Universal Periodic Review

41st session period - Brazil

Joint stakeholder contribution

Submitting organisations

Association for Progressive Communications (APC) (main)
Artigo 19 Brasil e América do Sul
Derechos Digitales
Intervozes - Coletivo Brasil de Comunicação Social

APC[1] is an international organisation and a network of non-profit organisations with whom it works to empower and support organisations, social movements and people, through use of information and communications technologies (ICTs). APC works at the intersection of technology and social, gender and environmental justice. Founded in 1990, APC has had consultative status to the United Nations Economic and Social Council (ECOSOC) since 1995. The APC network has 62 organisational members and 29 individual members active in 74 countries, mainly in the global South.

Artigo 19 Brasil e América do Sul[2] is a chapter of ARTICLE 19, a non-governmental human rights organisation founded in 1987 in London, whose mission is to defend and promote the right to freedom of expression and access to information around the world. Its name stems from Article 19 of the United Nations Universal Declaration of Human Rights. With offices in nine countries, ARTIGO 19 has been in Brazil since 2007, where it adopts diverse strategies, actions and partnerships in the most varied aspects of this agenda. The office headquartered in São Paulo defends freedom of expression and information and its importance for achieving and realising other fundamental rights in Brazil and South America.

Derechos Digitales[3] is a non-profit non-governmental organisation founded in 2005. It has consultative status to ECOSOC and its headquarters are in Santiago de Chile. Its work covers Latin America, and it is dedicated to the defence and promotion of human rights in the digital environment, especially those related to freedom of expression, privacy and access to knowledge and information.

Intervozes - Coletivo Brasil de Comunicação Social[4] is a civil society organisation founded in 2003 that works for the realisation of the human right to communication. For Intervozes, the right to communication is indivisible from the full exercise of citizenship, democracy and all other rights. The Collective operates in the areas of telecommunications, digital rights and broadcasting, seeking a democratic media system that respects human rights and freedom of expression. It is a member of the APC network and, in Brazil, of the Coalizão Direitos na Rede, a coalition of around 50 digital rights entities.

1. Association for Progressive Communications: https://www.apc.org
2. Artigo 19 Brasil e América do Sul: https://artigo19.org
3. Derechos Digitales: https://www.derechosdigitales.org
4. Intervozes: https://intervozes.org.br

I. INTRODUCTION

1. The Brazilian government was considered an international reference for the protection of rights in the digital environmental with its adoption of a Civil Rights Framework for the Internet in 2014. It took on a central role in promoting international standards for privacy in the digital age. However, at a national level, guaranteeing these rights faces serious limitations that over the last five years have undermined the exercise of other fundamental rights – a situation that worsened during the COVID-19 pandemic in 2020 and 2021.
2. This submission focuses on Brazil's fulfilment of human rights obligations in the digital context and seeks to strengthen recommendations focused on guaranteeing universal access to the internet in order to enable free expression and association; access to information, knowledge and culture; and the exercise of economic and social rights in a manner that is secure, respectful of privacy and autonomy, and free of any kind of discrimination. It is divided as follows: introduction; economic, social and cultural rights; civil and political rights; and recommendations to the Brazilian state.

II. ECONOMIC AND SOCIAL RIGHTS

Internet access

3. Access to the internet is increasingly essential for exercising rights. This became evident during the COVID-19 pandemic in 2020 and 2021, when the majority of activities for school, work and government services began to take place online. Data from 2020 indicate that 83% of Brazilian households had some kind of internet access and 81% of the population 10 years of age and older had network access. The proportion of households with access to a computer in that year was 45%.[1]
4. In Brazil, inequalities in internet access reproduce structural inequalities. When it comes to populations in vulnerable conditions, the situation is worrying: barely 30% of Brazilians in socioeconomic classes D/E had used a computer once in their lifetime, while the numbers are much higher for classes C (66%), B (91%) and A (88%). Inequality is also seen when analysing racial aspects: only 52% of Indigenous people and 57% of Black people had used a computer at least once in their lifetime. Among white people, the rate is 64%.[2] The kind of device used to access the internet is another indicator of inequality: 62% of Indigenous people and 60% of Black people used the network exclusively on their mobile phone, at a rate higher than that of white people (48%). When combined with the socioeconomic class perspective, that inequality worsens even further: 90% of people in classes D/E have only a mobile phone as a means for internet use, a yawning gap from the rest: 58% in class C, 25% in class B and 11% in class A.[3] Access inequalities are also territorial and are related to an uneven distribution of infrastructure: in urban areas, 86% of households have internet access whereas in rural areas, this rate is just 65%.[4]
5. When it comes to traditional peoples and communities and rural populations, the right to internet access, recognised by the Brazilian Civil Rights Framework for the Internet[5], is far from respected.[6] The majority of these populations connect using limited mobile phone data plans, which offer a limited number of applications, particularly social network platforms, under zero-rating agreements. Connection costs consume over 30% of the monthly income of families surveyed, according to data from the Coletivo Intervozes.

