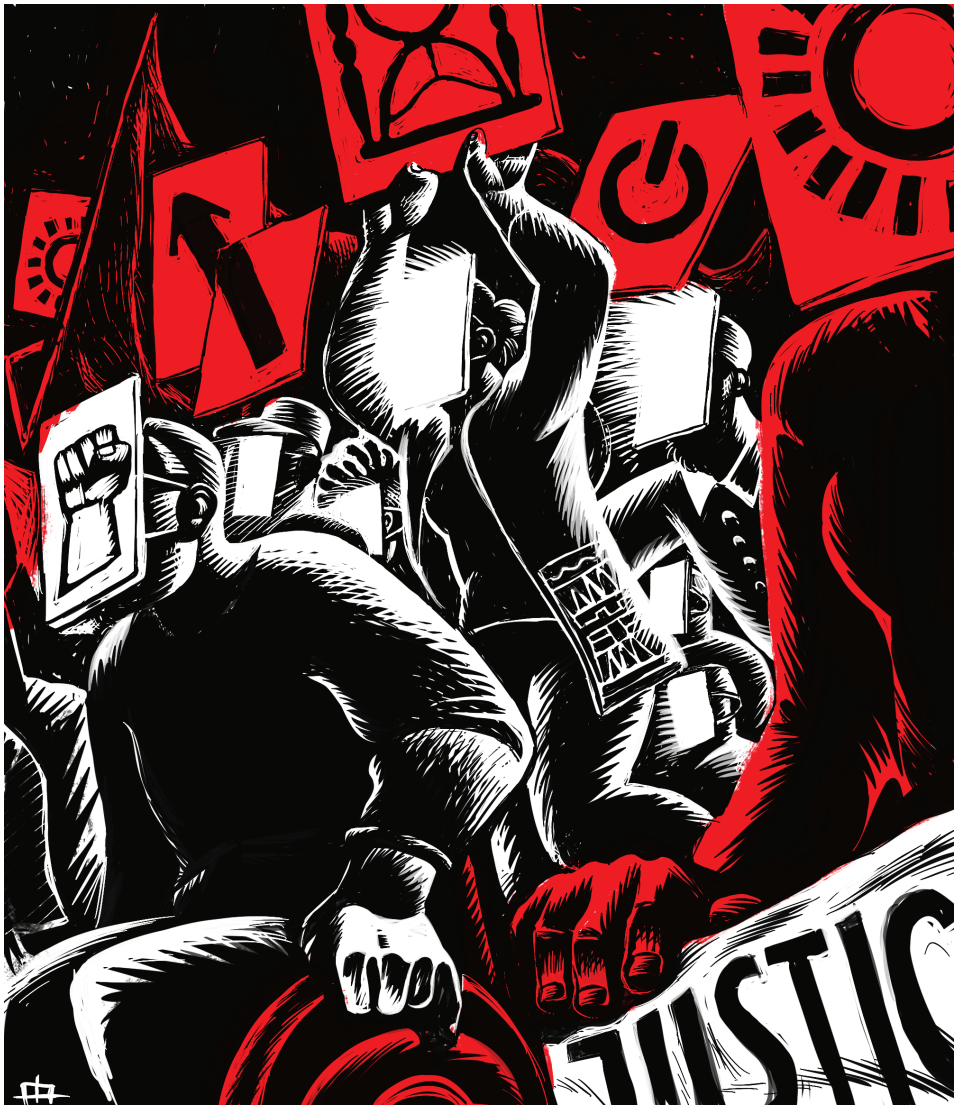
GLOBAL INFORMATION SOCIETY WATCH 2021-2022

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

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.

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