Governance*. Samskriti.

12 Youngs, R., et al. (2021). *Civil Society and the Global Pandemic: Building Back Different?* Carnegie Endowment for International Peace. https://carnegieendowment.org/files/2021-CRN_Global%20Pandemic.pdf

13 https://www.socialmediamatters.in

14 Interview with Social Media Matters CEO Pratishtha Arora, 27 January 2022.

15 Thadhani, A. (2021). *Preventing a Repeat of the COVID-19 Second-Wave Oxygen Crisis in India.* Observer Research Foundation. https://www.orfonline.org/research/preventing-a-repeat-of-the-covid-19-second-wave-oxygen-crisis-in-india

16 AFP. (2021, 4 May). India's youth fight the covid second wave with apps and oxygen. *Live Mint*. https://www.livemint.com/news/india/indias-young-fight-the-covid-second-wave-with-apps-and-oxygen-11620095849517.html

17 Interview with Software Freedom Law Centre volunteer legal counsel Radhika Jhalani, 7 February 2022.

TABLE 1.

Areas of focus for research and advocacy by Indian digital rights CSOs during the COVID-19 pandemic

	Areas of focus
1.	Potential and challenges of FinTech: Inclusive systems, regulatory mechanisms, digital infrastructure, crypto assets[18]
2.	Digital labour
3.	Reimagining data systems beyond gender binaries
4.	Rural connectivity: The last mile and engaging with digital rights and technology-related issues at the grassroots
5.	Data privacy, personal freedom and informed user consent
6.	The arbitrary imposition of Aarogya Setu[19]
7.	"Fake news", misinformation and disinformation
8.	Digital surveillance through technologies such as facial recognition systems
9.	Digital security, online safety and data empowerment
10.	Reimagining artificial intelligence (AI) futures: Inclusive systems, innovation, policy advocacy, regulatory mechanisms, digital infrastructure
11.	Digital technologies and education
12.	Digital justice for gender and disability inclusion
13.	Online violence against marginalised groups
14.	Reimagining the data commons
15.	Datafication of people's health
16.	Gender and the digital divide
17.	E-waste management and the circular economy of the electronics sector
18.	Access to livelihoods and entitlements
19.	Digital parenting

This is not confined to the SFLC. Working online, CSOs have been able to host more webinars and online conferences, in an environment where this was increasingly accepted as standard practice, allowing them to reach a wider audience.[20] This included the Internet Freedom Foundation (IFF), which launched a forum in 2020 to expand its public engagement efforts in a "democratic dialogue with citizens" on digital rights.[21] DEF engaged with a wider public by reinventing its "DEFDialogues" during the COVID-19 pandemic, which are available on YouTube and the DEF website.[22]

There was evidence of an increase in the use of social media, especially Twitter and Instagram, for policy advocacy and awareness raising on various rights-based issues, including digital rights. The Centre for Internet and Society also started a technology and policy podcast in 2020 called "In Flux", which is available on various streaming platforms.[23]

These initiatives occurred against the backdrop of an increase in the adoption of free/libre and open source software since the start of the pandemic.[24]

18 Markets around the world are increasingly integrating cryptocurrencies in their economies. For instance, Costa Rica announced that employees might get legally paid in cryptocurrency. As a result, its adoption in the country spiked. The Philippines is another example of cryptocurrency being championed. In 2020, the country's central bank approved nearly 16 cryptocurrency exchanges, placing the Philippines at the forefront of Southeast Asian countries in terms of the "crypto boom". India is also an emerging crypto market: according to a report by Chainalysis, India's crypto market increased by 641% between July 2020 and June 2021. Cryptocurrency also brought in new cohorts of investors to the market – youngsters and women. As a result, the government is increasingly looking at the introduction of strict regulations of crypto assets and penetration of the market by introducing Central Bank Digital Currencies (CBDC).

19 Aarogya Setu is an Indian COVID-19 "contact tracing, syndromic mapping and self-assessment" digital service, primarily a mobile app, developed by the National Informatics Centre under the Ministry of Electronics and Information Technology.

20 Tanidir, Y., et al. (2021). How did the COVID-19 pandemic affect audience's attitudes in webinars? *The International Journal of Clinical Practice, 75*(7). https://doi.org/10.1111/ijcp.14239

21 https://internetfreedom.in/year-in-review-scaling-up-iffs-operations-and-community

22 https://www.defindia.org/defdialogues

23 https://in-flux.cis-india.org

24 TechGig. (2021, 9 February). Open Source software developers were more active during COVID-19: Survey. *Tech Gig.* https://content.techgig.com/open-source-software-developers-were-more-active-during-covid-19-survey/articleshow/80764250.cms

Areas of focus for digital rights activists during the pandemic

Table 1 lists the broad focus areas for digital rights and technology-related issues among the following key Indian digital rights CSOs during the pandemic: Digital Empowerment Foundation,[25] Centre for Internet and Society,[26] IT for Change,[27] Internet Democracy Project,[28] NASSCOM Foundation,[29] Internet Freedom Foundation,[30] Centre for Catalyzing Change,[31] Social Media Matters[32] and Policy 4.0.[33] These areas of focus were either new areas for the organisations or areas that the organisations returned to due to the impact of the pandemic. The issues are in no specific order of priority. As the table suggests, there was a focus on the emerging digital economy and financial resources, and its impact on labour and employment, which included issues impacting on gender, the informal workforce and farmers. A renewed focus on surveillance technologies also emerged, including its implications for privacy and constitutional rights such as free speech, censorship and access to the internet. E-education and e-health related concerns were also covered. Most importantly, concerns around the digital divide were revisited with a renewed urgency. More than addressing these problems on a short-term basis, CSOs engaged in reimagining futures and issues that need sustainable focus and work in growing the digital society.

Networking and collaborating for greater public participation

CSOs in India have shown resilience during the COVID-19 pandemic by strategically entering into partnerships and networking with stakeholders, grassroots organisations and other CSOs to engage in people-driven work.[34] Collaborations were seen between CSOs and government agencies, local organisations, local people and communities, and even with migrant and diaspora organisations.[35]

CSOs solely engaged in the policy space like the Internet Freedom Foundation (IFF) also relied on extensive networking and collaboration. For instance, for their analysis of AgriStack,[36] IFF collaborated with various farmer groups and even sent a joint letter signed by 55 organisations to the Union Minister for Agriculture asking for further consultations with all stakeholders. The letter highlighted the need for statutory backing, and demanded greater transparency with regard to the financial details of the project.[37] In collaboration with close to 50 organisations, IFF also studied the Aarogya Setu app, critically mapped resistance to and criticism of the app, filed right to information requests to understand the development and roll-out of the app, and engaged in strategic litigation in the Kerala High Court against its arbitrary imposition.[38] In terms of its work on medical healthcare data policies it has collaborated with organisations in the medical healthcare space like the Forum for Medical Ethics and Research.[39]

Navigating the need for grassroots work on digital rights

With the restrictions imposed on mobility, CSOs had to adapt to innovative strategies to continue functioning, sometimes in remote locations. Many CSOs like Social Media Matters and Feminist Approach to Technology (FAT),[40] despite working on technology- related issues, typically engaged in field-work research and face-to-face capacity building and advocacy. However, after the pandemic they developed new methods, changed their approach, and adapted to the use of new digital tools so that they could continue their grassroots engagement. For instance, FAT mobilised its project participants – who are primarily adolescent girls from marginalised groups in rural, peri-urban and urban communities across Delhi, Bihar, Jharkhand and Pune – through smart devices that were either owned by the girls or distributed by FAT to remote locations. The pandemic prompted them to start a girl-led campaign called "Corona nahi Karuna" where they used the devices to gather information, distinguish between fake news and legitimate news, connect to organisations distributing

25 https://www.defindia.org

26 https://cis-india.org

27 https://itforchange.net

28 https://internetdemocracy.in

29 https://nasscomfoundation.org

30 https://internetfreedom.in

31 https://www.c3india.org

32 https://www.socialmediamatters.in

33 https://policyfourpointo.com

34 Datta, N. (2021, 25 February). Promoting resilience among CSOs through partnerships and people-driven work in India. *Global Standard for CSO Accountability.* https://www.csostandard.org/cso-standard/promoting-resilience-among-csos-through-partnerships-and-people-driven-work-in-india

35 Khan, F., Yadav, A., & Sahoo, S. (2021, 26 April). Pandemic, CSOs, and Collaboration - Perspectives from India. *Queen Mary Global Policy Institute.* https://www.qmul.ac.uk/gpi/projects/migpanbrin/blog/items/pandemic-csos-and-collaboration---perspectives-from-india.html

36 As a collection of digital databases, AgriStack would have some core features including a unique farmer identity number for each farmer, and some building blocks such as data on weather, the newest science and research on agriculture, agricultural commodity prices in India and abroad, and information and access to central government schemes, agricultural regulations and permissions.

37 https://internetfreedom.in/joint-letter-to-the-agriculture-minister

38 https://internetfreedom.in/kerala-hc-aarogya-setu

39 Interview with Internet Freedom Foundation (IFF) Executive Director Apar Gupta, 1 February 2022.

40 https://www.fat-net.org

TABLE 2

Shift in methods used for advocacy: Pre-2020 and post-2020

Number	Pre-2020	Post-2020
1	Field-based research	Limited field-based interventions/Remote research
2	In-person community engagement	Online community engagement
3	In-person capacity building	Online capacity building
4	In-person workshops	Online workshops
5	In-person conferences	Online conferences
6	In-person meetings	Online/telephonic meetings
7	Seminars	Webinars

rations as well as to different government schemes, and assist people in their communities in various ways. By doing this they created an emergency support system using smart devices.

However, the implementation of FAT's programmes online also resulted in the loss of participants for various reasons, such as a lack of access to devices, restrictions imposed by families on the girls owning devices, difficulties in managing school or college commitments, and increased household responsibilities.

Apart from these challenges, other issues included a lack of privacy and confidentiality at home during online sessions, an increase in household health problems due to the pandemic, and increased boredom, which affected online participation of the girls.[41] Some participants also left the project due to early marriage.

Gender safety and user-generated data under lockdown

For a platform like Safetipin,[42] whose advocacy work on "safe cities for women" relies on the data generated through the Safetipin app, the pandemic posed a major problem. The app functions through safety audits, whereby the user rates a specific location through geotagging on the basis of nine parameters: lighting, visibility, pedestrian routes to the location, openness, transport, people, security, gender usage and feeling. These parameters are each given different weightings and an algorithm calculates the safety scores. As more audits are performed by users, Safetipin collects more "accurate" information. This data is then used to write reports and shared with the stakeholders who further use it to execute certain projects.

However, during the months of the lockdown, due to restrictions on mobility, people either stopped stepping outside of their houses or travelled in private vehicles. Consequently, no new data was generated through the Safetipin app. The Safetipin team modified their methodology to conducting online surveys and physical safety audits in selected zones following proper COVID-19 protocols.[43]

Shifts to digital methods for research, capacity building and advocacy

The methods for advocacy shifted drastically for CSOs working on rights-based issues, including digital rights, during the pandemic. While most of this shift relied on digital technologies as broadly presented in Table 2, in some cases there was a shift towards a "community outreach" model of collecting data[44] (as seen in the case of Safetipin). Nevertheless, CSOs are reimagining their engagement with the digital world in a post-pandemic society and striving for a greater digital transformation.

Future challenges to digital rights advocacy in India

The pandemic has engendered unique challenges for every CSO working on rights-based issues, including digital rights. Some of the broad challenges faced by CSOs working on digital rights and technology-related issues in India are:

- **Lack of grassroots engagement:** Various socio-cultural and economic factors are playing a role in worsening existing inequalities along the lines of gender, caste and religion. Consequently, CSOs are unable to bridge the gap between learning, empowerment and advocacy solely through technology. Issues relating to the digital divide and digital illiteracy in India, like online education or access to critical information, were therefore heightened due to this crisis.

41 Interview with Feminist Approach to Technology (FAT) Executive Director Gayatri Buragohain, 27 January 2022.

42 https://safetipin.com

43 Interview with Safetipin programme head Sonali Vyas, 7 February 2022.

44 Youngs, R., et al. (2021). Op. cit.

- **Unfavourable funding environment:** The pandemic has exacerbated the existing economic inequalities in India. According to the statistics released by the Centre for Monitoring Indian Economy, 10 million people lost their jobs by May 2021. The labour participation rate has come down to 40% from a pre-pandemic level of 42.5%.[45] CSOs are also facing operational difficulties as the current funding environment does not allow investing in human resources.[46] The Foreign Contribution (Regulation) Amendment Bill, 2020 has further put caps on foreign contributions for CSOs, greatly affecting their capacity to be sustainable.[47] The lack of subsidies, inadequate tax exemptions, high administrative costs and expensive digital resources and services are creating a barrier for existing CSOs to scale up their operations, generate new opportunities and provide relief at the grassroots. These factors are also hindering new organisations from emerging.
- **Constrained digital skills and capacities:** With the increasing adoption of the digital, there is a need to invest in building the digital skills and capacities of CSOs in order for them to seamlessly function online in the future. This challenge is closely linked to the challenge regarding the unfavourable funding environment in India, as CSOs need to invest in human resources, collaborate with external agencies on mass digital training across different verticals, and invest in up-to-date digital tools for effective and efficient functioning.
- **An increase in arbitrary control and surveillance:** While India has seen a surge in the disruption of various civil liberties of its citizens in the past few years, discourses surrounding the violation of digital rights have also picked up pace as digital rights are increasingly being recognised as human rights. Since 2012, India has seen 556 cases of internet shutdowns.[48] These have come alongside repeated instances of the government cracking down on citizens' right to free speech.[49] Many experts have also raised concerns about the Draft Data Protection Bill (2021), which poses a threat to data privacy and the personal freedom of citizens.[50] Moreover, there are currently 82 facial recognition systems in place across India, strengthening the state's surveillance architecture.[51] There are many other concerns regarding citizens' digital rights, especially without adequate legal safeguards and a good regulatory framework for digital infrastructure. CSOs working on digital rights and other technology-related issues are increasingly dealing with the threat of being seen as confrontationist and anti-establishment, which is closing opportunities for them to freely participate in the civic space.
- **Lack of a collaborative space to find synergy and work with public agencies:** The civic space where CSOs can collaborate and work dialectically with public agencies is increasingly shrinking in India. Being the world's largest democracy, India needs adequate public participation to deliver on its citizen-centred policies where CSOs play an important role.

Conclusion

CSOs in India working on rights-based issues, including digital rights, have shown great resilience in the face of the COVID-19 pandemic by adapting to innovative digital strategies to continue functioning, and to provide support to those in need of essential services and resources. The CSOs largely managed the transition to a digital mode of operation and changed their approach and methods of advocating on critical digital rights issues.

However, the increased reliance on technology renewed concerns with respect to digital rights. Emerging debates about technology are intersecting with other social discourses like those on gender, caste, poverty and the environment. At the same time, these debates are dealing with matters such as free speech, digital security, accessibility, internet governance, digital surveillance, data privacy, and

45 BusinessToday. (2021, 1 June). 10 million lost jobs in Covid 2nd wave, 97% households' income declined: CMIE. *BusinessToday.in*. https://www.businesstoday.in/latest/economy-politics/story/income-of-97-households-declined-since-covid-19-pandemic-began-cmie-298381-2021-06-01

46 Bandhyopadhyay, K. K., et al. (2021). *Civil Society Support to COVID-19 Affected Families: Outreach and Resourcing in the Second Wave*. PRIA. https://www.pria.org/knowledge_resource/1625214248_Civil_Society_Support_to_C19_Affected_Families_During_2nd_wave.pdf

47 Bhatnagar, G. V. (2020, 22 September). Leading NGOs Believe FCRA Changes Will 'Kill' Voluntary Sector. *The Wire*. https://thewire.in/rights/fcra-amendment-ngo-sector-impact-grassroots-activism

48 The Software Freedom Law Centre's internet shutdown tracker provides real-time data on the number of internet shutdowns in India. At the time of writing this report, 556 cases of internet shutdown had been reported since 2012. https://internetshutdowns.in

49 Mchangama, J., & Mendiratta, R. (2021, 25 June). Supporting free speech, but not criticism of government. *The Indian Express*. https://indianexpress.com/article/opinion/columns/supporting-free-speech-but-not-criticism-of-government-7376023

50 Chari, S. (2022, 4 February). Data privacy too complex to be decided by mere voice vote. Debate Data Protection Bill first. *The Print*. https://theprint.in/opinion/data-privacy-too-complex-to-be-decided-by-mere-voice-vote-debate-data-protection-bill-first/820652

51 The Internet Freedom Foundation's facial recognition technology (FRT) tracker under Project Panoptic provides real-time data on the number of FRT systems installed across India. https://panoptic.in

censorship. Because of this, and more than before, CSOs working on critical digital rights and tech issues have started collaborating and networking with CSOs and other stakeholders advocating on more traditional issues.

However, while the shift to digital has opened up new avenues for a greater digital transformation, many are increasingly expressing concerns about the challenges that civic actors are facing in the creation of a robust network of digital rights advocates in India. Some of these challenges are: 1) a lack of direct grassroots engagement; 2) an unfavourable funding environment; 3) inaccessibility of cost-effective digital resources, platforms and services; 4) constrained digital skills and capacities; 5) growing arbitrary control and surveillance; and 6) a lack of a collaborative space to find synergy and work with public agencies.

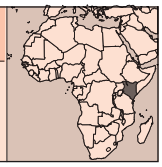
Action steps

Through consultation and critical engagement with various CSOs on the topic of the future of digital rights and technology-related issues in India, DEF and CSDD are proposing the following action steps:

- Make cost-effective digital resources, services and tools available to CSOs and grassroots communities to enable a democratic and inclusive digital ecosystem. Emphasise building the digital skills and capacities of CSOs to sustain a growing digital society.
- Through greater grassroots contact, nurture and encourage more digital rights and technology-based organisations to emerge at the community level.
- Encourage the creation of more collaborative digital forums by CSOs for a greater civic participation.
- Encourage greater engagement between CSOs, public agencies and local communities in the matters of emerging digital technology and rights issues.

KENYA

THE IMPACT OF THE COVID-19 PANDEMIC ON THE FUTURE OF ONLINE FREEDOM OF EXPRESSION IN KENYA



ARTICLE 19 Eastern Africa
Catherine Muya, Muthuri Kathure and Mugambi Kiai
https://www.article19.org

Introduction

Article 33 of the Constitution of Kenya guarantees every person the right to freedom of expression regardless of the medium. Despite this, in 2021, ARTICLE 19 ranked Kenya as "less restricted", with a global expression score of 61 out of 100, through a global metric that measures free expression across the world.[1] While "less restricted" may seem positive, it actually means the country still bears some challenges that inhibit the exercise of free expression both online and offline. These challenges are often either legal or administrative, i.e. they are associated with the legal or policy framework for free speech, or the implementation of these.

This report highlights the legal and administrative concerns related to the exercise of online free speech in Kenya and how the pandemic further impacted free expression online. It shows how existing and new legislation has been utilised to restrict free expression online during the pandemic and further analyses the impact of these changes on the future of free expression in the country. It ends with recommended actions to be implemented by different stakeholders to safeguard online freedom of expression in the country.

Background

Before the pandemic, activists in Kenya had some wins with respect to free expression, such as the declaration of the offence of criminal defamation, specifically relating to libel under section 194 of the Penal Code, as unconstitutional in 2017.[2] The High Court found that criminal sanctions ought to be reserved for the most serious offences, such as hate speech or incitement to violence, as stipulated under article 33 of the Constitution.[3] This decision was a win for online expression, ensuring that internet users would not be prosecuted for defamation.

Unfortunately, in 2018, Kenya enacted the Computer Misuse and Cybercrime Act, a law that introduced the offence of criminal defamation and 25 other provisions that have a chilling effect on online free expression.[4] In response to the act, the Bloggers Association of Kenya (BAKE),[5] supported by ARTICLE 19 Eastern Africa, filed a petition challenging the constitutionality of 26 provisions of this act.[6] However, in a judgement delivered in February 2020, the High Court held these provisions were constitutional and the provisions were still in effect and applied during the pandemic.[7]

Other concerns related to online free expression prior to the pandemic included the attempt by parliament in 2019 to pass a law to license bloggers and regulate the conduct of social media users.[8] The Kenya Film and Classification Board also made decisions before and during the pandemic that violated free expression and restricted access to certain films, particularly those with LGBTIQ content.[9]

Ahead of Kenya's third Universal Periodic Review (UPR) in 2020, ARTICLE 19 sent a detailed memorandum to the UN Human Rights Committee highlighting problematic provisions in Kenya's legal framework that entrench broad surveillance practices, and content-based restrictions to online free expression. These include legislation like the Prevention of Terrorism Act 2012 and the National

1 ARTICLE 19. (2021). *The Global Expression Report 2021: The state of freedom of expression around the world.* https://www.article19.org/wp-content/uploads/2021/07/A19-GxR-2021-FINAL.pdf

2 *Jacqueline Okuta & another v Attorney General & 2 others.* http://kenyalaw.org/caselaw/cases/view/130781

3 Ibid.

4 ARTICLE 19. (2018, 18 May). Kenya: Passage of flawed Computer and Cybercrimes Act threatens free expression. https://www.article19.org/resources/kenya-passage-of-flawed-computer-and-cybercrimes-act-threatens-free-expression

5 https://bake.co.ke

6 ARTICLE 19. (2018, 5 June). Kenya: Suspension of Cybercrimes Act provisions a welcome step to protect free expression. https://www.article19.org/resources/kenya-suspension-of-cybercrimes-act-provisions-a-welcome-step-to-protect-free-expression

7 ARTICLE 19. (2021). *Kenya: Briefing on attacks against journalists March 2020-July 2021.* https://www.article19.org/wp-content/uploads/2021/11/Covid-Response-Africa_Kenya.pdf

8 Muya, C. (2019). *Policy analysis on the Kenya Information and Communication (Amendment) Bill.* The Lawyers Hub Kenya. https://lawyershub.org/media/Policy_Analysis_on_Kenya_Information_and_Communcation_Amendment_Act_1_UXKIfMV.pdf

9 ARTICLE 19. (2018, 17 May). Kenya: Censorship by film classification board limiting free expression. https://www.article19.org/resources/kenya-censorship-by-film-classification-board-limiting-free-expression

Intelligence Service Act.[10] Although Kenya accepted all 26 recommendations on free expression from the UPR, ARTICLE 19 continues to document arrests and harassment of journalists among other restrictions to free expression.[11]

Impact of the COVID-19 pandemic on online free expression

Kenya instituted measures to curb the pandemic that impacted the exercise of online free expression. To begin with, at the onset of the pandemic, existing laws were used to regulate COVID-19 related misinformation and disinformation online, including section 22 and 23 of the Computer Misuse and Cybercrimes Act. The former deals with publishing false data with the intention that it be relied on as authentic, while the latter relates to publishing false information to cause chaos, panic or violence among citizens. In March 2020, the government announced that this law would be used to arrest and prosecute those publishing false information about the coronavirus.[12]

By September 2020, ARTICLE 19 Eastern Africa had documented 10 cases where internet users, including journalists and online communicators, were either arrested or threatened with prosecution for violating section 23 of the Computer Misuse and Cybercrimes Act.[13] Additionally, ARTICLE 19 Eastern Africa also documented the arbitrary use of the provisions in the two sections by the Directorate of Criminal Investigations (DCI) to compel detainees to take down or edit allegedly offending posts and websites.[14]

In November 2021, the National Computer and Cybercrimes Coordination Committee (NC4) was set up under section 4 of the Computer Misuse and Cybercrimes Act to aid in the implementation of the act. During the appointment of members of this committee, the authorities stated that the focus of the government and the committee would be to deal with purveyors of false information over social media.[15]

In addition to the use of existing laws, Kenya also enacted or attempted to enact laws to curb the pandemic that had a chilling effect on online free expression. In 2020, a senate ad hoc committee set up to deal with the COVID-19 situation in Kenya developed the Pandemic Response and Management Bill, which set out measures to curb the pandemic.[16] Part VII of the bill gave powers to the cabinet secretary to limit rights without subjecting these powers to effective judicial oversight.[17] Article 36 (b) also prohibited the circulation of false alarm or false warning on the pandemic, but in vague terms that failed to comply with international standards on limitations of free expression.[18]

The authorities in Kenya further adopted measures that impacted access to information and privacy. ARTICLE 19 believes the rights to free expression, access to information and privacy are complementary and mutually reinforcing. This has led to the development of principles relating to communication surveillance, mandatory data retention, anonymity and mandatory user registration, data disclosure by companies and search and seizure.[19] Unfortunately, during the first year of the pandemic, Kenya relied on health legislation to expand surveillance and in totality limit the right to data protection, which impacted online free expression.[20]

Through our project "Unseen Eyes, Unheard Stories", ARTICLE 19 found that the government relied on the Public Health (Prevention, Control and Suppression of Covid-19) Rules 2020 to expand the search and seizure powers of health officials; extend existing public CCTV systems to conduct mass surveillance on public spaces and enforce social distancing restrictions; use telecommunication data such as geolocation data to track and trace individuals and enforce quarantine; as well as to deploy a contact tracing app, "Jitenge MoH", which failed to comply with principles of data protection by design

10 ARTICLE 19. (2020). *Submission to the United Nations Human Rights Committee, List of Issues of Kenya, 128th Session*. UN Human Rights Treaty Bodies. https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2flCO%2fKEN%2f40935&Lang=en

11 ARTICLE 19. (2020, 28 September). HRC45: Kenya accepts UPR recommendations on free expression. https://www.article19.org/resources/hrc45-kenya-accepts-upr-recommendations-on-free-expression

12 Mutinda, T. (2020, 19 March). COVID-19: Arrest purveyors of fake news – Uhuru. *The Star.* https://www.the-star.co.ke/news/2020-03-19-covid-19-arrest-purveyors-of-fake-news-uhuru

13 ARTICLE 19. (2020, 30 September). Kenya: Journalists attacked and silenced during the COVID-19 Pandemic. https://www.article19.org/resources/kenya-journalists-attacked

14 ARTICLE 19 Eastern Africa. (2021). *Freedom of Expression and the Digital Environment in Eastern Africa: Monitoring Report January 2020-December 2020.* https://www.article19.org/wp-content/uploads/2021/02/Freedom-of-Expression-and-the-Digital-Environment-in-Eastern-Africa.pdf

15 Onyando, W. (2021, 4 November). Matiang'i warns fake news spreaders. *Nairobi News.* https://nairobinews.nation.co.ke/matiangi-warns-fake-news-spreaders

16 Bowmans. (2020). *COVID 19: Tracking Government Response in Kenya.* https://www.bowmanslaw.com/wp-content/uploads/2020/12/Bowmans-Kenya-Government-Response-Tracker.pdf

17 ARTICLE 19. (2021, 19 January). Kenya: Measures to tackle Covid-19 pandemic must not violate human rights. https://www.article19.org/resources/kenya-measures-covid-19-must-not-violate-human-rights

18 Ibid.

19 ARTICLE 19. (2017). *The Global Principles on Protection of Freedom of Expression and Privacy*. https://www.article19.org/data/files/medialibrary/38657/Expression-and-Privacy-Principles-1.pdf

20 ARTICLE 19 Eastern Africa, Pollicy, & KICTANet. (2021). *Unseen Eyes, Unheard Stories: Surveillance, data protection and freedom of expression in Kenya and Uganda during COVID 19*. https://www.article19.org/wp-content/uploads/2021/04/ADRF-Surveillance-Report-1.pdf

and default, while also collecting more information than was necessary.[21]

In addition to measures adopted by the authorities in response to the pandemic, the social impact of the pandemic itself had consequences for online free expression. The pandemic increased reliance on digital technologies as a means of association, expression, education and work, meaning more people spent time online. However, online harassment increased, disproportionately affecting women and children. In May 2020, the Directorate of Criminal Investigations (DCI) raised the alarm over an increase in online violence against children through forms such as child online grooming, cyberbullying and access to pornographic and sexual content, and advised parents to report these cases to their local DCI offices.[22] In the same period, ARTICLE 19 documented an increase in online violence against women in public spaces such as journalists[23] and women in politics,[24] as well as against sexual and gender minorities.[25] Structurally silenced women such as sex workers who switched to online tools to carry out their work also faced online harassment through non-consensual image distribution. Their customers disclosed intimate images or videos online without their consent, which had serious offline repercussions, as well as causing these women to avoid digital spaces.[26]

Challenges with digital inclusion, specifically the availability and affordability of the internet, also affected online expression. The GSM Association (GSMA) reports that women in Kenya were disproportionately affected by the pandemic, with some having to sell their mobile handsets to sustain themselves financially. Specifically, the report states, "Kenya was the only survey country where the gender gap in mobile internet use has widened, from 34 per cent in 2019 to 42 per cent in 2020."[27] Persons with disabilities also faced challenges accessing information during the pandemic, as there was no regular sign language interpretation for national COVID-19 briefings, or messages in Braille or other accessible formats.[28]

Unfortunately, social media platforms that were important spaces for online free expression were also used to perpetuate misinformation and disinformation on emerging political events that happened during the pandemic. These include attempts to amend Kenya's constitution through the Building Bridges Initiative (BBI) or reduce the impact of credible news like the Pandora Papers.[29] The BBI is a state-led initiative to amend the constitution in a manner devoid of public participation and, as ruled by courts, in a manner inconsistent with the Kenyan constitution.[30] Research also shows the use of paid influencers to target specific individuals who challenged the BBI process of amending the constitution and spread false information attacking their credibility, as well as the use of verified accounts and platform algorithms on Twitter to amplify these false narratives.[31]

For clarity, although the spread of misinformation and disinformation is wrong and of strong concern, it should be dealt with through civil and not criminal remedies, which are likely to have a disproportionate and chilling effect on freedom of expression. In line with international standards, individuals should be given an opportunity to prove the truth of their statements and the government should respond to them through full, honest and evolving communication with the public and careful and public correction of the misinformation and disinformation.[32]

21 Ibid.

22 Directorate of Criminal Investigations. (2020, 4 May). Cyber safety of children. *@DCI_Kenya (Twitter)*. https://twitter.com/dci_kenya/status/1257327420388098051?lang=en

23 Muya, C. (2021). *The Law Should Work For Us: Addressing Gaps in Kenya's Regulatory Framework to Build a Safer Internet for Women and Girls.* Open Internet Democracy Initiative. https://openinternet.global/sites/default/files/2021-09/The%20Law%20Should%20Work%20for%20Us.pdf

24 Gichanga, M., & Orembo, L. (2020). *Trends of Online Violence against Women in Politics During the COVID-19 Pandemic in Kenya*. KICTANet. https://www.kictanet.or.ke/mdocs-posts/trends-of-online-violence-against-women-in-politics-during-the-covid19-pandemic-in-kenya

25 ARTICLE 19. (2020, 6 October). Kenya: Free expression on sexual orientation and gender identity is a human right. https://www.article19.org/resources/kenya-free-expression-on-sexual-orientation-and-gender-identity

26 Bhalla, N., & Matiashe, F. S. (2021, 27 September). African sex workers face digital sex abuse as pandemic pushes them online. *Reuters.* https://www.reuters.com/legal/transactional/african-sex-workers-face-digital-abuse-pandemic-pushes-them-online-2021-09-27

27 GSMA. (2021). *The Mobile Gender Gap Report 2021*. https://www.gsma.com/r/wp-content/uploads/2021/06/The-Mobile-Gender-Gap-Report-2021.pdf

28 Kimumwe, P. (2020, 13 April). Why Access to Information on Covid19 is Crucial to Persons with Disabilities in Africa. *CIPESA.* https://cipesa.org/2020/04/why-access-to-information-on-covid-19-is-crucial-to-persons-with-disabilities-in-africa

29 The Pandora Papers refers to over 11 million confidential records made public by the International Consortium of Investigative Journalists, revealing a parallel economy that benefits the wealthy. Madung, O., & Obilo, B. (2021, 3 November). New Research: In Kenya, Disinformation Campaigns Seek to Discredit Pandora Papers. *Mozilla.* https://foundation.mozilla.org/en/blog/new-research-in-kenya-disinformation-campaigns-seek-to-discredit-pandora-papers

30 Kaburu, T. K. (2021, 4 September). The Kenyan Court of Appeal's BBI Judgement-IV: The Place of Public Participation in Constitutional Amendments. *Oxford Human Rights Hub.* https://ohrh.law.ox.ac.uk/the-kenyan-court-of-appeals-bbi-judgment-iv-the-place-of-public-participation-in-constitutional-amendments

31 Madung, O., & Obilo, B. (2021, 2 September). Fellow Research: Inside the Shadowy World of Disinformation-for-hire in Kenya. *Mozilla.* https://foundation.mozilla.org/en/blog/fellow-research-inside-the-shadowy-world-of-disinformation-for-hire-in-kenya

32 Rikhter, A. (2021). *International law and policy on disinformation in the context of freedom of the media.* Office of the OSCE Representative on Freedom of the Media. https://www.osce.org/files/f/documents/8/a/485606.pdf

ARTICLE 19 has also observed proposed amendments to Kenya's Copyright Act and National Cohesion and Peace Building Act that will impact how internet service providers deal with copyright-related content and hate speech. On the former, the amendments seek to water down provisions on notice and takedown procedures and interfere with the intermediary liability of internet service providers, pushing them to prefer to take down any allegedly infringing content and to police content online.[33] On the latter, the amendments seek to criminalise speech that is unpleasant even though this is not sufficient to be considered unlawful.[34]

Conclusion

From the above, it is clear that new and existing legislation was used to restrict free speech and expand surveillance. In addition, online free expression was negatively impacted by digital exclusion, misinformation and disinformation, and online harassment. Kenya will hold its general election in August 2022, which means that these challenges are also likely to be replicated or intensified in the near future. Already Kenya has reported an increase in incidents of alleged hate speech by politicians that if not dealt with may fuel offline conflict.[35]

A survey by the Reuters Institute revealed that 75% of news consumers in Kenya failed to differentiate between real and fake content.[36] This is concerning given the history of the use of political disinformation and foreign influence through projects such as Cambridge Analytica in the 2017 elections.[37] Although there are organisations engaged in fact checking, the reach of their work is limited and there is a need to increase the visibility of their efforts. Furthermore, there is a need to intensify media literacy among Kenyan citizens to increase knowledge on the potential harms and benefits of digital technologies in relation to free expression. Campaigns to intensify fact checking of certain information, so that already fact-checked information is made more available to citizens, and so that more citizens participate in fact checking, are also necessary.

Digital rights advocacy is also concentrated at the national and international level, with very limited participation from county or community-based organisations. These organisations, however, express an interest to learn and engage with digital rights issues.[38] There is a need to have community-based organisations advocating for legislation and policies that support digital inclusion and online free expression, including at the subnational level in the counties.

While Kenya is making efforts to promote digital inclusion, like creating a legal framework on community networks, knowledge on related regulations and how to use them to support digital connectivity in underserved areas is limited. There is a need to invest in the dissemination of this knowledge at the grassroots level. Overall, there is a need to address other factors deepening digital exclusion, such as the affordability of broadband and devices and taxation.

In the long run, unless the factors identified above are dealt with, they will continue to negatively impact the exercise of online free expression in Kenya.

Action steps

To address the above, the following action steps are recommended:

- Kenya needs to actualise the recommendations it received during its UPR and harmonise national legislation with international standards to ensure the law provides a good environment for the exercise of free expression.[39]
- Civil society should increase knowledge of digital rights and encourage digital rights advocacy at the grassroots level.
- Civil society should increase the number of programmes on media literacy and fact checking.
- Donors should increase funding to support digital rights advocacy and research for organisations at both national and grassroots level that will enable them to amplify their work to ensure that free expression online is realised.

33 ARTICLE 19. (2022, 12 January). Kenya: Copyright law must respect international standards of free speech. https://www.article19.org/resources/kenya-proposed-copyright-amendment-bill-must-respect-free-speech

34 ARTICLE 19 Written Memorandum on the National Cohesion and Peace Building Bill 2021.

35 Makong, B. (2021, 2 November). DPP vows action against hate mongers abusing free speech. *Capital News*. https://www.capitalfm.co.ke/news/2021/11/dpp-vows-action-against-hate-mongers-abusing-free-speech

36 Tangen, O. Jr. (2021, 31 December). Kenya: Troll trackers and the fight against the disinformation industry. *DW Akademie*. https://www.dw.com/en/kenya-troll-trackers-and-the-fight-against-the-disinformation-industry/a-60325620

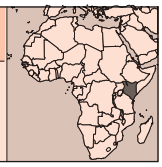
37 Warah, R. (2019, 9 August). Cambridge Analytica and the 2017 elections: Why has the Kenyan media remained silent? *The Elephant*. https://www.theelephant.info/features/2019/08/09/cambridge-analytica-and-the-2017-elections-why-has-the-kenyan-media-remained-silent

38 Consultation among human rights defenders in Kenya with the UN Special Rapporteur on the rights to freedom of peaceful assembly and of association in Nairobi organised by ARTICLE 19 on 31 January 2022, held at Ufungamano House.

39 ARTICLE 19. (2021, 28 May). Kenya: Harmonise legal framework on free expression with ICCPR recommendations. https://www.article19.org/resources/kenya-harmonise-free-expression-with-iccpr-recommendations

KENYA

LAYERED EXCLUSIONS: THE RAPID DIGITISATION OF GOVERNMENT SERVICES



NBO Legal Hackers
Francis Monyango
www.monyango.com

Introduction

The COVID-19 pandemic has accelerated the digitisation of many government services in Kenya. This digitisation had already been part of the government's plan, with the rollout and pilot phases taking place in different arms and departments. But due to the sudden implementation of the plans, digital rights issues have now become a priority.

This report offers and overview of challenges to the implementation of the Huduma Namba, a national ID number system in Kenya, and situates this in the context of government requirements making it mandatory to be vaccinated to receive government services. It argues that in the context of widespread digital exclusion in the country, what has been created is a situation of layered exclusions that need to be challenged by digital rights actors.

Huduma Namba

Kenya has established a digital National Identity Integrated Management System (NIIMS) through Executive Order No. 1 of (2018) and by the Statute Law (Miscellaneous Amendments) Act, 2018, section 9A. This includes the creation of the Huduma Namba (or Huduma Number), a unique and permanent personal identification number randomly assigned to every resident individual at birth or when an individual applies for official registration. It only expires upon the death of the individual. Upon registration, one will be issued with a Huduma Card, which will eventually replace the current identity card that all Kenyans currently have and use.

The government hopes that the Huduma Card will enable individuals to access various government services as well as use it as a travel document within the East African region. The card will have a person's data merged and installed in an electronic chip, therefore eliminating the requirement for other identity and personal information documents as is the case currently.

Officially, the pilot for the Huduma Cards started on 1 December 2020, and countrywide distribution started in February 2021. The government expected that all Kenyan adults who had been registered would be issued with their Huduma Cards by December 2021.[1]

The initiative resulted in two High Court actions, the first involving a petition by the Kenya Human Rights Commission (KHRC), the Nubian Rights Forum and the Kenya National Commission on Human Rights (KNCHR), which challenged the legality of the NIIMS project.

For their part, many members of the Nubian community who have been living in Kibera – a slum area of Nairobi – have found it difficult to get Kenyan citizenship, even though the community has existed in Kenya for more than a century. The community was started when people from Sudan were brought into Kenya during British colonial rule. Many members of the ethnic group have not been able to register for a Huduma Namba as they do not have the national IDs needed to do so. They called for the whole scheme to be scrapped given that the government says people will need a Huduma Namba to access public services.[2]

In the end, a three-judge High Court bench comprised of Judges Pauline Nyamweya, Mumbi Ngugi and Weldon Korir validated the legitimacy of the Huduma Namba in a judgment that addressed various issues. On whether the personal information collected is excessive, intrusive and disproportionate, the Court found that biometric data and GPS coordinates required in the amendments are personal, sensitive and intrusive data that requires protection. And even though there was no evidence brought by the petitioners of any violations of rights to privacy, the Court found that the amendments impose obligations on the relevant respondents to put in place measures to protect the personal data.

On whether there is a violation of children's right to privacy, the High Court found that section 9A of the Registration of Persons Act and NIIMS applies to children and that the legislative framework on the protection of children's biometric data collected in NIIMS is inadequate. On whether there are sufficient legal safeguards and data protection frameworks,

1 https://www.hudumanamba.go.ke/faqs

2 BBC. (2020, 31 January). Huduma Namba: Kenya court halts biometric ID over data fears. *BBC News*. https://www.bbc.com/news/world-africa-51324954

the Court found that while there is a legal framework for the collection and processing of personal data, adequate protection of the data requires the operationalisation of this legal framework.

However, since there was no specific regulatory framework that governs the operations and security of NIIMS, the Court found that the legal framework for the operations of NIIMS was inadequate, and posed a risk to the security of data that would be collected in the system.

On discrimination against the Nubian community, the Court stated that they were unable to discern violations of the right to equality and non-discrimination from the evidence presented before them. They stated that should there be challenges in other statutes or provisions, such challenges cannot properly be raised in the NIIMS case, in which the legislation in contention is entirely different. In the same breath, on exclusion, the Court found that there is a need for a clear regulatory framework that addresses the possibility of exclusion in NIIMS. Despite this possibility, they did not find it as a sufficient reason to find NIIMS unconstitutional.

The Court also ruled that there was sufficient public participation in the process to amend the Registration of Persons Act to create the NIIMS, and to justify miscellaneous amendments to related acts.[3]

However, the High Court struck down the government's decision to roll out Huduma Cards due to violations of the Data Protection Act (2019) on 14 October 2021. The Court found that the government had started collecting personal data from Kenyans without first determining how it would protect that data and that it had "not appreciated the import and the extent of the application of the Data Protection Act with respect to the collection and processing of data under the National Integrated Identity Management System." The court compelled the government to complete a data protection impact assessment, as required by the Data Protection Act, prior to processing data or rolling out Huduma Cards.[4]

This second judgment on the project is yet to be fully implemented. The judgment strengthens the prerequisites contained in the Data Protection Act for the implementation of the digital identity card. It also highlights that a proper understanding of the effects of digitisation of people's identity is necessary in a society where there is a high level of digital exclusion, and a corresponding low level of awareness of digitising personal identity.

Mandatory vaccination and effects of digitisation of government services

The government is on its post-pandemic "building back better" journey and had directed that all who will want to access in-person government services from 21 December 2021 must be fully vaccinated. This directive, which was not promulgated or published in the Kenya Gazette,[5] has digital rights implications as the vaccination certificates in Kenya are digital. On the one hand, this was likely to result in limitations to human rights, in a country where sectors of society have poor access to the internet and low digital literacy. It was also not clear if e-government services will be available to those without vaccination certificates.

Among others, unvaccinated Kenyans were to be excluded from or not able to access universities, hospital and prison visitations, immigration services, the Kenya Revenue Authority (KRA), the National Transport Service Authority (NTSA), and port services.