Right to education

6. In the face of the spread of COVID-19, the Brazilian government implemented urgent measures so students could continue their learning process despite the limitations imposed by restrictions on movement and isolation of the population. Lack of planning and structure in the policies adopted added to the precariousness of families' internet access, affected the success of these measures and resulted in school absenteeism rates that represented an increase of nearly 200% in the five-to-nine-year-old segment between 2019 and 2020.[7]
7. A survey by the National Institute for Educational Research and Study (INEP) showed the impact of the digital divide on access to education in rural areas: two million students in rural schools spent all of 2020 without access to digital content,[8] and distributing printed materials was the only alternative found in several places. In eight of nine states in the Brazilian Northeast, more than 20% of rural schools operated exclusively in this manner for the whole period of physical distancing.[9]
8. Where adopted, internet access policies for students in the public education system were inadequate and poorly focused on household connectivity, which led to the disconnection of numerous families, seriously hampering access to education during the pandemic. Again, structural inequalities are reproduced: official data indicate that Black and Indigenous children and young people in public schools represent more than 70% of students without household broadband or 3G/4G internet access.[10] The situation exacerbated the situation of inequality between an elite student body with internet access in appropriate conditions for continuing their studies and the majority of students in the public school system, who have only minimal internet connections through mobile internet plans and equipment that was inadequate for meaningful participation in everyday school life.[11]

Right to health

9. The right to health was affected by limitations on internet access, as well as by risks to privacy and data protection represented by the digitalisation of services and, in particular, by monitoring and control policies implemented in the context of the COVID-19 pandemic.
10. At the federal, state and municipal levels, partnerships between governments and private enterprise were developed to promote monitoring of the spread of cases or compliance with the social isolation measures applied. They involved the localisation of individuals using different technologies, such as geolocation or connection to cellular networks, but they displayed few safeguards and were not preceded by public debates and human rights impact studies that could have enabled the prevention of abuses. In addition to exposure to public and private surveillance systems, some solutions carried risks of re-identification of individuals, with a significant potential for discrimination.[12]
11. Applications created to offer access to official information on COVID-19 prevention and treatment measures, as well as for assistance in monitoring its spread (such as Coronavírus SUS, launched in 2020 by the federal government), also failed to offer sufficient guarantees in terms of the sensitive personal data collected and data handling conditions, such as the storage period, third-party access restrictions, etc.[13,14]
12. Even during the pandemic, several episodes of leaks, wrongful exposure of personal data, system vulnerabilities, serious failures and lack of sensitive information security were confirmed in Brazil, indicating inadequate public policies for dealing with sensitive data collected by public authorities in the area of health.[15]

Digitalisation of the state and social security

13. Analysis of public policies related to social welfare rights reveals that there is neither transparency, adequate training of personnel nor impact reports on the use of personal data involved. The digitalisation of social policies and the lack of an adequate public policy for internet access and data protection impedes the enjoyment of social rights and can even impose new barriers to the exercise of other rights. One example was Emergency Aid, the income transfer programme to address the impact of the COVID-19 pandemic on the most vulnerable.[16] Another is the implementation of automated systems in the area of public policies without guarantees for transparency and participation or impact studies analysing potential risks to the exercise of rights, as in the case of the National Employment System (Sistema Nacional de Emprego, SINE).[17]
14. According to data from the TIC Domicílios household survey on ICT use, during the COVID-19 pandemic, only 39% of rural families sought health information on the internet and only 16% used online public services (in urban areas, the rates were 55% and 39%, respectively).[18] Black women, who primarily access the internet exclusively by mobile phone (67%), conducted fewer financial transactions (37%), and accessed fewer e-government services (31%) and courses (18%) than white men (51%, 49% and 30%, respectively).[19]
15. The lack of 3G/4G internet access on mobile phones was a reason for 39% of socioeconomic class C, D and E users to stop accessing public policies, such that 33% stopped accessing public services and 28% stopped receiving some social benefit, such as Emergency Aid.[20]

