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

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

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

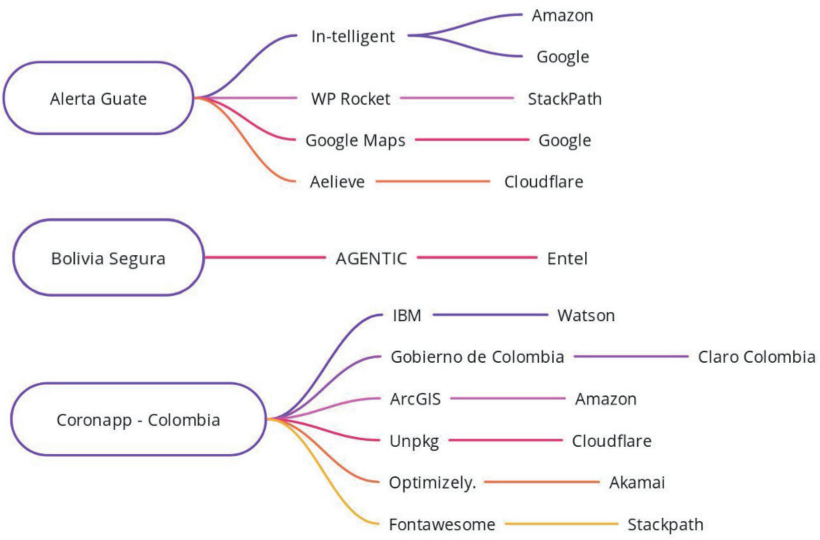


FIGURE 1 *(cont.)*