While the government offered the option of online access to services, this raises the problem of access to the internet and digital devices for the average Kenyan.

Within days following the announcement, the High Court suspended the government directive.

Access to the internet and digital devices

One of the biggest challenges in the digitisation of government services is access to the internet. The uptake of internet services increased in 2020 in light of COVID-19 pandemic mitigation measures that greatly reduced physical contact. To meet the internet demand, bandwidth capacity was increased by 29.6% to 8.1 million Mbps in 2020. The increase of capacity allowed networks to handle the sudden surges and new patterns in internet traffic.[6] According to the DataReportal 2021 report on Kenya, there were 21.75 million internet users in Kenya in January 2021 and internet penetration stood at 40%.[7]

The 2019 Kenya Population and Housing Census results show that 20,694,315 of individuals aged three years and older owned a mobile phone. More females (10,425,040) than males (10,268,651) owned a mobile phone. The data also shows that 22.6% of

3 Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties) [2020] eKLR.

4 Kenya Human Rights Commission. (2021, 18 October). Consortium applauds court judgement declaring Huduma Cards illegal; calls for further reforms. https://www.khrc.or.ke/2015-03-04-10-37-01/press-releases/754-consortium-applauds-court-judgement-declaring-huduma-cards-illegal-calls-for-further-reforms.html

5 http://kenyalaw.org/kenya_gazette

6 Kenya National Bureau of Statistics. (2021). *Economic Survey 2021*. https://www.knbs.or.ke/economic-survey-2021

7 Kemp, S. (2021, 11 February). Digital 2021: Kenya. *DataReportal*. https://datareportal.com/reports/digital-2021-kenya

individuals aged three years and older used the internet, while 10.4% used a computer. The proportion of the population aged 15 years and older who searched and bought goods and services online was 4.3%.[8]

These statistics show that 60% of Kenyans cannot access government services that are available online. Moreover, of those that do access the internet, a relatively small percentage actually use the internet for accessing goods and services. Therefore, accessing government services online is already a challenge for most Kenyans and the sudden digitisation of government services is leading to further exclusion despite the intention being inclusion.

Conclusion

One can see that COVID-19 has resulted in Kenya accelerating its journey in digitising government through projects that had started before the pandemic, such as the Huduma Namba and other e-government services, including eCitizen,[9] the Transport Information Management System,[10] the Kenya Revenue Authority's iTax online service,[11] and the National Education Management Information System (NEMIS).[12]

The key rights issues that this digitisation process highlights concern privacy and exclusion, with two judgments from the High Court handed down with respect to the Huduma Namba project.

What is clear is that the pandemic has rushed the plans for digitisation and pushed policy implementation to short-cut the steps that were necessary to ensure that these plans were inclusive, and came with the proper privacy safeguards. That the digitisation plans were problematic was already recognised prior to the pandemic – in 2015, the Commissioner of Administrative Justice declared a crisis in the issuance of legal documentation in Kenya.

Due to a lack of adequate digital literacy that is needed to enable people to access government services online, many use the help of intermediaries such as cybercafé staff. The challenge with this is that these people – who are not officially trained or mandated to serve as government intermediaries – then have access to a significant amount of personal information and are a potential weak link in the data privacy chain.

Digital literacy training would have helped in at least attempting to ensure that people using computing devices for government services would not need informal third-party assistance. However, the absence of a strategy specifically on this suggests the need for the government to better consider last-mile factors impacting on access before rolling out e-government platforms.

Digital exclusion is just one form of exclusion in Kenya, and the case of the Nubian community show that exclusions are multi-layered and intersectional. Similarly, by introducing the compulsory vaccination e-certificate to access government services, marginalised groups and communities are potentially further isolated from these services.

Transitioning to a digital identification system without first addressing the existing problem of widespread discrimination will not solve these problems. It will, rather, increase discrimination and exclusion.[13] The result now is that civil society needs to push back against the digitisation agenda, firstly, to properly understand the layered exclusions that it implies, and secondly, to ensure that any necessary safeguards to mitigate these exclusions are implemented retrospectively.

Action steps

Civil society organisations need to:

- Create awareness-raising material to inform people on their right to privacy and to support the communities that have been systematically excluded. This could be done in collaboration with relevant regulators and government bodies. A potential ally is the Office of the Data Protection Commissioner, which has shown interest in creating public awareness on the right to privacy.
- Form alliances with organisations representing excluded communities to strengthen advocacy collectives, and to engage meaningfully in litigation where necessary.
- Engage legislators on the human rights implications of the Huduma Namba. This is especially the case now that the Huduma Bill[14] is in Parliament. Civil society organisations need to push for laws and implementation processes that will not result in privacy breaches and the intersectional exclusion of people.

8 Kenya National Bureau of Statistics. (2019). *Kenya Population and Housing Census: Volume IV.* https://www.knbs.or.ke/download/2019-kenya-population-and-housing-census-volume-iv-distribution-of-population-by-socio-economic-characteristics

9 https://www.ecitizen.go.ke

10 https://tims.ntsa.go.ke/login_csp.jsp

11 https://itax.kra.go.ke/KRA-Portal

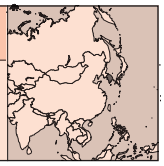
12 http://nemis.education.go.ke

13 Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties) [2020].

14 The Huduma Bill, 2021 proposes that all Kenyans receive the Huduma Namba and subsequently a Huduma Card. The Huduma Namba is based on the National Integrated Identity Management System (NIIMS) database and will be linked to all government services. Without the Huduma Card, a person will not be able to get government services. Part of the Bill reads, "Every resident individual shall have a mandatory obligation to present their Huduma Namba to be issued with a passport, apply for a driving license, register a mobile phone number, register as a voter, pay taxes, transact in the financial market, open a bank account, register a company or a public benefit organization, transfer or make any dealings in land, register for power connection, access universal healthcare services, or register a marriage."

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

DIGITAL RIGHTS AND THE PANDEMIC: LEARNING FROM PERSPECTIVES AND STRATEGIES FROM LATIN AMERICA

Derechos Digitales
Michel Roberto de Souza, Laura Nathalie Hernández Rivera and Jamila Venturini
https://www.derechosdigitales.org

Introduction

Problematic solutions were implemented by different states as part of their health strategies to control the spread of COVID-19. Research carried out by different organisations since the first months of the pandemic in Latin America raised serious concerns related to potential privacy violations, lack of transparency, surveillance, excessive processing of personal data in contact monitoring and tracing applications, and associated risks to other fundamental rights.[1] In trying to combat the pandemic, states placed their trust excessively in technological tools, without carefully assessing potential human rights violations.

In a context where techno-optimism is the dominant discourse, issues such as the increase in exposure notification apps, the use of facial recognition technologies, mandatory data sharing, automation and artificial intelligence (AI) have provoked a lot of debate in Latin America over the past two years. Likewise, debates on internet access policies have also been foregrounded in this period.

In this report we examine how digital rights advocacy priorities and advocacy actions in Latin America have shifted due to the pandemic. We identify several new terrains for engagement, including the human rights consequences of public interest technologies, the usefulness of litigation in protecting rights, and the need to rethink internet access policies in the region.

Latin America and pandemics in a glimpse

As the World Health Organization (WHO) declared a global pandemic on 11 March 2020, Latin American governments started to impose different measures to both prevent the spread of the virus (like quarantines, face masks and other sanitary restrictions) and inform the population on its advance, sometimes relying on technological tools or surveillance systems (such as automated exposure notifications,[2] facial recognition, mandatory data sharing, etc.). Alongside the deployment of health-related technologies by state and private parties, digitisation strategies were developed or implemented in areas such as security, education, social protection and work. However, these measures lacked robust strategies to ensure human rights were respected and vulnerable communities protected.

While governments had already been digitising many of their services, the pandemic, in several cases, forced the transfer of activities online, from the purchase of food and basic supplies to access to and participation in educational, labour and cultural activities. With the rush to lead their populations into a new "normal", little attention was given to the development of connectivity and digital literacy policies that allowed equality in the enjoyment of rights. At the same time, the widespread use of surveillance technologies was not followed by proper safeguards and discussions, raising concerns and gaining attention from the regional digital rights community.

At the other extreme, communities such as Indigenous groups reinforced their historical demands for access to the internet as a basic right that would ensure their safety through access to information and services during quarantine. In Colombia[3] and Brazil[4] they went to courts to force the state to protect their rights to health, life, food security, personal and

1 Hernández, L. (2021). *Uso de Tecnologías para el combate de la pandemia. Datos personales en América Latina*. Global Network Initiative. https://globalnetworkinitiative.org/wp-content/uploads/2021/11/COVID19-LAC-SPA.pdf; Venturini, J., et al. (2021). *Informe Observatorio Covid-19 del Consorcio Al Sur: Un análisis crítico de las tecnologías deplegadas 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(2).pdf

2 For more information on the development of geolocation and automated COVID-19 exposure notification apps, see Venturini, J., Canales, M. P., et al. (2021). Op. cit.

3 Albarracín, M., Bacca, P. I., Quigua, D., Olaya, C., Barragán, M., & Medina, J. (2021, 12 October). Solicitamos a la Corte Constitucional que tutele los derechos vulnerados a los pueblos indígenas del macroterritorio del Yuruparí. *Dejusticia*. https://www.dejusticia.org/litigation/solicitamos-a-la-corte-constitucional-que-tutele-los-derechos-vulnerados-a-los-pueblos-indigenas-del-macroterritorio-del-yurupari

4 Mattia Debastiani, J., Pilau Sobrinho, L., & Calgaro, C. (2020). Covid-19 y políticas anti-indigenistas en el Brasil: el caso ADPF 709/DF para el reconocimiento del derecho a existir. *Nuevo Derecho*, *16*(27), 1-21. http://bibliotecadigital.iue.edu.co/xmlui/bitstream/handle/20.500.12717/2255/1365-Texto%20del%20art%C3%ADculo-5202-1-10-20201130.pdf?sequence=1

collective security, water and a healthy environment. In Brazil, the Federal Supreme Court gave interim orders to the federal government to create an effective and urgent public policy to support Indigenous peoples due to the new coronavirus.[5] One of the recommendations made by the National Council of Justice was to immediately install "communication infrastructure (internet) in villages and surveillance posts to support inspection operations and monitoring of invasions in the area."[6]

In the following section, we present examples of how civil society has dealt with the issues of digital rights during the pandemic in Latin America in the face of the identified threats.

Technologies and human rights: An updated look over the past two years

Evidenced-based knowledge production to inform policy making

A series of problems were identified in the way mobile applications and other systems were implemented in Latin American countries as part of their respective health strategies during the pandemic.[7] A broader study led by the Al Sur Consortium analysed 16 apps and identified problematic points, such as: inequality in access to the internet and technologies; the existence of different applications in the same country; a lack of certainty about whether their use was voluntary; a lack of detail about the security measures adopted in the applications; a reluctance to make the apps' source codes open and transparent; few guarantees of effective control over the use of personal data submitted by users; and a lack of clarity about which institutions could access the data and under what circumstances and conditions.[8] The study concluded that certain aspects need to be considered when the use of technologies imposes risks to the exercise of fundamental rights. It showed that several applications did not respect the principle of legality in the material sense, insofar as limitations to rights were imposed through decisions of an executive power or through administrative decisions. The authors also pointed out that they found no evidence that states had carried out human rights impact assessments prior to the implementation of the technologies.[9]

In this scenario, different Latin American civil society organisations issued recommendations so that the main problems could be corrected. Al Sur recommended paying better attention to inequalities in connectivity; human rights impact assessments to ensure responsible decision making by governments and companies; the need for good data governance; and public transparency in the selection and deployment of the technologies.[10] Data Privacy Brasil also issued a series of principles and recommendations for the legitimate use of personal data in the fight against the pandemic.[11]

Advancing data protection through strategic litigation

While Argentina tries to oblige citizens to use their National Identity Document (DNI) in a hybrid version of the National Census of Populations, Households and Dwellings to be carried out this year, civil society resists. The Vía Libre Foundation filed a *habeas data* appeal,[12] arguing that the incorporation of the DNI in the census could affect the rights to privacy and self-determination in terms of personal data, and

5 APIB. (2020). *Nossa luta é pela vida - Covid-19 e povos indígenas: o enfrentamento das violências durante a pandemia*. https://emergenciaindigena.apiboficial.org/files/2020/12/APIB_nossalutaepelavida_v7PT.pdf

6 CNJ. (2020). Relatório analítico 6/2020 – Anexo Relatório do ISA-IPAM e Ofício nº 653/GAB. https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754595575&prcID=5952986

7 A study covering six Latin American countries identified the following problems: security issues and privacy risks in the design of the tools; excessive data collection in the early stages of application; the excessive proliferation and overlap of applications in the same country; a lack of clarity in linking the use of these tools with a general health strategy; contradictory provisions on the mandatory use of tools; a lack of certainty about how long the personal data collected will be in databases; limited transparency on the development and implementation of the tools and on the agreements signed between private entities and public administrations; and questionable appropriateness of the tools given the digital divide in some countries. Hernández, L. (2021). Op. cit.

8 Venturini, J., et al. (2021). Op. cit.

9 Yael, researching the Coronavirus UY app in Uruguay, in addition to agreeing with some of the findings of the previously cited studies, revealed another negative aspect in the implementation of this type of tool, which is not exclusive to the Uruguayan case. First of all, for the design and implementation of the application, no public call was made; rather, it was done through direct dealings with the company GeneXus, and no open call was made to evaluate the competitiveness of this option against other possible options, either. Secondly, there were no evaluation and monitoring mechanisms for the tool. Yael, D. (2021). *Coronavirus UY y la tecnología como solución a la pandemia*. Derechos Digitales. https://ia.derechosdigitales.org/casos/uruguay-coronavirus-uy

10 Venturini, J., et al. (2021). Op. cit.

11 These recommendations include: the need for technical and scientific reasoning about the necessity and efficiency of the use of personal data; the need for laws and other specific legal regulations to support cooperation between the public and private sectors; all measures employed must be guided by the least possible intrusion on privacy; definition of the purpose of data processing must be specific; the life cycle of the data must be well defined, that is, there must be a time limit for the storage of the data; measures to contain privacy risks must be defined in all cases; maximum transparency regarding measures and their governance must be provided; and open source technologies should preferably be used. Bioni, B., Zanatta, R., Monteiro, R., & Rielli, M. (2020). *Privacidade e pandemia: recomendações para o uso legítimo de dados no combate à COVID-19*. Data Privacy Brasil. https://www.dataprivacybr.org/wp-content/uploads/2020/04/relatorio_privacidade_e_pandemia_final.pdf

12 Fundación Via Libre. (2022, 1 February). Nos presentamos ante la justicia para lograr un #CensoSinDNI. https://www.vialibre.org.ar/nos-presentamos-ante-la-justicia-para-lograr-un-censosindni

conflicted with the Argentine personal data protection legislation. They argue that by including the DNI in the census, personal and sensitive data would be collected, which violates the protection of personal data, since the collection of certain types of information depends on express and informed consent and cannot be mandatory. The contradiction was generated because the census is mandatory, so in practice, it would also be mandatory to include the DNI information. In this case, the National Institute of Statistics and Censuses finally decided to remove the question about the DNI from the census form.[13]

In Brazil, besides the approval of the Brazilian Data Protection Law, two cases judged by the Brazilian Supreme Court represent important privacy developments. The first court action followed Provisional Measure 954 in April 2020, which made it mandatory for telecommunication operators to share personal data with the Brazilian Institute of Geography and Statistics. The Brazilian Bar Association challenged the measure in a constitutional lawsuit. In May, the Supreme Court decided that it was unconstitutional and determined that personal data protection was a fundamental right.[14] The second case questioned a unified database with citizens' information created through Decree 10.046 in 2019. A detailed analysis produced by Coding Rights with the support of Derechos Digitales[15] drew attention to the database and led to the filing of an action of unconstitutionality against the decree. A decision is still pending, but several civil society organisations are acting as *amici curiae* in the case.[16]

In Mexico, the Mexican National Institute of Transparency, Access to Information and Protection of Personal Data challenged in a constitutional lawsuit the amendment to the Federal Telecommunications and Broadcasting Law that created the National Register of Mobile Telephony Users (PANAUT).[17] The amendment compelled the Federal Telecommunications Institute to install, operate, regulate and maintain the PANAUT, as well as obliging concessionaires (entities that have been granted concessions to operate) and authorised telecommunications service providers to collect various personal data, including sensitive data, of users. Civil society also presented a brief as *amicus curiae* in this case.[18]

Understanding and resisting surveillance technologies

Solutions based on artificial intelligence (AI) can create serious violations of human rights. Facial recognition systems, for example, can suffer from biases that result in discrimination and barriers to the effective enjoyment of the rights of certain people belonging to historically marginalised groups. Also, the growing use of video surveillance systems and the use of biometric data represent a new challenge to the privacy of individuals that must be addressed from a multistakeholder and multidisciplinary perspective, adapting advocacy strategies to the evolution of technologies.

When used for surveillance purposes, such technologies reproduce the biases of social exclusion, in addition to threatening the rights to dignity, due process, presumption of innocence, privacy, and freedom of expression and association, among others. The use of these technologies has also been identified as one of the great challenges to the "affirmation of gender and for a broadening of the scope of citizenship."[19] Since the start of the pandemic, the use of software to spy on journalists and human rights activists has resulted in strong criticism and complaints in Mexico[20] and El Salvador.[21]

13 Hayon, A. (2022, 3 February). El Indec quitó el DNI del cuestionario definitivo del Censo. *Pagina 12*. https://www.pagina12.com.ar/399501-el-indec-quito-el-dni-del-cuestionario-definitivo-del-censo

14 Bioni, B., & Monteiro, R. (2020, 9 June). A landmark ruling in Brazil: Paving the way for considering data protection as an autonomous fundamental right. *Future of Privacy Forum*. https://fpf.org/blog/a-landmark-ruling-in-brazil-paving-the-way-for-considering-data-protection-as-an-autonomous-fundamental-right

15 Anastácio, K., Santos, B., & Varon, J. (2020). *Cadastro Base do Cidadão: a megabase de dados*. Coding Rights. https://codingrights.org/docs/megabase.pdf

16 This case was scheduled for trial in February 2022, but at the time of writing, the trial had not started. For more information about the case, see: Secaf, H., Saenger Nuñez, I., & Zanatta, R. (2021, 9 April). O Cadastro Base do Cidadão na Mira do Supremo. *JOTA*. https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/o-cadastro-base-do-cidadao-na-mira-do-supremo-09042021

17 INAI. (2021). Demanda de acción de inconstitucionalidad contra Decreto por el cual se reforman y adicionan diversas disposiciones de la Ley Federal de Telecomunicaciones y Radiodifusión. https://home.inai.org.mx/wp-content/documentos/AccionesYControversias/Demanda_INAI_PANAUT.pdf

18 R3D and others. (2022). Amicus curiae en la acción de inconstitucionalidad 82/2021 y su acumulada 86/2021. https://r3d.mx/wp-content/uploads/Amicus-PANAUT-08022022.pdf

19 Silva, M. R. (2022). Orbitando telas. *Sur – Revista Internacional de Direitos Humanos, 31*. https://sur.conectas.org/orbitando-telas

20 ARTICLE 19. (2021, 18 July). Nuevas revelaciones sobre el uso de Pegasus en México refrendan la necesidad de garantizar verdad, justicia y no repetición en el caso Gobierno Espía. https://articulo19.org/nuevas-revelaciones-sobre-el-uso-de-pegasus-en-mexico-refrendan-la-necesidad-de-garantizar-verdad-justicia-y-no-repeticion-en-el-caso-gobierno-espia

21 Scott-Railton, J., Marczak, B., Herrero, P. N., Razzak, B. A., Al-Jizawi, N., Solimano, S., & Deibert, R. (2022, 22 January). Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware. *The Citizen Lab*. https://citizenlab.ca/2022/01/project-torogoz-extensive-hacking-media-civil-society-el-salvador-pegasus-spyware

Civil society organisations adopted several strategies to deal with the various problems related to facial recognition and other surveillance technologies that increased during the pandemic. First, they have studied the use of these technologies by Latin American states and called for strict democratic controls, which include the criteria of legality, necessity and proportionality, and public supervision, at regional[22] and local[23] levels. In addition, various types of legal challenges have taken place in different countries, with examples of this being the strategic litigation seen in Brazil[24] and Argentina.[25] Civil society also worked with parliamentarians to propose bills that would prohibit the use of mass surveillance technology.[26] Another strategy was to urge the Inter-American Human Rights System to act, denouncing the use of surveillance technologies and their impact on freedom of expression during the pandemic at a hearing[27] and asking for the system to react to the use of spyware.[28] International civil society organisations also spoke out against the use of software to spy on human rights defenders and journalists.[29]

In recent years, several Latin American countries have developed national AI strategies in an effort to set basic principles for the use of the technology. However, some of the first initiatives to develop legislation on AI, such as a new bill in Brazil,[30] have been severely criticised by civil society. They argue that it is important to take advantage of instances that allow for public participation and input, on the one hand to improve public consultation processes and, on the other hand, to influence public policies that bring countries closer to a use of AI that respects human rights.

Exposing inequalities in access to the internet

In Brazil, studies produced by the Brazilian Institute of Consumer Defence (Idec) and Instituto Locomotiva show that the current reliance on mobile internet access by the majority of people is precarious and restricts basic rights by limiting access to education, health, financial and social assistance programmes such as emergency aid during the pandemic. This led to dissatisfaction among people and exacerbated existing vulnerabilities.[31]

Also in Brazil, two cases demonstrate the vulnerability and inequality in internet access during the pandemic. First, the president vetoed a law that attempted to guarantee access to online education during lockdowns. After great pressure from civil society, the National Congress overrode the presidential veto to implement public policies and give students access to the internet.[32] In the second case, the president vetoed the creation of internet hotspots in Indigenous communities. However, this veto was reversed by the National Congress, and the law was enacted in August of the same year – again, after enormous pressure from civil society.[33]

22 Venturini, J., & Garay, V. (2021). *Reconocimiento facial en América Latina: tendencias en la implementación de una tecnología perversa*. Al Sur. https://www.alsur.lat/sites/default/files/2021-11/ALSUR_Reconocimiento_facial_en_Latam_ES.pdf

23 Almeida, M. F., Romero, S., & Thiel, D. (2021). *La videovigilancia en Ecuador vulnera derechos ciudadanos*. Fundamedios. ttps://www.fundamedios.org.ec/wp-content/uploads/2021/12/Inf.-Videovigilancia_01-1.pdf

24 de Souza, M., & Zanatta, R. (2021). The Problem of Automated Facial Recognition Technologies in Brazil: Social Countermovements and the New Frontiers of Fundamental Rights. *Latin American Human Rights Studies, 1*. https://revistas.ufg.br/lahrs/article/view/69423

25 de Souza, M. (2021, 15 October). No bombardeen Buenos Aires: reconocimiento facial en CABA hoy. *Derechos Digitales*. https://www.derechosdigitales.org/16851/no-bombardeen-buenos-aires-reconocimiento-facial-en-caba-hoy

26 Aquino, M. (2021, 19 November). Projeto que bane reconhecimento facial expõe problemas da tecnologia. *Metrópoles*. https://www.metropoles.com/brasil/ciencia-e-tecnologia-br/projeto-que-bane-reconhecimento-facial-expoe-problemas-da-tecnologia

27 R3D. (2021, 27 October). El Estado mexicano debe esclarecer el uso de pegasus y garantizar su no repetición, piden organizaciones ante la CIDH. https://r3d.mx/2021/10/27/el-estado-mexicano-debe-esclarecer-el-uso-de-pegasus-y-garantizar-su-no-repeticion-piden-organizaciones-ante-la-cidh; Derechos Digitales. (2021, 27 October). Derechos Digitales expresa preocupación ante la CIDH por aumento del uso de reconocimiento facial en la región. https://www.derechosdigitales.org/16932/derechos-digitales-participa-de-la-en-la-cidh-en-la-sesion-uso-de-tecnologias-de-vigilancia-y-su-impacto-en-la-libertad-de-expresion-en-pandemia

28 APC et al. (2022, 19 January). Exposed: Civil society condemns use of Pegasus in El Salvador to spy on journalists and activists. https://www.apc.org/en/pubs/exposed-civil-society-condemns-use-pegasus-el-salvador-spy-journalists-and-activists

29 OEA. (2022, 31 January). La CIDH, RELE y OACNUDH expresan preocupación ante los hallazgos sobre uso del software Pegasus para espiar a periodistas y organizaciones de la sociedad civil en El Salvador. https://www.oas.org/pt/CIDH/jsForm/?File=/es/cidh/prensa/comunicados/2022/022.asp

30 Coalizão Direitos na Rede. (2021, 7 December). Brasil não está pronto para regular inteligência artificial. https://direitosnarede.org.br/2021/12/07/brasil-nao-esta-pronto-para-regular-inteligencia-artificial

31 Idec & Instituto Locomotiva. (2021). *Barreiras e limitações no acesso à internet e hábitos de uso e navegação na rede das classes C, D e E*. https://idec.org.br/sites/default/files/pesquisa_locomotiva_relatorio.pdf

32 The Brazilian Congress passed a law with the purpose of guaranteeing access to the internet for educational purposes for students and teachers of public basic education. It provided for the allocation of resources (around USD 650,000) from the Fund for the Universalisation of Telecommunications Services (FUST) to be used in the contracting of mobile data packages and purchase of equipment for students and teachers in public schools across the Brazilian states, the Federal District and municipalities that have adopted remote or hybrid learning. Coalizão Direitos na Rede. (2021, 14 April). Não há educação sem conexão: Nota da Coalizão Direitos na Rede pela derrubada imediata do veto presidencial ao PL 3477/20. https://direitosnarede.org.br/2021/04/14/nao-ha-educacao-sem-conexao

33 For instance, Law No. 14021/2020 set up social protection measures to prevent the spread of COVID-19 in Indigenous territories. Oliveira, J. (2020, 19 August). Congresso derruba vetos de Bolsonaro e obriga Governo a garantir UTIs a indígenas na pandemia. *El País*. https://brasil.elpais.com/brasil/2020-08-20/congresso-derruba-vetos-de-bolsonaro-e-obriga-governo-a-garantir-utis-a-indigenas-na-pandemia.html

Other countries faced similar challenges. Ecuador, for instance, tried to close several public centres for internet access that are key for connectivity in rural areas – the so-called "infocentros".[34] The measure would have affected the internet access of four million people,[35] but the decision was suspended after pressure from popular movements and other institutions.[36]

In Colombia, the problem of inequalities in access to the internet is due to the lack of infrastructure in different geographic regions, as well as the high cost of data in relation to the minimum wage.[37] The country nevertheless made a positive change to overcome this situation by enacting a law that declared the internet an essential and universal public service.[38] In Argentina, through the Decree of Necessity and Urgency No. 690/2020, ICTs and access to telecommunications networks were also considered essential and strategic public services. However, the measure was later suspended by the judiciary,[39] a move which was criticised by civil society.[40]

Conclusion

Throughout this report, we have briefly identified the trends in the use of technology in the context of the COVID-19 pandemic – especially measures taken by governments – as well as the strategies adopted by civil society organisations in the face of the different threats to the enjoyment of human rights that resulted from their implementation. As technologies evolve and their use becomes more common, it also becomes necessary for civil society to further develop an agenda that takes into consideration the various impacts such technologies have on society, including an increase in inequalities for particularly vulnerable groups that risk being left behind.

The technological measures implemented by states as part of their health strategies to mitigate the effects of the COVID-19 pandemic proved to represent risks not only to privacy and informational self-determination, but also to a vast number of economic and social rights. As the threat from the pandemic changed with the introduction of vaccination and restrictions were relaxed, we can reflect and learn from the diverse experiences in different countries over the past two years. But doing this we can prepare a renewed advocacy agenda that pays closer attention to those technologies that were either already being implemented before the pandemic or were implemented because of it. It is particularly concerning that the health emergency served as a justification for the digitisation and datafication of information and services in several areas, as well as for the acquisition of surveillance technologies that are increasingly used for other purposes. On the other hand, it seems to be extremely relevant for civil society to refocus on the issue of inequalities in internet access in communities where the digital gap is prominent.

This new scenario makes it necessary to rethink strategies to ensure respect for human rights, particularly in the digital sphere. In this regard, we highlighted the findings of evidence-based regional research and strategic litigation seen in different countries. Due to the increase in techno-authoritarianism in several states, research and developing recommendations for improvements and writing joint statements are very useful tools for civil society and can be complemented by other strategies. For example, these include filling *habeas data* and collective *amparo*[41] processes in constitutional matters, actively participating in the discussions at the Inter-American Human Rights System and presenting *amicus curiae* briefs. All of this should be done through the collaboration of human rights organisations flourishing in Latin America.

34 https://infocentros.mintel.gob.ec/estadisticas-infocentros

35 Dávalos, N. (2020, 20 July). "Más de 4 millones de personas serán afectadas por cierre de infocentros". *Primicias*. https://www.primicias.ec/noticias/tecnologia/millones-personas-seran-afectadas-cierre-infocentros

36 Defensoría del Pueblo de Ecuador. (2020, 24 July). La defensoría del pueblo presenta acción de protección en contra del cierre de Infocentros en el país. https://www.dpe.gob.ec/la-defensoria-del-pueblo-presenta-accion-de-proteccion-en-contra-del-cierre-de-infocentros-en-el-pais

37 Saavedra, V., Ospina, D., Upegui, J. C., & Torres, D. (2021). *Desigualdades digitales. Aproximación sociojurídica al acceso a Internet en Colombia*. Editorial Dejusticia. https://www.dejusticia.org/wp-content/uploads/2021/08/Docs71-DesigDigital-Web-Sep23.pdf

38 This legislation guarantees internet service in an "efficient, continuous and permanent way," making it available to everyone and in emergency situations. Ley No. 2108, 29 July 2021. Ley de internet como servicio público esencial y universal. https://dapre.presidencia.gov.co/normativa/normativa/LEY%202108%20DEL%2029%20DE%20JULIO%20DE%202021.pdf

39 Nuevo Diario. (2021, 21 December). Fue suspendido el DNU que declaró esenciales a las telecomunicaciones. https://www.nuevodiariodesalta.com.ar/noticias/judiciales-6/fue-suspendido-el-dnu-que-declaro-esenciales-a-las-telecomunicaciones-61648

40 Bizberge, A. (2020, 26 August). Declaran servicio público en competencia a la telefonía móvil, acceso a Internet y TV paga en Argentina. *OBSERVACOM*. https://www.observacom.org/declaran-servicio-publico-en-competencia-a-la-telefonia-movil-acceso-a-internet-y-tv-paga-en-argentina

41 "'Amparo' is a proceeding for the protection of fundamental rights in case of violations and it is a Latin American contribution to constitutional procedural law." Landa, C. (2011). El proceso de amparo en América Latina. *Anuario de derecho constitucional latinoamericano, Año XVII*, 207-226. https://www.corteidh.or.cr/tablas/r27649.pdf

Action steps

Considering what was discussed in this report, the following are our recommendations to improve advocacy on issues related to the use of technology, from a human rights perspective:

- Continue to report and document cases where the use of technologies potentially poses risks to human rights.
- Strengthen collaboration between organisations in research and advocacy against inequalities in internet access, especially in areas and population groups with higher levels of vulnerability.
- Working with other organisations, lodge complaints against infringements of human rights at the relevant institutions, in the shortest time possible.
- Form and strengthen coalitions for strategic litigation on digital rights.
- Actively participate in the sessions and cases of the Inter-American Human Rights System and when possible, participate as *amicus curiae*.
- Increase participation in national legislative processes through creating collective submissions from civil society.

LATIN AMERICA

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[1] – 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

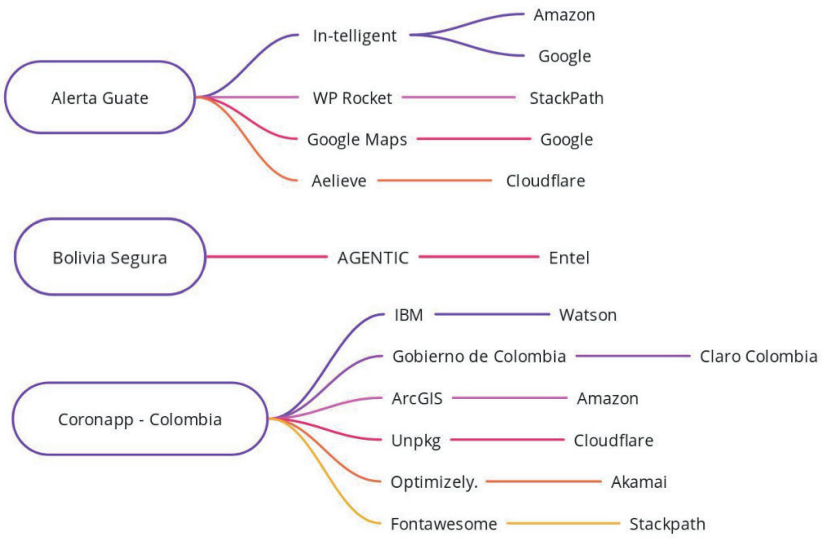


FIGURE 1 *(cont.)*

The service providers used by different apps

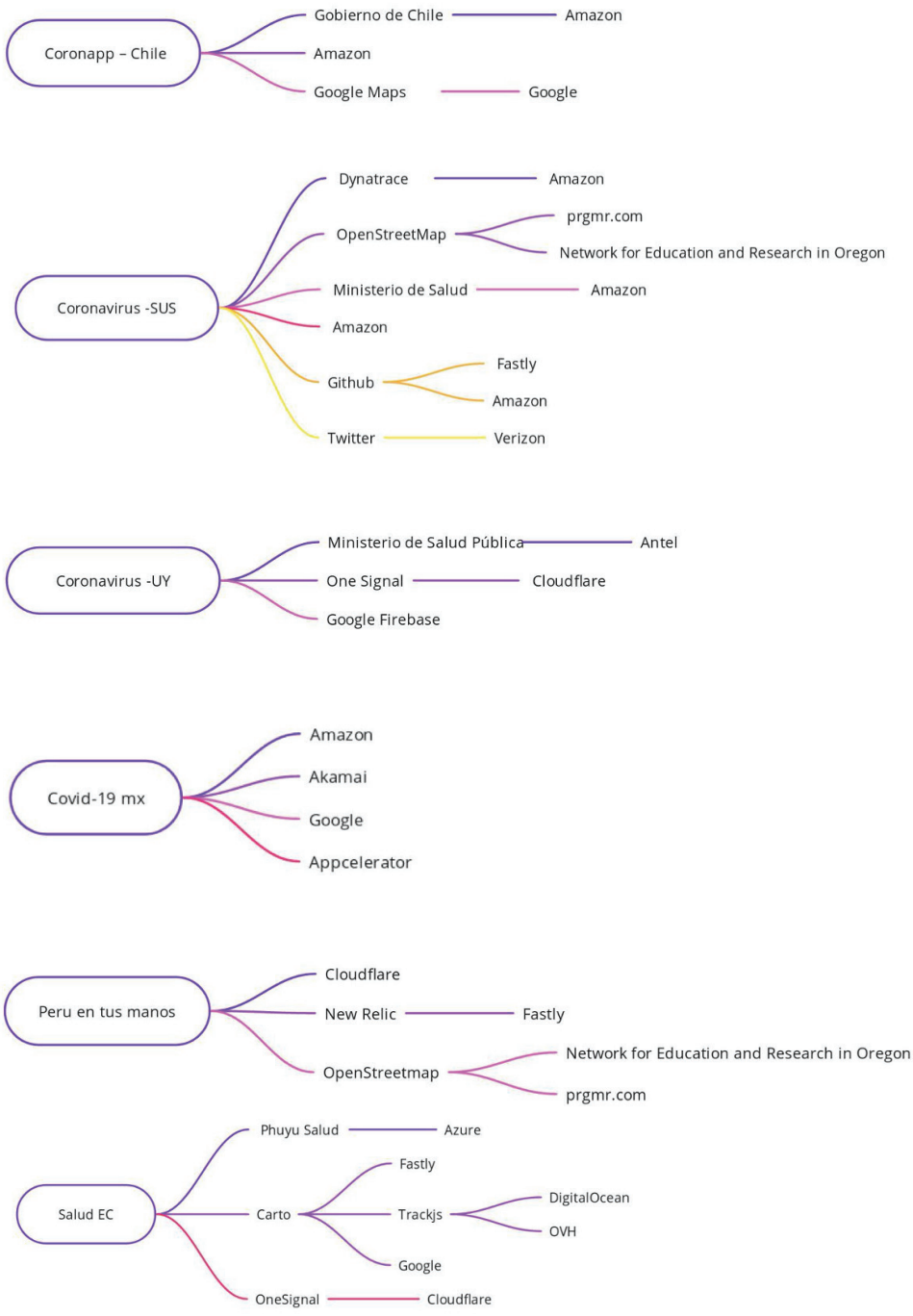
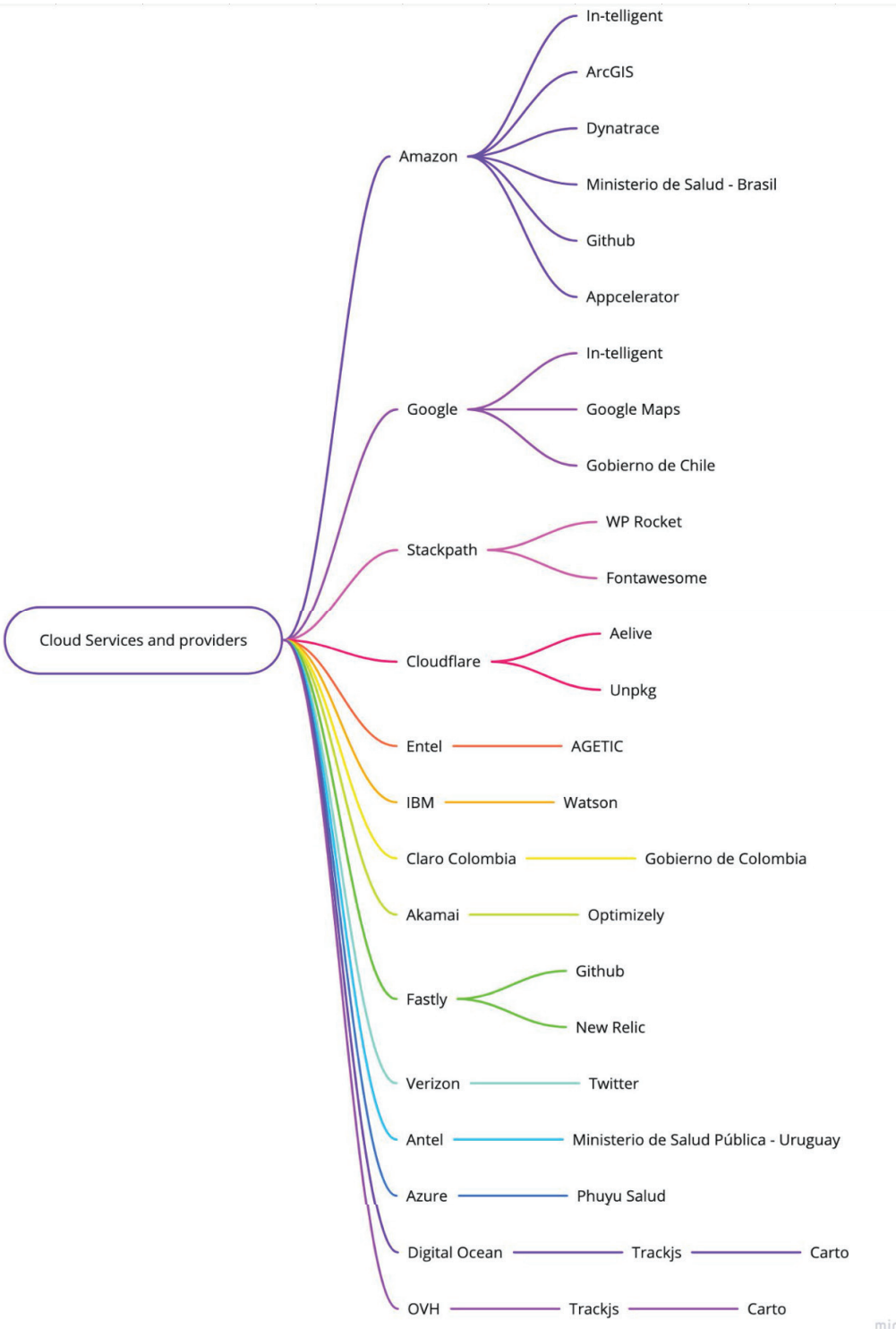


FIGURE 2

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

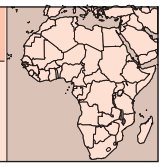
The following points need to be kept in mind when governments propose the use of technologies for monitoring public health or other crises:

- 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

MALAWI

FIGHTING ONLINE MISINFORMATION AND DISINFORMATION IN MALAWI AMIDST THE COVID-19 PANDEMIC: A MULTISTAKEHOLDER COLLABORATIVE APPROACH



University of Livingstonia, Malawi, and Kwame Nkrumah University of Science and Technology, Ghana
Donald Flywell Malanga and Eunice Adu Boahen
www.unilia.ac.mw; donaldflywel@gmail.com; www.knust.edu.gh; boatengeunice@ymail.com

Introduction

The rapid advancement in information and communications technologies (ICTs) in recent years has revolutionised the way we live and connect with each other. This digital revolution has brought unprecedented and transformational economic and social benefits.[1] However, the rewards of this digital transformation are also being overshadowed by the global spread of online misinformation and disinformation, also known as an "infodemic".[2] Digital rights such as freedom of expression, access to information online and online safety are all under threat by the rapid dissemination of false and malicious online information within and across national borders.[3] Prior studies have shown that online misinformation and disinformation are complex problems that do not suit a one-size-fits-all solution. To this end, effective mitigation can only be achieved through long-term strategies involving multistakeholder collaboration and cooperation between governments, digital platforms, civil society and other actors.

In Africa, online misinformation and disinformation have grown recently, both in form and prevalence. However, the challenges of combating them are equally burgeoning, and measures to curb them remain inadequate and often inappropriate.[4] Attempts by some African governments and digital platform companies to tackle them have been besieged by multiple challenges and policy shortcomings, with the lack of coordination and cooperation among key stakeholders being a major concern. These challenges were further exacerbated by the global COVID-19 pandemic.[5]

Malawi, being part of the global community, is not spared from online misinformation and disinformation. Undocumented reports indicate that while internet and ICT access is increasing, online misinformation and disinformation are also on the rise at unprecedented levels,[6] particularly during the COVID-19 pandemic period. As has been argued, tackling online misinformation and disinformation requires a multistakeholder effort due to the complexity and multi-layered problems associated with them.[7] To this end, this report, which shares the findings of interviews with 13 respondents from across different sectors in Malawi, adopts a multistakeholder approach to generate evidence on efforts in combating online misinformation and disinformation in the country amidst the COVID-19 pandemic.