III. CIVIL AND POLITICAL RIGHTS

Privacy and data protection

a. Surveillance technologies, facial recognition and biometric databases

16. The use of surveillance technologies with facial recognition systems has been spreading in both public and private sectors in Brazil,[21] putting at risk the exercise of fundamental rights mainly by people in vulnerable situations, women, Black people, poor people and transsexual people.[22] Facial recognition has been used by the public sector for various purposes, such as public safety, urban transport, schools, management of social benefits, border control and identity verification.[23]
17. In terms of public safety, the Ministry of Justice and Public Safety issued two ordinances – in 2019 and 2020 – aimed at promoting the installation of surveillance cameras with facial recognition technologies by public safety agencies.[24] Although these dispositions are no longer in effect, they demonstrated the federal government's interest in using biometric data for such purposes.
18. In July 2021, the Federal Police announced the implementation of the Automated Biometric Identification Solution with the goal of combining databases from state public safety offices.[25] In that context, it is relevant to highlight that since 2018, Law 13.675/2018 has been in effect; this law set up the Single Public Safety System (Susp) and provided for the integration, among others, of genetic and digital profile databases.[26] At the same time, an increasing implementation of facial recognition tools applied to images gathered in public spaces or those open to the public in different Brazilian states has been identified.[27]

19. The use of facial recognition for public safety purposes generates enormous concern due to several factors: first, the Brazilian General Data Protection Law (LGPD, Law 13.709/2018) does not regulate the handling of data for public safety and criminal prosecution purposes, instead determining that a specific law should regulate the subject. In addition, there is a general lack of transparency that would enable civil society to adequately analyse whether these biometric technologies comply with minimum parameters of legality, necessity and proportionality.[28] There have also been multiple public complaints regarding the reproduction of racist biases in the implementation of these tools.[29]
20. Despite the lack of official data on the use of this kind of technology and its results, independent studies indicate that the vast majority of the population incarcerated based on facial recognition is Black.[30] In a survey from March to October 2019, 151 people were arrested in five states, of whom 90% are Black.[31]
21. In addition to public safety, facial recognition systems have been implemented in different spaces: it is being tested for identification of passengers boarding flights in airports[32], as well as in public schools[33] and public transportation, among others.
22. As declared by different international bodies, including the Office of the UN High Commissioner for Human Rights, facial recognition in public spaces presents grave risks to human rights. For this reason, High Commissioner for Human Rights Michelle Bachelet requested a moratorium on the use of this kind of technology in public spaces.[34]

b. Cybercrimes and criminalisation of human rights defence in the digital sphere

23. In December 2021, Brazil approved adhesion to the Budapest Convention on Cybercrime. The text was approved with no reservations by the Brazilian state and generates concerns related to the criminalisation of information security researchers and activists. This is because the text and the projected penalties are applied with no consideration for the presence of malicious intent in the case of hacking into computer systems. The risk is heightened in light of the absence of a robust framework for the protection of personal data in the criminal sphere[35] and a legislative tendency toward violating the safety of digital rights defenders.
24. This trend can be seen in the scope of the Democratic State Act, which recently replaced the country's National Security Act. In the preparation of the new law, questions were debated such as typifying the crime of espionage, without outlining any exceptions or assurances for the oversight work done by journalists and civil society that often relies on international press reports or whistleblowers to defend fundamental rights.[36] Debate around these measures decries the risk of criminalising activities related to information security and digital activism in the country, reproducing an internationally identified trend.[37]
25. Access to computer systems can lead to the discovery of and alert to relevant security failures and acquisition of information on human rights violations. The possibility of criminalising behaviour related to the latter case can discourage the disclosure of this information of critical public interest, principally considering that Brazil does not have comprehensive legislation to protect whistleblower activities.
26. As recently as 2015, the then UN Special Rapporteur on freedom of expression, David Kaye, highlighted that encryption and online anonymity are fundamental conditions for the exercise of freedom of expression.[38] Thus, measures precluding anonymity, as presented by the Brazilian constitution, should not be interpreted in ways that create a scenario where information security researchers and other online activists are unprotected or subject to constant surveillance, as some sections of the Budapest

Convention – approved by the country in its entirety – could suggest. The inclusion of barriers to the identification of people online is a legitimate posture according to international human rights standards and does not violate the preclusion of anonymity, among other motives, because it does not completely impede a later identification and attribution of responsibility, where necessary.