The service providers used by different apps

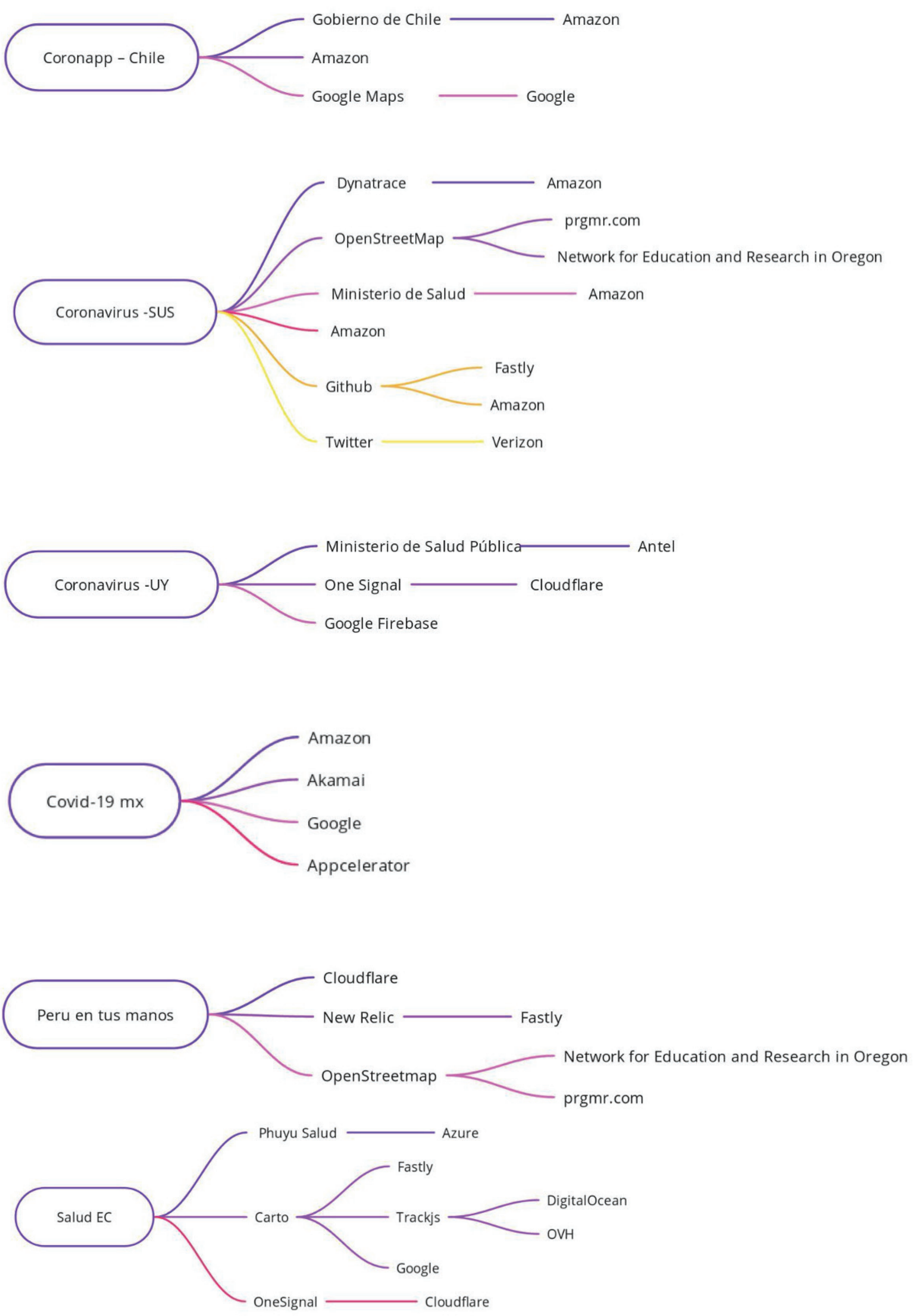
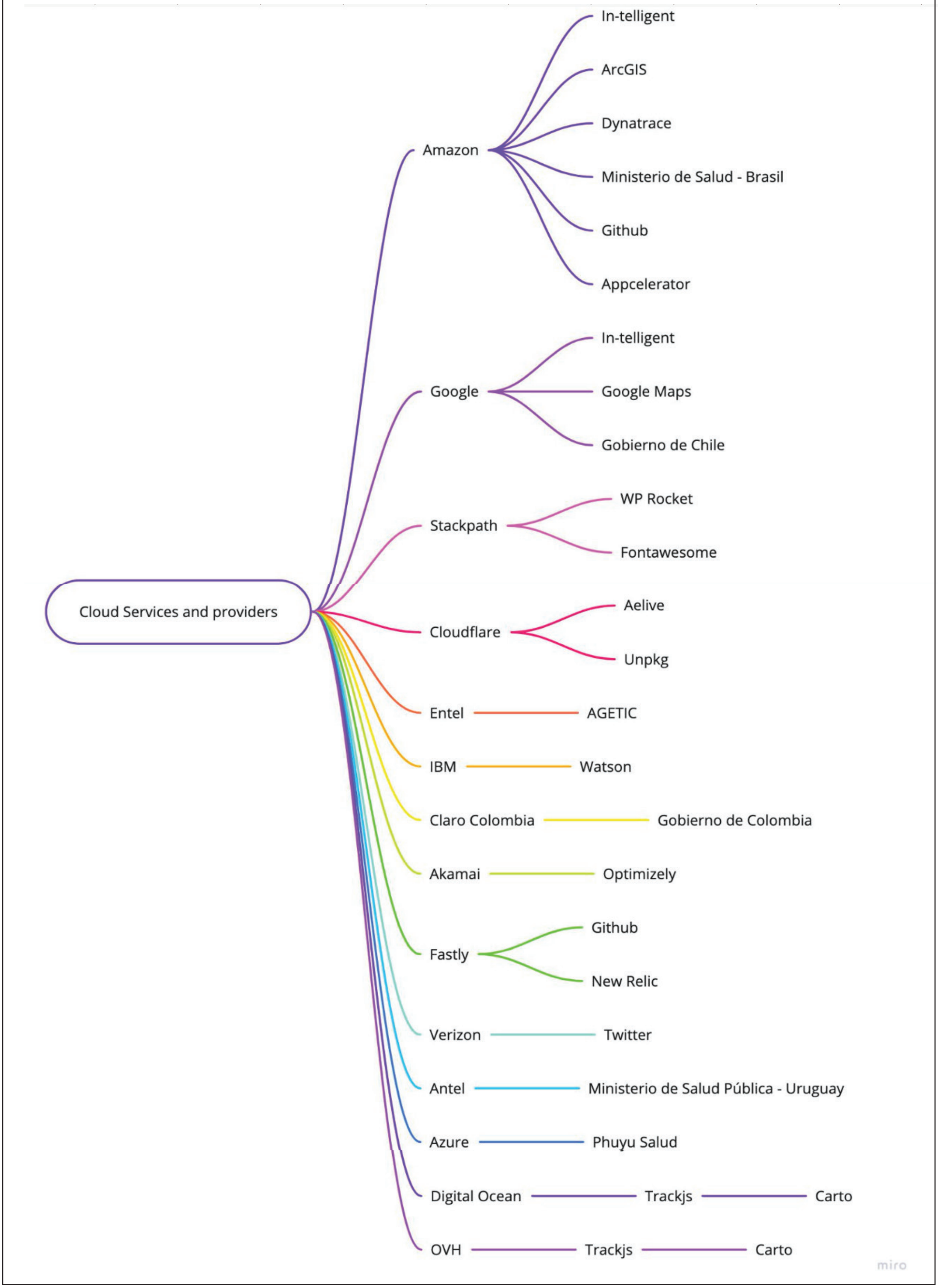


FIGURE 2

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

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