Study context

Malawi gained its independence from Great Britain in 1964. It borders Tanzania, Zambia and Mozambique. The country has an estimated population of 17.7 million people, of which 85% live in rural areas.[8] The gross domestic product (GDP) per capita is USD 636.8.[9] Most women work in the agricultural sector, which is a backbone of Malawi's economy. Of those in non-agricultural waged employment, 21% are women and 79% are men, and the numbers have remained the same over the years.

Despite Malawi having the lowest ICT penetration rate in the Southern African Development

1 Okeleke, K., & Robinson, J. (2021). *Exploring online misinformation and disinformation in Asia Pacific*. GSMA. https://www.gsma.com/asia-pacific/wp-content/uploads/2021/07/190721-Exploring-misinformation-in-Asia-Pacific-1.pdf

2 Paine, J. (2021, 25 June). The future of Asia's battle against online misinformation. *The Diplomat*. https://thediplomat.com/2021/06/the-future-of-asias-battle-against-online-misinformation

3 Colomina, C., Sánchez Margalef, H., & Youngs, R. (2021). *The impact of disinformation on democratic processes and human rights in the world*. European Union. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653635/EXPO_STU(2021)653635_EN.pdf

4 CIPESA. (2021, 26 October). Combating disinformation in Africa: Challenges and prospects. https://cipesa.org/2021/10/combating-disinformation-in-africa-challenges-and-prospects/

5 Ibid.

6 Kainja, J. (2020, 7 October). How lack of access to information and ICTs has fueled disinformation in Malawi. *CIPESA*. https://cipesa.org/2020/10/how-lack-of-access-to-information-and-icts-has-fueled-disinformation-in-malawi

7 Ngwira, K. (2021, 13 January). A view from Malawi: Combating fake news and the "infondemic". *Thomson Reuters Foundation*. https://www.trust.org/i/?id=9f827934-ce2c-4ad5-boed-d8abbce47881

8 https://data.worldbank.org/indicator/SP.POP.TOTL

9 https://data.worldbank.org/indicator/NY.GDP.PCAP.CD

TABLE 1.

List of respondents who were interviewed.

Code	Position	Sector
Resp 1	Lawyer	Government
Resp 2	Digital human rights defender	Civil society
Resp 3	Gender specialist	Civil society
Resp 4	ICT expert	ICT regulator
Resp 5	ICT expert	Private
Resp 6	Researcher	Academia
Resp 7	Media expert	Print media
Resp 8	Police officer	Law enforcement
Resp 9	Policy expert	Academia
Resp 10	Political and social commentator	Academia
Resp 11	Representative	Tech companies
Resp 12	Representative	Community-based organisation
Resp 13	Media professional	Online media

Community (SADC),[10] online misinformation and disinformation are on the rise. International Telecommunication Union (ITU) statistics show that 14% of the population uses the internet in Malawi while 52% of Malawians have mobile phones. Access to mobile broadband is estimated at 25.5% and fixed-line broadband is 0.06%.[11]

There are also gender disparities when it comes to ICT ownership in the country. About 34.2% of women own a mobile phone, and 3.9% own a desktop computer, while just 5.2% of them have access to the internet.[12]

Meanwhile, 3% of the population has internet access in rural areas compared to 24.3% in the urban population. Computer access in rural areas remains at 2.1% while it is 19.2% in urban areas.

Airtel (Mw) and Telecom Networks Malawi (TNM) remain the two dominant mobile operators in the country, while Malawi Telecommunication Limited (MTL) is the only fixed-service provider. The Malawi Communication and Regulatory Authority regulates the telecommunication sector in the country

Poor access to ICT services such as the internet is largely attributed to poor ICT infrastructure and high tariff charges imposed on ICT services. These include 16.5% value added tax (VAT) on internet services, 17.5% VAT on ICT gadgets, and 10% excise duty on mobile text messages and mobile data transfers.[13]

Access to the internet is cost-prohibitive for the majority of Malawians. For instance, a monthly data bundle of 10 gigabytes (GB) costs USD 21 with both Airtel and TNM. This cost is equivalent to half the minimum monthly wage of the majority of Malawians. Reflecting this, the Inclusive Internet Index 2021, which measures internet affordability, availability, relevance of content and readiness, ranked Malawi 114th out of 120 countries.[14]

Methodology

To achieve the objectives of the report, the researcher gathered data through literature and policy reviews, and conducted online in-depth interviews with key informants representing both state and non-state institutions. About 13 experts drawn from the ICT sectors, including journalists, media regulators, editors, digital platform experts, digital rights activists and civil society actors, participated in the study. Table 1 provides a list of respondents to the study, their positions and category of sectors they belonged to.

10 Malanga, D. F., & Simwaka, K. (2021). ICTs as potential enablers of the green economy in the Southern African Development Community. In A. Finlay (Ed.), *Global Information Society Watch 2020: Technology, the environment and a sustainable world: Responses from the global South*. Association for Progressive Communications. https://giswatch.org/node/6230

11 https://www.itu.int/net4/ITU-D/idi/2017

12 Malanga, D. F. (2019). Framing the impact of artificial intelligence on the protection of women's rights in Malawi. In A. Finlay (Ed.), *Global Information Society Watch 2019: Artificial intelligence: Human rights, social justice and development.* Association for Progressive Communications and ARTICLE 19. https://giswatch.org/sites/default/files/gisw2019_web_malawi.pdf

13 Kaiyatsa, M. (2020, 5 August). Digital rights remain under threat in Malawi despite historic win for democracy. *Global Voices*. https://advox.globalvoices.org/2020/08/05/digital-rights-remain-under-threat-in-malawi-despite-historic-win-for-democracy

14 https://theinclusiveinternet.eiu.com/explore/countries/performance

The data collected from the respondents was analysed thematically. Specific questions that respondents were asked included the following:

- What do you understand about online misinformation and disinformation?
- What is the prevalence of online misinformation and disinformation in the country?
- What factors do you think are fuelling the spread of online misinformation and disinformation?
- What are the impacts of online misinformation and disinformation?
- What do you think should be done to fight or tackle online misinformation and disinformation in the country?

Findings

Defining online misinformation and disinformation

Among those who participated in the study, there were significant disparities in the views on what constitutes online misinformation and disinformation. Some viewed online misinformation and disinformation as the same, since they both deal with spreading misleading and unverified information. Others viewed online misinformation as a "broader concept that deals with spreading fake news knowingly or unknowingly" (resp 5), while disinformation was "about spreading wrong information aimed at harming other people" (resp 7). From this it was clear that a lack of standardised or shared definitions of online misinformation and disinformation was a problem.

This lack of consensus on definitions has been reported previously by scholars. Nevertheless, some of the respondents' understandings were close to generally accepted definitions such as online misinformation referring to the spread of erroneous online information without the intention of causing harm and online disinformation being a deliberate, coordinated and malicious attempt to spread false information.[15]

Prevalence of online misinformation and disinformation and factors fuelling its dissemination

The study also solicited views from respondents on the nature and prevalence of online disinformation in Malawi.

There was a consensus among participates that during the COVID-19 pandemic, online misinformation and disinformation was a major concern and remains an existential threat, not only to public health, but also to democracy in the country. It emerged that the nature or forms of online misinformation and disinformation focused on public health, socioeconomic issues and violence, had a gender dimension, and included cybercrime. For instance, claims that the COVID-19 pandemic was caused by 5G networks circulated online, and there was fake news about the treatment of COVID-19 using various concoctions and herbal medicine. Respondents also acknowledged that gendered online misinformation and disinformation such as false, misleading or harmful content that exploits gender inequalities[16] or invokes gender stereotypes and norms are common.[17] Furthermore, respondents also noted that online misinformation and disinformation about the COVID-19 vaccine is rampant. "People are told that vaccine is meant to kill them, and it is associated with devil and the coming of 666" (resp 8). Consequently, this has led to low uptake of COVID-19 vaccines in the country.[18]

Moreover, politically motivated online disinformation is also increasing. For instance, there has been fake news circulating on various digital platforms aimed at discrediting political opponents.[19] This has exacerbated political violence in the country.

The observed motivations, according to the study participants, ranged from financial, to a delight in causing mischief, and stoking political tensions. Respondents also indicated that online misinformation and disinformation are fuelled by the mainstream media spreading fake news, the politicians using the media to discredit opponents, and the rapid increase in the usage of social media such as WhatsApp and Facebook.

Furthermore, it also emerged that the COVID-19 outbreak has intensified the spread of disinformation in the country. It is therefore evident that online misinformation and disinformation can be considered prevalent in the country. They exist in the form of misleading, fake, fabricated, manipulated and "imposter" content and are associated with public health, religious, political, gender, social and economic issues.

15 Colomina, C., Sánchez Margalef, H., & Youngs, R. (2021). Op. cit.

16 EU DisinfoLab. (2021, 20 April). Gender-based disinformation: Advancing our understanding and response. https://www.disinfo.eu/publications/gender-based-disinformation-advancing-our-understanding-and-response

17 Scott, V. (2021). *Understanding the gendered dimension of disinformation*. Countering Disinformation. https://counteringdisinformation.org/topics/gender/complete-document-gender-dimensions

18 Tembo, L. (2022, 2 January). Tackling COVID-19 vaccine misinformation through faith leaders. *UNICEF Malawi*. https://www.unicef.org/malawi/stories/tackling-covid-19-vaccine-misinformation-through-faith-leaders

19 Kondowe, R. (2019, 10 May). Despite a low internet penetration, Malawi is worried about fake news in its election run-up. *Quartz*. https://qz.com/africa/1616511/malawi-election-has-a-fake-news-problem-on-whatsapp-facebook

Impact of online misinformation and disinformation

Respondents were asked to provide their perceptions on the consequences of online misinformation and disinformation. The study found that online misinformation and disinformation have negative effects on people and society at large. Interviewees noted that they have impacted negatively on human rights and democratic processes,[20] and resulted in digital violence and the repression of marginalised groups such as women and minorities.[21] The impacts can be divided into several categories:

- **Impact on human rights:** Studies have shown that online misinformation and disinformation infringe on human rights. Respondents stated that it affected the right of freedom of thought and the right to hold opinions without interference. The right to privacy and freedom of expression both online and offline were hampered. In addition, online misinformation and disinformation also negatively affected the economic, social and cultural rights of citizens in the country.
- **Impact on democratic processes:** The arrival of COVID-19 coincided with the rerun of the presidential elections in 2020, after the 2019 presidential elections were annulled by Malawi's Constitutional Court for serious irregularities. In this regard, political misinformation and disinformation exacerbated the mistrust of democratic processes and institutions such as the courts and parliamentary processes, as well as of political figures. Some journalists and political figures have been frequent targets for online attacks. Due to the spread of online political disinformation, citizens may pull out from participating in public affairs, believing that behind-the-scenes political interference would make their participation ineffective.
- **Cyber violence and the repression of vulnerable groups**: Article 20(2) of the International Covenant on Civil and Political Rights states that "any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law."[22] Online disinformation is often associated with the rise of cyber violence against women, girls, children and other vulnerable groups.[23] Cyber violence includes a range of controlling and coercive behaviours such as cyber stalking or harassment on social media. In this study, participants acknowledged that online misinformation and disinformation result in an increase in gender-based cyber violence against women and girls.[24] This in turn has the potential to affect the victims socially, economically, emotionally and physically.[25]
- **Impact of the COVID-19 infodemic on citizens:** Respondents were also of the view that the COVID-19 infodemic, which increased the spread of fake news such as hoaxes and conspiracy theories about the pandemic and vaccines, has also led to a mistrust in public institutions, putting the lives of people at risk. Online disinformation spread during the pandemic has included disinformation legitimised by being falsely attributed to well-known public or political figures.[26] It also became clear that some of the regulations targeting misinformation and disinformation during the pandemic have involved new limits on press freedom and resulted in censorship tools that are likely to be used beyond the COVID-19 crisis.[27]

Approaches to fighting online misinformation and disinformation

In taking measures to address the entire spectrum of online misinformation and disinformation, it is important to look at the different actors involved, together with their actions taken.[28] In this study, participants were asked about the approaches that the government, digital platforms, civil society, and academia have taken to address the spread of online misinformation and disinformation in the country. It was noted that the respondents had different opinions:

- **Government:** On the part of the government, it was noted that existing laws can help to fight online misinformation and disinformation. These include the Penal Code (1930),[29] Communications Act (1998), Electronic Transaction and Cyber Security Act (2016), Access to Information Act (2016) and Data Protection Bill (2021).[30]

20 Colomina, C., Sánchez Margalef, H., & Youngs, R. (2021). Op. cit.

21 Okeleke, K., & Robinson, J. (2021). Op. cit.

22 https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

23 Malanga, D. F. (2021a). *Tackling gender-based cyber violence against women and girls in Malawi amidst the COVID-19 pandemic*. African Declaration on Internet Rights and Freedoms Coalition. https://africaninternetrights.org/sites/default/files/Donald_Flywell-1.pdf

24 Malanga, D. F. (2021b). *Survey of cyber violence against women in Malawi*. Proceedings of the 1st Virtual Conference on Implications of Information and Digital Technologies for Development. https://arxiv.org/ftp/arxiv/papers/2108/2108.09806.pdf

25 Malanga, D.F (2021a). Op. cit.

26 Pierri, F., et al. (2021). *Online misinformation is linked to early COVID-19 vaccination hesitancy and refusal*. arXiv. https://arxiv.org/abs/2104.10635

27 Colomina, C., Sánchez Margalef, H., & Youngs, R. (2021). Op. cit.

28 Ibid.

29 https://malawilii.org/akn/mw/act/1929/22/eng%402014-12-31

30 Malanga, D. F. (2020). *Londa: Malawi Digital Rights and Inclusion 2020 Report*. Paradigm Initiative. https://paradigmhq.org/report/londa-malawi-digital-rights-inclusion-2020-report

While there was a consensus among research participants on the need for the government to regulate harmful online content, others criticised the move as a precursor to suppressing civic space and freedom of expression. Participants questioned the effectiveness of these existing laws and ways in which the government has applied them to silence critics. Apart from legal measures, some participants identified raising the digital literacy of the general public as an essential means to combating misinformation and disinformation in Malawi.

- **Digital platforms:** Studies have shown that digital platforms such as Twitter, Facebook and YouTube, among others, have introduced a number of measures in recent years to tackle online misinformation and disinformation. Salient examples include content removal, platform bans and feature limits (such as limiting the number of words that can be typed or shared via Twitter), and fact-checking and digital literacy initiatives. However, in this study, the majority of participants identified few measures that digital platforms have used to combat online misinformation and disinformation in the country. The participants suggested removing online content and banning perpetrators from digital platforms as measures.
- **Civil society:** Civil society is critical in countering online misinformation and disinformation. This may involve a variety of programmes such as fact checking, advocacy focused on government or on online platforms, public awareness campaigns, identifying online disinformation narratives, and building trusted networks for sharing accurate information.[31] In this study, it was found that most research participants acknowledge that civil society organisations have not done enough to combat online misinformation and disinformation. However, it was noted that collaborations between and among digital platforms, government regulators and international organisations can help to build stronger resilience and cooperation in tackling online misinformation and disinformation challenges.
- **Academia:** In the context of academia, it was found that while acknowledging the bourgeoning of online disinformation and misinformation in the country, higher education institutions have done very little research on the topic. It was noted that digital literacy programmes in higher education have focused on students, and there was no wider policy initiative to expand digital literacy programmes to the general public, including for different age groups, as one of the ways of combating online misinformation and disinformation in the country.

Obstacles to combating online misinformation and disinformation

Despite the various approaches that the government, civil society and digital platforms are using to combat online misinformation and disinformation in the country, there are still a number of ongoing obstacles that undermine effective responses. The study found that the massive flow of information and content across national boundaries makes it difficult to fight online misinformation and disinformation, especially where there is disagreement on what constitutes misinformation or disinformation. It was also noted that the government has used existing laws to silence critics. This has a negative effect on freedom of speech, media freedom and political pluralism. Some civil society participants also accused the government of using existing laws to target their political opponents, religious groups, journalists and human rights defenders. Besides this, it was revealed that the government has little control over social media, where most misinformation and disinformation are shared and consumed.[32]

Furthermore, it was found that despite digital platforms making significant efforts to combat online misinformation and disinformation in the country, they face a number of challenges. The detection of online misinformation and disinformation on different platforms is difficult. The digital platform representative stated that online content encrypted by digital platforms make it difficult to detect misinformation and alert users about its spread.

Despite their efforts, digital platforms were criticised by some research participants for a lack of transparency. Digital platforms provide inadequate reporting on the scale of disinformation and misinformation and were not being transparent enough about what they are doing to manage them.

While the lack of consensus on definitions of online misinformation and disinformation among stakeholders makes it difficult to define proper strategies for addressing them, respondents agreed that a lack of engagement and collaboration between all stakeholders on the problem made it even more difficult to address the issue properly. These included policy makers, civil society, tech companies,

31 Studdart, A. (2021). *Building capacity for civil society to mitigate and counter disinformation*. Countering Disinformation. https://counteringdisinformation.org/topics/csos/complete-document-civil-society

32 Ngwira, K. (2021, 13 January). Op. cit.

academia, grassroots community-based organisations and media groups.

Conclusion

The study has revealed that online misinformation and disinformation are bourgeoning in the country. While the two phenomena are not new, a number of factors have fuelled them: the unprecedented growth of social media usage; the involvement of mainstream media in spreading false information; the influence of politics on the media; and the outbreak of the COVID-19 crisis. The study has also found that online disinformation and misinformation have impacted on human rights and democratic processes and increased gender-based cyber violence and the repression of vulnerable groups. Furthermore, it found that despite various initiatives to address the challenge (including legislation and interventions by digital platforms), the lack of coordinated and collaborative efforts among stakeholders remains a problem. While substantial progress has been made to combat online misinformation and disinformation in the country, ongoing challenges remain clear. To address these ongoing obstacles, multistakeholder and multidimensional approaches are required.

Action steps

Based on the findings of the study, the following multi-dimensional action steps are proposed:

- Improve media and information literacy: Empowering the users of platform services is a key element to increase the resilience of society to various forms of online misinformation and disinformation.[33] There is therefore a need to promote media and information literacy to counter online misinformation and disinformation. This will help users to navigate the digital media environment more effectively and identify online misinformation and disinformation when they occur. Actions for supporting media and information literacy programmes for people of all ages should be developed.
- Develop online tools for empowering both information users and providers: There is a need to develop tools for empowering users and information providers such as journalists to tackle online misinformation and disinformation and enhance positive engagement with fast and emerging digital technologies in the country.[34] Some examples of existing tools include Checkology, ClaimBuster, Fake Bananas, Botometer, Disinformation Index and NewsCheck Trust Index.[35]
- Strengthen transparency and accountability: There is a need to improve the transparency of online information sources, as well as the sources of funding that allow content to be developed. Fact-checking practices and initiatives need to be strengthened.[36] The lack of transparency among content developers may contribute to conspiracy theories, particularly if they are not willing to reveal their sources of funding and the way they operate. This in turn may lead to breeding online misinformation and disinformation.
- Promote research and development: There is a need to continue researching the impact of online misinformation and disinformation in Malawi, including reviews of the steps taken by different actors, in order to constantly encourage the necessary adjustments to responses.
- Protect the diversity and sustainability of the digital media ecosystem: This can be in the form of supporting actions that encourage press freedom and pluralism; the funding of projects that support quality digital journalism; and investing in research and innovative actions to improve technologies for online media services in the country.

33 European Commission High Level Expert Group on Fake News and Online Disinformation. (2018). *A multi-dimensional approach to disinformation: Report of the independent High Level Group on fake news and online disinformation*. European Commission. https://coinform.eu/wp-content/uploads/2019/02/EU-High-Level-Group-on-Disinformation-A-multi-dimensionalapproachtodisinformation.pdf

34 Ibid.

35 For more examples of tools see: Stellino, M. (2019, 24 January). 8 resources to detect fake news. *News Co/Lab*. https://newscollab.org/2019/01/24/8-resources-to-detect-fake-news and https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search.html

36 Lubisi, N. (2021, 20 October). A multi-stakeholder partnership to combat disinformation. *Media Monitoring Africa*. https://mediamonitoringafrica.org/media-release-a-multi-stakeholder-partnership-to-combat-disinformatio

MEXICO

LESSONS LEARNED ON THE DESIGN OF A STATE CONNECTIVITY PLAN FOR INDIGENOUS AND RURAL COMMUNITIES DURING COVID-19

Centro de Investigación en Tecnologías y Saberes Comunitarios
Carlos F. Baca-Feldman
https://citsac.org/en

Introduction

The arrival of the COVID-19 pandemic in 2020 marked a turning point in the social, political, economic and cultural life of almost every country in the world. Under these sudden and unexpected circumstances, access to the digital world appeared to many of us as the "great solution to the pandemic". However, since 2020, the inequalities generated by the digital divide have become increasingly evident, bringing with them a series of public policies and actions undertaken by various stakeholders.

This report reflects on the public policies aimed at expanding coverage and access to telecommunications services in Mexico, which have not been particularly successful during the pandemic. What we have observed is the repetition of public connectivity policies that have not been successful in the past.

The report offers a brief review of these federal strategies before considering the importance of local and state governments in creating enabling environments for the full access of their population to telecommunications services. The report then describes the design of a strategic connectivity plan, developed by the civil association Redes por la Diversidad, Equidad y Sustentabilidad (REDES) for the Coordination of Digital Policy (CPD), an office set up by the government of the state of Chihuahua which was in power from 2016 to 2021.

This report draws on the results of a collective process of research and analysis in which many organisations have been involved, including REDES, Construcción de Mundos Alternativos Ronco Robles, Rhizomatica, and the civil association Telecomunicaciones Indígenas Comunitarias, among other stakeholders who are committed to developing relevant digital strategies in Chihuahua.

What is the status of Mexico's national digital strategy?

A quick look at connectivity rates in Mexico shows that there is continuous growth in the number of internet users. According to a national household survey on technology availability and usage, *Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares 2020*,[1] the number of internet users over the age of six in 2015 was 62.4 million (57.4%), rising to a total of 84.1 million (72%) in 2020. This means that in five years, the number of total users increased by over 20 million, or 14.6% of the target population. However, a close analysis of the statistics suggests that this continuous growth has not been the same for *all* the people living in the country. For example, in rural areas only 50.4% of the population uses the internet, compared to 78.3% in urban areas. This data helps us to understand the problem that accessing and exchanging information through information and communications technologies (ICTs) poses for half of the rural population and a little more than 20% of the urban population in Mexico.

The actions developed by the Mexican federal government during the COVID-19 pandemic have focused on the dissemination of information, not on the expansion of access to telecommunications services among the unconnected population. For example, ICTs have been used to disseminate information about the pandemic through daily media conferences that have been streamed live on social networks and broadcast on some mass media, and television and radio were used to broadcast educational content to the millions of children who could not go to school. Yet public connectivity policies have not undergone significant changes since the arrival of the pandemic.

This does not mean that the importance of connecting the unconnected is not understood, but rather that the imagination and understanding of the problem by policy makers has not gone beyond the unsuccessful strategies that have already been developed. That is, they see the solution primarily through the expansion of coverage. Instead, it may be a matter of starting from communication and access to information needs rather than connectivity, so that public policies can become more targeted and relevant.[2]

1 INEGI. (2020a). *Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares*. https://www.inegi.org.mx/programas/dutih/2020

2 Baca-Feldman, C. F., Belli, L., Huerta, E., & Velasco, K. (2018). *Community Networks in Latin America: Challenges, Regulations and Solutions*. ISOC, APC, FGV Direito Rio & REDES AC. https://www.internetsociety.org/resources/doc/2018/community-networks-in-latin-america

Throughout the government of President Andrés Manuel López Obrador (2018-2024), actions related to the national connectivity strategy have been assigned to the Comisión Federal de Electricidad (CFE), under the name of CFE Telecom Internet para Todos ("Internet for All").[3] Although there is no well-defined comprehensive strategy,[4] we can highlight two actions undertaken by this agency. The first is the creation of the shared network and the second the implementation of "digital villages" in rural localities.

The shared network is a wholesale network operated by Altán Redes[5] where mobile virtual network operators (MVNOs) offer 4.5G services to end users. With this network, the government expects to provide coverage to 92% of the population by 2024.[6] However, although the shared network infrastructure has been deployed in a large part of the country, it has not become competitive in the market. Despite this, it is important to note that this network has allowed new players to enter the mobile telecommunications market , including the first Indigenous MVNO in the world: Wiki Katat, run by the civil association Tosepan Limaxtum.[7]

The digital villages consist of internet access points using the state's satellite capacity to connect rural localities.[8] However, recent history has proved that in many parts of the world, projects that aim to create access points in rural areas manage to solve an immediate problem, but lack sustainability strategies that would allow them to function in the medium and long term.

Because of these challenges, it is necessary to look at the problem from different angles to achieve enabling environments that allow for efficient and sustainable connectivity projects over time. Following this, it is crucial to address the fact that the connectivity strategy promoted by a government should not seek to centralise its projects, concentrate solely on extending coverage, or think only in the short term. In general, to mitigate access barriers, it is necessary to contextualise and reflect on the livelihoods, development objectives and communication needs that exist in the localities to be served.[9]

In this sense, the role of local and state governments becomes fundamental: because they are closer to their populations, they can design very diverse strategies and address issues from a different point of view.

What are the challenges of designing a connectivity policy in Chihuahua?

The strategic connectivity plan for the northern state of Chihuahua, developed by the civil association REDES in a consultancy for the CPD, was part of the hyper-convergent connectivity plan[10] through which the state backbone network was expanded and modernised and issues of redundancy were dealt with. The main questions they addressed were 1) how to enable the state's infrastructure to meet its connectivity targets, and 2) how to support the drive for universal coverage and appropriation of ICTs.

The state of Chihuahua has specific challenges in the development of a digital strategy. It is the largest state in the country, covering 12.6% of the total Mexican territory. Some 43.5% of this is taken up by the Sierra Tarahumara mountain range, one of the most rugged territories in the country. In addition, the population density is only 15 inhabitants per square kilometre – 7.5% of the population lives in communities of less than 250 inhabitants while 9.5% lives in towns of between 250 and 5,000 people.[11] It is also important to note that four Indigenous peoples live in Chihuahua's territory: the Pimas (O'oba), the Guarijíos, the Tepehuanos and the Rarámuris. Almost all of these Indigenous peoples are highly marginalised, whether they live on the outskirts of the main cities or in one of the 5,349 rural Indigenous communities in the territory.[12]

3 https://www.gob.mx/cedn

4 The main criticisms of this strategy have been the lack of a diagnosis and analysis of the challenges faced by the country's unconnected population, as well as the need to address barriers that go beyond coverage and the repetition of unsuccessful government programmes. More information is available in Spanish in Flores Ramírez, G. (2021, 17 August). La Estrategia Digital Nacional que no es. *El Economista.* https://www.eleconomista.com.mx/opinion/La-Estrategia-Digital-Nacional-que-no-es-20210817-0013.html

5 https://www.altanredes.com

6 There is no definition yet of what will happen to the 8% of the population that will not be covered by this scheme. Models such as community networks have been proposed, but there is no real effort to develop such schemes.

7 This initiative is part of a comprehensive autonomous communication project developed by the Unión de Cooperativas Tosepan Titataniske in the Sierra Norte of Puebla, which includes different ICTs such as community intranets, community radio and creation of local content, among other projects.

8 Bravo, J. (2022, 7 January). Aldeas inteligentes. *Revista Proceso*. https://www.proceso.com.mx/opinion/2022/1/7/aldeas-inteligentes-278711.html

9 A methodology that allows the choice of relevant technologies in community contexts can be found in: Parra Hinojosa, D., & Baca-Feldman, C. (2021). *¿Y si repensamos las tecnologías para la comunicación?* REDES AC. https://bit.ly/2OhnXCQ

10 El Economista. (2019, 1 August). Chihuahua invertirá 600 millones de pesos para red de telecomunicaciones. *El Economista*. https://www.eleconomista.com.mx/estados/Chihuahua-invertira-600-millones-de-pesos-para-red-de-telecomunicaciones-20190801-0127.html

11 INEGI. (2020b). *Censo Nacional de Población y Vivienda*. https://www.inegi.org.mx/programas/ccpv/2020

12 Comisión Nacional para el Desarrollo de los Pueblos Indígenas. (2010). *Catálogo de Localidades Indígenas*. https://www.inpi.gob.mx/localidades2010-gobmx/index.html

In terms of access to ICTs, 78% of the population uses the internet and 80% uses mobile phones.[13] However, these percentages correspond mainly to 65.5% of the population living in the state's two largest cities. In terms of territorial coverage of 4G mobile networks, Telcel, the largest mobile operator in Mexico, covers only 4.8% of the state, while Altán Redes covers 2.3%. Both have the highest coverage. Their competitors AT&T and Telefónica do not even reach 1%.[14]

Although the state's strategic plan does not specifically focus on the actions needed to address the COVID-19 crisis, it does intend to address one of the main problems underlying the inequalities exacerbated by the pandemic: full access to telecommunications services. The problems brought by the current pandemic intersect with others that pre-existed in Chihuahua, such as the presence of extractive industries and organised crime, the lack of economic resources, irreversible environmental deterioration, discrimination against the region's inhabitants, and a dependency on charitable organisations.

In this context, a public digital policy must be sufficiently robust, and consider all the necessary interrelated factors that determine meaningful access, while remaining open enough to avoid creating projects that depend only on the state. In other words, it has been necessary to closely analyse the intersectionality of factors that must be addressed to deal with a crisis such as the one arising from COVID-19 in terms of access to digital services.

Outcomes and proposals of the strategic plan for connectivity in Chihuahua

A key element in connectivity strategies must be the attentive choice of technologies relevant to each context, and the existing ways of life and needs of the people in these contexts. Because of this, the main methodology used in the consultancy was the idea of "percolation".[15] This methodology proposes the identification of three main elements – the ways of life, the characteristics including the communications needs of the users, and the characteristics of the physical environment of the territory – and produces appropriate alternative access models that can be developed.

For example, in order to determine the most appropriate network for each of the social groups in the Sierra Tarahumara, during field research, Indigenous authorities pointed out that while it was important for them to communicate with each other, it was not necessarily crucial to have access to the internet all the time. In contrast, the mestizo people living in the region emphasised the importance of access to information and online tourism and agriculture services. This distinction was fundamental to understanding that a connectivity strategy is not just about internet access, but about the uses of technologies that are specific and necessary in each context.

Considering this information and other data such as the size of the locality and its political organisation, it was proposed to use high frequency (HF) networks for communities of up to 200 inhabitants, almost all of them Indigenous. This was suggested not only because of the range of HF networks (a few thousand kilometres), ease of use, and price, but also because of the history of local use of HF devices, which the people called *radiecitos chismosos* (gossip radios).

In the larger localities or meeting points in the region, internet connectivity is offered through the resale of tokens for Wi-Fi connectivity lasting one hour to several days. But the cost of these services for users is very high, and there is no real benefit for those who resell the tokens in the communities. This contrasts with the accepted idea that through internet access, the economic conditions of the population will improve. In reality, the people are negatively financially affected by internet access as it implies a very high cost for families. Therefore, a public connectivity policy in these cases must work in coordination with regional internet service providers (ISPs) and people from the communities themselves. For example, free access points can be established in exchange for infrastructure subsidies to reach communities. In the strategic connectivity plan, combinations of local ISP services, community mesh networks and local 4G MVNOs were proposed for communities bigger than 200 inhabitants.

The final document was divided into two parts. The first part consists of an infrastructure and services plan, which addresses elements such as the use of the active and passive infrastructure of the state network, and changes to regulation to encourage access to information on coverage and essential

13 INEGI. (2020a) Op. cit.

14 Instituto Federal de Telecomunicaciones. (2020). *Quién es Quién en Cobertura Móvil en México*. http://www.ift.org.mx/sites/default/files/contenidogeneral/politica-regulatoria/qesqmovil2020t4.pdf

15 The percolator is an instrument used to make coffee through the circulation of pressurised water. Due to the increase in temperature, it manages to transmit the essence of the coffee. In this case, the methodology refers to the identification of characteristics that shape community life to discover the essence of the processes that create the community, allowing the choice of relevant technologies. More information in Mallalieu, K., & Rocke, S. (2007). Selecting Sustainable ICT Solutions for Pro-Poor Intervention. In H. Galperin & J. Mariscal (Eds.), *Digital Poverty: Latin American and Caribbean Perspectives*. International Development Research Centre. http://dirsi.net/sites/default/files/dirsi_07_DP06_en.pdf

infrastructure. The second part focuses on the design of a public policy model for universal coverage and ownership of ICTs, including these main elements:

- Collaboration with local ISPs for the deployment of infrastructure and improvement in the quality of services.
- Development and support of technical training programmes aimed at community technicians.
- Promotion of technological innovation, entrepreneurship and applied research in community contexts.
- Creating the conditions for training in content production and dissemination, and the preservation of local content.

In mid-2021, an opposition government took power in the state of Chihuahua, bringing Javier Corral's administration, which had run the state from 2016 to 2021, to an end. Since then, many of the projects undertaken during the previous administration have been dismantled. The CPD disappeared, and the strategic connectivity plan has remained a document only.

However, the importance of this process, beyond government implementation, was the strengthening of a network of key actors dedicated to developing strategies to mitigate the lack of connectivity in the Sierra Tarahumara. By February 2022, the network had held training workshops on the creation of audiovisual content by children, trained community technicians in the deployment of HF radio networks, and developed cybersecurity strategies for civil society organisations working in the territory.

Conclusion

The process of designing a state connectivity strategy taught us many lessons. These included the importance of creating public connectivity policies for local or state governments, in Mexico and other countries with a similar political structure, without absolute dependence on what is dictated at the national level. To achieve this, solutions must be provided in collaboration with key actors, such as local wireless ISPs, civil society organisations and universities, but above all with the target communities themselves.

It is also important to stress that although the COVID-19 pandemic has intensified people's need for connectivity, we should always address this problem in relation to the many other issues they face. In other words, public connectivity policies are indispensable today, but to develop them properly it is necessary to look beyond the same "infrastructure-only" strategies that have failed time and again.

Regardless of the possibilities of implementing the recommended actions, a good example has been set by the Chihuahua state government under Corral by allowing the development of the plan, taking the necessary time to understand the communication needs and the context of the local communities from an external viewpoint. This may also present benefits for other local or state governments that want to consider this experience as a reference for the design of their own connectivity policies.

One last remark: despite the push for connectivity as a vital necessity from which it is impossible to escape, as far as possible, it remains important to allow for communities to be disconnected. Access, in other words, should be determined by community needs, rather than by a top-down coercion of internet use through the provision of essential services online only. This is why is important to keep in mind a digital strategy that outlines the most appropriate communications platforms for each person, community or organisation. It is important to define how, when and for what purpose communities want to connect. How would the role of states and the different key actors change if this was the approach? This is a question that remains crucially open.

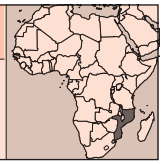
Action steps

To develop meaningful state-level connectivity plans, it is important to:

- Consider the information access needs of those who do not have access to the internet, as well as those who are already online. Simply providing information online is not sufficient to meet the information needs of the population. This was a key learning from the COVID-19 crisis.
- Think in terms of solving communication needs rather than simply connecting communities.
- Consider challenges in relation to each other, rather than in isolation from each other. The pandemic has taught us that understanding how issues relate to each other is a starting point for sustainable and useful connectivity projects.
- Think about how to collaborate with local governments and stakeholders like ISPs in defining connectivity strategies that are contextually relevant and sustainable.
- Always take into consideration the choice of relevant technologies and the communities' right to be disconnected from the internet.

MOZAMBIQUE

THE NEED TO STRENGTHEN A BROAD-BASED HUMAN RIGHTS MOVEMENT IN MOZAMBIQUE



Dércio Tsandzana[1]
@derciotsandzana

Introduction

With the emergence of the COVID-19 pandemic, there has been increased attention on the state-citizen relationship, and the fact that many governments have used the law to restrict civic space, for example, by putting limitations on freedoms for citizens to demonstrate.[2] The government of Mozambique is one such government. This report discusses the state of human rights during the COVID-19 pandemic in Mozambique, focusing on the threats against activists and the strategies that have been used by civil society organisations to report through digital platforms in the country.[3]

The findings are based on a collection of cases and narratives of human rights violations that occurred during the COVID-19 pandemic, as well as ethnographic observation carried out in the virtual space (netnography),[4] by following internet social networks and news reports. Since Mozambique is a Portuguese-speaking country, the main references were consequently translated into English.

Mozambique is a country with low internet access (23%), which creates inequalities between the different regions throughout the country. Of the country's 7.54 million internet users, around three million people connect to social media networks, most of them using Facebook.[5] The telecommunications market is dominated by three major service providers. These are Tmcel, Vodacom and Movitel. According to the 2017 After Access Survey conducted across 16 countries in the global South, Mozambique had among the lowest mobile phone and internet penetration rates at that time, 30% and 10%, respectively.[6] In 2019, Research ICT Africa (RIA) reported that Mozambique had the lowest mobile phone adoption level (50%) and, at 36%, the second highest gender disparity level after Rwanda's, which was 38%.[7] RIA's nationally representative information and communications technology (ICT) access and use survey was part of a survey of 20 countries in the global South (10 in Africa) that canvassed barriers to access for people who were not connected, as well as the challenges to optimal internet usage even where there was coverage or an individual had connectivity.

Beyond the laws, the threat to freedoms in Mozambique

Mozambique introduced its first legal provision regarding civic participation in its 1990 constitution, reflected, months later, in the laws on the right to free association and the rights to freedom of assembly and to demonstrate. The constitution of Mozambique (article 48) guarantees the rights of freedom of expression and access to information. It stipulates that all citizens have the right to freedom of expression, as well as the right to information; and that freedom of the press includes, in particular, the freedom of journalistic expression, creativity and access to information. Despite these constitutional provisions, the country faces several challenges with respect to freedom of expression.

State-run outlets dominate the Mozambican media sector, and the authorities often direct these outlets to provide coverage favourable to the government. While there are a few independent media outlets that provide important coverage, their journalists frequently experience government pressure, harassment and intimidation, which encourages self-censorship.[8] The revision of the Press Law is still under discussion and is expected to be passed by the parliament in 2022. However, it has been

1 PhD candidate, Political Science, France.

2 Pereira, C., Forquilha, S., & Shankland, A. (2021). Revisitar o Espaço Cívico Moçambicano em Tempo de Crise. *Informação sobre Desenvolvimento, Instituições e Análise Social, 145P*. https://opendocs.ids.ac.uk/opendocs/handle/20.500.12413/16935

3 Pereira, C., & Forquilha, S. (2020). *Navigating Civic Spaces in Mozambique: Baseline Report*. Institute for Social and Economic Studies. https://opendocs.ids.ac.uk/opendocs/handle/20.500.12413/16563

4 Kozinets, R. (2011). *What is netnography?* [Video]. SAGE Research Methods. https://dx.doi.org/10.4135/9781412995511

5 Kemp, S. (2022, 15 February). Digital 2022: Mozambique. *DataReportal*. https://datareportal.com/reports/digital-2022-mozambique

6 https://researchictafrica.net/data/after-access-surveys

7 Gillwald, A., Mothobi, O., & Rademan, B. (2019). *The State of ICT in Mozambique*. Research ICT Africa. https://researchictafrica.net/wp/wp-content/uploads/2019/07/2019_After-Access_The-state-of-ICT-in-Mozambique.pdf

8 https://freedomhouse.org/country/mozambique/freedom-world/2021

developed without sufficient stakeholder input, and includes provisions that many feel will be used against the media. Some activists also say that this is also not an appropriate moment to approve the law,[9] due to the risks of it being used to censor the media while the country is locked in a war that has affected northern Mozambique since 2017.[10]

In recent years, different instruments for measuring civic participation, such as Afrobarometer surveys or democracy indices, have been showing a tendency for democracy and, consequently, for civic space to deteriorate in Mozambique. For example, Afrobarometer surveys show that from 2011 to 2015 the demand for democracy dropped from 25% (2011-2013) to 9% (2014-2015), one of the sharpest declines in sub-Saharan Africa among countries covered by the survey.[11] Civil society groups meanwhile claim that the authorities monitor criticism of the government posted online.[12] There have also been reports of government intelligence agents monitoring the emails of opposition party members.

In this context I focus on some initiatives that have been implemented by civil society organisations and civic groups for the promotion of human rights amidst the COVID-19 pandemic.

The struggle for access to information during COVID-19 in Mozambique

The Mozambican government declared a COVID-19-related state of emergency in late March 2020, instituting restrictions on assembly and movement – but since September 2020, the country has been under a "state of public calamity". Although sometimes similar to a state of emergency, a state of public calamity is decreed by the government in the face of a catastrophe or disaster that results in great damage and losses.[13] It is important to note that the decree that instituted a state of emergency barred the media from transmitting COVID-19 information that is "contrary to official information", which allows for the arbitrarily restriction of journalistic information and the state's interference in editorial independence.[14] Citizens must follow several restrictive measures that limit the circulation of people and goods, according to the state of emergency decree.[15] To ensure the rapid flow of critical, accurate public health information during this time, several digital platforms have emerged in the private and public sector. However, these platforms and initiatives lack clarity in terms of how they work and what potential impact they may have on data privacy and personal security.[16]

Civil society organisations and digital rights

With the COVID-19 pandemic, connectivity challenges increased, and consequently left many people unable to enjoy their digital rights. Infrastructure could not cope with increased demand and many more people now needed to be online but could not afford to be. This has increased the digital divide. The violation of human rights in Mozambique also seems to have been a major concern for many civil society organisations.[17] For example, in 2020, citizens denounced the excessive use of force by the police to enforce the state of emergency. At that time, a civil society organisation called Centre for Democracy and Development (CDD) created a telephone hotline to receive complaints from citizens of human rights abuses.[18] In 2021, civil society organisations launched the Mozambican Network of Human Rights Defenders (RMDDH),[19] a network that was created to protect activists and report cases of human rights violations in Mozambique.[20] The RMDDH is composed of various civil society organisations and works to protect human rights defenders. Since its creation, the network has published several public notes denouncing cases of human rights violations.