Freedom of expression, violence and access to information

a. Surveillance of journalists and human rights defenders

27. In recent years there has been a growing adoption of measures for cyber surveillance of the population conducted by agencies linked to the federal government and involving attempts to acquire espionage systems questioned by international human rights authorities. The Bureau of Integrated Operations (SEOPI), an agency linked to the federal government's Ministry of Justice and Public Safety, for example, used a public tender to procure an espionage system from the Harpia Tecnologia Eireli company; the procurement was suspended by the Federal Court of Auditors in November 2021.[39] Complaints also point to an alleged attempt at coordination for procuring the Pegasus system by Carlos Bolsonaro, son of the president of Brazil[40], despite the lack of legal standing to intervene in the administrative proceeding related to intelligence operations at the federal level, the exclusive domain of the Brazilian Intelligence Agency (ABIN). The press also informed of attempts to purchase other surveillance systems in 2022, among them the tool known as DarkMatter.[41]
28. In addition to the accusations of procuring surveillance systems with great potential for violating fundamental rights, the government has also been using OSINT (Open-Source Intelligence) in investigations conducted by State and Federal Public Prosecutors Offices without there being any corresponding regulation.[42] The practice opens space for potential human rights violations: in 2021, there were reports of the government keeping files on and classifying people based on their political positions, with the goal of monitoring based on political positions.[43] This kind of monitoring has already resulted in the arrest of one man due to information posted on his social network profile, content that was considered by the Military Police to be "incitement to violence" against the president.[44] The individual did not represent any organised group or entity and the surveillance was presumably based on his critical view of the current administration.
29. Another example of growing surveillance practices was the preparation of an "anti-fascist dossier" by the federal Ministry of Justice in 2020.[45] The report sought to map civil service workers who were against Bolsonaro, based on gathering information about these individuals available on social networks.[46] The Federal Supreme Court ruled to prohibit the preparation of the dossier in 2021.[47]

b. Online gender-based violence

30. In a country characterised by high rates of domestic and gender-based violence, digital media have also been increasingly used to attack women and LGBTIQA+ people. The modes of attack involve racist photomontages, hacking of social network accounts with racist and misogynist intent, threats, slander and false accusations, among others.[48]
31. During the pandemic, with the migration of a large share of activist group activities to the online context, complaints of attacks multiplied, along with hacking of meetings with shocking images and sounds, a phenomenon that became known as "zoombombing" because it initially occurred most frequently on the Zoom platform.[49]

32. In 2021, the SaferNet National Centre for Cybercrime Reporting in Brazil received 5,347 reports of LGBT-phobia, 6,888 reports of racism and 8,174 reports of violence and discrimination against women.[50]

c. Disinformation and violent political speech

33. Online gender-based violence is combined with political violence on different occasions in Brazil, e.g. when public authorities use their personal social networks to attack or retaliate against women journalists and activists. Likewise, President Jair Bolsonaro himself on different occasions exposed women journalists, questioning their motives, disseminating disinformation, making insinuations of a sexual nature and/or sharing personal data on women professionals who investigate reports of corruption involving the federal government or the president's family members, in an evident attack on their freedom of expression. One example involves statements regarding Constança Resende in 2019; on that occasion, the president shared an audio that was revealed to be false to imply bias in the journalist's work.[51] In 2018, account administrators for journalist Patrícia Campos Mello were also targets of attack after publishing a report by the journalist on possible illegalities in Bolsonaro's campaign.[52] These and other cases have been taken to the Inter-American Commission on Human Rights through hearings that took place in 2020.[53]
34. In 2018, during the presidential election campaign, various online attacks against political groups and journalists were confirmed. In September of that year, a Facebook group called "Mulheres contra Bolsonaro" [Women against Bolsonaro] was taken down and its moderators received direct attacks.[54]
35. Online political violence and disinformation also affect candidates and people elected to office and – in a society characterised by racism, homophobia and transphobia – it is even more intense in the case of members of historically socially vulnerable groups. A survey by TretAqui.org showed that machismo, ideological hatred, racism and LGBT-phobia were the main lines of attack against candidates in the first round of 2020 elections.[55]
36. The dissemination of misleading content has been directed toward attacking democratic institutions, seeking to undermine the population's confidence in elections. The damages of disinformation are significant for human rights and for democracy outside electoral periods as well. The dissemination of disinformation also occurs via public agents who actively contribute to the creation of a polarised, anti-democratic environment.[56]
37. Jair Bolsonaro, his family and other political actors who support them have been using social media platforms to mobilise and inflame their ultra-conservative base. The president has already been accused of practising hate speech and xenophobia due to attacks on minorities and marginalised groups, such as Black people, women and the LGBTIQA+ population.[57] The chief executive's posture on social networks resulted in the exclusion and blocking of certain content posted by Bolsonaro by the platforms themselves.[58]
38. Discussions concerning disinformation and violence in political speech also relate to the role of social media platforms and the lack of transparency in the curation and prioritisation of content, as evidenced by research carried out by Intervozes[59] and as highlighted with concern by organisations from the region.[60]

