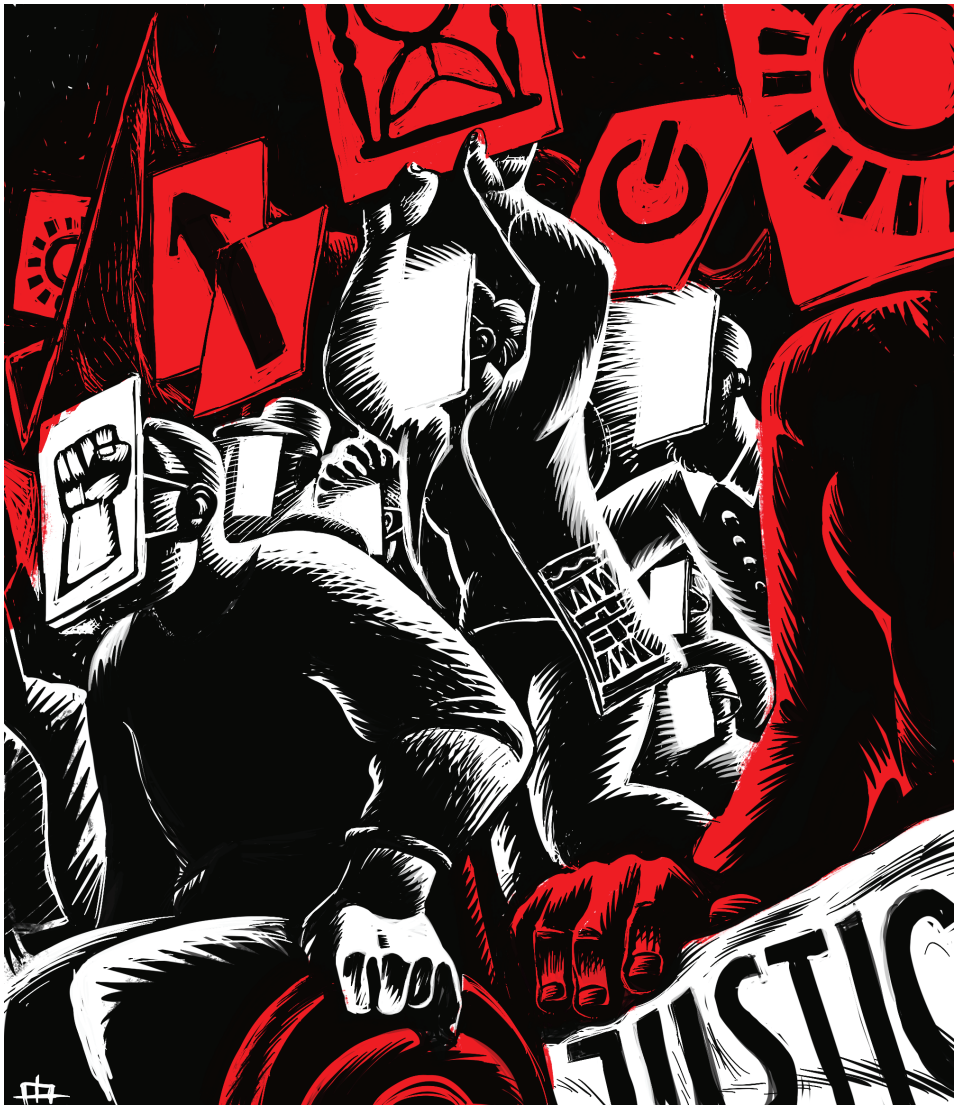
GLOBAL INFORMATION SOCIETY WATCH 2021-2022

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

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.

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