9 Lusa. (2022, 10 February). New media law in Mozambique "is terrible" for journalists' – NGO. *Club of Mozambique*. https://clubofmozambique.com/news/new-media-law-in-mozambique-is-terrible-for-journalists-ngo-209305/

10 MSF. (2021, 16 April). Fear and loss for people fleeing violence in Cabo Delgado. https://www.msf.org/people-lose-family-livelihoods-cabo-delgado-mozambique

11 Pereira, C., & Forquilha, S. (2020). Op. cit.

12 https://freedomhouse.org/country/mozambique/freedom-world/2021

13 Daniel, G. (2020, 17 September). Estado de Emergência e de Calamidade Pública. *GDA Advogados*. https://www.gdaadvogados.com/pt/publicacoes/insights/estado-de-emergencia-e-de-calamidade-publica/210

14 Tsandzana, D. (2021, 19 January). In Mozambique, a tug of war between public health and digital rights during the pandemic. *Global Voices*. https://globalvoices.org/2021/01/19/in-mozambique-a-tug-of-war-between-public-health-and-digital-rights-during-the-pandemic (accessed 7 November 2021).

15 https://www.rsm.global/mozambique/sites/default/files/br_87_i_serie_suplemento_2020.pdf.

16 Tsandzana, D. (2021, 19 January). Op. cit.

17 Massarongo-Jona, O. (2021). A pandemia da COVID-19 no espaço da Lusofonia: a visão de direitos humanos no direito moçambicano. *Cadernos Ibero-Americanos de Direito Sanitário*, *10*(2), 258-266. https://doi.org/10.17566/ciads.v10i2.764

18 Matias, L. (2020, 5 May). Covid-19: Cidadãos moçambicanos denunciam abusos da polícia. *DW*. https://www.dw.com/pt-002/covid-19-cidad%C3%A30s-mo%C3%A7ambicanos-denunciam-abusos-da-pol%C3%ADcia/a-53343318

19 Júnior, A. (2020, 6 October). Ativistas moçambicanos lançam Rede Nacional de Defesa dos Direitos Humanos. *VOA*. https://www.voaportugues.com/a/ativistas-mo%C3%A7ambicanos-lan%C3%A7am-rede-nacional-de-defesa-dos-direitos-humanos/5611072.html

20 https://redemoz-defensoresdireitoshumanos.org

Despite the low level of access to digital platforms, some local organisations have used the internet to promote human rights in times of crisis, such as Txeka, a digital platform for promoting the political participation of young people, particularly women.[21] Its Facebook page, which is the main tool for its activism, is followed by more than 29,000 users.

Since the beginning of the pandemic, Txeka has been working to remedy cases of violence through online campaigns on its social media platforms. Its particular focus has been gender-based violence, and it has been publishing a minimum of four posts daily about legal provisions for the protection of women and girls, both online and offline, on its Facebook feed.

This initiative also addresses online violence, reporting on cases that have occurred in the last years in Mozambique. Many of its activities are promoted through the use of videos and illustrative animations. The example of Txeka represents the new face of a struggle, where the use of digital platforms becomes an opportunity to promote human rights alongside digital rights in Mozambique.

COVID-19 has led Mozambican other civil society organisations to reinvent themselves, particularly those linked to the defence of press freedom or safeguarding justice, which, in the context of the pandemic, means monitoring cases of violations of individual and collective freedoms.

However, the government control over civic space continues to be one of the greatest obstacles to civil society activism. There are also geographical variations regarding the closure of civic space, in the sense that the further away from the country's capital and urban centres one is, the more closed the space becomes and, because of that, the more difficult to navigate it is. Civil society organisations based in the outlying provinces are unable to explore the possibilities afforded by the legal framework in the same way as those organisations based in Maputo.[22] Although they do use internet platforms for activism, this use is relatively infrequent compared to organisations based in Maputo. In part this is due to the limited financial, material and human resources available to civil society at the provincial level. Personal experience also suggests that internet access in terms of access speeds and infrastructure is worse in the provinces compared to the capital.

It should be pointed out that cases of state intimidation with negative consequences for freedom of expression have not been confined to the media, but have also affected ordinary citizens. On 16 February 2021, Mozambique's President Filipe Nyusi pardoned two individuals who had appeared in a video insulting him, after the case became widely discussed in the country.[23] In the video, two men who were stuck in a traffic jam in Maputo minutes before the start of the curfew – which was put in place in the Mozambican capital on 4 February 2021 – complain about the restrictive measures linked to the COVID-19 pandemic. Using insults, the two criticise the curfew given the chaotic traffic situation and place the blame on the president.

The video went viral on social media and was even broadcast by the STV television channel. Subsequently, the National Criminal Investigation Service opened an investigation against the two men for the crime of slander,[24] leading to the arrest of one of them. Three days later, according to the outlet *Folha de Maputo*,[25] the man was released after a judge accepted a request from the Mozambican Bar Association arguing that the crime of slander requires a complaint filed by the offended party, which in this case would be the Mozambican president.[26]

Conclusion

The COVID-19 pandemic shifted attention and civic energy to the national public health emergency.[27] As a result, civic action, which was marked by the emergence of new actors and new coalitions, appears to have focused on issues such as health and emergency aid, considering their relevance to controlling the spread and effects of the virus, rather than the issues of daily life that have been affected by the government's responses to the pandemic, such as gender-based violence, livelihood challenges, education, and law and order. Nevertheless, some organisations have managed to build campaigns and projects in these spaces, some turning to internet platforms to support their advocacy.

In general, most civil society organisations in Mozambique operate without significant legal restrictions. However, rights defenders and members

21 https://www.facebook.com/TxekaMoz

22 Pereira, C., & Forquilha, S. (2020). Op cit.

23 Tsandzana, D. (2021, 22 February). Mozambique's President pardons young men who insulted him in viral video. *Global Voices*. https://globalvoices.org/2021/02/22/mozambiques-president-pardons-young-men-who-insulted-him-in-viral-video

24 Jornal Notícias. (2021, 12 February). Jovem detido por injuriar PR. https://www.jornalnoticias.co.mz/capital/maputo/jovem-detido-por-injuriar-pr

25 Folha de Maputo. (2021, 17 February). PR perdoa jovens que o ofenderam num vídeo nas redes sociais. https://www.folhademaputo.co.mz/pt/noticias/nacional/pr-perdoa-jovens-que-o-ofenderam-num-video-nas-redes-sociais

26 Tsandzana, D. (2021, 22 February). Op cit.

27 Anderson, C., et al. (2021). *Navigating Civic Space in a Time of Covid: Synthesis Report*. Institute of Development Studies. https://opendocs.ids.ac.uk/opendocs/handle/20.500.12413/16602

of groups perceived as critical of the government continue to report acts of intimidation. This intimidation appears to have increased at the start of the pandemic, when the government used its legislative powers under the state of emergency and state of public calamity, which is still in effect at the time of writing. While this suggests that civic space for activism is shrinking in the country, a trend not helped by the ongoing war in the northeast of Mozambique, it also needs to be remembered that civil society participation and civil dynamics have always been relatively limited, mainly due to the restrictions imposed by authoritarian practices, low internet connectivity and media centralisation by the public entities.

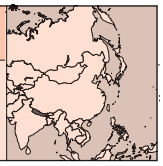
Action steps

In this context, the following action steps are recommended:

- There is a need to encourage collective activism among civil society organisations working for human rights broadly in Mozambique. This will enable unity of effort and better long-term results. One way to do this is to strengthen the Mozambican Network of Human Rights Defenders (RMDDH), allowing it to expand its network, by organising initiatives beyond its local networks, so more people are likely to benefit from its activities.
- Similarly, there is a need to establish a broad network involving other civil society organisations that are experienced in promoting digital rights, to encourage friendship and solidarity between organisations.
- Civil society organisations should invest in digital security, so that their activities are carried out in a protected environment, including where their privacy and data are protected.

NEPAL

GOING ONLINE DURING THE PANDEMIC: LESSONS AND REFLECTIONS



Body & Data and APC
hvale vale and the Body & Data team: Rita Baramu, Kabita Rai, Youba Rai, Shubha Kayastha, Neha Gauchan, Sapana Sanjeevani, Shripa Pradhan, Anuska Sthapit, Mahima Pradhan, Prasun Subedi, Pramila Shrestha and SJ
https://bodyanddata.org

Body & Data, a sexual and gender rights organisation based in Nepal, had a conversation with APC's hvale vale to reflect on how the COVID-19 pandemic changed or shaped the ways in which they do their advocacy work around digital technology-related issues. The conversation was held on BigBlueButton, recorded and transcribed.

Introduction

It takes time to learn and it takes more time to structure learning, transforming fragments of individual and collective experience into something that can resemble a practice, a change in behaviour. For activists and civil society actors, this means a "change" in the "how" we go about advocacy and the "what" we advocate for.

In the wake of the COVID-19 pandemic we followed our intuition, trusted our relationships and moved from traditional in-person office work and in-person conferences to virtual rooms, webinars and massive online conferences, where we learned to become embodied avatars of our social justice feminist causes.

Over two and a half years after that change that was imposed on us, it is important to reflect on what remains beyond our immediate, reactive responses to stay connected. We need to explore if and how our responses have evolved, evaporated or stayed with us, and if they have become an integral part of the work we do and of the way we do it.

Advocacy and advocates lived in a distributed, precarious dependency during the pandemic, mediated by digital technologies. Going online meant that advocacy could be augmented, discarded, attacked or criminalised through the very digital technologies that mediate their interactions.

And since technology is never neutral, and all new and less new virtual spaces and platforms are owned and intrinsically intertwined with the politics and positionality of their owners and maintainers, platforms are, at the same time, a pre-condition for advocacy and, somehow, an advocacy issue in themselves.

Digital rights advocacy includes advocating for accessible, meaningful, affordable and open infrastructures, which entails the intersection of hardware, software, knowledge and relationships. The "how" and the "what" conflate.

Traditionally, people marched and occupied squares, reclaiming access to physical decision-making rooms. In the digital era of strategic fragmentation and algorithm-managed realities, our advocacy is equally about and is equally happening through and via the very same spaces whose politics impact, threaten and frame the digital or internet rights we advocate for.

In this scenario, meaningful access to platforms becomes advocacy. The question is how to use the online and now hybrid spaces not as episodic bridges to stay connected, but as integral, continuous, permanent spaces where advocacy can thrive.

It is important to look at and name how organisations, collectives and activists have moved or can move from the emergency of the moment to a strategic use and understanding of commercial as well as autonomous infrastructure that can enable their advocacy, and that they can advocate for.

This report captures some of the experiences of Body & Data, a Nepali-based organisation, and their trajectory as a feminist digital rights organisation. It tries to capture not only the changes that the organisation made, but how their new digital spaces influenced and intertwined with what they advocated for.

The story

> *A couple of days after we started working virtually, I was thinking like, "What do I use at home?", because I have this table in my room that is like ages old, from when we used those desktop computers, a computer bought in my college days, right, and it's not really comfortable and I used one of my dining chairs to work. I'm glad I had that table in my room, that I didn' t have to go rushing, buying things to start with.*
>
> Shubha, Body and Data team member

Grounded and locked into our own local realities, homes and rooms. Separated by one another, local and global collectives and organisations had to step up or reinvent ways of strengthening and supporting collective and individual memory, re-creating and

sustaining a shared sense of mission, imagining daily online working practices as tactile and embodied. With online experiences being as diverse, fragile and precarious as the many locations and positionalities of the advocates, this was not easy or possible for everyone.

Advocacy counted on bodies and physical spaces! Intervention in local or global venues, press conferences, workshops. The material distribution of printed text and posters. One or many of these would offer unavoidable intersections, opportunities to share evidence and build alliances. All of this froze!

The hidden costs of being online for work with a strong, reliable and stable connection or with access to tools that would guarantee one's privacy and safety became visible, and issues of affordability and meaningful connectivity became evident, contributing to the sense of precariousness and dependency:

> *Technology was really helpful because during lockdown it was the only thing on which I relied to talk to other people, friends, colleagues and family. At the same time there were issues [...] the electricity was up and down, on and off – it would be really difficult when the meeting was happening and the electricity goes down. [...] And it was not only electricity. I used Wi-Fi from my mobile network and it was expensive and it impacted our work and advocacy quite directly.*
>
> Rita, Body & Data team member

It was a sudden realisation for many that all interactions would have to be mediated by technology. The longer the time, the higher the alienation – and the realisation that technology was as necessary as water, air, land, food.

As a feminist digital rights organisation, Body & Data already had a wealth of experience to draw on in this area. Meaningful access, the right to association online, the internet as public good, were and are part of their digital rights advocacy agenda. But where they found themselves was in a no-humans-land, entrapped inside and by the machine; and they knew that if they wanted to thrive, they could not rely on what they knew or solely on what was available – they had to create their own alternatives:

> *One of the main concerns we had around our activities was creating a safe space, making people comfortable coming to us, that was our concern. [...] When we started we had multiple calls and suggestions from many people [...] that helped us through, and now we have this alternative that we can always go to.*
>
> Kabita, Body and Data team member

Paradoxes cannot be solved; once acknowledged it takes a leap in the void, an act of magic to move through them and beyond them.

Closer than ever: What was it and how did it work?

> *APC's "Closer than ever"[1] statement was [...] warm and at the same time [was] giving lots of hope. We really felt okay. It was, is, really closer than ever in multiple senses, and I think that was something to really remember and carry on in our further activities as well.*
>
> Kabita, Body & Data team member

APC's "Closer than ever" approach supported Body & Data. During weekly meet-ups, several aspects of working from a distance were discussed, such as so-called "productivity" and internal communication tools, but also care, digital fatigue, and so on. The weekly "calls and guidance" helped the organisation "through the transitioning process, to move the work virtually." As they put it, "[t]he team felt supported and held during the difficult time."[2]

Besides this, the Body & Data team invested in and engaged in multiple sessions on media management and organisational technical infrastructures, enhancing their skills on managing their own infrastructure in order to be independent:

> *I remember our first storytelling workshop online, we were really scared and nervous as to how to create a safe space while being apart physically. We were able to use our Nextcloud space for the participants to send their works, share their ideas and work amongst themselves. Personally, for me, that was one of the moments that truly hold the essence of how closer we are virtually.*
>
> Shripa, Body & Data team member

Humans adapt and change. Building these new online collective selves was an act of hope, trust and hard work. Their happening and fluidity informed both the issues being advocated for, and the way of working, giving digital rights advocacy access to both familiar and new, larger audiences, and investing these interactions with nuances born by the everyday use and experience of technology that they did not have access or proximity to before.

> *There were lots of changes and uncertainty whether to go with our already set plan. [...] Thinking through the plan again, redesigning things. So if we were planning something we were paying attention to what would be the different aspects in the now, and that was really like helpful to our work. [...] A lot of the work did not stop somewhere [...]. It was tampered with, obviously, but there was something different – we would see [new things] as possibility.*
>
> Kabita, Body & Data team member

1 APC. (2020). *Closer than ever: Keeping our movements connected and inclusive – The Association for Progressive Communications' response to the COVID-19 pandemic*. https://www.apc.org/en/pubs/closer-ever-keeping-our-movements-connected-and-inclusive-association-progressive

2 Expanding the EROTICS Network in South Asia: Body & Data final narrative report.

But, as Kabita and Neha explain, they were not used to working remotely, so they took this on as a collective responsibility. Some of the change that occurred during 2020 became a kind of established new reality as a second lockdown was introduced in Nepal. The Body & Data team and their new team member could use the infrastructures as well as the policies built as a response to the first emergency:

> *We really did lots of communications looking for mutual understanding of the things like checking in or planning for any activities, and really giving more time and energy and attention. That was very much an important thing we did. [...] We built guidelines to work from home or working from distance and on what you're working too. [...] The process was collective and most of the activities we do in this and that policy are things we formalised which guides our whole work. [...] All of that was based on our day-to-day experience. So when we had to go back again to virtual work [...] we had something we could use so it was an easier transition.*
>
> Kabita, Body & Data team member

Body & Data's relationship with technology deepened and became more complex. As an organisation they used technological tools and platforms such as email, a website and social media accounts as part of their standard communication. They already had specific advocacy and capacity practices with their core communities such as digital storytelling. But what they developed and where they landed in their use and advocacy is described as more cohesive and complex:

> *Working with the organisation's tech infrastructure while not being a techy, was a fascinating and rewarding experience. It could have been a daunting task, but with support from other feminist techies as well as the values that guide us on what kind of tech we want to use (open source, encrypted and safe), the journey become more exploratory. It opened new horizons for how tech can be used for advocacy for us as an organisation.*
>
> *One of the important steps in advocacy is how we communicate with each other within the team; that was a highlight as well as a challenge during remote working. During the first two years of the pandemic, we got to manage and have more autonomy over our own server space, bringing applications and resources that were useful to us – Nextcloud, Riseup, calendars, etc.; finding collaborative spaces, as well as strategies so that we weren't left alone in our boxes of the screen.*
>
> *We set up weekly meetings through Zoom or Jitsi to have space for check-ins with each other because we missed informal conversations during lunch hours. The spirit of check-ins during meetings still stays with us.*
>
> *Collaborative working spaces like Riseup, or etherpads that were used for minutes, showed how online collaboration works beyond Google services. We are still exploring how to integrate collaborative open source software with our servers.*
>
> *We had made decisions about which communication channels to use for what specific purposes. We set up a tech infrastructure guideline – that guided new team members as well as old team members on how to effectively use the tech resources. All of these small examples helped us navigate the pandemic and also strengthen our internal communications.*
>
> Shripa, Body & Data team member

Today they work seamlessly in person and remotely using a mash-up of tools and platforms. Some they own, such as their Nextcloud repository and website, which they manage independently; some they routinely access and use because of their partner and membership relationship with APC; and some are commercial services they are subscribed to:

> *At the beginning as a team we used to talk on Signal [...] When we started using Mattermost then I realised oh, it's so much easier to talk over Mattermost because you have so many channels. [...] That was one of the shifts that we had, [...] APC providing us Mattermost, for free on the APC server. It's a support we still feel.*
>
> Shubha, Body & Data team member

Using commercial services was quite different. Accessing Zoom required international bank cards and Nepal did not allow this until very recently. So Body & Data had to create their own system for sending money outside the country. A friend living abroad in India would purchase and pay for the Body & Data Zoom account, and then get reimbursed via her Nepali bank account.

However, by using this mixed infrastructure, drawing on what was available, and what could be relied on, a safe space for interactions was created, as Sapana, a new team member, explains:

> *When I started at Body & Data [...] I joined the office physically for 20 days or something and then the second lockdown happened and it was really the first time I was working virtually using official spaces, such as Mattermost or Nextcloud. [...] The space was not intimidating at all, and was really reassuring that the communication within this channel had lesser risk or no risk of like my information, whatever I share, would get like leaked or something. [...] That safer environment and safer space helped me. [...] If you would tell me one year or one and a half years before that like official work is possible, like all of it through a virtual space, I would not have believed you. And I would not have participated, most likely.*
>
> Sapana, Body & Data team member

Sapana knows that doing work in a physical space brings another joy. A joy that during 2022 and 2021 was missed. Still she recognised that working online, though different, does not necessary diminish the quality of interaction, but that this also depended on

the Body & Data team actively using the technology to create a meaningful and supportive space online:

> *It gives us space to be, unlike my previous working spaces, vulnerable, and to accept that is okay; if I'm not getting this thing, ask for help and there is always someone to listen to you and address it as much as possible.*
>
> Sapana, Body & Data team member

Advocacy: The "how" and the "what"

Body & Data is a "digital rights organisation focused on creating a free, open and just internet that respects autonomy of individuals and upholds their dignity."[3]

Under the umbrella of public health, the Nepali government, like many others, introduced contact tracing systems to prevent the spread of the virus by tracking potential virus carriers. However, it not only raised many issues around privacy, consent and security, but compromised and threatened the psycho-social security of people.

Personal information like passport numbers and phone numbers were shared online, resulting in hate speech, death threats and social exclusion as well as psychological harm against people that tested positive. People that were particularly discriminated against, such as foreign workers, migrants and people of certain castes or religions (like Muslims), found themselves without protection or recourse to justice because the government did not anticipate and understand the implications of their decisions, and had no mechanisms to address these issues:

> *We started monitoring media, documenting digital rights issues relating to privacy, violence, digital ID, freedom of expression, and we started internet freedom conversations in our native speech. We did that event monthly. [...] That was also new. While working virtually we explored those advocacies.*[4]
>
> Neha, Body & Data team member

As a response to the problem of misinformation, for example, Body & Data organised a campaign around online gender-based violence and misinformation, reaching 150 people through its webinars.

As the team suggests, even simple changes to their online advocacy approach had an important effect:

> *I felt that going into virtual space gave more; like we kind of explored new interventions of advocacy. Before we were doing social media and posting [to support] our campaign. We would post like videos; but then in 2021 we started having a newsletter [...] that was also a way of our advocacy.*
>
> Neha, Body & Data team member

By producing different advocacy outputs online, the work of doing advocacy had to change too:

> *The things we started producing, such as organisational statements regarding incidents that were happening and were very problematic, were important to raise voices. We started that and we are continuing doing it. [It was] because of the particular situations that we got introduced to those issues, those problems and needs, and we had to keep our eyes on them. [...] I think we were considering the situation and [...] how things like misinformation were happening. That was not only giving us issues to consider in our work, but also the way we work.*
>
> Kabita, Body & Data team member

However, they also found that even offline, when the first lockdown ended, their way of thinking about organising advocacy had changed:

> *When we were planning for even small gatherings, [approaching] people we wanted to work with or planning for our activities, any campaign, or any workshop, any webinars, we were thinking on the nuances; for example, how the masks will be integrated, how that's gonna impact in a different way. That was I think given more attention and time.*
>
> Kabita, Body & Data team member

The Body & Data team feel that participating online in national and international events was important and helped broaden their knowledge. It helped to "accelerate advocacy as well as contributed to developing strategies for further activities in a more effective way. It [was] also very important to occupy spaces, intervene and increase visibility."[5] Body & data occupied different platforms, expanding their advocacy and focusing on the emerging intersections between digital rights, internet freedom and the impact of COVID-19 on the rights of marginalised people in Nepal. While they were already advocating against the stigmatisation of women and marginalised groups such as Muslims, Dalits, etc., they expanded their outreach and understanding from "everyday sexism, Islamophobia, classicism, casteism" to misinformation online:

> *Beyond the tech infrastructure work, looking at remote working, my definition of what working and advocacy could look like has broadened. It has made me question how things were running and how things are running and who we are excluding in the work. The remote working environment has been advocated by the disability community for years. Going to specific places for advocacy and activism has implicit privileges – who has the access to go to these places for advocating their issues.*

3 Expanding the EROTICS network in South Asia: Body and Data final narrative report.

4 Body & Data team members engaged in the Boju Bojai podcast about feminist internet, privacy and freedom of expression, the queer movement, language and visibility in the Nepalese context.

5 Expanding the EROTICS network in South Asia: Body and Data final narrative report.

There were limitations of working virtually – missing the hugs, the subtle glances and understanding nods, the non-verbal ways of affection, etc.

But it also opened new horizons into how to do things – to be more open and say what one feels. It brought a new language for care – emojis, personal DMs reminding to drink water, lurking behind with specific people after the meeting so we could just talk about how our day went, setting deadlines for decisions and feedbacks [in a way that] we don't misinterpret them as not taking time caring, and being able to experiment with tech, while not being a techy.

Shripa, Body & Data team member

But as many organisations across the world have found, online advocacy has both its limits and its possibilities:

I guess one of the things we were not able to do after the COVID was travel across the country and also internationally. That affected our capacity as a team because otherwise members of the team would have gotten the opportunity to travel, be in international spaces where they would meet other activists, and feel like okay, we're not alone in this. So I guess that is something that was missed out.

In terms of the digital rights spaces, like RightsCon and APrIGF [Asia Pacific Regional Internet Governance Forum] and stuff like that, I don't think it would be possible for us to join if it was not for virtual. [There would] either be travel funding or a visa issue, or one or the other. But that space got opened up. [...] It used to be one person from Body & Data [who could attend] but now, you know, all of us could go. It is advocacy spaces, but it is not exactly advocacy spaces, but yeah, it opened up.

The funny thing is we started getting invitations to speak in platforms where it's mostly like, you know, men – not even digital rights, basically IT-related men working – and it was kind of interesting. We got invitations to speak in a couple of things, but I always felt out of space whenever I was in those forums, because I could not feel if people were listening. [It was as if] they just did events to do events.

Shubha, Body & Data team member

Being online all the time produced a kind of existential exhaustion, and, after two years, a new energy was needed:

Because during the lockdown phase everything was online, people realised that online events are really important and online advocacy was important at the time; but it is not the same sentiment right now, because they just want to go to the normal, physical spaces.

We are tired of our online presence. We also want to go to the physical spaces and have that interaction with people. Still I think both online and physical spaces advocacies are going on. We are trying to do mixed advocacy here.

Rita, Body & Data team member

Action steps

What can we learn from the Body & Data experience during COVID-19?

- Tech infrastructure is not a luxury. Funders need to provide civil society organisations, collectives and activists with unrestricted funds to build and maintain their own autonomous infrastructure.
- Working only online produces new approaches to advocacy, and can result in discovering new areas of advocacy that need attention – the "how" can influence the "what".
- Working online only increases the ability for civil society activists to participate, and introduces them to new spaces, even if the value of some of these spaces can be uncertain.
- It is critical to create safe spaces for interaction online, which can be achieved using mixed commercial and open-source infrastructures if necessary.
- Working online only produces its own kind of existential exhaustion – there is a need to reinvigorate ourselves through human contact.
- There is a need to continue using and engaging with online and in-person advocacy spaces and strategies. The benefits of one does not mean the benefits of the other cannot be realised.
- Reach the ones who are not connected through internet using creative means and strategies.
- Remember to celebrate and adapt to thrive in difficult times, and to nurture collective memories.

I am grateful for the possibility of this conversation. It not only created a space for a collective reflection, it also became a nurturing memory, a place of the heart to go to when things return and become difficult again – a collective yet personal resource of how we can adapt, thrive and weave our actions and advocacy with our emerging realities.

NIGERIA

THE IMPACT OF COVID-19 AND SOCIAL MEDIA RESTRICTIONS ON CITIZEN ENGAGEMENT IN NIGERIA

African Centre for Climate Actions and Rural Development (ACCARD)
Freeman Elohor Oluowo
www.accard.org

Introduction

During the COVID-19 pandemic, civil society and human right organisations exposed government corruption, including financial misappropriation and the hoarding of food intended for aid, as well as human right abuses in Nigeria. This led to the so-called #EndSARS protests in 2020, a ban on Twitter for seven months, and a brutal clampdown on protestors by the security establishment.

While the government's relentless efforts to clamp down on social media have narrowed the space for civil society engagement, it is also likely to contribute to increasing human rights violations and corruption in Nigeria. At the same time, the increase in youth unemployment, blamed on the COVID-19 pandemic and consequent economic lockdown and restrictions, does not properly take into account the economic implications of the government's repression and censoring of social media.

In the context of the #EndSARS protests, this report discusses the efforts by the government to restrict social media, and the potential impact on human rights and the economy.

Background

Online platforms such as Facebook, Twitter, Instagram, TikTok and YouTube provide citizens the opportunity to express their concerns, spread information in real time as well as engage directly with those who govern them. However, with reports of social media abuses, what governments and their institutions across the world consider as efforts aimed at ending the menace of misinformation and disinformation[1] are resulting in new measures to monitor and regulate the use of these platforms.

Legislation targeting social media is not new in Nigeria. Calls to regulate it intensified after the 2015 general election due to the influence that digital media platforms had in the process, with many of these efforts spearheaded by the Buhari-led federal government, which came into power.

In November 2015, Deputy Senate Leader Ibn Na' Allah sponsored the Frivolous Petition Bill 2015, otherwise known as the "anti-social media bill", which was referred to the Senate Committee on Judiciary, Human Rights and Legal Matters for further recommendations.[2] Also, in March 2018, the then deputy chief whip of the Senate, Abdullahi Aliu Sabi, introduced a bill seeking the prohibition of hate speech in the country. The bill was withdrawn by the lawmakers due to a backlash from Nigerians and rights watchdogs outside of the country. However, it was re-introduced by the Senate in November 2019.

The hate speech bill proposed a jail term of no less than five years or a fine of no less than less than NGN 10 million (USD 24,000), or both, for offences like harassment on the basis of ethnicity and race.[3]

The government, in a more desperate move, established a national commission for the prohibition of hate speech and gave legislative power to the National Broadcasting Commission (NBC) to regulate social media platforms in the country. These moves came with the backdrop of 16 laws already in existence which enabled the Nigerian state to acquire citizen data and conduct surveillance operations.

There is a growing use of social media among Nigerians, with many finding these platforms an easy and cheap means of communication. Nigeria's social media users were estimated at 33 million in January 2021,[4] mostly young people. It is a significant number, although relatively small for a country with a population of over 200 million people. Nevertheless, any attempts by government to regulate social media will be viewed as a deliberate attack on young people, a move to suppress the voices of young

1 Santas, T., & Inobemhe, K. (2021). Social Media Regulation in a Democratic Nigeria: Challenges and Implication. *MCC, 5*(1), 71-88. https://www.researchgate.net/publication/353429624_Social_Media_Regulation_in_a_Democratic_Nigeria_Challenges_and_Implication

2 Agbedo, O. (2021, 26 June). Social media regulation: Between failed attempts and Buhari's current move. The Guardian. https://guardian.ng/saturday-magazine/cover/social-media-regulation-between-failed-attempts-and-buharis-current-move

3 Ibid.

4 Kemp, S. (2001, 11 February). Digital 2021: Nigeria. *DataReportal*. https://datareportal.com/reports/digital-2021-nigeria

people – and possibly to cover up the maladministration and corruption in the government.

This is disturbing for a country with an unemployment rate which stood at 33.3% in the fourth quarter of 2020[5] – and could be worse in the future, if nothing is done to address current youth unemployment. According to the National Bureau of Statistics, the unemployed figure represents a labour force of about 23,187,389 persons in Nigeria, either doing nothing or working for less than 20 hours a week. The age group categories with the highest rates of unemployment were persons between the ages of 15 and 24 (53.4%) and 25 and 34 (37%).[6]

Twitter ban during the 2020 #EndSARS protest

Many countries, including Nigeria, are seen to infringe on the fundamental and constitutional rights of their citizens to access information and to freedom of expression and association. They use legislation, policies and programmes aimed at limiting citizens' access to valuable information and their participation in democratic processes.

The Nigerian government's recent attempts to regulate social media were framed as an attempt to push back against fake news. However, in a dramatic manner, on 4 June 2021, Nigeria banned Twitter, joining countries like China, Iran, North Korea and Turkmenistan where social media have been suspended or banned outright.

The Twitter ban happened during the so-called #EndSARS protests – when social media platforms, especially Twitter, were used by the youth to call for the disbanding of the Nigerian Police Force Special Anti-Robbery Squad (SARS), which had been accused in the past of extortion, harassment, brutality, killings and other abuses, including rape. Young people had expressed their frustration during the COVID-19 lockdown measures and stay-at-home orders, as well as their dissatisfaction with the political handling and hoarding by politicians of goods, especially food items, that were meant to be distributed to cushion the effect of the pandemic on citizens. Attempts by the youth to break into warehouses across the country in search of the hoarded food were blocked in some places by the SARS, and arrests made. In their frustration, young people took to the streets, using social media – and several hashtags[7] – to organise their protests.

The federal government, announcing the Twitter ban through Information Minister Alhaji Lai Mohammed, said the use of Twitter was "capable of undermining the corporate existence of Nigeria." While this was a direct result of the perceived role of Twitter in the #EndSARS protests, and the consequent destruction and looting of government property, Twitter had also deleted a post on the protests by President Mohammadu Buhari, where he referred to Nigeria's civil war between 1967 and 1970, saying that most of those "misbehaving" by burning electoral offices and police stations were too young to understand the gravity of war, and threatening to deal with arsonists and looters in "the language they understand."[8]

Consequently, the NBC implemented the president's orders, and directed all network providers to block access to Twitter services in the country. It further instructed all social media platforms and online broadcasting services to register and obtain an operational licence, or face sanctions.

Although some users bypassed internet service providers in the country by using virtual private networks (VPNs) to access Twitter for the seven months of the ban, the decision sparked an outcry and many public debates. While some argued in support of the government ban, many accused it of a knee-jerk reaction to Twitter deleting the president's post, which according to Twitter violated its global community policies. However – and not far from the truth – the ban was also seen as one way for the government to vent its anger at young people, and the accusations levelled against it.

Impact of the Twitter ban on the Nigerian economy

Communication technology is responsible for an estimated 10% of Nigeria's gross domestic product (GDP).[9] The online benefits for an economy where an estimated 33 million people use social media, including business owners for direct advertising or engaging their clients and customers, cannot be underestimated or politicised.

After 222 days, the Nigerian federal government lifted the ban on Twitter operations in the country. NetBlocks estimated an economic loss of NGN 104.02 million (USD 250,600) every hour, amounting to a NGN 2.46 billion (USD 5.9 million)

5 Elebeke, E. (2021, 15 March). Nigeria's unemployment rate rises to 33.3%. *Vanguard*. https://www.vanguardngr.com/2021/03/nigerias-unemployment-rate-rises-to-33-3

6 Popoola, N., et al. (2021, 16 March). Unemployment rate hits 33.3%, 23.18million Nigerians jobless – NBS. *Punch*. https://punchng.com/unemployment-rate-hits-33-3-23-18million-nigerians-jobless-nbs /

7 These included #EndSARS, #ReformPoliceNG, #OccupyLekki, #OccupyNigeria, #OccuppyNASS, #SaveNigeriaGroup and #OurMumuDonDo ("Our foolishness is enough").

8 Agbedo, O. (2021, 26 June). Op. cit.

9 Olojo, A., & Allen, K. (2021, 24 June). Social media and the state: challenging the rules of engagement. *Institute for Security Studies*. https://issafrica.org/iss-today/social-media-and-the-state-challenging-the-rules-of-engagement

daily loss.[10] This is depressing and economic sabotage for a country with an unemployment rate of 33.3% in the same year, affecting mostly young people. The knowledge of the economic sabotage may have prompted civil society organisations including Socio-Economic Rights and Accountability Project[11] to challenge the decision of the federal government in court.

Peaceful protestors attacked at Lekki Tollgate: A panel investigates

One of the worst incidents of police violence during the protests happened in Lekki, a coastal city in Lagos state in the southwest of the country. On 20 October 2020, young people were peacefully protesting police brutality in Nigeria at the Lekki Tollgate. Security forces, on the invitation of the Lagos state government, allegedly opened fire to disperse the protesters while they were waving the country's flag and singing the Nigerian national anthem. This resulted in many protestors sustaining injuries and reports of deaths.

Footage of the sad incident trended on social media, particularly on Twitter, exposing serious human right violations by state actors in Nigeria. The federal government, by way of exonerating itself from the global condemnation of the incident, mandated the governors of the 36 states in Nigeria, as well as the Minister of the Federal Capital Territory Abuja, to set up an investigative panel of inquiry on reported cases of police brutality across the country, with one hearing specifically reviewing the Lekki Tollgate incident.

Ironically, the panel's report, which has since been published, was rejected by the government. It documented several cases of police brutality, extortion, human rights abuses and killings by military personnel and other security agencies at the Lekki Tollgate on 20 October 2020, and the day after.

The panel found that the "Nigeria Army [which had been invited by the Lagos State Government to intervene] shot, injured and killed unarmed helpless and defenseless protesters without provocation or justification, while waving the Nigeria flag and singing the National Anthem."[12]

The Lagos panel indicted the security personnel responsible, and for trying to cover up their actions by removing bullet cartridges from the scene.

The Lagos state government, yet to implement the white paper of the report, denied inviting the army to the Lekki Tollgate when it happened.

The panel received about 235 petitions connected to the activities of the already disbanded Nigeria Police Force Special Anti-Robbery Squad (SARS). These included extortion, harassment and the killing of citizens they were meant to protect. Of this number, 45 of the petitions already have judgments delivered by competent courts of law in their favour, but the complainants have yet to receive any compensation from the Nigerian police or federal government.

The impact of COVID-19 and social media restrictions on civil society engagement

Most civil society organisations, particularly in the global South including Nigeria, are struggling to stay afloat and sustain their engagements. In Nigeria, both government censorship and restrictions on social media, and the COVID-19 outbreak, which imposed restrictions on physical gatherings and in turn affected funding support for non-COVID-related activities, have had a huge impact on civil society activities.

From the suspension of Twitter in early June 2020, to the enactment of the anti-social media bill and hate speech bill,[13] to the amendment of the Nigeria Broadcasting Commission (NBC) Act under parliamentary consideration, laws have been formulated to repress civil society engagement and criminalise information sharing both in print media and online.

Between 2015 and 2021 alone, the Closing Civic Spaces database documented over 300 incidents cracking down on freedom of expression, assembly and association in Nigeria.[14]

Also, we surveyed over 50 civil society and human rights organisations in Nigeria, in order to better understand the direct impact of COVID-19 and social media restrictions on civil society engagement on the ground. They all said the pandemic, government censorship, clampdowns on freedoms and social media regulations have significantly impacted on their activities. According to them, the situation is worse under the COVID-19 pandemic because their access to both local and international funding has become limited.

10 Dataphyte. (2022, 15 January). Twitter ban, Tinubu's tweeps, and N500bn tantrum. https://www.dataphyte.com/latest-reports/special-report/twitter-ban-tinubus-tweeps-and-n500bn-tantrum; Conroy-Krutz, J. (2021, 7 June). Nigeria Has Banned Twitter. Here's What This Could Mean for Its Democracy and Online Activism. *Global Citizen*. https://www.globalcitizen.org/en/content/nigeria-twitter-ban-could-hurt-economy

11 https://serap-nigeria.org

12 Lagos State Ministry of Justice. (2020). *Lagos State Judicial Panel of Inquiry on Restitution for Victims of SARS Related Abuses and Other Matters: Consolidated Report on General Police Brutality Cases*. https://lagosstatemoj.org/wp-content/uploads/2021/12/Consolidated-Report-of-the-Judicial-Panel-of-Inquiry-on-general-Police-brutality-cases.pdf

13 Ibezim-Ohaeri, V., Olufemi, J., Nwodo, L, Olufemi, O., Juba-Nwosu, N., & TIERS. (2021). *Security Playbook of Digital Authoritarianism in Nigeria*. Action Group on Free Civic Space. https://closingspaces.org/the-security-playbook-of-digital-authoritarianism-in-nigeria

14 https://closingspaces.org

They find the new measures more challenging, and the fear of arrest or harassment by security agencies, already monitoring online posts and other activities of civil society organisations and human rights activists, has resulted in individuals exiting the civil engagement space.

Conclusion

The Buhari-led federal government's unrelenting efforts to regulate the use of social media and online platforms in Nigeria will have both short- and long-term negative impacts on press freedom, civil society engagement and citizens' participation in democratic governance.

The passage of the anti-social media bill, the censorship of the media and new measures in place to regulate social media platforms, like the suspension of Twitter, will also undoubtedly have huge economic knock-on implications for a country with a high unemployment rate that mostly affects young people. The political, economic and financial losses during the Twitter ban are yet to be fully understood. However, the regulations are likely to further constrain the activities of civil society organisations already struggling to stay afloat, especially under the COVID-19 pandemic, which disrupted global funding flows. A number of people and organisations are now exiting the civil society space.

If the attack on citizens' engagement continues in Nigeria, citizens may lose their right to freedom of expression as outlined in the 1999 constitution and the Open Government Partnership,[15] to which the country is signatory. This will further worsen the existing human rights abuses and violations and, importantly, the activities of civil society organisations working to strengthen Nigeria's fragile democratic processes.

Like never before, civil society actors and human right activists are campaigning against impunity and bad governance, demanding accountability for widespread injustices, while mounting pressure on federal and state authorities to address issues of public concerns. Much of this advocacy is taking place on social media platforms.

Action steps

The following key actions steps are necessary in Nigeria:

- There is an increasing need for civil society organisations to be able to properly verify available information online before using the information for advocacy. In this regard, training is needed in fact checking and other skills such as understanding and interpreting data.
- There is need for civil society organisations to build in-house research and advocacy capacity to properly address the shutting down of online civic space through new regulations.
- Civil society organisations need to better collaborate among themselves and form network organisations will help them to speak with one voice.
- They need to collaborate with academic and research institutions to reduce the cost of developing data sets to conduct evidence-based advocacy and to help sustain their engagements.
- In times of crisis, such as now, there is a need for civil society organisations and activists to as much as possible remain balanced, objective and firm in their engagement with the government, to avoid giving it excuses for further restrictions on social media, and harassment of activists through legal means.

15 https://www.opengovpartnership.org

PERU

HAVE THE PRIORITIES OF DIGITAL RIGHTS ORGANISATIONS CHANGED IN PERU?

Independent
Carlos Guerrero Argote

Introduction

This report considers the impact of the COVID-19 pandemic on the advocacy priorities of digital rights organisations in Peru. First, it presents the changes produced by the deployment of different technologies between 2020 and 2021, as well as their effects on digital rights. The report then analyses how these changes affected the organisations and their advocacy agendas. Finally, some conclusions and recommendations are proposed.

It finds that although the pandemic has strengthened networks of actors working on digital rights, and virtual work has increased the workload and fatigue of activists, the pandemic does not appear to have impacted significantly on the longer-term advocacy agendas of digital rights organisations working in Peru.

Background

In March 2022, it will be two years since the Peruvian government first declared a state of emergency, a few days after the first case of COVID-19 was confirmed in the country.[1] Many things have happened over these two years. Regarding digital rights, Peru has seen a rise in the widespread use of different technologies with an impact on privacy and other human rights, promoted by both public and private sector actors. In many of these cases, the impact has been more negative than positive and has put at risk the people it was intended to benefit, very often without consequences.