d. Legislative and judicial measures for regulating online speech

39. In recent years, several legislative initiatives have been proposed with the aim of responding to the challenges of digitalisation, such as the concentration of large digital

platforms, abusive policies related to the exploitation of personal data, and these same platforms' low level of response to the proliferation of hate speech on their networks. Many of bills proposed, despite seeking supposedly legitimate goals, ended up adopting ineffective and disproportionate mechanisms that could represent a real risk to the freedom of expression. Two important examples in the last five years were the attempts to legislate on the liability of intermediaries and disinformation.[61]

40. The rejection of filtering and blocking measures or the promotion of a legal notification system to hold intermediaries responsible for the content of third parties was established as a central bulwark for the guarantee of freedom of expression online. This is what the Brazilian Civil Rights Framework for the Internet provides for. The goal is to protect platforms and research mechanisms from undue liability for user behaviour and thus discourage the removal of content without a court order. However, recent challenges presented by the dissemination of harmful content over social networks, as well as an understanding of the role of large platforms in prioritising or not prioritising that content, have been generating new attempts at accountability. In the National Congress, in 2022 more than 30 projects were processed with the goal of combating disinformation. A portion of these target amending the Civil Rights Framework for the Internet on issues of privacy, freedom of expression and holding intermediaries accountable.
41. In 2021, Bolsonaro tried, through a Provisional Measure (MP 1.068), to incorporate new rules for moderating content by digital platforms and to change the legal regime set forth by the Civil Rights Framework. The change would require more bureaucracy to suspend or cancel accounts, in addition to defining the restitution of banned content, and it was presented in a context of legal pressure for the removal of abusive content shared by the president's supporters. The Provisional Measure – an executive order – is not the right mechanism for innovating regulation of this issue and it was sent back to the executive branch, losing its effectiveness. It became one more bill on the subject currently being debated in the National Congress.[62]
42. Bill (PL) 2630/2020, known as the "Fake News Bill", is also making its way through the legislature. Initially a source of concern due to its proposed control measures, the bill was revised and brings a series of stipulations related to regulating digital platforms and a provision requiring that the principles of public administration also be applied to the social network profiles of political agents.
43. Application blocking has also been a cause for concern debated since 2016 by the Federal Supreme Court, following a series of legal decisions that provided for access to message content, including by breaking end-to-end encryption. The ruling has been suspended since 2021.[63] In March 2022, Minister Alexandre de Moraes ruled to block the Telegram app throughout the country, setting daily fines of R$ 100,000 for any person who tried to use it.[64] The order was revoked three days later.[65] Blocking Telegram has also been proposed by the Superior Electoral Court due to the lack of response regarding the contribution of Brazilian authorities.[66]
44. Finally, the expansion of measures criminalising legitimate expression online continues to be an area of extreme concern. Measures contained in the previously mentioned Democratic State Act, for instance, broadly criminalise so-called "mass disinformation" or "insurrection" and "propagation of facts known to be untrue" and can deepen an environment of self-censorship that impacts not only freedom of expression, but also access to information.[67]