It is possible to identify some patterns in the deployment of these technologies. Initially most of them were focused almost exclusively on addressing problems related to the spread of COVID-19. Here we can point out, for example, the development of the so-called "corona apps". In April 2020, the Presidency of the Council of Ministers announced the launch of a contact-tracing application called *Perú En Tus Manos* ("Peru in Your Hands"),[2] which came to be criticised for its lack of effectiveness and transparency in design and use of personal data.[3]

Then, when the health measures implemented in the country forced the digitalisation of in-person activities, multiple remote control and surveillance technologies began to proliferate, mainly in the workplace and education environments. In 2021, a regional study was published on the impact on privacy of e-proctoring, a surveillance technology that uses facial recognition and artificial intelligence to prevent impersonation and plagiarism during student evaluations. The study found that at least 20 Peruvian universities had used e-proctoring software and in at least one case a security breach of personal data was identified.[4]

While digital rights organisations in Peru had to face the challenge of dealing with these new threats, they also had to adapt their own internal processes because of the COVID-19 outbreak. Although by the time of writing this report, all kinds of reports and policy papers have been published on the status of digital rights in the Latin American region, very few consider whether there have been changes in agendas and projects taken on by digital rights organisations, something that could affect their advocacy plans and funding priorities in the coming years.[5]

New threats, work overload, but few changes in priorities

In order to learn more about their internal changes, we conducted semi-structured interviews with

1 Diario La República. (2020, 16 March). Gobierno declaró estado de emergencia por coronavirus en Perú. https://larepublica.pe/politica/2020/03/16/coronavirus-peru-martin-vizcarra-declara-estado-de-emergencia-nacional-por-30-dias

2 Presidencia del Consejo de Ministros. (2020, 3 April). Gobierno implementa aplicativo para identificar situaciones de riesgo y detener cadena de contagio por COVID19. *Gob.pe.* https://www.gob.pe/institucion/pcm/noticias/111820-gobierno-implementa-aplicativo-para-identificar-situaciones-de-riesgo-y-detener-cadena-de-contagio-por-covid19

3 Morachimo, M. (2020, 8 June). Aplicación "Perú en tus manos" sigue dejando más preguntas que respuestas dos meses después. *Hiperderecho*. https://hiperderecho.org/2020/06/aplicacion-peru-en-tus-manos-sigue-dejando-mas-preguntas-que-respuestas-dos-meses-despues

4 Guerrero Argote, C. (2021). *¿Vigilados en la escuela?: Impacto en la privacidad a partir del uso de tecnologías de e-proctoring en la región de Latinoamérica.* https://descargas.lacnic.net/lideres/carlos-guerrero/carlos-guerrero-informe.pdf

5 Recently, The Engine Room, a non-profit organisation, published *Strengthening intersectional approaches to data and digital rights advocacy during the pandemic*, a report that contains just such information. See: https://www.theengineroom.org/wp-content/uploads/2022/01/DDR-Report-26-02-22.pdf

three digital rights organisations: Centro de Estudios en Gobernanza de Internet,[6] Hiperderecho[7] and Instituto para la Sociedad de la Información y Cuarta Revolución Industrial (ISICRI).[8] All of them have been working on issues related to the local digital ecosystem in the last two years. We also analysed organisations that we were not able to interview, but whose work allows us to glimpse changes in their activities.

The new (old) normal: Corona apps and fake news

Something common to the interviewed organisations seems to be the fact that the sudden imposition of remote work did not imply a drastic change in the development of their activities, at least in the short term. This was due to several factors, including: their high level of technology adoption, previous teleworking experiences, and the small size of their teams.[9] On top of this, there was the fact that most of these teams lived in Lima (the capital city), where the greatest connectivity coverage is concentrated.

For this reason, it is not surprising that the reaction of these organisations to the appearance of technologies such as the corona apps and their negative impact on privacy has been well coordinated and in line with previous work, especially in the field of surveillance technologies deployed by governments. For example, Hiperderecho monitored the Perú En Tus Manos application and other tools throughout 2020 and 2021, through its "COVID-1984"[10] website, and without any additional funding.[11] Meanwhile, Democracia y Desarrollo Internacional (D&D Internacional), a non-profit that works on issues related to digital democracy, and with experience in research and advocacy actions on "fake news" during elections, did not seem to have had a problem adapting its work to advocacy on fake news related to COVID-19.[12]

This situation seems to have been similar elsewhere in the region. For example, regional reports produced by the non-profit Derechos Digitales[13] and the Al Sur coalition[14] also focused on the surveillance technologies used during the pandemic.

The rise of private surveillance

Alongside the increase in virtual work and life came one of the biggest changes in the digital rights landscape: the growth in the use of private surveillance technology. Although they existed before the pandemic, with the arrival of COVID-19 there was a massive demand for these tools, especially for remote surveillance of workers, the invigilation or proctoring of online exams, and parental control. The response to this new situation seems to have been more limited than in the case of known threats. There were only two advocacy research initiatives focusing on this area in Peru – one in 2020 by Derechos Digitales[15] and another in 2021, which ISICRI participated in.[16] Both considered the impact on privacy of the use of e-proctoring in the country, and in both cases the initiatives were financed by the *Fondo de Respuesta Rápida para la Protección de Derechos Digitales en América Latina* (Rapid Response Fund for the Protection of Digital Rights in Latin America), an emergency funding programme created by Ford Foundation and managed by Derechos Digitales.[17]

Was the little attention given to private surveillance due to a lack of interest? Or perhaps a question of resources? Although it is not possible to point out one or several causes for this lack of response by digital rights organisations, when asked about the dangers of the rise of private surveillance, the organisations we interviewed indicated that although they considered these issues to be important, they did not plan to include them in their 2022 advocacy agendas. This was due in part to the prioritisation of other projects, but also due to the perception that these topics did not align with the work of their local and regional partners and potential funders.

Increased workload and new partnerships

Despite being more prepared for remote work, as the pandemic progressed, the organisations we interviewed said they felt the wear and tear that was

6 https://www.facebook.com/CGIUSMP

7 https://hiperderecho.org

8 https://www.isicri.edu.pe

9 At the time of the interviews, all the organisations had fewer than 10 workers.

10 A tribute to the book *1984* by George Orwell.

11 https://hiperderecho.org/covid1984

12 Ford, E., & Weck, W. (Eds.) (2020). *Internet and the pandemic in the Americas: The first health crisis of the digital era.* https://democraciadigital.pe/sites/default/files/libro-internet-and-the-pandemic-in-the-americas.pdf

13 Canales, M. (2020). *La herejía tecno-optimista florece en pandemia: Un repaso crítico a las tecnologías disponibles.* Derechos Digitales. https://www.derechosdigitales.org/wp-content/uploads/herejia-tecno-optimista.pdf

14 Al Sur. (2021). *Informe Observatorio Covid-19 del Consorcio Al Sur: Un análisis crítico de las tecnologías desplegadas en América Latina contra la pandemia.* https://www.alsur.lat/sites/default/files/2021-06/Informe%20Observatorio%20Covid-19%20del%20Consorcio%20Al%20Sur%282%29.pdf

15 Derechos Digitales. (2020, 28 October). Perú: cuestionamientos por uso de reconocimiento facial en admisión universitaria. https://reconocimientofacial.info/peru-uso-de-reconocimiento-facial-en-examen-de-admision-a-universidad-publica-genera-cuestionamientos

16 https://www.isicri.edu.pe/proyectos1/ni-un-examen-virtual-ms-repensando-el-uso-de-herramientas-de-eproctoring

17 https://www.derechosdigitales.org/preguntas-frecuentes-frr/#Que_es_el_FRR

the result of working online, including the difficulty of separating personal life from work. In addition to some internal organisational problems, their workload was increased through a high number of inquiries and requests for support from members of their communities. Hiperderecho and ISICRI commented that sometimes they received daily messages from victims of electronic fraud, identity theft and online gender-based violence.

The increase in cybercrime can be explained in part due to the growth of Peruvian internet usage between 2020 and 2021.[18] At the same time, the problem of serving marginalised communities that did not have internet access and were suffering because of the digital divide persisted. The hosting of meetings, events and workshops and the sharing of content through digital platforms also seems to have affected to some extent the ability of digital rights organisations to meet the objectives of their projects. For example, ISICRI had to reformulate several of its projects in 2021 due to the impossibility of carrying out activities that required in-person participation.

However, not everything seems to have been negative. Along with the increase in internet users, there was also a growth of grassroots organisations that eventually connected with digital rights organisations or funders to work on joint agendas. For example, the FotografxsAutoConvocadxs photography collective[19] joined Hiperderecho in 2021 to develop projects on police surveillance during protests.[20] Observatorio de Plataformas,[21] an initiative that seeks to improve the working conditions of delivery platform workers in Peru, also secured more resources to continue its work thanks to the Friedrich Ebert Foundation.[22] In both cases, the connections with these grassroots organisations were made due to their greater presence of on social media.

No major changes in priorities

None of the organisations we interviewed seem to have modified their programmatic agendas in substantive ways. The organisations noted that since the COVID-19 pandemic, most of their projects had changed, but in general these changes were just minor modifications, including extending deadlines. Instead of entirely new projects, the general practice was to add a "COVID impact analysis component" to old projects, but nothing more. Even in the case of ISICRI, which in 2021 worked on the e-proctoring research, the organisation says it does not contemplate continuing to work on this particular issue in 2022.

The common perception of the organisations we interviewed seems to be that throughout 2020 and 2021, there was a saturation of proposals from civil society related to COVID-19 issues. This would have given rise to a large number of projects focusing on the pandemic, which would have taken up most of the funding available for research and advocacy. With the current remission of the pandemic and the abandonment of the intensive use of certain technologies that were supposed to be risky for digital rights (such as corona apps or private surveillance), it does not seem strategic to continue pushing an agenda that revolves around these issues.

Conclusions

Has the situation presented above occurred only in Peru? Is it a region-wide situation? While all the organisations interviewed agreed that the COVID-19 pandemic has raised awareness of various issues (the digital divide, data protection, online gender-based violence, freedom of expression, etc.), it does not seem that this is translating into a radical transformation of priorities or programmatic agendas.

The question remains whether the lack of interest shown in prioritising emerging problems such as private surveillance is due to a lack of capacity, a difficulty in organisations analysing the potential longer-term impacts of the pandemic on digital rights, evidence that the digital rights landscape has not shifted much, or simply because of a shift in donor agendas. Although the emergency funds mentioned in this article made it possible to carry out actions on these issues, this does not necessarily mean that ordinary sources of funding – and organisations' advocacy agendas – cannot respond to the new sustained threats to digital rights produced by the pandemic or any other catastrophic event in the future. However, in Peru, and given our limited sample of organisations, it does not appear that they are being used to do this.

While it may be that the longer-term implications of the impact of COVID-19 on digital rights are not yet apparent, it is a concern if this suggests that interventions on COVID-19 were donor-driven,

18 Agencia Andina. (2022, 6 January). Audiencia digital en el Perú lideró crecimiento en América Latina, según estudio. https://andina.pe/agencia/noticia-audiencia-digital-el-peru-lidero-crecimiento-america-latina-segun-estudio-875761.aspx

19 https://www.flickr.com/photos/191780089@N08/albums?fbclid=IwAR1SWCMSPirkKk4Jo5HgQizABAipRFCmZolcN75vdGeeZAp6MPwnixNwlng

20 Hiperderecho. (2021, 21 May). Presentamos: ¿Quién vigila a los vigilantes? https://hiperderecho.org/2021/05/presentamos-quien-vigila-a-los-vigilantes

21 https://opdperu.org

22 Dinegro Martínez, A. (2021). *Delivery y empleo: Diagnóstico sobre las condiciones laborales en las plataformas digitales*. Friedrich-Ebert-Stiftung. https://library.fes.de/pdf-files/bueros/peru/17952.pdf

short-term, and did not emerge from an identification of potential new systemic threats to digital rights by the organisations themselves. This suggests that there may be more work necessary in analysing the real implications of the pandemic on digital rights, particularly from a country-specific perspective.

On the other hand, the pandemic does seem to have seen a push towards collaboration between organisations that had not previously had common agendas, especially grassroots movements or activist groups which were not formally organised. This is a positive development, and appears to have been catalysed by the increase in the use of the internet by organisations across Peru during the worst days of the pandemic.

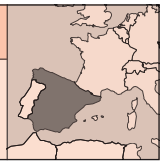
Action steps

The following action steps are recommended for digital rights organisations in Peru:

- *Regional spaces:* Digital rights organisations should support the creation of regional spaces for dialogue among their peers, in order to share experiences and best practices allowing them to improve their ability to react to new threats that are not usually part of their agendas or lines of work. These spaces can also be used to understand better how to deal with the fatigue produced by the new dynamics of remote work, anticipating that the current situation will continue for a few more years.
- *Analysing new threats:* Digital rights organisations should conduct an analysis of new threats arising from the pandemic in order to identify the potential for these threats to persist over time, even after the pandemic is over. This is necessary to properly understand if advocacy priorities need to be rethought, and new strategies developed.
- *Stronger networks:* Digital rights organisations should take advantage of the increase in the use of the internet for interaction and work by organisations involved in different fields, which is still the case, to strengthen their contact with organisations they may not be aware of, including through joint projects and by offering capacity-building support. This would allow stronger advocacy networks to be created that can strengthen digital rights in Peru in the future.
- *Donor fatigue:* Funding organisations should evaluate the success of emergency funds released to respond to COVID-19, including whether or not they may have detracted from the potential of funding longer-term digital rights issues that may have emerged during the pandemic.

SPAIN

FOR BETTER OR WORSE? THE IMPACT OF AN ACCELERATED TRANSITION TO ONLINE WORK AND LIFE



Pangea and the eReuse.org initiative
Lorena Merino, Mireia Roura and Leandro Navarro
https://pangea.org and https://www.ereuse.org

Introduction

The beginning of 2020 was the year of the COVID-19 pandemic, when the first lockdowns took place, which were the strictest during the first half of the year. The limitations to mobility and contact, which impacted work, education, social contact and businesses, and shifted our daily schedules and routines, led to a boom in teleworking and the "digital world" that has changed the lives of people for better and worse simultaneously. When the Spanish government declared the first state of alarm, citizens moved from public spaces into their homes, and from their homes to their screens.

For Pangea, the first year of the pandemic meant an increase in the workload, with our services mainly focused on helping our members to be able to continue working from home during times of confinement.

But about 15% of households in Catalonia were unable to do so, as they did not have a computer at home with which they could remain connected to the world, or exercise fundamental rights such as accessing education or public services. In our eReuse project,[1] we witnessed how precarious the situation of many families was, and how resources impacted the possibilities of accessing information and communications technologies (ICTs) – from the most basic things like having a computer, to connecting to the internet or having the necessary software to interact properly or do work at home.

According to the United Nations Development Programme (UNDP), the school enrolment ratio due to the digital divide fell worldwide in the first months of the pandemic to levels seen in 1985.[2] While it was difficult and costly for families with school children to engage in remote learning, those who had lost their jobs struggled to stay online. Older people were affected too. The digital world is not easily accessible and sometimes is difficult to understand and manage.

Two years later, for those who could get online, much of their work and activities have shifted to the digital world, with many businesses and universities now considering hybrid models of work, teaching and interaction. We are getting used to it. But will it be good for people and the planet?

The rapid transition to a new digital normal

In Pangea's day-to-day work, the first queries we received and our main workload were in the area of our email service. Many of our partners had their email accounts configured with POP3 on their office and work PCs. In the first weeks and months we received many requests for help to reconfigure their email accounts on their PCs at home in order to be able to continue working. These queries were for help in setting up email accounts in different email programs (Thunderbird, Outlook, Gmail, etc.) and to access and copy messages saved by POP3 on office PCs. There was also a significant number of queries from members who switched directly to Roundcube, a webmail manager that we have available for Pangea members.

The other large bulk of enquiries was for help in using the Nextcloud[3] service. The use of this service skyrocketed in 2020. The number of Pangea members who started using it or extended its use in order to have their organisation's files in the cloud for teleworking grew significantly. We went from just over a hundred accounts in Nextcloud in 2019 to 500 accounts by the end of 2021. The amount of space occupied has also grown significantly, exceeding 1.6 TB in Nextcloud. Apart from Pangea's Nextcloud service, some partners also used Google Drive and Dropbox, and sometimes they asked us for support in using these services even though we do not offer them.

In addition to help with email and using Nextcloud, there were also many enquiries and demands for videoconferencing services and services for seminars and online training. Pangea does not offer any of these services, but they are offered by the Guifi.

1 https://eReuse.org

2 UNDP. (2020). *COVID-19 and Human Development: Assessing the Crisis, Envisioning the Recovery*. https://hdr.undp.org/en/hdp-covid

3 https://en.wikipedia.org/wiki/Nextcloud

net Foundation with whom we collaborate closely, so we advised and recommended to members that they use Jitsi and BigBlueButton and approach the Guifi.net Foundation for help. Advice and recommendations were also given on other available platforms, such as Zoom. Despite the demand, the fact that the Guifi.net Foundation offers the services, and the limited capacity of our infrastructure and the work of our staff, we decided against the possibility of offering the services directly to our members, preferring instead to continue the collaboration with the Guifi.net Foundation.

Other services about which we have been consulted were remote desktops (we do not offer the service and unfortunately, we have not found a free software alternative that we could recommend, falling back on commercial and paid options such as TeamViewer or Google tools), and virtual private networks (VPNs). We have offered advice to some member organisations about setting up their VPNs and accessing their local server to be able to telework, but this has been limited advice.

We do not have precise data on the increase in the workload that COVID-19 has meant for our activities, but as a qualitative assessment we can say that the number of email messages received or answered at suport@pangea.org went from 2,412 in 2019 to 3,827 in 2020, exceeding 900 support tickets in 2021. So far the level of this workload has stayed the same in 2022 – suggesting that the solutions members explored are still being used, and were not a once-off fix for the lockdowns.

We do not have data on the number of calls received, but qualitatively we can see that the number of calls tripled in the first quarter of 2020, taking up many days of the support person's half-day work time, as well as extra time answering messages left on our answering machine. The telephone workload decreased a lot during 2021, returning to what was usual in pre-pandemic times. We associate this mainly with the fact that many people have already organised themselves for telework and do not need the extra help needed at the start of the pandemic.

The tech "side effects" of the pandemic

In the light of all this information, it should not be forgotten that this landing of the "digital world" in our daily lives, from work to our personal lives, which COVID-19 has accelerated exponentially, has brought with it side effects that are sometimes not as wonderful as we might think.

For example, having to telework and become more active socially online in order to adapt to the new situation, together with the uncertainty and insecurity derived from the restrictions and their effects on employment, economics, etc., has led to "digital burnout" for many people. In part this is a result of not being able to manage teleworking well, working longer hours than required or than usual, with no real disconnection between work and family life, with everything being done in the same space at home. This may not be the case for everyone, but in the case of Pangea's staff, and certainly in terms of work hours, the extra effort that was needed was very noticeable during 2020 – we had to help all the members who needed it and not leave anyone behind. For the members, it was critical and urgent to be able to telework, and for us this urgency meant a work overload, with not enough time to properly disconnect or to be able to rest.

Digital inequality became a blatant inequity that the government was forced to address. And it did so through the old familiar linear economy model, with the government of Catalonia putting out a tender for the acquisition of more than 300,000 laptops for some 82 million euros. The number was insufficient for the existing needs and the solution turned out to not be so effective: in January 2021, eight months later, only 5% of the laptops had reached their destination. The shortages of devices and components and stockouts highlighted the underlying lack of resilience of the capitalist system globally, and of the linear economy, in particular.

Indeed, while demand for new PCs has grown with the rise of teleworking and home schooling, supply has decreased due to supply chain problems (especially with respect to computer chips) and transportation problems. While analysts forecast refurbished PC sales to grow at a compound annual growth rate (CAGR) of 11% between 2019 and 2027,[4] reuse centres in Catalonia have seen significant increases in sales of functional equipment as consumer patterns are slowly changing.

The pandemic brought out the worst and the best in society. Hundreds of initiatives began to emerge in the territory with the aim of alleviating the digital divide. Citizen activities to donate and repair computers followed one after the other in the best possible way – the situation did not allow for an assessment of which devices were useful, or which beneficiaries needed additional skills to use them properly. However, while citizen mobilisation helped to narrow the digital divide as much as it could, it also awakened the old trauma of the level of inequality in society, which remains unresolved.

The eReuse project manages the donation of computers from public and private entities to social

4 https://www.transparencymarketresearch.com/refurbished-computers-laptops-market.html

entities, sending them to companies that refurbish them for reuse or recycle them when they are not reusable. During the first two years of the pandemic, our eReuse software recorded a significant increase in the number of devices donated, refurbished and traced for subsequent recirculation. Thousands of devices were recirculated to the most disadvantaged population at an average price of about 40 euros of refurbishment cost per tower – a cost which was taken up by crowdfunding campaigns, local cooperation projects and public institutions or paid by the end-users themselves. This is a much more advantageous price for the public coffers than the 300-400 euros per laptop that was tendered for the purchase of new devices.

These numbers were made possible thanks to the cooperation between about 20 social and solidarity economy organisations, which collect, refurbish and distribute equipment, even in a chaotic context where demand was soaring during the peaks of the pandemic.

During the first two years of the pandemic, headlines highlighting the "digital divide" had their moments in the media and on social networks. This marketing of inequality has contributed to making the inequalities more visible and to deepening our understanding of its multiple facets, while encouraging the involvement of citizens, businesses, non-profits and public administrations. In general, there has also been a shift from emergency or welfare action by citizens or corporate social responsibility campaigns to political action and solutions based on public-community partnerships. In this framework, working groups, networks, public funds and facilities to ensure access to devices and the internet, as well as to alleviate skills and knowledge gaps, have increased considerably.

However, there are still more questions than answers, and new challenges emerge. For example, while connectivity exists, it sometimes is available at unfair prices and under unfair conditions. We find families spending around and beyond 10% of their disposable income to pay for the internet and devices for their digital life and work. This situation has prompted the Spanish government to reform the Telecommunications Law to ensure that retail prices are accessible to citizens with low incomes or social support needs.

Conclusion

The pandemic has forced us to rethink the way we work and relate to each other and has created new needs. This has presented us with choices among different options which entail different economic costs, individual and collective costs, as well as side effects (e.g. exploitation of our data and conditioning of our choices through advertising).

It has left a more skilled population accustomed to online activities. It has also left a more isolated and precarious population – those who have not been able to "go digital". It has changed and advanced the way we relate digitally with public and private organisations. It has also made us aware of the risks and limitations of the online world compared to the offline world.

These changes, and the normalisation of the digital, have helped those with sufficient resources and training more, and have therefore widened the gap between those who do and do not have them. Access to the offline world begins with walking into the public space. In contrast, access to the digital world requires a digital device and a connection, which come at an economic, educational, privacy and environmental cost. We need to buy digital media on the market and pay with money and our data to be present in an increasingly privatised and extractive digital world.

Our digital "life" requires a sustainable digital world for people and nature, as a global public good. We must ensure that we have the freedom to participate – that this participation is not a barrier for anyone. We need to have a device and a connection, be able to share or publish our ideas, satisfy our needs, and be able to interact with companies or public entities without being forced to use or contract commercial services that limit, exploit or exclude us. We need to have the autonomy to decide (what hardware to have, what software to use, how to connect to the digital world), with the confidence of understanding clearly what is being done with our data and how things work, so that we are not deceived and manipulated through self-interest and the use of biased data. We need the peace of mind of knowing that this digital world does not contribute to destroying the planet, but rather to protecting it in a way that supports us and supports future generations.

Action steps

Given that more people are online now, and that hybrid ways of socialising, working and learning are becoming the norm, we need to rapidly upscale the public debate on exactly what the sustainable and ethical use of technology means. The following key issues need to be taken into consideration:

- What are the ethical choices that we need to make when contracting internet and online service providers? Key flashpoints include whether or not the services use open source or proprietary systems, whether they are extractive or

non-extractive business models (e.g. do they rely on data extraction and manipulation for profit?), and how their activities impact on digital rights.

- With regard to economic models, choices need to be made between diversity or uniformity of products and services, local or global services or products, the use of private companies or cooperatives working for social inclusion or promoting a solidarity economy, and a privatised versus commons governance model for digital infrastructures.
- The production and use of devices need to be considered: How does a linear versus circular economy contribute to or detract from local development, the economy, people, and the natural environment? What are the impacts of our devices on sustainability?
- The need for training and support in technological decision making and the sustainable use of technology should be considered. How to prevent data capture by public and private actors that limit our rights needs to be thought through, and how best to exercise and expand human rights online. Related to this, there is a need for open data and flexible and free digital tools for community awareness and action.
- Biased, unreliable information is free and easy to find on the internet. Verified information – which is properly referenced, argued and reliable – requires ways to fund its development, and is a requirement for digital sovereignty, more citizen freedom, and less manipulation of public discourse.

SUB-SAHARAN AFRICA, MIDDLE EAST AND NORTH AFRICA, AND LATIN AMERICA

COLMENA: A STORY OF TECHNOLOGICAL CO-CREATION WITH LOCAL AND COMMUNITY MEDIA

DW Akademie and Redes por la Diversidad, Equidad y Sustentabilidad A.C. (REDES A.C.)
Adrián López Angulo, Adriana Veloso Meireles, Carlos Henrique Gontijo Paulino, David Ramírez García, María Álvarez Malvido, Nils Brock and Vivienne Gager
www.dw.com/en/about-us/s-9519 and www.redesac.org.mx

The challenge of communicating a pandemic

No community on earth has escaped the COVID-19 pandemic, which has been intensively documented by the media across the world. This includes community radio and online media outlets organised by the communities themselves, which offered indispensable platforms for grassroots voices, especially in rural and Indigenous territories of the global South. These "communicators" were important "translators" of online and other information for communities and had to rapidly update their knowledge on aerosols, vaccines and how to locally organise health and care strategies.[1] Community media rely on interpersonal contact to collaborate, build agendas for advocacy, and produce and air their productions. Though personal computers can be found in most community radio stations, this is not the case in many homes. Mobile phones and online access became a lifeline to continue working. However, what started as an opportunity to explore new tools and ways of relating online quickly increased a reliance on commercial software.

Our report[2] explores the ways in which communicators became aware of the different values embedded in online spaces and tools in comparison to the locally developed models of "shared ownership" practised in their collectives. Whether conscious or not, it was a moment when many community media started to translate their right to communicate to be meaningful in digital spaces – a debate that sparked interest in finding or creating alternative tools for online media practice. One of these alternatives is Colmena, a free/libre and open source media toolbox that brings together in one application all the essential workflows for local and community media production.

From multi-site research to a collective response

The pandemic imposed different challenges and restrictions on the workflows of community media. Some had to completely close their studios during national lockdowns, as was the case of Radio Confeniae, transmitting from the Ecuadorian Amazon. Others, like Gulf Radio, located in a fishing community in Kenya, had to restrict access to small staff teams and could not host programmes with guests. And even where stations could almost broadcast in the way they did before the pandemic, as was the case for Radio Vénégré in Burkina Faso, they quickly had to adapt to the challenge of insufficient responses by local authorities or "fake news" circulating on the health crisis.

Despite these disparate situations, a common experience was the need to rapidly adapt to the use of new digital tools to be informed and inform others about the spread of the coronavirus. But besides the advantages of digital tools, the communicators also started to perceive new risks with the use of proprietary tools (economic exclusions, privacy, new digital hierarchies), and insightful debates within the community media environment were sparked around the safety, sustainability and ownership of these means of production.[3]

To engage with these discussions, DW Akademie executed a multi-site research project, under the auspices of its Global Crisis Initiative (GKI).[4] A general survey of 34 participating media outlets from different regions across Latin America and Africa, defining themselves as "community media", confirmed

1 For an example of a regional analysis, from a South African perspective, see: Health-e News. (2021, 31 March). Community media left behind in the fight against the COVID-19 infodemic. https://health-e.org.za/2021/03/31/community-media-challenges-covering-covid-19

2 This report covers the following countries: Bolivia, Brazil, Burkina Faso, Colombia, Ecuador, Ghana, Guatemala, Kenya, Mexico, Morocco, Peru, Tunisia and Venezuela.

3 Media outlets like Boca de Polen from Mexico quickly understood that these digital tools made them more vulnerable, as Janis Carillo points out with regard to privacy concerns: "We have detected the needs but we don't know how to solve them. Awareness is there, which is sometimes the most complicated thing."

4 More about the GKI, launched in January 2021, can be found here: https://www.dw.com/en/initiative-transparency-and-media-freedom-crisis-resilience-in-the-global-pandemic/a-57443977. The body of the research included a document review, market/actor network analysis, the mapping of media workflows, focus group discussions, regional workshops, a survey and an interview series.

that FM radio remains by far the most popular media format in rural communities. While the importance of audio-based radio is undeniable, two-thirds of the outlets surveyed employ strategies for publishing audio, text and multimedia content online. Further, a series of in-depth interviews revealed that technological choices for online communication were often informed by the necessity to find a quick solution in the context of the pandemic.[5] After this gathering of user stories, the ongoing process of co-creating Colmena started.

Teaming up were Redes por la Diversidad, Equidad y Sustentabilidad A.C (REDES A.C.), an NGO based in Mexico, DW Akademie, and a group of initially 12 and later 22 media outlets[6] from Latin America and Africa. Working together, the first concept of an open source, virtual newsroom was developed. The main challenge, especially in rural spaces with limited online connectivity, was to provide a lightweight, secure and mobile toolkit that allows media outlets to exchange critical information, publish their work and stay in contact with their audiences. At the same time, an increased need for safe online spaces and digital inclusiveness was identified. And by listening to the different realities and cultural contexts of the partners, a common need was confirmed: to address intersectionality, gender and diversity issues, acknowledging the different contexts and territories in which radio stations are located.

Putting all the identified observations and ideas of the communities at the centre, and working with a team of expert developers, we started to translate them into practical technology.

Participatory action in practice

Colmena's co-created design process included community, rural and Indigenous media and other organisations, like Bolivia's first feminist online review Muy Waso and free/libre software activists in Latin America and Africa, using a methodology based on participatory action research (PAR). This approach seeks to take a step back from technology, following a path of reflection that starts from the territories and dreams of the communities themselves. PAR provided a means for dialogue among the radio stations, media collectives and DW Akademie and REDES AC. It was a way to create a shared understanding of how the daily workflow and content creation of each media outlet or station is organised. This was vital knowledge, since our toolkit is meant to contribute to diverse and collective communications practices and ways of living and sustaining life.

For the media collectives, this approach provoked the key question of how the lives of individual collaborators, as well as their collective and organisational processes, had been affected by COVID-19. What prevented them from carrying out their daily activities? The dialogue confirmed their "difficulty in remaining in contact with communities" and their need to "restructure their internal collaboration working from afar."[7] The biggest loss was definitely a common physical space and the daily interaction that happened there.

The move to "virtual spaces" in rural communities became a challenging task. The participating media pointed out the high costs of connectivity and the limited online access in their territories, together with the lack of information to find free digital tools. Therefore, many of them used commercial software solutions.[8] A great dependency on for-profit platforms became evident, resulting in additional costs or, if used "for free", exposing them to the harvesting of their user data in a problematic way – including for independent and investigative journalists working in communities.[9] Another hard lesson shared by the community media was the experience of how little the proprietary tools could be combined with other tools, or modified to suit their needs. Workflows for analogical FM transmission – let's say a live interview in a radio studio – now involved several devices and software tools.

Was there really no integrated solution at hand? The media outlets began to envision "a commonly owned platform to exchange files", a design that would "take into account poor connectivity", and "backup and publishing solutions" that would enhance the creative capacities of community, collective, Indigenous and rural media. Most importantly,

5 A total of 22 interviews were conducted between January and March 2021, with a special focus on rural communities.

6 The participating media are: Muy Waso (Bolivia), Remando/Voz de la Confeniae (Ecuador), Radio Sayaxché (Guatemala), Boca de Polen (Mexico), Radio Ocaina/Red Cantoyaco (Colombia), Unión de Mujeres Aymaras del Abya Yala (Peru), Red de Radios Comunitarias y Software Libre (inter-regional), Rádio Comunitária Aconchego (Brazil), Copiô Parente! (Brazil), Saúde, Alegria e Sustentabilidade (Brazil), Radio Ada/Ghana Community Radio Network (Ghana), Radio Breezy/Ghana Community Radio Network (Ghana), Gulf Radio (Kenya), Radio Amani (Kenya), Pwani FM (Kenya), Radio Rahma (Kenya), Radio Vénégré (Burkina Faso), Radio Mères en Ligne (Morocco), E-Joussour FMAS (Morocco), and Radio Nefzawa (Tunisia).

7 Both quotes are comments that were made and documented during the first exploratory workshop sessions.

8 As Jenny Paucar from the Peruvian Union of Aymara Women of Abya Yala (UMA) points out: "We had never heard about Zoom and the possibility to meet in those [digital] spaces. So when did this become interesting? When we could no longer gather in on-site meetings."

9 For the participating media, WhatsApp was the tool used for internal communication, Google Drive led in file sharing, and Zoom was the preferred platform for video conferencing. These and other commercial solutions dominated workflow organisation.

they wanted "to have it all integrated in one place."[10] The collaborative naming of our tool was also part of the co-creation process. The media outlets all proposed concepts and metaphors from their distinct cultures and spaces. From this and other ideas, possible names emerged, with the group finally settling on "Colmena", which in Spanish means "beehive". The name and the corresponding branding both emphasised a common and co-owned space for collaboration: a space where bees (communicators) can meet to work and share pollen (information) for the creation of honey (content) that gives continuity to collective life.[11]

To put this beehive into action, a "special" development team was needed. Besides the technical skills, there was a need for a shared ethical grounding and a common perspective on threats that community media face going online. More than ever, human rights and principles such as freedom of expression and privacy are at risk due to the authoritarian advances made in countries and the dominance of big tech in its business model based on data mining. So-called surveillance capitalism provides little space for grassroots communities to thrive and collaborate towards an open web.[12] The persons accepting the challenge to code Colmena brought with them expertise and involvement in agile open government initiatives and were well aware that Colmena would have to take into account questions of low connectivity and the digital divide.[13]

The tech team put much emphasis on interactive design and "built-in" diversity. Usability issues and user experience were taken into account from the very early stages of development. This guaranteed that the diverse needs for using the software were catered for. It was also collectively decided to make Colmena available in six languages (English, Spanish, Portuguese, French, Swahili and Arabic) and to allow user-driven translation to make the tool available for various interpretations and cultures.

In addition to the development team, we also had to define a coherent (open source) production environment for Colmena, and the choice was a software factory system called GitLab.[14] It provides the infrastructure to apply agile project management methodologies and thereby deliver ongoing updates and increments to the coding. The platform also allowed the team to incorporate the feedback from communities, and respond to their different cultures and customs. This dialogue constantly nourished the progress of features and the overall design. In technical terms, Colmena consists of two main components: (1) a lightweight progressive web application (PWA) working on a wide range of mobile and desktop devices for easy online/offline creation and collaboration; and (2) a secure and decentralised cloud management platform for up to 1,000 users, offering sharing, storage and publishing tools. Combining both environments, Colmena offers all essential tools for local and community media production workflows: high quality face-to-face mobile recording; a recording studio for online interviews; live audio streaming; text and audio editing tools; a publication and dissemination area connected to the main media platforms; and working groups with the possibility of easily sharing various types of files for collective production. Summarised, it offered most of the tools that community media need for production in an all-in-one secure and free package. The long-term vision of the project is to use an ethical infrastructure (hosting) to offer a sustainable alternative to big tech services.

Working with the concept of privacy by default, the application values information security and the data protection of users. It ensures the interoperability of content by adopting international protocols like Dublin Core for metadata. As it is designed for low-connectivity environments, Colmena includes the principle of universal access, with a mobile-first approach in the beginning and an interest to explore potentials for interoperability with community-driven and sustained approaches to securing connectivity.[15] The debate of technological principles and digital rights inspired proposals that

10 As Paúl Salas from the Ecuadorian community radio network (CORAPE) pointed out: "It would be interesting to have an app to capture the voice with quality, be able to edit on the phone and be able to send. It is essential to facilitate the dynamics of journalists."

11 To share a piece of this debate, let's listen to the co-founder of Muy Waso magazine from Bolivia, Michelle Nogales: "We dream of having a safe space to share our data, with a place that brings together the content, a quality tool, fast and free. With this platform we dream of having everything in one place, on your phone or computer, with free and open source software. A beehive as a place where we all get together to work, where there is what we need to have our final products."

12 For an interview with Shoshana Zuboff, who coined the concept of "surveillance capitalism", see: Kavenna, J. (2019, 4 October). Shoshana Zuboff: 'Surveillance capitalism is an assault on human autonomy'. *The Guardian*. https://www.theguardian.com/books/2019/oct/04/shoshana-zuboff-surveillance-capitalism-assault-human-automomy-digital-privacy

13 By such innitatives, we especially refer to projects that were part of the "Pontos de Cultura" created by the Brazilian Ministry of Culture in 2010. This programme included intensive work with open source software and tried to put into practice a "digital inslusion" strategy. https://pt.wikipedia.org/wiki/Pontos_de_Cultura

14 Find out more about GitLab here: https://gitlab.com/gitlab-org/gitlab

15 This includes practical experiences in designing and setting up intranets in Indigenous and rural communities by REDES A.C. (see: https://www.redesac.org.mx/intranets), as well as the even broader approach of "community networks", which focuses on the creation of an enabling environment for communities to connect themselves, as pursued through the local networks initiative by APC and Rhizomatica (see: https://www.apc.org/en/tags/community-networks).

translated participatory media making, interculturality, intersectionality and gender perspectives into collaborative online and offline action. Rather than being driven by a theoretical understanding of its usefulness, the collective ideas that underpinned the development of Colmena were practical, and always driven by the question: How could it be a safe and diverse space for all?

Based on this guiding question, and through a collaborative approach, a gender analysis was conducted in parallel to the development of Colmena. This has highlighted the potential for Colmena to proactively promote gender equality. The need for a space to listen and exchange on gender-related issues became vital to the project – it showed that while there was a longing to share experiences and collaborate on gender-related concerns and challenges, there was also a need for a space where the documentation of security and digital rights issues was transparent. For us this meant integrating an intersectional gender perspective into the entire project, and aligning the technical implementation of Colmena in a way that helped to overcome gender-specific barriers.

One result was us creating a safe space as a permanent feature in Colmena. This involved setting up a dedicated "honeycomb" (a closed chat group) for women. The initial idea was developed in more detail in subsequent workshops and conceived as a space where relevant content, workshops and training materials could be shared between women, and where women could communicate openly with each other.

Meanwhile, the media collectives began to mobilise their communication skills around Colmena. They developed translations of the menus and static content of the website, engaged in online debates and held training sessions on the use of free technologies, such as on free/libre software and licences, podcasts, autonomous servers and audio editing. These accompanied the development process of the platform. This proactiveness of media outlets and collectives was vital to the development of Colmena, and helped the developers understand and respond to the needs and visions of the communities that were going to use the media toolbox.

This flexibility is key in a world that is still adjusting to a post-COVID situation. The project is committed to strengthening all communicators who produce content that helps communities flourish. And though we hope that many beehives will join the Colmena project, the open source software is also available to other media outlets, community initiatives and the open source community who want to build alternative digital ecosystems.

Inclusive co-creation as a key for human-centred and nature-positive technologies

In times when information becomes a matter of sustaining life and care, community radios and media have been shown to have played a central role in responding to the COVID-19 health emergency across the world.[16]

As the Colmena experience demonstrates, digital strategies are important to allow community communicators to operate with safe tools that dialogue with the collective values and practices of their territories.[17] By involving media outlets from Latin America and Africa in the creation of the software, we were able to design a solution (or rather an offer) that is sensitive to shared realities in the global South and ready to be used, modified and improved to suit daily routines.

Undertaking such a journey, one that locates diversity as the starting point, has its own challenges, such as finding the right communication channels that bridge linguistic barriers and time zones, as well as identifying common grounding priorities, needs and desires that can shape a project like Colmena as a "hive" that is meaningful and accessible to all.

Designing a tool that responds to local needs across the world could only have been undertaken as a collective effort. In this sense, the approach of co-creation that was necessary to build Colmena has become a beehive itself: a process-oriented journey rather than a technological solution that is meaningful in the relationships that are woven through the reflections and the collective knowledge created in the testing processes.

One of the key learnings of this dialogue is the need for constant capacity building to make such a collaborative process truly transformative. Related to the great cultural diversity embedded in the initiative, each media outlet brought with it specific weaknesses and strengths. But while in-person training was not possible due to the pandemic, our online approach still turned those differences into a productive force for mutual learning and creation.

Taking one step back from the dialogue with rural and Indigenous communities, Colmena can also be read as an attempt to practically answer how democratic and collaborative governance processes

16 This argument is supported by several case studies worldwide, such as this one from an Indian perspective: Laskar, K. A., & Bhattacharyya, B. (2021). Community radio stations' production responses to COVID-19 pandemic in India. *Media Asia, 48*(4), 243-257. https://doi.org/10.1080/01296612.2021.1970421

17 Brock, N., Gager, V., & García Gago, S. (2021, 10 September). Colmena open source software: Community media brave the pandemic with a "beehive". *DW Akademie*. https://www.dw.com/en/colmena-open-source-software-community-media-brave-the-pandemic-with-a-beehive/a-59147718

can be applied to software development. The situated application of free/libre software philosophies and methodologies is a feasible path to follow, and is not restricted to hackers. Instead it is open to collaborative efforts involving diverse participants. It can be essential to promoting open communications systems based on human rights principles, as well as nature-positive digital solutions, and responding to the challenges of maintaining them.[18]

Action steps

The following advocacy priorities are suggested by the Colmena project:

- Create alternative communication solutions with Indigenous and community-based activists, journalists and radio producers that allow them to share and collaborate meaningfully in the development of those solutions. In this way, these initiatives will contribute to advocacy pushing for the right to communicate in a concrete way by showing how the right can be achieved on the ground.
- Build alliances between organisations (media outlets, the free/libre software community, academia, human rights and other civil society organisations) to support community-centred, co-owned infrastructure.
- Support the long journey towards the autonomy and sovereignty of Indigenous and community media through collaborative tools that respond to their own ways of creating, producing, preserving and sharing information, content, languages and stories.
- Reflect on how an intersectional gender approach can be embedded in the technical implementation of the project to overcome gender-specific barriers.
- Explore and promote nature-positive technologies when developing collaborative media tools, even though this is a difficult and challenging task.

18 To truly become nature-positive in such a short amount of time was a challenge and remains a "technological debt" for the ongoing development of Colmena. While the lightweight PWA design allows for a broad use of already existing hardware (and even a bit of upcycling), the currently used cloud infrastructure has a negative impact on nature due its carbon emission footprint. Our commitment is to become "carbon zero" in the next 12 months and to further engage in circular economy and upcycling reflections.

SUDAN

THE IMPACT OF COVID-19 AND US SANCTIONS ON DIGITAL RIGHTS IN SUDAN

Information and Communication Technologies Syndicate
Wala Ahmed Elfadul Mohammed, with Sidrat Elmontaha, Mohamed Elhassan, Mohamed Said and Mukhtar Atif Elshiekh
wala.ahmed@outlook.com

Introduction

United States (US) economic and technology sanctions have played a major role in the digital divide and decades of economic isolation of Sudan. In December 2018, peaceful demonstrations started in the country and continued for over eight months, with protestors calling for democracy and the removal of the dictatorial regime of Omer Al-Bashir. In August 2019, a new transitional government was formed, with Abdalla Hamdouk appointed as prime minister of the country. The transitional government faced challenges to meet its new democratic objectives and to balance its authority with that of the military, which had been in power since independence from British colonisation.

The struggle of the transitional government to implement change was worsened by the impact of the pandemic, in a country already hard hit by sanctions. These challenges included failing educational and health care systems, crippled economic development, a collapsed private banking sector, unreliable and very sporadic power generation, and a worsening digital divide. In this context, on 25 October 2021, a year and a half into the pandemic, the Sudanese military led by General Abdel Fattah al-Burhan staged a military coup. While the pandemic catalysed underdevelopment in Sudan, this has been incomparable to the impact of US sanctions on the country. With respect to digital rights, the primary advocacy goal remains mitigating the impact of sanctions, before any meaningful discussion on shifts in digital rights priorities as a result of the pandemic can be possible.

This report discusses the impact of sanctions on Sudanese citizens. It argues that sanctions are an outdated way to force regime change, and that instead of change they end up empowering autocratic regimes in their control over citizens.

The impact of US technology sanctions on Sudan

Sudan has a total diverse population of 44.38 million people with a Human Development Index score of 0.510 in 2019.This ranked the country in the lowest category, positioning it at 170 out of 189 countries and territories. Tribal conflict, a lack of awareness about the importance of education, and chronic underdevelopment contribute to the poor schooling of children in Sudan.[1]

In 1997, the US imposed economic sanctions against the government of Sudan because of its continued sponsorship of international terrorism. These included a comprehensive trade embargo and blocking the assets of Sudan's government.[2]

Sanctions were expanded in 2006 with several new prohibitions limiting the export of US goods, technologies and services to Sudan. Prohibited items were contained in the Commerce Control List (CCL), and included software, telecommunication equipment and e-governance systems, among other technologies.[3]

In 2017, the US revoked longstanding economic sanctions against Sudan. As a result, US persons are able to trade, make transactions and do business with individuals and entities in Sudan. However, these actions established the Bureau of Industry and Security (BIS) in the US as the sole licensing agency for export of items to Sudan.[4]

The president of the new transitional government submitted the statutorily required report certifying that Sudan had not provided any support for acts of international terrorism to the US Congress. After this, the determination regarding Sudan as a state sponsor of terrorism was rescinded, effective 14

1 UNDP. (2020). *Briefing note for countries on the 2020 Human Development Report: Sudan*. http://hdr.undp.org/sites/default/files/Country-Profiles/SDN.pdf

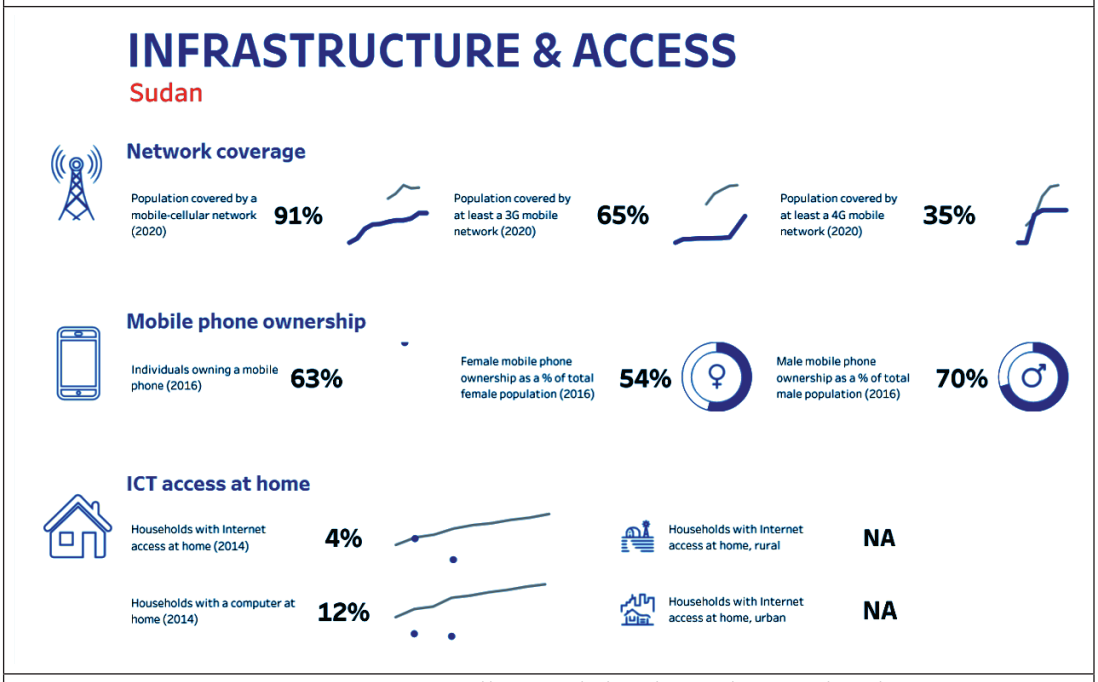
2 Morland, A. (2017, 6 October). US ends 20 years of sanctions on Sudan. *The New Humanitarian*. https://www.thenewhumanitarian.org/news/2017/10/06/us-ends-20-years-sanctions-sudan

3 Bureau of Industry and Security. (2021, 19 January). Implementation in the Export Administration Regulations of the United States' Rescission of Sudan's Designation as a State Sponsor of Terrorism. *Federal Register*. https://www.federalregister.gov/documents/2021/01/19/2020-29037/implementation-in-the-export-administration-regulations-of-the-united-states-rescission-of-sudans

4 U.S. Department of State. (2022, 4 February). U.S. Relations with Sudan. https://www.state.gov/u-s-relations-with-sudan

FIGURE 1.

ICT infrastructure and access in Sudan



Source: https://www.itu.int/en/ITU-D/Statistics/Dashboards/Pages/Digital-Development.aspx

December 2020. Yet, still, technology and software licenses under the CCL are restricted, which means they require authorisation from the BIS.[5]

Impact of US technology sanctions on information and communications technology (ICT) infrastructure

Most of the studies reviewed for this report, and interviews conducted with stakeholders, demonstrate the failure of the sanctions imposed on technology to reach their desired result in most cases. Instead, the sanctions resulted in citizens suffering limited access to basic education and health services, and the country facing economic collapse, with the transitional government not being able to progress in the country's development. The COVID-19 pandemic has also revealed the impact of technological isolation when the whole country was completely paralysed during the pandemic lockdown.

For several months before the military coup in October 2021, there had been resentment among the civilian and military and militia leaders, with each blaming the other for the failing economic situation. The absence of e-government systems had also affected the ability of the transitional government to manage the country's resources and projects. Restricted access to ICTs had impacted the digital divide in Sudan as well. Although five submarine cables pass through country, the internet penetration rate is low compared to countries that access the internet through the same cables in South Asia, the Middle East and other African countries in the region. To put this into perspective, it is estimated that only 35% of the population is covered by 4G in Sudan (see Figure 1), compared to 96% in neighbouring Egypt. The internet is considered as the main enabler to implement e-government services and to provide public services to citizens. However, Sudan's E-Government Development Index (EGDI) score for 2020 was 0.3154 and it ranked 170th out of 193 countries, compared to Egypt with an EGDI score of 0.5527 and ranked at 111th, and Saudi Arabia with a score of 0.7991 and ranked 43rd.[6]

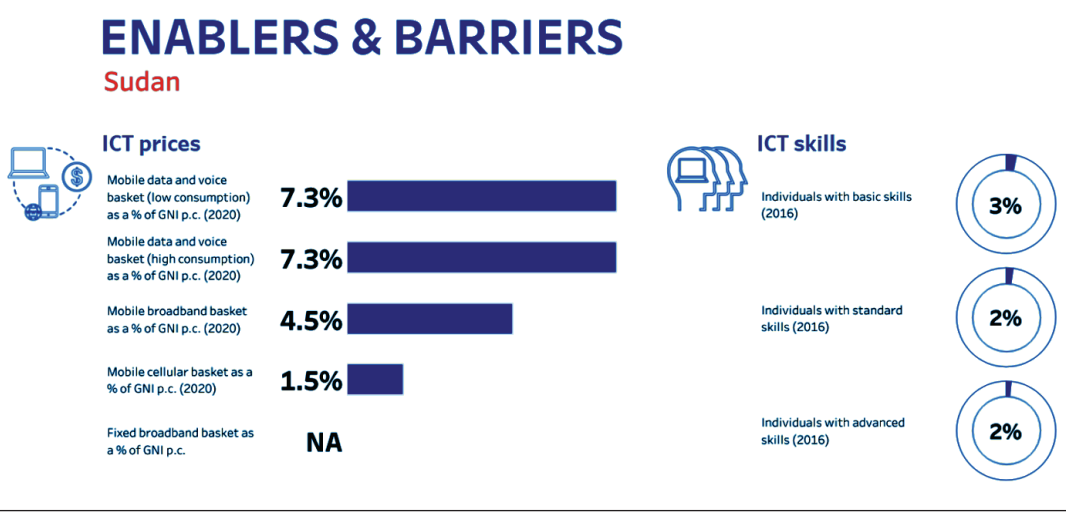
Sanctions have limited any plans for implementing an e-government programme designed by ICT professionals in Sudan. They have prevented the government from forming relationships with

5 https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information/sudan-and-darfur-sanctions

6 https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/162-Sudan

FIGURE 2.

Enablers of and barriers to digital development in Sudan



Source: https://www.itu.int/en/ITU-D/Statistics/Dashboards/Pages/Digital-Development.aspx

large international ICT companies from the US and Western Europe, and restricted access to security software, discouraging public institutions and civil society organisations from using technologies in the first place, and leaving the private and banking sectors vulnerable to cyber attacks.[7]

Technology sanctions also empowered the National Intelligence and Security Services (NISS) in their efforts to suppress activism – even though they were intended to put pressure on the regime. Activists are restricted from updating their software, leaving them exposed to surveillance and potential attack by the highly trained security officers in Sudan. In 2014, Citizen Lab reported that that the NISS had access to Hacking Team's Remote Control System (RCS), which allowed it to monitor political activists and detain them. RCS's capabilities include the ability to copy files from a computer's hard disk, record Skype calls, intercept emails and instant messages, and read passwords typed into a web browser. Furthermore, RCS can turn on a device's webcam and microphone to spy on the target.[8]

The NISS also had access to ProxySG servers from cybersecurity and network management company Blue Coat Systems that enabled the government to intercept internet traffic. This raised the issue of how the software had been sold to Sudan, which had been under sanctions for decades, empowering the old regime to restrict access to information or record private communications.[9]

According to research also conducted in 2014, regimes targeted by sanctions often exaggerate the negative effect of sanctions on the economy to prevent the population from revolting against them. States have also been found to intentionally deteriorate economic growth in order to increase the economic hardship of the population so that any revolt proves costly for citizens. Although the sanctions target the elite, due to their strong economic position, their funds hidden around the world, and international collaborators, it is the local population who feel the impact the most.[10]

Meanwhile, research conducted by the University of Oxford and the University of Khartoum highlighted the significant impact of tech sanctions on the content and continuity of academic research and education, given that they are increasingly reliant on software, hardware and other equipment. As the rate of technological innovation speeds up,

7 Li, Q., & Abdalla, O. (2014). The E-Government in Sudan: Challenges, Barriers and Prospects. *Proceedings of the 2014 International Conference on Global Economy, Commerce and Service Science.* https://www.atlantis-press.com/proceedings/gecss-14/10979

8 Marczak, B., Guarnieri, C., Marquis-Boire, M., & Scott-Railton, J. (2014, 17 February). Mapping Hacking Team's "Untraceable" Spyware. *The Citizen Lab*. https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/

9 Marquis-Boire, M., Anderson, C., Dalek, J., McKune, S., & Scott-Railton, J. (2013, 9 July). Some Devices Wander by Mistake: Planet Blue Coat Redux. ***The Citizen Lab***. https://citizenlab.ca/2013/07/planet-blue-coat-redux/

10 Oechslin, M. (2014). Targeting autocrats: Economic sanctions and regime change. *European Journal of Political Economy, 36*, 24-40. https://doi.org/10.1016/j.ejpoleco.2014.07.003

sustained periods of sanctions left Sudan's academic communities considerably out of date.[11]

The lack of internet connectivity in schools also meant that the flow of information in and between schools and the local education administrations, states and federal ministry of education was slow.[12]

The growth of tech startups has been stagnating in Sudan, making external and foreign investments in startups almost impossible. Samir Mohammed is a member of the ICT Syndicate and the founder of DATAQ, a data-driven research company. It helps clients to generate new value from their data sources, and collects, organises and analyses different sources of data in order to provide market insights for clients, which include small and medium-sized businesses. He commented, "I am struggling and looking for workaround plans to buy Power BI software online and I cannot access online tools. It is also challenging to get funds to invest in my start-up."

According to UNCTAD, the lack of digital innovation platforms in many developing countries has a significant impact on their development. It results in using global innovation platforms in the technological innovation pathways that might not align with local market needs in developing countries. Furthermore, digital enterprises in developing countries will continuously miss opportunities to compete in the global innovation market, thus hindering their ability to scale.[13]

Moreover, sanctions lead to women experiencing a higher level of economic burden, and also to women's rights decreasing. They have a negative impact on women's access to economic and social status, and under the country's traditional patriarchal norms and attitudes, women face violations every day. The social and economic burden on women increased during the pandemic, especially those with limited digital skills. However, there is simultaneously an absence of reliable data on digital take-up in Sudan. This lack of statistics impedes not only the visibility and understanding of the specific challenges faced by women but also the ability to address the "gender digital divide".[14]

Digital advocacy challenges in Sudan

The ICT Syndicate was formed by ICT professionals during the revolution in May 2019. The Syndicate aims to save the revolution's gains as well as enrich it, by forming a non-governmental body that urges civilian authority and advises government institutions. We planned to conduct the first assembly meeting in January 2020, but because of the pandemic lockdown, this plan was delayed until October 2020. Due to the lack of internet accessibility and availability of technology tools – as a consequence of, for example, limitations on licences for communications platforms in Sudan – conducting meetings online using Zoom was impossible with members from other states in Sudan. This meant we could not organise and prepare for awareness-raising workshops, and had to find alternative ways to secure a Zoom licence by using the Zoom accounts of international members to work online.

In an interview conducted by the Syndicate with Ammar Hamadien, the director general of National Information Center during the transitional government, Hamadien stated:

> The US sanctions have had a negative impact on the growth of digital services and ecosystems. The inaccessibility of software tools and hardware and the reservation of companies that are based in the US has forced digital enthusiasts to turn to open source software, which in many incidents posed great cybersecurity vulnerabilities to companies and end users. Therefore, digital development in Sudan is at the early stages, given the current demographics of the country and the large percentage of the population that is still offline.

Internet shutdowns are very common in Sudan. Throughout the revolution, the military blocked social media platforms, and blocked the internet for almost two months for political reasons in 2019. The internet was also blocked during the Certificate of Secondary exams in September 2020 during the pandemic to stop the sharing of exam papers online.[15]

The restructuring of ICT institutions has also been included in the Syndicate's advocacy agenda. The military has dominated the telecom sector, including the revenue generated from telecom services. In August 2019, as part of institutional reform, the Ministry of Information and Communications Technology was disbanded, giving the president of

11 Bezuidenhout, L., Karrar, O., Lezaun, J., & Nobes, A. (2019). Economic sanctions and academia: Overlooked impact and long-term consequences. *PLOS ONE, 14*. https://doi.org/10.1371/journal.pone.0222669

12 UNCTAD. (2019). *Digital Economy Report 2019. Value Creation and Capture: Implications for Developing Countries*. https://unctad.org/system/files/official-document/der2019_en.pdf

13 Ibid.

14 Drury, A. C., & Peksen, D. (2014). Women and economic statecraft: The negative impact international economic sanctions visit on women. *European Journal of International Relations, 20*(2), 463-490. https://doi.org/10.1177/1354066112448200

15 SMEX. (2020, 12 November). Military-Controlled Telecom Sector and Internet Shutdowns in Sudan. https://smex.org/military-controlled-telecom-sector-and-internet-shutdowns-in-sudan

the Sovereignty Council, Abd El-Fatah Elburhan, the authority to govern the Telecommunication and Post Regulatory Authority. In December 2019, the Syndicate submitted memos to the council to advise on the necessity of reforming the Ministry of Telecommunication and reforming communications laws so that they would be brought in line with digital rights.

Recently, the Syndicate interviewed the head of the Sudanese Consumers Protection Association, Yassir Mirghani. The association had volunteered alongside the lawyers' union to file a case in court against telecom companies that blocked the internet during the military coup. Mirghani said that the association was working to save citizen rights and that it would advocate for digital rights alongside citizen rights. Currently, the Syndicate is working to strengthen partnerships with different associations and entities to ensure the digital rights of Sudanese citizens are in place.

To conclude, the imposition of US sanctions – especially on technology – had a significant impact on the underdevelopment of Sudan as a nation, as well as on civil society and public institutions. Specifically, the sanctioned items on the CCL led to an increase in the digital divide. This includes the lack of access to technology, a slow uptake and penetration of internet technologies, the suppression of digital rights and spaces to express democratic rights, and the increased exposure of citizens and companies to cyber attacks given their reliance on open source software.

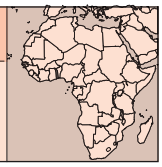
Action steps

The following actions are recommended for Sudan:

- The UN Security Council, the EU and the US should investigate countries and US companies selling surveillance systems to the NISS and the military junta, and instead of broad-based restrictions, target government leaders, the military and militias in Sudan with personalised sanctions.
- The US should remove BIS authorisation of items under the CCL, to facilitate the following:
  - Allow US companies to support small-to-medium-sized companies, startups, and the private sector in general so that they can grow their digital capacity.
  - Encourage the use of e-commerce platforms in Sudan.
  - Assure that Sudanese citizens have the freedom to access information and academic and technology resources and platforms without restrictions.
  - Encourage Sudanese academic research participation globally, and expand the operation of the UNESCO office in Sudan.

TOGO

THE HUMAN RIGHTS IMPACT OF DIGITAL SURVEILLANCE DURING COVID-19



AW Free Foundation
Emmanuel Agbenonwossi
http://awfreefoundation.com

Introduction

As the coronavirus pandemic takes its terrible toll on both human life and livelihoods, governments, public health authorities, companies and individuals have responded with extraordinary measures. To protect the health of people, governments and institutions put in place restrictions on movement and mechanisms for tracking and reporting on infections. In Togo, the pandemic has led policy makers to expand public health surveillance by taking advantage of new technologies to control the spread of the virus.

This report discusses the rights challenges that have emerged in the implementation of the TOGO SAFE contact tracing app[1] and a travellers' health registry,[2] and the use of artificial intelligence (AI) to determine the vulnerable households likely to receive state assistance.[3]

Background

Togo is a Sub-Saharan West African country sandwiched between Ghana to the west, Burkina Faso to the north, Benin to the east and the Atlantic Ocean to the south. It had an estimated population of 8.5 million inhabitants as of 2021,[4] with a demographic growth rate of about 2.5%. Over 50% of the population lives below the poverty line (under USD 1.25 per day).[5] Poverty is strongly linked to under-nutrition – food insecurity at household level is prevalent across the country and is particularly high in the northern regions.

Togo's constitution, adopted in 1992 and last revised in 2019, calls for a bicameral legislature, but the Senate has not been established yet. Members of the 91-seat National Assembly, which exercises all legislative powers, were elected for a five-year term in December 2018, with the Union pour la République (UNIR) party retaining in clear majority.[6]

UNIR leader Faure Essozimna Gnassingbé, the incumbent 54-year-old president who was re-elected in presidential elections two years later, has been in office since 2005 after the death of his father Eyadema Gnassingbe, who led the country for 38 years after seizing power in a coup in 1967.

The Togolese constitution lays the foundation for data protection and explicitly guarantees the protection of personal information, anonymity, and confidentiality of communications. According to article 29 of the constitution, "the State guarantees the secrecy of correspondence and telecommunications. Every citizen has the right to the secrecy of his correspondence and of his communications and telecommunications."[7]

This article was supported by the Data Protection Act of 29 October 2019,[8] which provides a comprehensive framework for the protection of the individual's privacy and of personal data. This was preceded by a right to information law[9] passed by the National Assembly in 2016, which safeguards freedom of access to public information and documentation.

Although these laws are a major step forward, the absence of the Data Protection Commission,[10] which is the national independent authority responsible for upholding the fundamental right of

1 https://www.youtube.com/watch?v=1RsGOr6R1Po&ab_channel=MPENITTogo

2 https://voyage.gouv.tg

3 Moustapha, M. (2020, 25 June). Togo : Novissi, un programme de revenu universel de solidarité et un modèle pour l'Afrique. *The Conversation*. https://theconversation.com/togo-novissi-un-programme-de-revenu-universel-de-solidarite-et-un-modele-pour-lafrique-140834

4 https://www.worldbank.org/en/country/togo/overview#1

5 World Food Programme. (2018). *Togo Transitional ICSP (January 2018-June 2019)*. https://www.wfp.org/operations/tg01-togo-transitional-icsp-january-2018-june-2019#:~:text=Togo%20is%20classified%20as%20a,1%2C%2025%20per%20day

6 AFP. (2018, 24 December). Togo president's party wins majority in parliament: provisional results. *France 24*. https://www.france24.com/en/20181224-togo-presidents-party-wins-majority-parliament-provisional-results

7 https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/38025/110367/F-1481961433/TGO-38025%20(VERSION%20CONSOLIDEE).pdf

8 https://www.dataguidance.com/notes/togo-data-protection-overview

9 Africa Freedom of Information Centre. (2016, 31 March). Togo votes for freedom of access to information law. https://africafoicentre.org/blog/2016/03/31/togo-votes-for-freedom-of-access-to-information-law

10 Daigle, B. (2021). Data Protection Laws in Africa: A Pan-African Survey and Noted Trends. *Journal of International Commerce and Economics, February*. https://www.usitc.gov/publications/332/journals/jice_africa_data_protection_laws.pdf

individuals to have their personal data protected, leads to violations.

Unlawful data-driven measures to mitigate the impact of COVID-19

In times of crisis, such as the current COVID-19 pandemic and its economic and social repercussions, public governance matters more than ever. On 1 August 2020, in its statement on the reopening of the Gnassingbe Eyadema International Airport, the Togolese government urged citizens to download the TOGO SAFE app[11] to supplement the state's efforts in battling the pandemic. Its download was once pitched as a voluntary step taken by citizens, but a directive now makes this compulsory for travellers and those who wish to do a PCR test. The "success" of contact tracing apps in developed countries such as France has been cited as a reason for the introduction of this app in Togo.

The move has raised questions on the efficacy of the contact tracing app, and of the balancing of the right to privacy and the right to health.

Most epidemiologists and health experts in the country have emphasised the importance of contact tracing in containing the speed at which the virus spreads. However, civil society organisations across the globe and digital rights experts in Togo have argued that effective contact tracing "needs to engender trust and respect human rights."[12] Frameworks for contact tracing must be evidence-based and, more importantly, align with constitutional thresholds for the right to informational privacy.

In this context, many experts highlighted the violations of the app, and the state's obligation entrusted by the constitution to preserve the anonymity of the individual in order to legitimately assert a valid state interest in the preservation of public health. First, it must have a legitimate basis. Second, it must pursue a legitimate aim. Third, it should have a rational nexus to the aim. Fourth, there must not be any less restrictive ways to achieve this aim. Fifth, it must outweigh the harm caused to the rights holder.

The TOGO SAFE app failed the very first prong of the proportionality standard because it does not have a regulatory framework to govern its functioning and to ensure procedural safeguards. While the country has a data protection law, the absence of an agency to uphold the law means that regulations, even if they were drafted, cannot be properly implemented. In the absence of these regulations, sensitive personal data collected by this app about the health and movement of a substantial number of the population could be misused for profiling and mass surveillance even after the COVID-19 outbreak is over.

In addition to lacking legislative basis, the app deviates from international best practices for contact tracing apps and fails to comply with data protection standards on the following counts:

- Lack of consent: The use of the app cannot be considered voluntary after the government's directive. Therefore, there is no scope for people in certain circumstances – i.e. travellers and those who want a PCR test – to refuse consent or opt out.
- Lack of transparency: Unless there is publicly available information about what processes and techniques are followed for aggregation and anonymisation of the personal data collected by the app, it is impossible to ignore the justified worry of re-identification of the personal data collected.
- Lack of algorithmic accountability: The terms of service of the app exempt the government from any liability arising out of the misidentification of an individual's COVID-19 status. This is highly problematic, as an individual can potentially lose their income and freedom of movement with little recourse in the event of a false positive.
- Unauthorised data sharing: There is no prohibition on the sharing of the personal data with third parties and the privacy policy of the app fails to mention which government departments will have access to the data. Because of this, there exists a risk of sharing such data with law enforcement agencies for punitive purposes.

Law versus practice

Governance arrangements have played a critical role in Togo's immediate responses to the pandemic, and will continue to be crucial both to the recovery and to building a "new normal" once the crisis has passed.

Through the Data Protection Act, Togo intends to regulate the collection, processing, transmission, storage, use and protection of personal data.

The period of sanitary restrictions to contain the virus was a period during which this law revealed its limits in practice. For example, the collection of data to control the flow of travellers revealed shortcomings in the context of the management of the pandemic.

In this respect, the collection of data by the public authorities is problematic when considering both

11 https://aeroportdelome.com/togo-safe-pour-tous-les-voyageurs-a-destination-du-togo

12 Adiakpo, S. (2021). *Londa: Droits Numériques et Inclusion au Togo 2020*. Paradigm Initiative. https://paradigmhq.org/wp-content/uploads/2021/06/Droits-Num%C2%AEriques-et-Inclusion-au-Togo.pdf

the principles of necessity and proportionality, while data is also not collected with the informed consent of data subjects.

Necessity

It is appropriate here to ask questions about the need for certain personal data to be collected. This is particularly the case with respect to the health information portal for travellers using Gnassingbé Eyadema International Airport. The portal records data that will be used in the COVID-19 screening test of travellers. This portal collects the same data for all travellers, whether they are leaving the country or entering the country.

In this regard, beyond the information requested on the traveller's civil status and recent destinations, the name of the traveller's father and mother is also compulsory, which is unnecessary information, given that the virus has nothing to do with genetic predispositions to ill health. Even if the virus was hereditary, the request of parents' personal data from travellers is unnecessary.

Furthermore, in the context of the collection of vaccination data, information on the traveller's profession is also requested, presents risks of non-transparency (what will this information be used for?) and discrimination (unemployed or people from certain professions might be discriminated against). Such information is subject to abuse.

Proportionality

No information is available on the length of time that personal data collected regarding vaccination will be stored and whether it will need to be updated or stored indefinitely for archiving purposes in the public interest, such as for scientific, historical research or statistical purposes. Article 53 of the Data Protection Act offers guarantees against unlimited data retention.

The data collected is also not accessible to data subjects as prescribed by article 39 of the Data Protection Act. In this regard, there is no possibility of data subjects accessing this data or modifying it if necessary as guaranteed by article 46 of the Act.

Of concern, our informal inquiries revealed that data collected by the government was in fact used to feed other government databases. We understand that the data collected was shared for three types of government services, without further information provided.

Data misappropriation

In Togo, all the government agencies that have been collecting people's data have not set a clearly defined agreement for people's consent. According to the Data Protection Act, processing personal data is generally prohibited, unless it is expressly allowed by law, or the data subject has consented to the processing.

The basic requirements for the effectiveness of a valid legal consent are defined in the Data Protection Act. According to the law, consent must be freely given, specific, informed and unambiguous. However, all government platforms in the country, including the TOGO SAFE app, have no terms and conditions agreements for the data owner to read and approve.

According to the law, for consent to be informed and specific, the data subject must at least be notified about the controller's identity, what kind of data will be processed, how it will be used and the purpose of the processing operations, as a safeguard against "function creep".

Where relevant, the controller has to inform the data subject about the use of the data for automated decision making, and about the possible risks of data transfers in the absence of appropriate safeguards. The consent of the data subject must be bound to one or several specified purposes which must then be sufficiently explained. If the consent should legitimise the processing of special categories of personal data, the information provided to the data subject must expressly refer to this.

The consent must be unambiguous, which means it requires either a statement or a clear affirmative act. Consent cannot be implied and must always be given through an opt-in, a declaration or an active motion, so that there is no misunderstanding that the data subject has consented to the particular processing of his or her data.

The law also requires the data subject must be informed about his or her right to withdraw consent at any time. The withdrawal must be as easy as giving consent.

These guarantees could have been offered to the people in Togo in accordance with the law, instead of directing them to a PDF version of the Data Protection Act, which is a large amount of indiscriminate information that is difficult for the uninformed public to read. Directing people to the legislation governing data clearly does not guarantee that the provisions of the law are observed in the collection and use of their personal data.

There is also a certain lack of transparency in the management of information related to vaccination. To date, there is no open data on the number of vaccines administered in the country.

Failure to regulate the use of artificial intelligence

The legal vacuum on the issue of artificial intelligence (AI) has opened the door to huge disparities in the development of AI-based solutions during the

pandemic in Togo. When coronavirus reached Togo in March 2020, the government, like those in many countries, responded with stay-at-home orders to suppress contagion and announced an economic assistance programme to replace lost income. But the way the country targeted and delivered that aid was in some ways more tech-centric than others.

The government launched an aid system called Novissi,[13] meaning "solidarity" in the local Ewe language, developed during 10 intense days of work starting in late March 2020. The payments that the government sent to the population were targeted, and used machine-learning algorithms to identify signs of poverty in satellite photos, and using mobile phone data.

The turn to satellite and mobile phone data was driven, in part, by a shortage of reliable data on citizens and their needs. The government asked researchers at the University of California at Berkeley who specialise in AI to develop an alternative. According to the information obtained, the use of experts from this university made it possible to develop an algorithm that crosses satellite and telephone data to better target citizens in need.

According to our information, the algorithm was used to determine the vulnerable households that should receive social assistance.[14] The first filter analysed top-down images of the most precarious habitats, the state of roads, the quality of roofs and the frequency of planting.

The second filter, which is most problematic, is the use of the mobile phone data of citizens. The mobile phone data of citizens was collected from the telcos without the consent of the user. Important data such as frequency and duration of calls, amount of airtime, etc. was used by the algorithm. This led to several biases and serious rights violations, because the use of mobile phone data *de facto* excludes the rural population that does not use mobile phones because they lack the means to do so. The data also does not indicate the real precariousness of the targeted populations given that mobile money services – which was one of the data points collected – are not present in all rural areas of the country.

The issue of the use of AI is unclear in Togo[15] and the absence of a legal framework is likely to open the door to even more serious abuses. Today, innovative solutions are being developed in Togo but are not regulated. A legal framework would help mitigate the rights violations.

Conclusion

The spread of the COVID-19 novel coronavirus and its rapid escalation into a pandemic in the early months of 2020 marked the first truly major, widespread global health emergency of the information age. In Togo there is much interest in privacy given that the country engaged in collecting massive amounts of personal data of citizens in response to the pandemic. The positive steps taken by the government to mitigate COVID-19 demonstrate the importance of regulating data collection and the impact on the privacy rights of citizens. There may be a justification for gathering, storing, processing and sharing personal data – however, COVID-19 must not be a reason for collecting personal data in a way that the data rights of people are infringed.

The lack of clarity in the purpose for collecting a large amount of data in the first place, and what happens to the collected data once the pandemic is over, has become an issue for public scrutiny. Therefore, to allay any concerns and fears in the minds of the public, the onus is on the government to reassure people that their personal information will remain confidential and secure from unauthorised access.

Also, to be prepared for any privacy concerns likely to arise in the long term and to be response-ready to face future health crises similar to that of COVID-19, it is crucially important for the government to develop a framework for emerging technologies that will be readily available to protect individual privacy during a pandemic. It is also critical that it creates the necessary Data Protection Commission, and ensures that it has the capacity to do its job. Any national-level privacy mechanism should provide safeguards and guarantee the protection of privacy of its citizens.

Action steps

The following action steps should be considered for Togo, drawing on the issues discussed in this report.

In the short term:

- The government should immediately create the Data Protection Commission, and provide it with the necessary capacity to oversee the proper implementation of the Data Protection Act.
- A dedicated regulatory framework justifying and guiding the execution of data-driven measures is also necessary. Apps and other

13 AFD. (2020, 4 September). Togo : Novissi, la solidarité au temps du Covid-19. *AFD*. https://www.afd.fr/fr/actualites/togo-novissi-solidarite-covid-19

14 Hervieu, S. (30 September). Intelligence artificielle : au Togo, un algorithme contre la pauvreté. *L'Express*. https://www.lexpress.fr/actualite/monde/afrique/intelligence-artificielle-au-togo-un-algorithme-contre-la-pauvrete_2158963.html

15 Togo First. (2021, 29 August). Quel est l'état de préparation du Togo à l'intelligence artificielle ? https://www.togofirst.com/fr/tic/2908-8388-quel-est-l-etat-de-preparation-du-togo-a-l-intelligence-artificielle

data-driven measures should not be deployed in a vacuum of regulatory guidelines. General principles can be helpful to avoid and identify abuses by authorities.

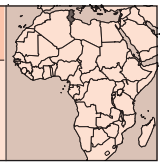
- The government should ensure that whenever the health emergency has ended, systems that have been developed should be terminated and personal data should be deleted. Specific measures developed to manage the pandemic should be time- and purpose-bound. Safeguards should be put in place to prevent mission creep.
- Civil society organisations should work to prevent illegitimate COVID-19-related digital surveillance.

In the medium-to-longer term:

- The government should maintain a human rights-based approach throughout the application of technologies that collect or work with data. Responses have to be non-arbitrary, necessary and proportionate, as well as non-discriminatory.
- Solutions deployed by the government should not be used as a way to illegitimately target specific groups and individuals or violate their fundamental rights.
- The government should make it a fundamental requirement that future apps or platforms that collect personal data have an opt-in clause. In addition, explicit and individual consent is required.
- The government and stakeholders should make sure that data shared through any app or systems should be collected and used solely for legitimate public health goals that must be clearly and specifically described.
- The government should ensure that apps and other systems should collect, process and store as little data as absolutely necessary to fulfil the public health aim. This also means that the purpose has to be clear from the outset.
- The government should also ensure that the development of future data-driven measures should be carried out with accountability kept in mind. This means that governments should be transparent about the policies in place and about what type of data is being collected, by whom, by which means, and how it is being used. Transparency is necessary for people to understand how the data-driven mechanisms operate, which data is stored, and why. This enables individuals to make an informed decision on whether they want to use the app or participate in a data-dependent programme.
- The government should ensure that data-driven initiatives respect the principles of privacy and data protection by design and by default. Any initiative must support data anonymisation, and use state-of-the-art cryptographic techniques, among other measures, to secure data and prevent harm in case of leaks or breaches.

TUNISIA

DIGITAL INNOVATION RESCUES TUNISIA FROM THE COVID-19 OUTBREAK – BUT INTRODUCES NEW RIGHTS CONCERNS



iGmena
Hamza Ben Mehrez
www.igmena.org

Introduction

On 10 March 2022, Tunisia had registered 1,017,907 COVID-19 cases, 27,874 deaths and 961,303 people who had recovered.[1] Although the country has successfully contained the first and second waves of the virus, many citizens, as part of the informal workforce of the country which accounts for 50% of the GDP, have found themselves in situations of economic and social difficulties.[2]

Technology has been central in the response to the virus in several government, private sector and civil society initiatives. This has included, as in many other countries, online registration for vaccination. By 8 September 2021, 5,987,855 people had been registered on the Evax.tn platform,[3] which allowed them to book COVID-19 vaccination appointments. While many of these initiatives have brought health care closer to citizens, they also raise potentially unexplored rights issues that need further elaboration.

Technology-based initiatives introduced during COVID-19

COVID-19 contact tracing app

Tunisia launched a contact tracing mobile phone app that identifies and alerts users if they have been in close contact with someone who later reports having contracted COVID-19. The E7mi ("protect me" in English) application, which is available on Android, was developed by a Tunisian startup specialised in digital marketing tools for foreign companies. If a user tests positive for COVID-19, Tunisia's Observatory of Emerging Diseases contacts other users whose mobile phones have been detected close to the infected user's device to notify them of the risk.

Digitising prescriptions

Through the Tunisia Community College Scholarship Programme and the Tunisia Undergraduate Scholarship Programme, nearly 500 Tunisian youth gained valuable experience in the United States and helped digitise prescriptions in coordination with a local COVID-19 task force. Through the system, patient information is sent directly to a doctor's computer so the doctor can prescribe medication and send the prescription directly to pharmacy staff. Pharmacists can then prepare the medication prior to the patients' arrival so that patients do not have to stand in long lines and risk exposure to the virus while waiting for their medication.[4]

Face shields/3D printing technology

The German automotive parts manufacturer Kromberg & Schuber developed face shields using 3D printing technology. The company was able to produce around 30 masks, all of which were donated to the regional hospital in Beja to fight COVID-19.[5]

Innovation for assessing x-rays

There were three separate projects that allowed for the fast examination of chest x-rays to determine if a patient had COVID-19. iCompass, a deep learning startup, developed a platform using artificial intelligence (AI) for an instant diagnosis of the coronavirus from chest x-rays, allowing rapid screening for potential COVID-19 patients. Meanwhile, Tunisian engineers in collaboration with local civil society organisations created a web-based platform that scans lung x-rays and evaluates whether patients are likely to be suffering from COVID-19. The technology provides a 90% reliable indication of the probability of infection. Similarly, teachers and students at the Tunisian Engineering and Technology Institute developed a web-based platform that examines Ct/XR images using AI with the support of the German development agency GIZ, the Italian Society of Medical Radiology and tech

1 https://www.worldometers.info/coronavirus/country/tunisia

2 Gallien, M. (2018). *Understanding Informal Economies in North Africa: From Law and Order to Social Justice*. Friedrich-Ebert-Stiftung. https://library.fes.de/pdf-files/iez/14573.pdf

3 https://www.evax.tn/index.html

4 Belloumi, W., & Cook, C. (2020, 17 June). Supporting COVID-19 relief efforts in Tunisia. *IREX*. https://www.irex.org/success-story/supporting-covid-19-relief-efforts-tunisia

5 Oxford Business Group. (2020, 9 April). Innovation at the heart of the Covid-19 crisis in Tunisia. https://oxfordbusinessgroup.com/news/innovation-heart-covid-19-crisis-tunisia

giant IBM.[6] This has been in use since mid-March 2021.Thousands of lung x-rays from both healthy people and COVID-19 patients have been fed into these platforms, allowing AI to learn to recognise the marks of the virus on the lungs.[7]

"Jasmin", the intelligent robot

Since 10 July 2020, the medical staff of Sahloul University Hospital in the governorate of Sousse have been using "Jasmin", an intelligent robot made in Tunisia by Enova Robotics and iCompass, the first in Africa. Jasmin was developed as part of the Safe Tunisia Challenge, a competition launched on 17 March 2020 by the Novation City technology park in Sousse in collaboration with the Ministry of Industry and GIZ. The robot reduces and streamlines the workload in the hospital by minimising the interactions of medical staff with patients affected with COVID-19. It uses a triage system to assess patients arriving at the hospital and directing those suspected of having contracted the virus to a COVID-19 unit. Jasmin is equipped with a thermographic camera and can measure the temperatures and oxygen levels of patients. This means that doctors do not have to come into direct contact with patients who may have contracted the virus before they enter care. It also assists doctors in monitoring the state of health of patients after diagnosis.[8] Its interaction with patients is user-friendly and is in the Tunisian dialect.[9]

PGuard ground vehicle

A leading startup in robotics and AI called Enova Robotics created the PGuard ground vehicle robot, which was acquired by the Ministry of Interior to assist with the enforcement of the country's lockdown rules. The device includes infrared and thermal cameras, an audio system, GPS, and a sound and light alarm system that allows officers to request identification papers and issue verbal warnings to those breaching COVID-19 lockdown rules.[10] The number of PGuard robots deployed by the ministry has not been reported. Some citizens welcomed the initiative, while others said the robot "moved too slowly" to be effective. However, several videos have since appeared on social media showing people being stopped by a PGuard. The PGuard robot can give a preliminary visual diagnosis and use its sensors to measure certain things – and one will soon be working at a hospital in Tunis. In terms of rights concerns with robotic policing, Tunisian citizens were satisfied with the invention that would help minimise physical contact between citizens and the police.[11]

New rights challenges and ways of working

The use of technological innovation has been vital in Tunisia's fight against COVID-19 in the areas of infection prevention and control, as well as the maintenance of essential health services at the community level with strategies adapted to their local context. There are at least three implications of these developments, the first concerning the intensification of digital rights issues with respect to privacy, the second concerning the use of robotic policing for the first time in Tunisia, and the third related to the potential risks associated with automated health care.

Rights implications on privacy

The use of contact tracing apps, which are often implemented in partnership with the private sector and with few privacy safeguards, have raised privacy concerns in many countries across the world. In Tunisia, the contact tracing mobile phone app E7mi was developed by the Ministry of Health. It tracks the location of citizens registered on the platform and includes other personal data such as phone numbers and national identity card numbers. It does not have clauses that state when it will no longer be broadcasting data from phones and app stores, nor an indication of a limit for the use of data once the app is no longer necessary. Although Tunisia introduced a data protection bill in 2018 to comply with the Council of Europe's Convention for the Protection of Individuals against Automatic Processing of Personal Data, the bill is no longer a priority for the Tunisian Parliament.[12] Any contact tracing app should incorporate privacy protection measures into the design of services to enhance data security, collection and storage. In Tunisia, companies involved in the design of these platforms should obtain consent

6 Fusco, R., Grassi, R., Granata, V., Setola, S. V., Grassi, F., Cozzi, D., Pecori, B., Izzo, F., & Petrillo, A. (2021). Artificial Intelligence and COVID-19 Using Chest CT Scan and Chest X-ray Images: Machine Learning and Deep Learning Approaches for Diagnosis and Treatment. *Journal of Personalized Medicine, 11*(10). https://doi.org/10.3390/jpm11100993

7 AFP. Covid-19: Tunisia researchers use AI, X-rays to create online virus scan tool. *The Star.* https://www.thestar.com.my/tech/tech-news/2020/04/18/covid-19-tunisia-researchers-use-ai-x-rays-to-create-online-virus-scan-tool

8 Web Manager Center. (2020, 31 March). « SAFE TUNISIA » le nouveau challenge 100% en ligne de Novation City pour endiguer le COVID-19. http://www.webmanagercenter.com/2020/03/31/447087/safe%E2%80%AFtunisia-%E2%80%AF%E2%80%AFle-nouveau-challenge-100-en-ligne-de-novation-city-pour-endiguer-le-covid-19

9 La Press avec TAP. (2020, 10 July). CHU Sahloul: Le Robot tunisien «Jasmin», allié de taille dans la lutte contre le Covid-19. La Presse. http://lapresse.tn/67762/chu-sahloul-le-robot-tunisien-jasmin-allie-de-taille-dans-la-lutte-contre-le-covid-19

10 Jawad, R. (2020, 3 April). Coronavirus: Tunisia deploys police robot on lockdown patrol. *BBC*. https://www.bbc.com/news/world-africa-52148639

11 Ibid.

12 Samaro, D., &. Fatafta, M. (2020, 18 June). COVID-19 contact-tracing apps in MENA: a privacy nightmare. *Access Now.* https://www.accessnow.org/covid-19-contact-tracing-apps-in-mena-a-privacy-nightmare

before using consumer data (such as social security numbers, geolocation, or financial and health information) by promoting easy-to-understand privacy notices for citizens to access their data in proportion with the sensitivity of the data and the nature of its use.[13]

Rights implication of robotic policing

Several issues need to be considered with respect to robotic policing. Worldwide, robotic policing is being taken more seriously, and in 2016 in the United States a robot charged with explosives was used to kill a sniper who had fired into a crowd, killing five police officers.[14] The primary issue is that laws in Tunisia governing public order policing do not address the issue of robotic policing.

The introduction of the PGuard robot is not immune to ethical concerns relating to the use of robots for policing. For instance, robots might have human-like behaviour, but not human consciousness, which is important to ethical policing and decision making during crises. Robots also depend on the trustworthiness of those who design the algorithm for their operation – in this case the state and technical partners. There are also concerns about the impact on future jobs, with the potential for unemployment in the policing sector to increase. Tunisian police using a service robot should also always be able to regulate a robot's autonomy, especially in cases when the consequences of the robot's actions cannot be totally controlled.

Robotic policing systems need be regulated, and issues such as the legal responsibilities and liabilities of parties addressed. Regulations are vital to deal with the potentially serious ethical and operational challenges raised by the removal of human control. Robotic policing requires the cooperation of human subjects to be effective – but this cooperation is unachievable without proper public consultation. Full transparency and meaningful limitations are crucial when it comes to these and other categories of surveillance tools, including independent oversight from specialised civil society organisations and pressure groups.[15]

Rights implications of automated health care

In Tunisia, which has an advanced medical system and infrastructure, it is easy to imagine a future where machines will replace doctors with devices that can diagnose and recommend treatment within hours or maybe minutes. The most obvious risk is that AI systems will sometimes be wrong, and that patient injury or other health-care problems may result. If an AI system recommends the wrong drug for a patient, fails to notice a tumour on a radiological scan, or allocates a hospital bed to one patient over another because it predicted wrongly which patient would benefit more, this would result in avoidable patient harm.[16]

Other risks include the difficulty when fragmented and disorganised health data is spread across various data systems in health care. Patients can often change insurance and health care providers frequently, making data acquisition and algorithmic analysis of the data a challenge. Regulations also need to be created to attend to the strict confidentiality and privacy laws required when dealing with medical records, and patients need to properly be informed on the use of their medical data, and provide proper consent for its use.[17]

Action steps

In light of these challenges, the following action steps are recommended for civil society in Tunisia:

- Civil society organisations need to understand the dangers of infringing privacy through algorithmic bias and how AI tools might affect the people and communities they serve. Civil society can play a vital role in highlighting these challenges and dangers among communities where algorithms are used.
- Civil society organisations should work with policy makers in formulating new laws and regulations designed to govern algorithms that make their use fair, accountable and transparent.
- Civil society should be aware of the potential of robotic policing to create new ethical challenges when implemented in communities. Civil society can tackle this challenge by both leading the debate on how the use of AI in robotic policing can minimise the potential risks associated with its use, and be at the foreground of pushing for proper regulations in this regard.
- Civil society must speak out about the potential dangers of automated health care. This particularly relates to the proper management of medical data, and regulations that govern informed consent for the use of this data.

13 Brennan, M. (2016, 11 August). Mobile App Privacy Considerations. *LexisNexis*. https://www.lexisnexis.com/authorcenter/the-journal/b/pa/posts/mobile-app-privacy-considerations

14 Joh, E. (2016, 16 November). Police Robots Need to Be Regulated to Avoid Potential Risks. *The New York Times*. https://www.nytimes.com/roomfordebate/2016/07/14/what-ethics-should-guide-the-use-of-robots-in-policing/police-robots-need-to-be-regulated-to-avoid-potential-risks

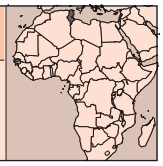
15 Wareham, M. (2021, 24 March). Don't Arm Robots in Policing: Proposed New York City Law a Model for Regulation. *Human Rights Watch*. https://www.hrw.org/news/2021/03/24/dont-arm-robots-policing

16 Nicholson Price, W. (2019, 14 November). Risks and remedies for artificial intelligence in health care. *Brookings*. https://www.brookings.edu/research/risks-and-remedies-for-artificial-intelligence-in-health-care.

17 Patel, U. (2020, 22 October). Artificial Intelligence in Healthcare: Top Benefits, Risks and Challenges. *TriState Technology*. https://www.tristatetechnology.com/blog/artificial-intelligence-in-healthcare-top-benefits-risks-and-challenges

TUNISIA

CREATIVE EXPRESSION IN TUNISIA: SURVIVING A PANDEMIC



Technoloxia
Yosr Jouini
www.technoloxiagroup.com

Introduction

In 2020 alone, over 700 cultural activities in Tunisia were either suspended or cancelled due to the COVID-19 pandemic. Going digital offered alternatives for both artists and citizens to revitalise the cultural scene and to re-examine the barriers for creative freedom in the country. However, moving artistic performances online has also raised questions on whether the internet is a safe place for cultural expression, what social and legal barriers may hinder freedom of expression online, and the challenges of poor connectivity and low digital literacy outside of the country's main economic centres.

The context for creative expression

In 2011, an uprising in Tunisia toppled the 23-year rule of autocratic president Zine el Abidine Ben Ali. Since then, citizens have for the most part enjoyed unprecedented political liberties and creative freedoms. However, social taboos, oppressive laws and the absence of a supporting cultural policy have suppressed the culture and arts scene, which continues to be overlooked as a field worthwhile for investment, and is a struggling field.

Despite the newfound liberties following the uprising, endemic corruption, socioeconomic challenges, security threats as well as political instability remain major obstacles for the democratic transition of the country. In an unprecedented move, on 25 July 2021, just over a year into the pandemic, Tunisian President-elect Kais Said announced the dismissal of the prime minister, a freeze of the elected parliament, and his rule by decree. The constitution adopted in 2014 has also been suspended, with the exception of two chapters related to rights and freedoms, including the right to freedom of expression and the freedom of creative expression.

The impact of COVID-19 on the Tunisian cultural scene

In a petition published on social media in July 2021, the Union of Dramatic Arts Trades expressed its indignation and deep concern at the deteriorating situation for artists and the shrinking of cultural spaces, which was then almost non-existent compared to almost two years previously.[1] While artists like everyone else needed to deal with the health crisis, the government's attempts to curb the spread of the virus tended to rush the restrictions over cultural activities ahead of other sectors. By 13 March 2020, it had cancelled all cultural and sporting events and shut down movie theatres and all other cultural venues. These measures were re-imposed every time the country witnessed a surge in the number of recorded COVID-19 cases.

In response to the pandemic's repercussions on the cultural scene, the Ministry of Cultural Affairs launched the Fonds Relance Culture (FRC),[2] a cultural recovery fund. The FRC is a mixed endowment funded by the private and public sectors that centralised financial contributions in order to support young artists and performers. The fund offers several forms of aid and support, such as interest-free loans so that cultural activities can continue, and aid for unanticipated expenses (such as ticket refunds as a result of cancellations, a drop in revenue, etc.) to help relaunch activities relevant to the redevelopment of the economy of the cultural sector.[3]

However, cultural actors interviewed for this report described the state response as insufficient and criticised it for excluding alternative and less mainstream forms of cultural expression.

Going digital: The emergence of new opportunities and old challenges

As the proverb says, "Necessity is the mother of invention" – and the pandemic and restrictive measures to contain it have pushed cultural actors to launch new digital initiatives to revitalise the local cultural scene.

One pioneering initiative is "Festival le chapeau", a digital festival with live musical performances initiated by Klink,[4] a Tunisian digital booking platform for artists. The festival allowed the audience to en-

1 Drissi, A. (2021, 27 July). Pandémie et vie culturelle: Les artistes s'indignent. *La Presse*. https://lapresse.tn/104285/pandemie-et-vie-culturelle-les-artistes-sindignent

2 https://fr.unesco.org/creativity/covid-19/fonds-relance-culture-de-tunisie

3 Ibid.

4 https://klink.tn

gage with the performers and financially support them directly. However, the initiative faced challenges in finding partners and businesses to sponsor the shows.[5]

The consumption of art online and paying for it remains a new concept for the Tunisian audience. The lack of respect for intellectual property and unauthorised use of artistic content remains an important barrier to the sustainability and vitality of the local cultural landscape. Tunisia is a member of the World Intellectual Property Organization and has an arsenal of legal texts protecting intellectual property. The country established the Tunisian Copyright Protection Organization (OTDAV),[6] an agency responsible for overseeing copyright, while the Tunisian Internet Authority is responsible for administering the .tn country code top-level domain name. However, the application of the copyright laws remains limited with regard to the arts and culture field. This is a challenge that artists in the musical and theatrical scene have been facing for years – and it was one that re-emerged during the pandemic as the internet became the only medium of distribution for artistic performances. In a webinar organised by the OTDAV amid a COVID-19 surge, the participants emphasised the urgent need to raise awareness among artists of their moral and financial rights, as well as the need to educate different stakeholders including lawyers, judges and the private sector on the legal particularities of artistic products.[7]

An additional option could also be to use alternative licences such as Creative Commons licences that allow creators to decide which rights they reserve and which rights they waive, so that users and other creators use, share, distribute and build upon the original works. These sorts of alternatives offer wider flexibility for non-traditional artistic products such as graffiti and their distribution in digital form.[8]

Digital accessibility, a pillar or obstacle for moving digital

While moving online presented itself as a new potential for some artists and cultural groups, much has been lost in the transition. In an interview with Amira Guebsi, the executive manager of Collectif Créatif,[9] a Tunisian civil society organisation, the difficulties faced in maintaining the social impact of the arts for underprivileged communities was highlighted. As an organisation with an important presence on the ground and in the local community, COVID-19 paralysed their work and activities, especially when funders revoked their funding. The communities that used to be pillars of their cultural projects found themselves excluded due to the curfews and restrictions imposed on cultural events. While many organisations have offices in the capital or major cities and used to frequently visit artisans and craftspeople in other regions of the country, the restrictions on inter-cities travel not only restricted mobility but also revealed the huge connectivity gap and digital literacy differences between the economic hubs in the country and less financially resourced cities and regions. Accessing and affording the internet remains a challenge, even for those residing in the country's main cities. In other regions, including towns near borders, poor telecommunications infrastructure makes it even more difficult to get online, adding to the difficulties faced by older artisans working in the crafts sector in these regions who have little to no computer skills.

Going digital nevertheless opened new opportunities for cross-regional partnerships. For instance, Collectif Créatif has developed a new online project where art is co-produced by artists of different nationalities.

Cultural expression and creative freedom online: From imprisonment to self-censorship

Tunisia's 2014 constitution and the country's ratification of the central international human rights instruments guarantee the right to artistic freedom. Despite such guarantees, artistic freedom is not fully upheld and protected in Tunisia. Artists are exposed to threats, assaults and prosecution. A number of artists including rappers,[10] graffiti artists[11] and visual artists[12] have been arrested in the past based on vaguely worded legal texts – such as the penal code, which criminalises defamation and the insult of public officials – that have served as repressive tools for political biases. In 2013, rapper Weld el 15 was sentenced to six months suspended imprisonment for public indecency on the basis of the content of a song, "El Boulisya Kleb" (translated as "Cops

5 https://open.spotify.com/episode/62b6OaKmbO8nBdummCU6Vx

6 http:/www.otdav.tn

7 https://www.facebook.com/AuServiceDesAuteurs/videos/158008236242972

8 Rizk, N. (2015). Revolution, Graffiti and Copyright: The Cases of Egypt and Tunisia. *The African Journal of Information and Communication, 16*. https://hdl.handle.net/10520/EJC189556

9 https://collectifcreatif.org

10 Human Rights Watch. (2013, 5 September). Tunisia: Rappers Sentenced to Prison. https://www.hrw.org/news/2013/09/05/tunisia-rappers-sentenced-prison

11 France 24. (2012, 27 November). "فقراء" تونس ينادون "الغرافيتي ليس جريمة. https://www.france24.com/ar/20121127-تونس-غرافيتي-فن-رسم-حيطان-زوالة-فقراء-ثورة-حرية-تعبير-توقيف-محاكمة-مساندة

12 Franceinfo. (2016, 6 December). Tunisie : deux artistes menacés de prison. https://www.francetvinfo.fr/culture/arts-expos/sculpture/tunisie-deux-artistes-menaces-de-prison_3316153.html

are Dogs"), which he released online.[13] The actress in the video clip was also found guilty for the same charges and received a fine.

During the pandemic – so far – no artist has faced charges in relation to their artistic work and its online diffusion. However, societal taboos often lead to artists self-censoring when posting art for larger audiences online. Shahrazed Amous, the founder of Klink and "Festival le chapeau", said in an interview that in the choice of media platforms, their policy against hate speech and harassment was critical for organisers, with the goal to provide a safe space for artists.[14]

Conclusion

Although the cultural and creative sector is one of the fastest-growing economic sectors in the world, in Tunisia, it remains one of the most overlooked sectors for public and private investment. Since the pandemic hit, actors in the cultural scene took the initiative to revitalise the sector. Going digital became essential and central to creation, production, distribution and access to cultural expression. However, this also introduced new challenges for the creative sector such as inequalities in internet access and the digital skills gap. In particular, community-based creative work suffered, given the low level of internet connectivity at the grassroots. Other challenges include the sustainability of cultural activities in the face of unlawful use of artistic material, the lack of financial compensation for art, and the restriction of creative freedom either through repressive laws or societal taboos, which have led in some cases to a greater level of self-censorship by artists who have found a wider audience through the internet.

Action steps

The following steps are necessary to revitalise the cultural sector in Tunisia:

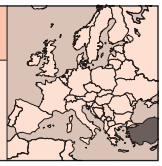
- The state needs to adopt an inclusive cultural policy that supports young artists in the sector. This needs to promote access to creative goods and services and take into account different forms of cultural expression.
- The state needs to reform oppressive legal texts restricting internet freedom and creative expression. Reforms should include clarifying unclear and vague provisions in the penal code used arbitrarily and disproportionately to imprison artists, provisions for defamation, and articles in the telecommunications code, criminal procedure code and other texts that silence criticism of authorities, among others.
- The private sector should help make cultural activities more accessible as part of its social responsibilities. Funding is desperately needed to support the creative sector. Among other things, it could support the capacity building of artists who already work online, or who are new to the internet.
- All stakeholders should contribute to the creation of an enabling environment for cultural creation that allows artists to express themselves freely and not have to resort to self- censorship.

13 Attorney General v. Weld el 15. https://globalfreedomofexpression.columbia.edu/cases/attorney-general-v-weld-el-15

14 https://open.spotify.com/episode/62b6OaKmbO8nBdummCU6Vx

TURKEY

PUSH-BACK AGAINST CIVIL SOCIETY IN THE DIGITAL SPHERE: LAYING THE FOUNDATIONS FOR FUTURE COLLABORATIONS ONLINE



Hun Legal Consultancy
Gürkan Özturan
www.hunlegal.com

Introduction

Over the last two decades, digital platforms and social media have enabled people to express themselves much more freely than before. As a result, globally, social movements have benefited from the new possibilities enabled by these platforms, which have become useful spaces to advocate for social change. Governments also took further steps in this period to keep the new social spaces under control.

Turkey has been one of the foremost countries in terms of introducing restrictive measures to keep public discussion and discourse under control online. During the COVID-19 pandemic – which was first confirmed in the country on 11 March 2020 – there were multiple new attempts to control the digital space, media and civil society in the country.

New restrictions to civil society and the digital sphere

At the height of the COVID-19 pandemic, Turkey passed multiple laws in its parliament, with these laws coming into force soon afterwards. In addition to legal changes through parliamentary processes, the country's president announced its withdrawal from the Council of Europe Convention on preventing and combating violence against women and domestic violence (more commonly known, ironically, as the Istanbul Convention). These developments impacted civil society, contributing to the downward trend in rights and liberties in Turkey, indexed by rights groups over the past decade.

During Spring 2020 – the first months of the pandemic – politicians linked to the governing alliance proposed that one of the most important areas to regulate in the country was the sphere of digital platforms.[1] This was to make sure that public discourse remained under control after journalists critical of the government's pronouncements on the pandemic, and its lack of measures to prevent a wider outbreak of the virus, were accused of causing panic through their social media posts. In the first two months of the pandemic, as the health minister's daily announcements on the country's coronavirus status raised the public's suspicion, the Ministry of Interior announced that over 10,000 social media users had been identified as spreading false information and publishing "provocative" posts,[2] with 1,105 being listed as suspects being investigated and 510 detained for their social media activities.

As part of an emergency coronavirus economic relief measure, Turkey drafted a relief package bill[3] which included eight clauses on coercing tech companies to submit to requests made by the government on removing content, blocking access to content and users, revealing information, and appointing legal representatives to engage the government – and to do all these within the first 72 hours of the request. If this was not done, the service provider would have to pay massive monetary fines or be prepared to have their services blocked.

In the summer of 2020, Turkey also passed an amendment to Law No. 5651 (Law on the Regulation of Broadcasts via Internet), which is popularly known as the "Social Media Law".[4] With this amendment, proposed changes that failed to pass when they were first put forward in April were all accepted. These involved allowing mass surveillance of internet users in Turkey, the narrowing of bandwidth, introducing sanctions against social media companies operating in the country unless they complied with the orders of the government, and the removal of content deemed undesirable by government officials.

In addition to regulating the digital sphere, Turkey also passed Law No. 7262 (Law on the Prevention of Financing and Spread of Weapons of Mass

1 Bellut, D. (2020, 21 April). Turkey's Erdogan clamps down further on media amid coronavirus crisis. *DW*. https://www.dw.com/en/turkeys-erdogan-clamps-down-further-on-media-amid-coronavirus-crisis/a-53192898

2 Hürriyet Daily News. (2020, 22 May). Turkey detains 510 people for 'provocative' COVID-19 posts on social media. *Hürriyet Daily News*. https://www.hurriyetdailynews.com/turkey-detains-510-people-for-provocative-covid-19-posts-on-social-media-154989

3 Sinclair-Webb, E. (2020, 13 April). Turkey Seeks Power to Control Social Media. *Human Rights Watch*. https://www.hrw.org/news/2020/04/13/turkey-seeks-power-control-social-media

4 Santora, M. (2020, 29 July). Turkey Passes Law Extending Sweeping Powers Over Social Media. *The New York Times*. https://www.nytimes.com/2020/07/29/world/europe/turkey-social-media-control.html

Destruction), more popularly known as the "Civil Society Law".[5] This specifically targeted civil society, and would potentially block activities of non-governmental organisations that do not share the same views as the governing party. It exposes organisations to sanctions, such as the dismissal of board members and replacement of the board by government-appointed trustees, the freezing of bank accounts, and the suspension of all activities without having to provide evidence of any illegal activity, and even without a court order, putting the activities of these civil society actors on hold and preventing rights movements from operating freely.

Online resistance and responses to the pandemic

Turkey's government attempted to control the social discourse by increasing pressure on civil society, independent media and society in general. The legal amendments adopted during the pandemic period aimed at hiding information that was valid from people at a crucial time, then subverting the facts by creating alternate explanations on statistics, prosecuting critical publications and finally attempting to block any social support activities that relied on digital advocacy.

In the first days of the pandemic, while there was increasing unease regarding the uncertainty of the coming weeks, for a brief period of time, the government eased its usual restrictions and pressure on the media, as it lifted the restrictions on critical and independent media participating in press conferences held by the officials. It was crucial for the ministry to sustain proper crisis communication in order to clear up public concerns and quieten the panic. For a long time, this had not been the case, as any critical question by an independent journalist was met by harsh reactions by officials or in some cases physical intervention by security guards. However, the pandemic changed these restrictive conditions for a period of time.

This anomaly did not last long. Soon harsher reactions targeting critical speech were put in place. Starting in the first month of the pandemic, the announcements by the Ministry of Health were contested by the raw data published by the Istanbul Metropolitan Municipality, and the Turkish Medical Association (TMA) recorded the contradictory numbers in reports from their local chapters.[6] These reports later became the basis of criticism that appeared on social media, which showed an increased frequency of usage due to extended lockdowns and curfews across the country.

The discussions on social media continued with the help of the TMA and other associations that demanded more transparency. Eventually, Minister of Health Dr. Fahrettin Koca announced in September 2020 that he had deliberately provided misleading daily statistics to the public,[7] shattering the remaining trust in the government's ability to manage the health crisis.

Amidst the crisis of a lack of transparency and deliberate misinformation supplied by the government, the laws that would further limit online information were heavily criticised by civil society, but passed nonetheless. There was strong reaction to amendments to the Social Media Law, which was drafted in secrecy without informing civil society or even the opposition parties in the parliament. According to the new law, service providers or content publishers would no longer only receive access-blocking orders for content deemed problematic, but also content removal orders.

The Media Research Association in Turkey monitored the law's impact on media freedom, revealing that in the first year of the law's implementation, there were almost 1,200 news articles that were removed.[8] When the law was being passed, civil society networks gathered to advocate against passage of the law, and communications networks were established on messaging platforms. Furthermore, various new media channels published extensive commentary on the law[9] to inform the public of the risks this legislation bore.

The government's claims justifying the Social Media Law focused on the spreading of misinformation and misleading the public with the intention to make profit. These claims were also reflected in the Civil Society Law that was passed in December 2020, increasing the government's control over civil society and introducing new barriers to their engagement online. Civil society would no longer be allowed to collect donations for charity as part of online solidarity campaigns.

5 Yackley, A. J. (2020, 27 December). Turkey tightens government control over civil society groups. *Financial Times*. https://www.ft.com/content/0c097861-7c02-45c4-88b5-5d0d6af32fb8

6 Istanbul Medical Association. (2020, 4 May). Healthcare in Istanbul during Coronavirus – VII 27 April-3 May Weekly Report. https://www.istabip.org.tr/5799-korona-gunlerinde-istanbul-da-saglik-vii-27-nisan-3-mayis-haftasi-raporu.html

7 Evrensel. (2020, 30 September). Minister of Health Koca confessed to announcing only the number of heavily sick instead of all positive cases. *Evrensel*. https://www.evrensel.net/haber/415385/saglik-bakani-koca-vaka-sayisinin-degil-hasta-sayisinin-aciklandigini-itiraf-etti

8 Media Research Association. (2021). *Impact of Social Media Law on Media Freedom in Turkey Monitoring Report*. MEDAR. https://medarder.org/wp-content/uploads/2021/12/Impact-of-Social-Media-Law-on-Media-Freedom-in-Turkey-Monitoring-Report-Extended-Research.pdf

9 https://www.youtube.com/watch?v=py3uZ2dEtgc

In response, civil society organisation networks organised a joint campaign on social media against the law and continued their public online discussions criticising the government, in doing so creating the foundation for joint action in the future. Even though the law was passed and came into force, the network established by the civil society organisations led to intersectional support groups being formed, which shaped the digital advocacy efforts in the months to come.

When, in the beginning of 2021, Turkey's government announced its intention to withdraw from the Istanbul Convention, it also announced that it would allow bar associations to be split up, potentially creating partisan bar associations, and pass an animal protection law that would be more harmful for animals than useful. In this context, the intersectional communications network that had been created earlier proved to be useful in multiplying the messages of the women's movement, human rights defenders, animal rights activists and environmentalist groups.

Over time, the concerns of the women's rights movement became mainstreamed through digital spaces, not only among civil society, but also in the commercial field. Big companies, including prominent ones such as Koç Holding and Boyner, openly opposed the government's decision to withdraw from the Istanbul Convention,[10] marking a milestone in terms of women's rights and LGBTIQ movements' success in advocacy and awareness raising.

While the latest Civil Society Law would enable the Ministry of Interior to conduct frequent audits and issue heavy monetary fines and even take steps that could lead to imprisonment of the board members of civil society organisations, the dissolution of a civil society organisation, or the appointment of trustee board members to conduct their activities in accordance with how the ministry sees fit, many civil society organisations ceased to operate or slowed down their activities. While some found ways to cooperate with security officials to obtain the necessary permits to conduct their digital advocacy campaigns, others, including some of the most influential organisations, simply stopped declaring opinions or making statements.

Furthermore, some of the organisations contacted during the drafting of this report emphasised that, alongside the impact of the law, their work with solidarity networks that were created over the course of years had slowed or stopped due to the deep impact of the pandemic restrictions and their failure to digitise their daily operations.

However, this was not the case for everyone. During the pandemic many organisations also initiated online publications and webinars, opening up their previously closed-group activities to larger audiences. With Meta announcing a change in privacy terms for its messaging app WhatsApp, which has been popularly used by civil society organisations and activists in Turkey, a heated online discussion advocating for migrating from WhatsApp ensued. Many organisations, as a result, moved their communications networks to other messaging platforms such as Signal or Telegram,[11] causing a mass digital migration like never before.

The interconnectedness of these civil society publications and webinars initiated during the pandemic reached beyond the country's borders, as local activists and researchers from Turkey participated in events held in other countries and hosted global speakers, asking for their opinion on local matters. The forced digitisation of activists during the pandemic urged many smaller organisations to adapt their activities to more digital-friendly settings, which in turn allowed them to reach much wider audiences, multiplying the impact of their advocacy efforts and the dissemination of information.

A significant example of this kind was the so-called Boğaziçi Resistance, which started in 2016 due to the unlawful appointment of a rector at Boğaziçi University, bypassing campus elections. This gained fresh momentum in the beginning of 2021 as a result of a new rector being appointed amidst curfews across the country. The reactions to this political move on the country's most prestigious university were amplified online, with students forming discussion networks, organising online protests, issuing statements, hosting exhibitions and webinars, writing op-ed articles, and organising alternative graduation ceremonies, among other activities coordinated by Boğaziçi Watch.[12] Two of the most significant activities conducted by Boğaziçi Watch were the transnational solidarity petition,[13] which received almost 5,000 signatures from academics around the world, and the Judith Butler lecture,[14] which received international attention.

10 Önder, N. (2020, 5 August). Updated list of companies that referred to "Istanbul Convention lets one live". *Marketing Türkiye*. https://www.marketingturkiye.com.tr/haberler/istanbul-sozlesmesi-yasatiri-destekleyen-kuruluslar

11 Önder, N. (2021, 8 January). Great migration from WhatsApp to Telegram has begun. *Marketing Türkiye*. https://www.marketingturkiye.com.tr/haberler/whatsappten-telegrama-buyuk-goc-basladi

12 https://bogazicinobeti.org

13 Boğaziçi Watch. (2021, 8 January). Support Academic Freedom for Boğaziçi University Students and Faculty. https://docs.google.com/forms/d/e/1FAIpQLSc_m3StSsK4Zm8Rp54aBMey5fgrCnEfX6_cMV5knhIsjaTrBA/viewform

14 https://www.youtube.com/watch?v=2IKTb4HHGKI

Another social movement that stood out for its digital action during the pandemic was Red Ribbon Istanbul,[15] an HIV/AIDS activist association, which was initiated digitally in 2016 and had a strong digital presence. The association was quickly able to adapt to the new circumstances and not only coordinate advocacy efforts but launch solidarity action in supplying medicines to people with HIV/AIDS in Turkey and other European countries, in addition to frequently publishing and sharing information on the hardships experienced by people with HIV/AIDS during the pandemic, and the possibilities of accessing treatment.[16]

Aside from civil society organisations, Needs Map,[17] which was founded in 2015, launched a solidarity campaign for social support, using a digital map that helped to identify needs in communities across the country. Meanwhile, a socially active rock band, Mor ve Ötesi,[18] engaged in solidarity concerts which were streamed on social media, with the revenues being donated to musicians who had lost their income during the pandemic.[19]

Conclusion

Despite the negative developments in the legal field with the passing and implementation of repressive laws and regulations during the pandemic, many social movements and civil society organisations increased their digital outreach and reached new audiences, gained new members and volunteers, and increased their visibility. Many other organisations also initiated online projects in the form of live-streaming closed-group training sessions, which enabled them to reach audiences previously out of their physical reach. During this period, civil society organisations also initiated joint programmes enabling capacity building for civil society and independent media, such as the independent media and journalism training sessions organised by the Journalists Union of Turkey,[20] Media Research Association[21] and Media and Law Studies Association.[22] Furthermore, online activities organised by the Checks & Balances Network[23] and the Freedom Research Association[24] shed light on the salient issues in society.

Online training programmes, awareness-raising campaigns or even popular online social events organised by civil society organisations with the aim of contributing to society's general psychosocial well-being multiplied the impact of online activism and inspired more organisations to become active digitally. Some of these organisations and social movements have been featured on the Civil Society Hour programme on Dokuz-8TV[25] and some others have received awards at the Friedrich Naumann Foundation,[26] Turkey's annual Oscar Awards.[27]

The impact of these activities can be seen in the increasing number of applications for funding with the aim of building capacity for digital outreach activities by smaller civil society organisations in Turkey, and the applications made to an EU programme for micro-financing targeting civil society and activists called Sivil Düşün.[28]

Action steps

The following action steps are recommended for Turkey:

- More intersectional activities should be organised by civil society organisations working on various focal areas to expand the scope of their work and multiply audiences through collaboration. Despite good examples of organisations reaching out to circles outside of their usual target groups, generally these organisations address most of their activities to the same groups. In order to break out of these natural echo chambers, wider outreach campaigns are needed, possibly with support from socially active artists and activist celebrities to help multiply the impact of initiatives exponentially.
- An archive on the digital transformation of civil society organisations should be created, promoting best practices by exemplary organisations.
- Conventions for civil society organisations that had proven to be useful before the pandemic should be organised again. They should include digital outreach strategies to connect smaller

15 https://www.kirmizikurdele.org/about-us

16 RedRibbon Istanbul. (2021, 19 November). HIV AIDS Congress. https://twitter.com/RedRibbonTR/status/1461591029975597056

17 https://www.ihtiyacharitasi.org

18 https://www.youtube.com/watch?v=7RW8n4iXZbA

19 ArtDog Istanbul. (2021, 1 December). Harun Tekin's 'ticketed online concert experiment' https://artdogistanbul.com/harun-tekinden-biletli-online-konser-deneyi

20 https://tgs.org.tr

21 https://medarder.org

22 https://www.mlsaturkey.com/en/home

23 https://www.dengedenetleme.org

24 https://oad.org.tr

25 https://www.youtube.com/playlist?list=PLEDANnoa4CaMFdwoyXg6aIxQPal9RWgss

26 https://www.freiheit.org/turkey

27 FNF Turkey. (2021, 1 March). Restart 21: How did it pass, remember and celebrate. https://www.freiheit.org/tr/turkiye/yeniden-baslasin-21-nasil-gecti-hatirlayalim-ve-kutlayalim

28 https://www.youtube.com/watch?v=DDYyF3WNw78

organisations and individual activists to these processes.

- Global tech companies should consult local organisations and internet users when developing or amending their community rules and regulations.
- Civil society organisations operating in Turkey should increase their lobbying efforts to inspire positive changes to laws regulating non-governmental organisations.
- A digital rights bill should be drafted by the current alliance of democratic opposition parties, in close cooperation with civil society actors, independent lawyers, academics, rights defenders and tech experts, to sustain a free and open internet that can inspire positive change in the years to come.
- There need to be more international and transnational exchange programmes between Turkish and international civil society organisations to learn from international experiences and examples. These programmes were disrupted due to the downturn in Turkey's economy and the plummeting of the Turkish lira against other currencies in recent years.

URUGUAY

THE NEED FOR A NEW DATA GOVERNANCE AGENDA BASED ON HUMAN RIGHTS

Data and Society Lab (Datysoc)
Ana Karen Tuduri Cairo and Fabrizio Scrollini[1]
https://datysoc.org

Introduction

Uruguay is considered a full democracy and one of the most progressive countries in Latin America. Nevertheless, the COVID-19 pandemic brought new challenges and priorities to Uruguayan civil society groups working in this space. There are three key challenges that could be shifting the advocacy landscape: government transparency, including digital surveillance; gender-based violence; and virtual education. Uruguay was hit by the pandemic amidst a change of government, which increased the difficulties to address these governance challenges

This report explores these issues, and argues that the most effective way to deal with the multiple obstacles they present is to push for a revitalised data governance agenda for the country based on human rights.

Government transparency

Uruguay has been a consistent champion of open government and open data. It ranked second in the Americas in the United Nations Global e-Government Index 2020,[2] first in the Regional Open Data Barometer 2020,[3] and 18th in Transparency International's Corruption Perceptions Index 2021.[4] Uruguay follows the lead of the European Union on data protection and has recently adopted Convention 108 of the European Council, one the most progressive regulatory frameworks in the world.[5]

But how did the COVID-19 pandemic affect transparency and privacy?

As a first digital response against the pandemic, the government and a large number of private stakeholders collaborated and developed the first version of the Coronavirus UY app. The app was developed by the firm GeneXus, which worked with a number of other private companies. It was sponsored by the Uruguayan Agency for Electronic Government and the Information and Knowledge Society (Agesic).

Initially this app provided general information on the pandemic and allowed the user to consult it if they felt they had symptoms of the virus, and to schedule an appointment with a medical service provider.

At that time, the concerns expressed by civil society were the lack of a contract with the companies developing the app, and why GeneXus and its partners were not chosen on the basis of a fair competitive public tendering procedure.[6]

In June 2020, the government announced that a new version of the coronavirus app would implement a COVID-19 exposure notifications application programming interface (API)[7] developed by Google and Apple.

As a consequence, a citizen made a request for access to public information about the source code of the application, the companies linked to the development of the app, and whether or not a contract had been signed with Google and Apple. However, the response received only provided clarity on the link between the Coronavirus UY app and the Salud.uy programme, an initiative that promotes the use of information and communications technologies (ICTs) in the health sector.[8]

After several consultations, the government confirmed to the media that it did not sign a contract with Google and Apple, and accepted their offer after studying their terms and conditions only.[9]

Civil society nevertheless warned the government about the privacy risks associated with the use of the app's contact notification system, and said that the source code should be published as a guarantee of transparency, allowing it to be audited by any citizen.[10]

1 Fabrizio Scrollini contributed to this report as an independent researcher.

2 https://www.uruguayxxi.gub.uy/en/news/article/uruguay-climbs-positions-and-consolidates-itself-as-a-regional-leader-in-e-government

3 https://barometerlac.org/?_year=2020&indicator=ODB

4 https://www.transparency.org/en/cpi/2021/index/ury

5 https://www.impo.com.uy/bases/leyes-originales/19030-2012/1

6 Red de Gobierno Abierto. (2020, 4 April). Declaración: Transparencia y datos abiertos en el contexto de la crisis del Covid-19 en Uruguay. https://rga.uy/coronavirus

7 https://developers.google.com/android/exposure-notifications/exposure-notifications-api

8 https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/saluduy

9 Carve Media. (2020, 20 July). Uruguay no firmó ningún contrato ni acuerdo con Apple y Google para utilizar el sistema de alertas para el Covid-19. https://carve850.com.uy/2020/07/20/uruguay-no-firmo-ningun-contrato-ni-acuerdo-con-apple-y-google-para-utilizar-el-sistema-de-alertas-para-el-covid-19

10 Red de Gobierno Abierto. (2020, 4 April). Op. cit.

According to several Uruguayan experts, the use of any contact tracing technology implies security risks. Therefore, it is a basic condition that the contact notification system respects the protection of personal data and the principles of prior informed consent and voluntary use.[11]

There is also a need to better understand the terms and conditions of its use, the legal framework and public rules that allow its use, and any personal data exchange agreements between the government and the developers. An evaluation of its impact on human rights is also needed, including how the digital divide limits access to mobile devices.[12]

According to Uruguayan researchers from the GUIAD group,[13] a public debate on these issues is needed, as well as on whether the government has the capacity to monitor the app's evolution.[14]

The evolution of digital surveillance

Digital surveillance is an established practice in Uruguay. In 2020, the Ministry of the Interior acquired the UCINET software developed by Analytic Technologies that allows the monitoring of networks to track criminal organisations in the country. In June, news broke that the Ministry's cybercrime division had identified 200,000 citizens for online speech that could be against law, and 2,000 groups identified as mainly left-wing oriented. Because of this, as data seemed difficult to check, the NGO OBSERVACOM[15] filed an access to public information request to find out if the government was monitoring social networks to identify and eventually prosecute hate speech and other possible security threats. The request also asked for clarification on what hate speech and security threats mean in the context of the digital surveillance.[16] The request was rejected based on a Ministry of the Interior decree which classifies all information related to the materials and supplies used by police officers as reserved for reasons of national security. Further, authorities are now systematically denying basic information about the surveillance system.[17]

In 2020, automated facial recognition software and associated support services were procured through a public bidding process, without a legal framework that enables its use.[18] After the purchase of the software, Budget Law No. 19924 introduced two articles that provide a legal framework for the creation of a facial identification database for public security purposes under the authority of the Ministry of the Interior.[19] The database is created by migrating the data from the National Directorate of Civil Identification. It is worrying that these articles give the Ministry of the Interior discretion as to the possible uses of the facial identification database.

Civil society has warned that these articles were approved without an analysis of the impact on personal data, nor proper parliamentary discussion. A group of civil society organisations has sent a letter to the Senate, asking that the articles be removed from the draft of the Budget Act.[20] Despite the fact that some legislators took a position to remove the articles or require a court order for the use of that facial identification database, no agreement was reached and the articles were approved.

The only information currently available on the potential uses of the software is contained in the tender document issued by the Ministry of the Interior. There is no regulatory framework or protocol for police use of the software that guarantees the protection of fundamental human rights.

Datysoc and Amnesty International Uruguay proposed the inclusion of this issue in the 5th Open Government National Action Plan.[21] They are seeking a space to discuss transparency in the use of automated surveillance systems and a space for citizen participation in the co-regulation of the new surveillance systems.[22]

11 Betarte, G., Campo, J. D., Delgado, A., Ezzatti, P., Forteza, Á., González, L., Martín, Á., Muracciole, B., & Ruggia, R. (2020). *Desafíos de seguridad y privacidad en el diseño e implementación de soluciones de rastreo de proximidad*. PEDECIBA. https://www.redgealc.org/site/assets/files/11587/covid_ct_position_betarteetal-1_1.pdf

12 Verrastro, V. (2022, 21 January). Coronavirus.Uy: cinco lecciones a casi dos años de pandemia. *Derechos Digitales*. https://www.derechosdigitales.org/17599/coronavirus-uy-cinco-lecciones-a-casi-dos-anos-de-pandemia

13 GUIAD is a group of multidisciplinary experts from the University of the Republic – one of the most relevant in the country – created to provide analysis on the COVID-19 crisis. See: https://guiad-covid.github.io

14 Scrollini, F., Baliosian, J., Etcheverry, L., & Moncecchi, G. (2020, 26 August). Uruguay's COVID-19 contact tracing app reveals the growing importance of data governance frameworks. *LSE Latin America and Caribbean Centre*. https://blogs.lse.ac.uk/latamcaribbean/2020/08/26/uruguays-covid-19-contact-tracing-app-reveals-the-growing-importance-of-data-governance-frameworks

15 https://www.observacom.org

16 El Observador. (2021, 7 May). Cómo funciona el ciberpatrullaje y el reconocimiento facial: la mesa de diálogo solicitada al gobierno. https://www.elobservador.com.uy/nota/como-funciona-el-ciberpatrullaje-y-el-reconocimiento-facial-el-pedido-al-gobierno-20215618260

17 Ibid.

18 https://www.comprasestatales.gub.uy/consultas/detalle/id/744940

19 https://www.impo.com.uy/bases/leyes/19924-2020

20 Datysoc. (2020, 17 November). Organizaciones de la sociedad civil y académicas expresan su preocupación por reconocimiento facial en el Proyecto de Ley de Presupuesto de Uruguay. https://datysoc.org/2020/11/17/organizaciones-de-la-sociedad-civil-y-academicas-expresan-su-preocupacion-por-reconocimiento-facial-en-el-proyecto-de-ley-de-presupuesto-de-uruguay

21 Uruguay is a member of the Open Government Partnership (OGP) and as a result needs to submit annual plans to advance open government principles in the country. These plans should be agreed between government and civil society.

22 https://quinto-plan.gobiernoabierto.gub.uy/proposals/24-mesas-de-dialogo-sobre-uso-de-sistemas-de-vigilancia-automatizada

At the moment, these technologies are being deployed without an adequate human rights-focused framework. It is a priority to develop this framework, and to discuss a moratorium on the use of these surveillance tools without more evidence on their impact on human rights.

Gender-based violence

Gender-based violence escalated in Uruguay, as in other countries, during the pandemic. According to data from the second national survey on the prevalence of gender-based violence carried out in 2019, eight out of 10 Uruguayan women said they had suffered gender-based violence due to their mere status of being women, and one out of five said they had suffered gender-based violence in the last 12 months since the survey was completed.[23]

Over the past three years, calls about gender-based violence to a telephone guidance service run by the National Women's Institute have increased considerably.[24] These calls increased during the pandemic, peaking in the first three months of 2020.[25]

However, formal complaints of gender-based violence have not increased over the last three years, suggesting a disconnect between formal complaints and incidents of gender-based violence.[26] According to the 2020 annual homicide report carried out by the National Observatory on Violence and Crime of the Ministry of the Interior, in 2020, 37 women were killed, but it is not clear how many of these can be categorised as femicides.[27] In 2021 the Ministry started a new methodology to count femicides and identified 21 cases.[28] Nevertheless, the civil society website Feminicidio Uruguay recorded 21 femicides in 2020 and 30 in 2021.[29] An access to information request made in the context of this report to the Public Prosecutor's Office got a reply that there was no technical means to fully identify femicides in their database. The lack of clarity in criteria shows the difficulty in assessing the situation in Uruguay.

What do we know about gender-based violence online?

In 2020, the second national survey on the prevalence of gender-based violence produced some data related to sexual violence through digital media: 2.5% of women over 15 years of age reported having experienced some type of violence in the digital sphere in the last 12 months, and 5.5% of women aged 15 or over declared having experienced some type of digital violence by their partner or ex-partner.[30]

Despite the survey, there is currently little open data available on gender-based violence online. The few data points available are marginal and partial and do not allow an intersectional analysis of the forms of digital violence, their manifestation and particularities, and are not sufficient for evidence-based public policy planning. Civil society organisations recognise that it is necessary to produce detailed information on digital violence, as well on the multiple types of violence identified in Law 19580 on gender-based violence against women,[31] including psychological or emotional violence, violence due to prejudice towards sexual orientation, economic violence, symbolic violence, and obstetric violence.[32] However, despite the list being identified in law, there are no registries or databases on these different types of violence. In an access to information request made in the context of this research, the Public Prosecutor's Office released data showing that complaints of disclosure of intimate images without consent and grooming have increased in the last three years.

The reality is that the lack of resources, including budget cuts suffered by institutions such as the Ministry of Social Development and the National Women's Institute, makes it impossible to properly apply the law. In addition, it is essential to create more courts specialised in gender violence that develop processes with a comprehensive approach and treatment of the problem, including attending to online violence.[33]

23 Semblat, F., et al. (2020). *Segunda encuesta nacional de prevalencia sobre violencia basada en género y generaciones. Informe general de resultados*. https://www.gub.uy/ministerio-desarrollo-social/sites/ministerio-desarrollo-social/files/documentos/publicaciones/Segunda%20encuesta%C2%Aonaciona.pdf

24 Instituto Nacional de las Mujeres. (2021). *Dossier 25 de Noviembre de 2021: Día Internacional de la Eliminación de la Violencia contra las Mujeres*. https://www.anep.edu.uy/sites/default/files/images/2021/noticias/noviembre/211125/DOSSIER%20PARA%20EL%2025%20DE%20NOVIEMBRE%20DE%202021-version%20final.pdf

25 Demirdjian, S. (2020, 24 June). Violencia de género durante la pandemia: una puesta a punto de la respuesta del Estado. *la diaria*. https://ladiaria.com.uy/feminismos/articulo/2020/6/violencia-de-genero-durante-la-pandemia-una-puesta-a-punto-de-la-respuesta-del-estado

26 Ministerio del Interior. (2022, 18 January). Ministerio del Interior presentó cifras de delitos en 2021. https://www.minterior.gub.uy/index.php?option=com_content&view=article&id=9580

27 Ministerio del Interior. (2021). *Homicidios 1º de Enero al 31 de Diciembre (2020 – 2021)*. https://www.minterior.gub.uy/observatorio/images/pdf/2022/HC_-__31_de_Diciembre_2021.pdf

28 Ministerio del Interior. (2021, 30 November). Ministerio del Interior presentó datos sobre violencia doméstica y de género. https://www.minterior.gub.uy/index.hp?option=com_content&view=article&id=9469

29 https://sites.google.com/view/feminicidiouruguay

30 Semblat, F., et al. (2020). Op. cit.

31 https://www.impo.com.uy/bases/leyes/19580-2017

32 Others include: violence due to gender identity or gender expression, sexual violence, labour violence, violence in the educational field, sexual harassment, street violence in the street, political violence, media violence, femicideal violence, dfomestic violence, community violence, institutional violence and racial or ethnic violence.

33 Fernandéz, L. (2021, 31 July). Se postergan los juzgados de género: el lado más fino de la piola. *la diaria*. https://ladiaria.com.uy/opinion/articulo/2021/7/se-postergan-los-juzgados-de-genero-el-lado-mas-fino-de-la-piola

Finally, there are cultural issues that will demand a different approach. The normalisation of digital violence means that it is often not perceived as an infringement of rights by those who suffer it.

As it is, the support mechanisms for victims of gender-based violence are still in their infancy and legal measures are inadequate, despite evidence suggesting that the pandemic exacerbated gender-based violence, with a limited response from government authorities.

The challenge of ensuring access to education online

One of the challenges faced in 2020 was to ensure access to online education for all. For that reason, connectivity and internet access have become very relevant.

According to a study by the state-owned telecommunications firm Antel, which was accessed by the newspaper *El País*, there are 22,716 people without internet access in Uruguay, out of a population of 3,473,727. The study found that 3,115 people in the countryside have access to 2G (LTE) technology, 390,986 have access to 3G (LTE) and 2,693,447 have access to 4G (LTE).[34] Coverage is therefore almost universal, but with different degrees of quality and speeds.

In order to deal with the demand for access for educational purposes during the pandemic, Plan Ceibal – a government project to ensure access to the internet, devices and education to every school child[35] – partnered with telecommunications service providers and the National Education Board (ANEP) to get free internet access for the use of educational tools, or with discounts and exemptions for students, families and teachers.[36] Plan Ceibal, ANEP and the telecommunications companies Antel, Movistar and Claro also agreed to promote and ensure access to hybrid education.[37]

A problem with platforms

During the closure of educational centres due to the COVID-19 pandemic, Plan Ceibal and ANEP created "Ceibal at Home" in an effort to transform a face-to-face learning programme into a distance learning solution.[38] But despite this effort to provide continuity to education, it was only partially successful. Aristas – the first report on educational performance of students between third and sixth grade in primary school – shows that in the first semester of 2020, 90% of public school teachers connected with their students through the Ceibal platform, while in private schools, other platforms were used as often as the Ceibal platform. The study also found that the use of WhatsApp for education was greater in public schools (70%), while in private institutions the use of email increased.[39]

There are several points to consider about the use of platforms such as Google for Education, including the interests of the company and the privacy of students and teachers. Currently, according to statements made by Google's manager for Latin America to *El País*, there are 50,000 active users of Google educational tools in Uruguay.[40]

With regard to the use of WhatsApp as an official means of communication with students, it must be taken into account that when using the free service, data such as the mobile phone number, the operating system, information about the networks used, the geographical location and profile details and statuses of the students and teachers are captured by the company.

Due to this new reality, children and vulnerable groups are now exposed to various uses of their private data that could harm them, including the use of their digital profiles for commercial purposes.

Understanding this new reality and generating an adequate framework to govern it is a necessity for Uruguay.

When copyright gets in the way of education

Another challenge to online education in Uruguay during the pandemic is that most learning materials were covered by copyright law dating back to 1937, which does not respond to the needs of accessing knowledge in the digital age. The needs impact authors, producers and publishers, as well as educational and cultural institutions, such as universities, libraries and archives.

34 Fernandéz, P. (2021, 11 May). Hay 22.716 personas sin internet en Uruguay y vale unos US$ 12 millones conectarlas. *El País*. https://www.elpais.com.uy/informacion/sociedad/hay-personas-internet-uruguay-vale-us-millones-conectarlas.html

35 https://www.ceibal.edu.uy/es

36 Montevideo Portal. (2021, 14 April). Plan Ceibal acordó con empresas telefónicas y alumnos se podrán conectar sin gastar datos. https://www.montevideo.com.uy/Noticias/Plan-Ceibal-acordo-con-empresas-telefonicas-y-alumnos-se-podran-conectar-sin-gastar-datos-uc783631

37 Alonzo Palmer, M. C., & Osorio, C. (2021). *Evaluación de las necesidades de recuperación en el contexto de la pandemia por Covid-19: Sector educación*. SINAE Uruguay & PNUD Uruguay. https://www.gub.uy/sistema-nacional-emergencias/sites/sistema-nacional-emergencias/files/documentos/publicaciones/PDNA_Aplicacio%CC%81n_EDU_ipm_COVID-19_Uruguay_2021.pdf

38 Ripani, M. F. (2020, 15 July). Ceibal en casa: la experiencia de Uruguay como ejemplo a nivel mundial. *Plan Ceibal*. https://www.ceibal.edu.uy/es/articulo/ceibal-en-casa-la-experiencia-de-uruguay-como-ejemplo-nivel-mundial

39 Instituto Nacional de Evaluación Educativa. (2021). Aristas 2020. Primer informe de resultados de tercero y sexto de educación primaria. https://www.ineed.edu.uy/aristas-2020-primer-informe-de-resultados-de-tercero-y-sexto-de-educacion-primaria.html

40 Malek. M. (2021, 5 August). En Uruguay hay 50.000 usuarios de las herramientas de Google for Education. *El País*. https://www.elpais.com.uy/vida-actual/uruguay-hay-usuarios-herramientas-google-for-education.html

A more flexible system of copyright is required, based on current international regulations, which guarantees authors the effective exercise of their rights, while also ensuring the right to education, access to information, and to culture, science and research.

With regard to education, it must recognise the use of digital environments and tools, and educators as content creators.

Specifically, Datysoc believes that the copyright law should:

- Include exceptions for educational, research and private study purposes that do not involve profit, without establishing restrictions on the physical spaces where these activities are carried out or restrictions on the type of institution that carries them out.
- Guarantee the possibility of carrying out certain acts of reproduction, distribution, adaptation and communication of works, as well as the creation of selections or compilations of readings.
- Expressly clarify that the exceptions apply to online teaching and learning activities.
- Establish a definition of study materials that covers any type of work and is neutral with respect to the type of medium, format and technology. There should be a specific clarification that this applies to audiovisual works and images used for education purposes.
- Establish a generic exception that enables non-consumptive uses of works for research purposes, especially those uses related to text and data mining techniques and artificial intelligence procedures.
- Explicitly enable the circumvention of technological protection measures when the exceptions operate for purposes of education, research and private study.[41]

Conclusion: An emerging agenda for digital rights in Uruguay

In this report we have argued that government transparency, including on digital surveillance, gender-based violence and government services, were negatively affected by the COVID-19 disruption.

While previously being committed to open governance, the government has shown significant reticence to valid questions posed about its use of surveillance technology. It is also possible to argue that a new administration did not have experience in some of these topics and had to deal with them under maximum pressure. Furthermore, in areas such as surveillance, the agenda of the new administration did not include a focus on transparency and accountability. It remains to be seen whether the current administration is willing to sustain a commitment to openness and transparency in these vital areas for human rights and security.

It is not possible to fully assess the impact of the pandemic on gender issues, most notably gender-related violence, due to the absence of data. However, insufficient resources have been set aside to attend to this deficit, even though more data is needed to properly enact gender-related laws. At the same time, support mechanisms and legal remedies for the victims of gender-based violence, including online violence, are inadequate.

While Uruguayan public telecommunications infrastructure played a critical role in supporting government services, including education, the government response showed the lack of a coherent governance framework to deal with the pandemic. Dependence on global corporations to deliver key services is also a significant vulnerability in terms of rights, particularly those of children.

Action steps

The most important next step that needs to be taken to address these issues is to foster a multistakeholder internet governance agenda that focuses on respecting human rights. This agenda needs to update the current data governance framework. In order to do this. two principles are essential: 1) openness to multistakeholder work and 2) an intersectional approach.

Genuinely diverse multistakeholder groups are likely to deliver better governance frameworks in the Uruguayan setting. An intersectional approach, considering different forms of social discrimination, will also be needed to ensure governance frameworks and their implementation are transparent, fair and inclusive.

The most progressive country in Latin America needs to innovate to walk the talk in the digital age.

41 Datysoc. (2021). *Plataforma abierta sobre flexibilidades al derecho de autor. Hacia el equilibrio con los derechos culturales y el interés público en Uruguay*. https://datysoc.org/plataforma-abierta-flexibilidades-al-derecho-de-autor

VENEZUELA

TELEWORKING DURING COVID-19 AND THE DEFENCE OF INTERNET FREEDOMS

EsLaRed
Sandra L. Benítez U.
www.eslared.net

Introduction

In Venezuela, as in most countries, the government declared a "state of alarm" in 2020 due to the COVID-19 pandemic, as established by Decrees 4160,[1] 4198,[2] 4247,[3] 4286[4] and 4361.[5] In these decrees, among other prevention measures, restrictions on circulation and the suspension of activities in certain areas or geographical zones, the suspension of school attendance and academic and work activities throughout the national territory, and social distancing were implemented. The implementation of the measures generated a series of changes that altered the traditional ways of relating, forms of participation, work models and educational modalities. Particularly, there was a widespread use of digital technologies in homes and in companies, schools and universities, which turned to teleworking, distance education and online meetings as a way to communicate and exchange information. In this context, the government's measures to manage the pandemic included attempts to manage information and communications through greater controls and the use of surveillance technologies.

This report discusses the impact of the pandemic on teleworking in Venezuela and its effects on internet freedoms. For this, the legal framework that promotes teleworking in the country is identified, and the risks that teleworking imply for the defence of internet rights are analysed. Finally, recommendations are made on how to improve the situation.

Legal framework

Venezuela has a broad legal framework that protects the rights of workers, guaranteeing the safety and hygiene of the work environment, among other labour protections. These rights are enshrined in the Constitution of the Bolivarian Republic of Venezuela[6] in articles 87 to 97, and in the Organic Law on Labour and Workers (LOTTT).[7] Activities related to the use and management of digital technologies at work are established in the Organic Law on Prevention, Conditions and Work Environment,[8] Law on Technology and Innovation,[9] Law of Infogovernment,[10] National Information Technology Plan,[11] Telecommunications Law,[12] Law Against Hate and for Peaceful Coexistence and Tolerance,[13] Law Against Computer Crimes,[14] and Law on Data Messages and Electronic Signatures.[15] These laws guarantee, among other rights, access, security, privacy and freedom of expression.

The framework that protects teleworking is nevertheless the LOTTT, which refers to remote work in articles 209 to 217, as well as articles 8 and 9 of Decree 4160,[16] in which the government first declared the "state of alarm" in 2020. In the international arena, the International Labour Organization (ILO)

1 Pandectas Digital. (2020, 13 March). Decreto N° 4.160, mediante el cual se decreta el Estado de Alarma en todo el Territorio Nacional. https://pandectasdigital.blogspot.com/2020/03/decreto-n-4160-mediante-el-cual-se_17.html

2 Pandectas Digital. (2020, 12 May). Decreto N° 4.198, mediante el cual se decreta el Estado de Alarma en todo el Territorio Nacional. https://pandectasdigital.blogspot.com/2020/05/decreto-n-4198-de-fecha-12-de-mayo-de.html

3 Pandectas Digital. (2020, 10 July). Decreto N° 4.247, mediante el cual se decreta el Estado de Alarma en todo el Territorio Nacional. https://pandectasdigital.blogspot.com/2020/07/decreto-n-4247-mediante-el-cual-se.html

4 Tribunal Supremo de Justicia. (2020, 18 September). Sala Constitucional del TSJ declaró la constitucionalidad del Decreto del estado de alarma por pandemia del Covid-19. http://www.tsj.gob.ve/-/sala-constitucional-del-tsj-declaro-la-constitucionalidad-del-decreto-que-prorroga-estado-de-alarma-por-pandemia-del-covid--1

5 Pandectas Digital. (2020, 3 November). Decreto N° 4.361, mediante el cual se decreta el Estado de Alarma en todo el Territorio Nacional. https://pandectasdigital.blogspot.com/2020/11/decreto-n-4361-mediante-el-cual-se.html

6 http://www.conatel.gob.ve/constitucion-de-la-republica-bolivariana-de-venezuela-2

7 http://www.onapre.gob.ve/index.php/publicaciones/descargas/viewcategory/43-ley-organica-del-trabajo-los-trabajadores-y-las-trabajadoras

8 https://www.medicinalaboraldevenezuela.com.ve/archivo/LOPCYMAT.pdf

9 http://www.conatel.gob.ve/ley-organica-de-ciencia-tecnologia-e-innovacion-2

10 http://www.conatel.gob.ve/ley-de-infogobierno

11 http://www.conatel.gob.ve/pueblo-y-gobierno-potencian-tecnologias-de-informacion

12 http://www.conatel.gob.ve/ley-organica-de-telecomunicaciones-2

13 https://www.ghm.com.ve/wp-content/uploads/2017/11/41276.pdf

14 http://www.conatel.gob.ve/ley-especial-contra-los-delitos-informaticos-2

15 http://www.conatel.gob.ve/ley-sobre-mensajes-de-datos-y-firmas-electronicas-2

16 Pandectas Digital. (2020, 13 March). Op. cit.

established guidelines and standards with recommendations to follow during COVID-19[17] that embrace the right to work as a human right.

César Augusto Carballo Mena says that few changes have been made to the regulation of teleworking in Venezuela during the pandemic,[18] which generates legal loopholes. For this reason, the ILO recommendations represent an opportunity to strengthen teleworking in the country and promote the defence of internet rights and freedoms.

Analysis of the defence of internet freedoms in Venezuela

Current situation

Changes in labour and social dynamics, and the confinement of people during the pandemic, meant that Venezuelans needed to create new ways of participating. This resulted in greater internet consumption and use of digital technologies. However, this national context was clouded by constant electricity and internet failures,[19] a product of the political, economic, social[20] and technological[21] crisis that exists in the country, and that makes remote practices unviable. At the same time, there were greater controls of information and communications by the government.

While the government has tried to make the internet and online information accessible to people through various programmes, these programmes are almost inaccessible to the population, due to the high costs of internet connectivity, and the precarious purchasing power and low salaries of many people in the country. The minimum salary is USD 2.5 a month, which shows the crisis that Venezuelans are experiencing and contrasts with the accumulated inflation that is registered at more than 600%,[22] alongside extreme poverty.[23]

The following sections elaborate on this social dynamic and the changes in priorities that have been established in the country.

New surveillance strategies

The government applied new surveillance strategies on the handling of information during the pandemic, which affected freedom of expression and privacy. Information on COVID-19 was considered a priority resource and an area for political surveillance. In particular, the dissemination of information on social networks and websites were monitored by the National Telecommunications Commission (CONATEL), resulting in accusations against those who contradicted the official version on issues related to COVID-19, but also those who criticised the government's management of the pandemic.

The report of the Third Cycle of the Universal Periodic Review (UPR)[24] for Venezuela in 2022 indicates that since 2018 the government has bought telephone hacking technology from Cellebrite.[25] This is evidence of the government's efforts to monitor, identify and collect data, which was also done during the pandemic.

The shutting down of media critical of the government and the number of violations of internet rights increased during the pandemic.

Digital rights advocate David Aragort has pointed out that "Venezuelan cyberspace is subjected to a growing and systematic policy of censorship."[26] He has also indicated that, during the pandemic, in addition to hacking and DDoS attacks, larger attacks were used, such as in the case of the Heroes of Health platform, which on two occasions was the victim of a combined phishing and DNS spoofing attack, through the national telephone company of Venezuela (CANTV), and that the government used troll and bot accounts to harass and carry out

17 International Labour Organization. (2020). *Safe return to work: Guide for employers on COVID-19 prevention*. https://www.ilo.org/actemp/publications/WCMS_744033/lang--en/index.htm and International Labour Organization. (2020). *Guía de orientaciones de Seguridad y Salud en el Trabajo frente a la COVID-19 para personas empleadoras y trabajadoras del hogar*. https://www.ilo.org/wcmsp5/groups/public/---americas/---ro-lima/documents/publication/wcms_755065.pdf

18 Carballo Mena, C. A. (2021). *Régimen jurídico del teletrabajo forzoso. Venezuela: modelo minimalista e informal*. http://www.cielolaboral.com/wp-content/uploads/2021/04/venezuela_carballo_noticias_cielo_n4_2021.pdf

19 Rondón, F. (2020, 16 October). Teletrabajo en Venezuela, un reto en un país donde falla la luz y el internet. *Voz de América*. https://www.vozdeamerica.com/a/venezuela_teletrabajo-venezuela-fallas-internet-servicio-electrico/6068707.html

20 EsLaRed. (2021). *Marco Económico y Social sobre la calidad de vida y servicios de internet en Venezuela, durante el año 2020*. https://eslared.net/sites/default/files/2021-01/MarcoEconomicoySocial.pdf

21 EsLaRed. (2021). *Marco Tecnológico sobre los servicios de internet y bloqueos comunicacionales en Venezuela, durante el año 2020*. https://eslared.net/sites/default/files/2021-01/MarcoTecnlogico.pdf

22 Semana. (2021, 23 December). El salario mínimo que regirá en Venezuela para 2022: equivalencia en pesos colombianos. *Semana*. https://www.semana.com/mundo/articulo/el-salario-minimo-que-regira-en-venezuela-para-2022-esto-equivale-en-pesos-colombianos/202104

23 ENCOVI. (2021). *Condiciones de vida de los venezolanos: Entre emergencia humanitaria y pandemia*. https://assets.website-files.com/5d14c6a5c4ad42a4e794d0f7/6153ad6fb92e4428cada4fb7_Presentacion%20ENCOVI%202021%20V1.pdf

24 Hoja informativa del EPU Venezuela: Libertad de expresión e información. Contribuciones de la sociedad civil venezolana al 3er ciclo del EPU. https://drive.google.com/file/d/1PPVSSQ14OzQ_WvZWlz6rZAgWcIgEYuWc/view

25 https://cellebrite.com/en/home

26 Alcalde, C. (2021, 9 September). Informe: gobierno aumenta esfuerzos para "controlar" plataformas digitales en Venezuela. *Voz de América*. https://www.vozdeamerica.com/a/venezuela-informe-aumenta-controles-plataformas-virtuales-/6219591.html

defamation campaigns on social networks against dissidents.[27] Likewise, Freedom House published a report in which it classifies Venezuela as a country that does not have internet freedom, ranking it 28th out of 100, with 100 being the country that has the most internet freedom.[28]

In investigations carried out by the organisation Espacio Publico,[29] it was shown that in 2020:

- Eighteen radio stations, four print media and two digital media were closed by the regulator CONATEL.
- At least 965 complaints of violations by government officials were registered, of which 36.89% involved intimidation, 19.07% censorship, 13.47 restrictions, 9.64% threats, 8.08% verbal harassment, 6.53% judicial harassment, 5.49% aggression, 0.52% aggression and 0.31% death. The complaints were typified by Espacio Público.[30]
- On at least 66 occasions, blocks or impediments to online access were applied by the government. Of the total number of blocks, 23 were applied to digital media and 43 to portals or web platforms.
- On 18 March, CANTV blocked the website coronavirusvenezuena.info7, which had been launched hours before by the country's legal and democratic national assembly, and which was created to provide information to citizens about COVID-19.
- On 4 June, CANTV blocked access to the plan-paisvzla.com8 website, an action that was later replicated by the private operators Digitel and Movistar. The blocking was of the DNS type and was recorded during the live broadcast of an event by Juan Guaidó, an opponent of the government.
- On 29 March, the human rights organisations Venezuelan Association for Alternative Sex Education, the Venezuelan Prison Observatory and Promedehum suffered attacks on their Twitter accounts.
- Thirty-one people were arrested for exercising their right to free expression.

27 Ibid.

28 Maya, M. J. (2021, 4 October). La libertad de internet retrocede cada vez más en Venezuela. *openDemocracy*. https://www.opendemocracy.net/es/libertad-internet-retrocede-cada-vez-mas-venezuela

29 Espacio Público. (2021). *Informe 2020: Situación general del derecho a la Libertad de expresión en Venezuela*. https://espaciopublico.ong/informe-2020-situacion-general-del-derecho-a-la-libertad-de-expresion-en-venezuela

30 Ibid.

Government efforts to strengthen internet access

In the midst of this environment of surveillance, the government prioritised internet access and set up new internet service providers (ISPs), making room for new connections in different regions of the country. This was due to the need to activate strategic programmes in response to the pandemic, such as the Each Family a School Programme,[31] which was promoted by the government and the United Nations Office for the Coordination of Humanitarian Affairs (OCHA),[32] the University at Home Plan,[33] and the Strengthening of Spaces to Access the Internet programme.[34] However, a study carried out by the Metropolitan University of Caracas indicated that the aforementioned programmes cannot be applied successfully due to the critical situation of services in the country.[35]

Teleworking in Venezuela

Faced with this cluster of situations, teleworking was activated as a contingency modality in the face of the need to boost the economy and attend to priority activities such as education and health. However, the precarious conditions of infrastructure and access, alongside surveillance and controls, affected its take-up and prevented its proper functioning. At the same time, teleworking was negatively affected by the violation of internet rights.

In this context, the following observations have been made:

- Jair de Freitas, lawyer and director of LabLabor,[36] indicates that "when it comes to telecommuting, the employer in Venezuela must supply the work implements and cover expenses in terms of services (electricity and internet), as well as security protocols."[37] It is important to

31 http://cadafamiliaunaescuela.fundabit.gob.ve/index.php/programa-tv

32 ReliefWeb. (2020, 5 April). Venezuela: Alternativas para la continuidad educativa ante el cierre preventivo de escuelas por el COVID-19 (26 de marzo 2020). https://reliefweb.int/report/venezuela-bolivarian-republic/venezuela-alternativas-para-la-continuidad-educativa-ante-el

33 Venezolana de Televisión. (2020, 30 December). Plan Universidad en Casa continuará en 2021 con sistematización de educación a distancia y método de Flexibilización 7+7 Plus. https://www.vtv.gob.ve/plan-universidad-casa-2021

34 http://fundabit.gob.ve/index.php/espacios/cbit

35 Centro de Derecho Humanos de la Universidad Metropolitana. (2020). *Informe sobre las afectaciones al derecho a la educación durante la pandemia de COVID-19: Caso de la Universidad Metropolitana, Venezuela.* https://www.unimet.edu.ve/wp-content/uploads/2020/12/Informe-Derecho-a-la-Educaci%C3%B3n.pdf

36 https://www.lablabor.com.ve

37 Davies, V. (2021, 10 February). Tres datos sobre el teletrabajo en Venezuela que deben ser tomados en cuenta por trabajadores, empleadores y legisladores. *Contrapunto*. https://contrapunto.com/economia/empresas/tres-datos-sobre-el-teletrabajo-en-venezuela-que-deben-ser-tomados-en-cuenta-por-trabajadores-empleadores-y-legisladores

highlight that in the country there are no clear technical regulations on teleworking, so workers are vulnerable to computer attacks and information theft.

- According to a study carried out by the consulting firm Conestructuras, the main weaknesses that companies have when implementing teleworking in Venezuela are quality of services, lack of defined processes and knowledge of platforms for teleworking, availability and cost of equipment, poor quality of software technicians, absence of a remote work culture, lack of discipline, lack of experience, employee work supervision, and computer security issues.[38]
- Carlos López, support manager at ESET Venezuela, reported that "with teleworking in Venezuela, attacks on organisations have increased exponentially."[39] He added that this is why "companies must protect access to their data within the office and their employees' computers, to prevent theft of information and data in general." López also pointed out that companies must shield themselves to avoid risks of computer crimes during teleworking,[40] and stressed the need for data protection measures and tools such as data encryption systems, virtual private networks (VPNs),[41] and antivirus and security applications.
- On the other hand, José Adelino Pinto, a professor at UCAB, indicated that teleworkers conducted 94% of their communications on WhatsApp, 92% on institutional emails and 74% on video calls.[42] All of these are services vulnerable to computer crimes.[43]

As a summary, teleworking during the pandemic represented an alternative for the private and public sectors to continue their work. However, the multidimensional crisis that the country is going through affected its development and highlighted the vulnerabilities of companies and workers in a cyberspace exposed to computer crimes and controlled by the government. Given this reality, internet freedoms are compromised and the violation of internet rights increases through telework.

Conclusion

In Venezuela, specific regulations on teleworking are necessary, since the protection of data and information of companies and workers is required. It is also important to look into the legal aspects relating to labour rights that affect the teleworker.[44]

The pandemic promoted teleworking but also exposed the poor preparation of companies who had to face issues related to infrastructure and services. For example, companies were unable to cover the costs of the use of the internet from homes, which affected the performance of workers and violated the right to work. The lack of skills and experience among workers on the management and use of remote applications and computer security also needs to be noted.

In the meantime, the proliferation of computer crimes, the lack of technological know-how among workers and the use of vulnerable applications exposed companies to theft of data and sensitive information.

In the international arena, Venezuela is recognised as a country that violates internet rights and freedoms. The deficiency of internet access and services and social control policies hamper effective teleworking and violate internet freedoms.

Finally, while strategic government projects attempted to expand access to the internet during the pandemic, low salaries prevented access to services.

Action steps

The following action steps are recommended for Venezuela:

- State bodies in charge of legislation must respond to the legal gaps that affect telework in order to guarantee better conditions for workers and commitments from employers. In this way, more efficient practices are promoted that will result in a better performance of the organisations when remote activities are required.

38 Perdomo, L. (2020, 13 August). Teletrabajo en Venezuela, entre la gerencia arcaica y servicios deficientes. *El Diario.* https://eldiario.com/2020/08/13/teletrabajo-venezuela-servicios-deficientes

39 Davies, V. (2021, 10 February). Op. cit.

40 Seguros Venezuela. (2020). *Empresas y colaboradores deben blindarse para evitar riesgos de delitos informáticos en teletrabajo*. https://www.segurosvenezuela.com/wp-content/uploads/2020/07/Sin-Adiccion-2do-trimestre-2020.pdf

41 EsLaRed. (2020). *Guía de buenas prácticas para saltar el bloqueo comunicacional en la web*. https://eslared.net/sites/default/files/2021-01/guia_buenas_practicas_saltar_bloqueo_web.pdf

42 El Ucabista. (2020, 20 April). Entre teletrabajo y dificultades económicas: así sobrellevan las empresas venezolanas crisis del COVID-19. https://elucabista.com/2020/04/20/entre-teletrabajo-y-dificultades-economicas-asi-sobrellevan-empresas-venezolanas-crisis-covid-19

43 Frequent computer crimes in Venezuela include fraud in commercial transactions, phishing, catfishing and foreign currency scams, among others. See: https://losdescarados.eslared.net

44 Legal aspects include those related to mandatory teleworking, protocols to implement teleworking, ways to access the media, services and information, protocols on the use of resources and computer security, and limits on the duration of the working day and costs incurred in teleworking.

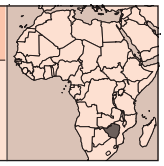
- The government must implement policies that encourage teleworking in the country and increase accessible alternatives to the internet. In addition, it must regulate the use of surveillance and control technologies when states of alarm are established. This is particularly important because the national executive can authorise decrees unilaterally during states of alarm, and because it is clear that we do not have any real, independent democratic powers in the country.
- The government must implement strategies to stabilise basic internet services, since the deficiency of internet services is affecting the performance of the productive sector, as well as education and teleworking.
- Both the government[45] and companies must implement effective strategies to train public and private workers on the management of digital technologies. In this way, better performance is guaranteed and computer crimes that affect organisations and that put privacy and the information of individuals and organisations at risk can be avoided.
- The impact of teleworking must be measured to guarantee a more comprehensive and impartial vision of its effectiveness, taking into account its risks and benefits for all sectors. Hugo Londoño, a private consultant, has determined that workers are looking for a hybrid work environment where face-to-face and remote work are combined, and employers are looking to minimise expenses with teleworking. However, this must include proper infrastructure and security.[46]

45 Pinto, C. (2020, 3 September). Propondrán ideas para legislar en materia de teletrabajo en Venezuela. *Globovisión*. https://www.globovision.com/article/propondran-ideas-para-legislar-en-materia-de-teletrabajo-en-venezuela

46 Londoño, H. (2020, 14 May). Resultados de «¿Cómo van los teletrabajadores venezolanos?». *Con-Café*. https://www.con-cafe.com/2020/05/14/resultados-de-como-van-los-teletrabajadores-venezolanos

ZIMBABWE

INTERNET RIGHTS AND ACCESS CHALLENGES IN ZIMBABWE DURING COVID-19: WHAT NOW?



Independent researcher
Patience Shawarira
patie.shawarira@gmail.com

Introduction

This report focuses on Zimbabwe, where I am currently based. It draws on interviews conducted with representatives of media civil society organisations such as the Zimbabwe chapter of the Media Institute of Southern Africa (MISA Zimbabwe),[1] Digital Society Africa[2] and Magamba Network,[3] among others. These organisations are working on digital rights and digital technology-related issues, and provided me with valuable insights on new digital rights advocacy priorities.

Civil society organisations doing advocacy work on digital rights and digital technology-related issues in Zimbabwe, like their counterparts in other countries in the world, have had to shift their advocacy work online to ensure continuity in their campaigns during the COVID-19 pandemic. Yet for many this mediated form of communication introduced difficulties, such as not being able to speak to constituencies who did not have effective internet access. At the same time, the pandemic made many civil society organisations more aware of the importance of digital rights – an awareness that digital rights actors should leverage in future advocacy for a free internet in Zimbabwe.

Background

Zimbabweans rejoiced when Emmerson Mnangagwa succeeded former president Robert Mugabe, who was forced out of office in late 2017. The thinking was that the new president would deliver on his refrain that the country was now "open for business".[4]

But frustration has risen over the lack of improvement in the collapsed economy. Zimbabweans have sunk into poverty as food prices continue to go up, and some people can no longer afford the exorbitant fares for public transport.

Like any developing country faced with a massive economic meltdown and high inflation rates, before COVID-19 Zimbabweans had been preoccupied with ensuring the day-to- day livelihoods of their families and putting food on the table. As in other parts of the world, they were drawn to digital platforms for news on the pandemic, which has wreaked havoc in most people's lives, with numerous deaths and illnesses being recorded since its onset. Digital platforms such as Facebook and Twitter replaced face-to-face interactions as people resorted to sharing information and news via these platforms. This was necessitated by lockdown restrictions which saw people spending months indoors and some having to move their workspaces to their homes, start conducting business online, and rely on the internet for education.

Moving online introduces new challenges, but more awareness of digital rights

Prior to the COVID-19 outbreak, civil society organisations mainly conducted advocacy work through face-to-face seminars, workshops and field visits. They also engaged the media in face-to-face discussions on television and radio. However, due to the pandemic, communication was heavily mediated by online communication tools such as Zoom, Microsoft Teams and Google Meet.

MISA Zimbabwe's legal and ICT officer, Nompilo Simanje, noted that this continuity for campaigns was important, but was also limited by the digital divide:

> Civil society organisations had to include online-related advocacy strategies so as to continue with their implementation, since physical meetings were banned or restricted. This included learning and adapting to new tools for communication, new methods for awareness raising and also exploring safer platforms. The challenge, however, was centred on reaching the targeted audience due to the digital divide and issues around digital literacy and affordability of data.

Simanje said that this reliance on the internet foregrounded problems such as affordable access and disinformation:

1 https://zimbabwe.misa.org

2 https://www.digitalsociety.africa

3 http://magambanetwork.com

4 Al Jazeera. (2019, 18 January). Zimbabwe imposes internet shutdown amid crackdown on protests. *Al Jazeera*. https://www.aljazeera.com/news/2019/1/18/zimbabwe-imposes-internet-shutdown-amid-crackdown-on-protests

> The advent of the COVID-19 pandemic resulted in an increased reliance on the internet space for access to information, for work purposes, for e-learning purposes, among other uses; hence several digital rights issues had to be prioritised, which include internet affordability and also issues relating to misinformation and disinformation.

She further noted that the right to privacy online became a critical priority for digital rights, as did the need for internet users to be aware of digital safety and security issues.

However, she said this new advocacy landscape also highlighted the importance of digital rights and why all civil society organisations should prioritise advocacy related to access to information online, free expression and the right to privacy.

Human rights violations

The Zimbabwean government is constitutionally bound to uphold people's rights to free expression and access to information. However, with the advent of the pandemic, new challenges arose, such as those that emerged after the government was exposed to an increase in public scrutiny online, and the ruling Zimbabwe African National Union – Patriotic Front (ZANU-PF) government drew a lot of criticism for failing to revive the economy.

In response, the government came up with subversive measures to stifle dissent on digital platforms.

Simanje noted that the government's response to disinformation had a negative impact on freedom of expression:

> It is critical to note also that there were emergency laws that were put in place for purposes of the COVID-19 pandemic which affected free expression, especially laws on the criminalisation of fake news.

Other measures included arresting journalists who shared opposing views to the ruling party online, as well as using pro-ZANU-PF party agents called *Varakashi* to stifle dissent.

According to Tawanda Mugari from Digital Society Africa, Varakashi are "pro-ZANU-PF agents", or people who use social media platforms such as Twitter to bully people who are anti-ZANU-PF and are vocal about it online.

Like other measures to limit freedoms, the state-sanctioned cyber bullying of those with dissident views stifles freedom of expression and can have a long-term impact on citizens' right to express themselves freely online. As one journalist told the International Press Institute:

> I have had subtle threats directed at me on social media by some government officials and anonymous accounts that support the government each time we have published stories that make the authorities uncomfortable.[5]

A report from Human Rights Watch notes that Zimbabwe has been one of the worst offenders when it comes to using COVID-19 as an excuse to crack down on journalists.[6] On 20 July 2020, Hopewell Chin'ono, who had voiced support for anti-government protests online, was charged with inciting violence and communicating falsehoods. MISA Zimbabwe director Tabani Moyo commented at the time on the arrest of Chin'ono, saying his arrest was intended to intimidate citizens and journalists in Zimbabwe, calling it a "dangerous trend":

> This immediate case points to a clear case of trying to effect a chilling effect on the media. How do you come to a conclusion that Hopewell has violated any law of the country for providing an opinion on a video clip that has thousands of people communicating on it? Why, why arriving at Hopewell, a journalist for that matter? So, it is an assault on the media. Secondly, it is meant to send chilling effect not only to the media, but to the users of the online spaces. This is a dangerous trend we are seeing.[7]

Mugari noted the shift in prioritising digital rights among civil society organisations as they rallied together and spoke strongly against the harassment and intimidation of online journalists and political activists. However, he also noted that journalists had to practise self-censorship with regard to the stories they could publish.

Addressing the digital divide

According to Mugari, the scope of work for civil society organisations involved in digital rights activism in Zimbabwe shifted as they now had to intensify advocacy on cyber laws and bridging the digital divide. People in rural areas were left behind as most of them did not have smartphones and data that allowed them to connect to the internet.

5 Maukonen, R. (2021, 17 March). In Zimbabwe, one year of COVID-19 saw surge in harassment of free press. *International Press Institute*. https://ipi.media/in-zimbabwe-one-year-of-covid-19-saw-surge-in-harassment-of-free-press

6 Mavhunga, C. (2021, 11 February). Zimbabwe Among African Countries Using COVID-19 to Crack Down on Journalists, Report Finds. *VOA*. https://www.voanews.com/a/africa_zimbabwe-among-african-countries-using-covid-19-crack-down-journalists-report-finds/6201904.html

7 Mavhunga, C. (2021, 9 January). Zimbabwe Police Arrest Journalist for Third Time in 6 Months. *VOA*. https://www.voanews.com/a/press-freedom_zimbabwe-police-arrest-journalist-third-time-6-months/6200541.html

It is important to note that Zimbabwe has failed to invest effectively in infrastructure that supports digital technologies. Electricity, for example, is still a challenge in rural areas and in urban areas, particularly in high-density suburbs, which affects internet connectivity.

In a 2021 report, Paradigm Initiative notes the high cost of data in Zimbabwe, which currently stands at USD 4 for 1 GB mobile prepaid broadband. This cost means the majority of Zimbabweans cannot afford it. MISA Zimbabwe notes that the prohibitive high cost of data is discriminatory and infringes on people's right to access information provided for by the constitution and the African Declaration on Internet Rights and Freedoms.[8]

To try to address this issue, Simanje said that MISA Zimbabwe held digital rights and literacy campaigns during the pandemic, which included awareness-raising campaigns on cybersecurity and on the data protection bill.[9]

It also launched Information Hubs (or Wi-Fi hotspots)[10] in urban and rural areas, namely in Gweru, which is a town in the Midlands province; Lupane, which is a rural area in Matabeleland North; Gwanda, located in rural areas in Matabeleland South; and Nyanga, a town in Manicaland province. This was in an effort to increase access to information and knowledge through internet services.

Implications of these changes

Some digital rights activists, such as Lukman Adams, viewed the emphasis on digital rights advocacy priorities as a positive development. Adams said this will translate into a wider appreciation of the importance of digital technologies and digital rights advocacy, which will mean that digital inclusion can be achieved for the betterment of society.

However, he added that in jurisdictions where the government interfered in the digital rights of its citizens, the implications might be devastating, since they are likely to be victims of internet shutdowns and unlawful surveillance.

His caution is not unfounded. In Zimbabwe, a total internet shutdown was witnessed in July 2019 during fuel price hike protests. For the first time, Zimbabweans had organised a protest using social media against the increase in fuel prices.

Upon realising the power that digital platforms and especially WhatsApp were having, the government saw fit to come up with counter-measures to the protests, one of which was to demand a total internet shutdown. This meant that Zimbabweans were unable to effectively plan and roll out their protests using WhatsApp and online platforms such as Facebook and Twitter. Critics said this was an attempt to hide growing reports of a violent crackdown on the protests.[11]

In February 2022, internet service access was restricted during a Citizens Coalition for Change (CCC) rally held at Zimbabwe Grounds in Highfields, one of Harare's oldest suburbs. NetBlocks established that the internet was throttled, limiting live streaming and access to online content. Reports indicate that multiple media houses failed to broadcast the rally in real time because of this.[12]

Nyasha Mukapiko from Magamba said that by throttling the internet during the CCC rally, internet service providers infringed on people's right to access information online. Simanje noted that the Zimbabwean government might continue to use the law as a weapon to limit the exercise of rights online.

Meanwhile, Lukman added that some jurisdictions might also want to use the increasing interest in digital inclusion, particularly internet access, to make excessive profits by introducing new taxes and charges.

Conclusion

This report identified a rising interest in digital rights issues in Zimbabwe, following the need for people to move online during the COVID-19 pandemic. It is likely that digital rights will continue to be a priority going into the future, as more and more social and economic activities move online. There is therefore a simultaneous need to ensure that no one is left behind and for priority attention to be given to the digital divide. This will take a lot of work and commitment from civil society organisations, working together with the government and internet service providers. Laws that are friendly to online users, journalists and political activists need to be strongly advocated for to avoid a narrowing of the online space, in the process infringing on people's rights to access information and to freely express themselves.

8 Matimbe, T. (2021). *Londa: Zimbabwe Digital Rights and Inclusion 2020 Report*. Paradigm Initiative. https://paradigmhq.org/wp-content/uploads/2021/05/lr-Zimbabwe-Digital-Rights-Inclusion-2020-Report.pdf

9 New Zimbabwe. (2020, 22 March). MISA-Zimbabwe launches free internet WiFi to marginalised communities. *New Zimbabwe*. https://www.newzimbabwe.com/misa-zimbabwe-launches-free-internet-wifi-to-marginalised-communities

10 Media Institute of Southern Africa Zimbabwe. (2020). *An Analysis of Social Media Use in the SADC Region: 2014-2020*. https://data.misa.org/entity/4sgzarl1vce?file=1624258998903w3z3ke5tz37.pdf&page=6

11 Al Jazeera. (2019, 18 January). Op. cit.

12 Pindula News. (2022, 20 February). Internet Slowdown Limits Coverage Of CCC Rally. *Pindula*. https://zero.pindula.co.zw/internet-slowdown-limits-coverage-of-ccc-rally

Action steps

Below are some action steps for consideration by civil society organisations working in Zimbabwe, which draw on the interviews conducted for this report:

- Civil society groups need to reinvigorate their attention on the digital divide, including through providing disconnected groups and people on the margins of society with access to digital technology as well as training in digital literacy skills.
- Civil society organisations also need to intensify their advocacy on data costs.
- They should prioritise advocacy related to accessing information online, free expression and the right to privacy.
- Civil society will also have to strengthen its advocacy on internet shutdowns, which are likely to be imposed in the future, as well as against unlawful surveillance. There is a need to advocate for reviews and amendments of all laws that limit digital rights.
- They need to continue to raise awareness on the importance of digital rights.

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