e. Access to information and personal data protection

45. The Brazilian state has had an Access to Information Law (LAI) since 2011, which has made possible over one million information requests to federal executive branch agencies and entities. Ten years after it was approved, however, repeated attempts at amending the LAI have been seen – especially using decrees and ordinances – and these have led to threats to transparency in the country. Among these attempts we highlight MP 928/2020, which tried, unsuccessfully, to impose the suspension of deadlines for responding to requests for access to information during the pandemic; Decree 9.690/2019, which tried to drastically increase the number of authorities with veto power over access to information; and Ordinance 880/2019, which makes the secrecy of documents produced by the Ministry of Justice and Public Safety more commonplace.
46. In addition, in recent years a broad and abusive interpretation of Article 31 of the LAI has increased; it refers to the handling and sharing of personal information, to justify the concealment of information of public interest in an obvious attack on the right to access. Analysis of these cases shows that the classification adopted runs counter to the purpose for which the LAI was issued: establishing transparency as the rule and secrecy as the exception. Data considered confidential pursuant to this rule include respecting the names of civil servants who post on the Bureau of Communication Twitter profile; data from the Palácio do Planalto access badges of the president's children; and the disciplinary proceedings that absolved a general and ex-health minister for having participated in a political demonstration alongside the president, among others. The above-mentioned LGPD, the data protection legislation approved in 2018, has also been wrongfully used as a pretext for denying access to public information.[68]
47. Counter to the purported attempt at personal data protection, in 2019 the government vetoed from the LGPD an important mechanism that targeted the prohibition on sharing the personal data of those requesting information from public institutions or private law legal entities.[69] Its aim was to protect the identity of people requesting information to avoid ungrounded denials of access, possible restrictions or retaliation/persecution.
48. The identified attacks on public transparency could make citizen oversight of government actions difficult and hinder the determination of eventual crimes of responsibility, e.g. in the handling of measures to face the pandemic, or the involvement of government agents in the preparation and dissemination of false information and hate speech on the internet. The actions mentioned subvert, on principle, the premise that guided the establishment and enactment of laws like the LAI and the LGPD: protecting ordinary people from the state, and not shielding the actions of powerful political agents from public scrutiny.

IV. SUMMARY OF RECOMMENDATIONS TO THE BRAZILIAN STATE

49. In light of the identified violations of the exercise of human rights in the digital environment in Brazil, their impact on the enjoyment of rights in the offline context, and consequently, the non-fulfilment of international commitments assumed by the country, including in the scope of the Sustainable Development Goals, we recommend to the Brazilian state:

A. The urgent creation of public policies for digital inclusion that contain a target plan prioritising populations in vulnerable conditions and which contemplate:

a. the universalisation of high-quality internet access;
b. broad-based participation of the population in processes for formulating, reviewing and evaluating connectivity policies, including rural populations and traditional peoples and communities;
c. education for digital media focused on the critical reception of content, communication practices based on human rights principles and digital security; and
d. the promotion of alternatives for connectivity, including community networks, with guaranteed free technical assistance in the territories of traditional people and communities.

B. The periodic production and dissemination of up-to-date data and statistics that are disaggregated by race, gender, age, locality and income on internet access in the country to guide public policy making, including possible emergency measures in contexts of social isolation in the areas of education, health and/or social welfare in order to avoid the worsening of pre-existing structural inequalities;

C. The urgent adoption of crosscutting measures to adapt public services to the requirements of the General Data Protection Law in terms of the rights of people who are owners of data processed by public authorities, including:

a. the guarantee that third parties involved in processing this data comply with the standards in force;
b. the guarantee of the integrity and correction of vulnerabilities found in government electronic systems, including of the Ministry of Health, as well as ensuring security policies, control of existing data and appropriate remedial measures in cases of leakage and wrongful exposure of personal data, in particular sensitive data; and
c. providing transparent information on the criteria for collecting, processing and sharing information and creating channels for resolving doubts and replying to requests related to personal data management.

D. The urgent adoption of measures to strengthen the independence of the national data protection authority so that it can oversee the compliance of public and private institutions with the rules set forth in the LGPD and offer guidelines regarding the interpretation of mechanisms established in the law.

E. The abstention from implementing digitalisation, automation or artificial intelligence policies in the public sector without having previously met the following requirements, which should also be contemplated in contexts of possible emergency:

a. impact studies ensuring that the policies do not lead to the exacerbation of historic inequalities, discrimination or risks to the exercise of human rights, including economic and social rights and privacy;
b. prior consultation processes that involve potentially affected groups and/or their representatives;
c. periodic independent and transparent monitoring and evaluation plans; and
d. explicit guarantees to citizens in relation to the exercise of the rights to review, reparation and non-recurrence of illegal acts.

F. The adoption of a moratorium limiting the use of facial recognition technologies in public spaces until international consensus is reached on the security of these technologies in relation to the fulfilment of human rights and the prohibition of their use for public safety purposes or for controlling access to government spaces or services.

G. The guarantee of respect for and adoption of norms that limit the use of surveillance technologies besides facial recognition to the principles of legality, necessity and proportionality established by human rights standards; establish legal redress mechanisms consistent with the obligation to provide effective remedy to victims of abuse; and create mechanisms that ensure public or community approval, supervision and monitoring of surveillance technology purchases.

H. The revocation, non-adoption or review of norms that enable online surveillance and the criminalisation of human rights and information security activists; and attention to the criteria of legality, necessity and proportionality in the implementation of any act of intervention in private communications, as set forth by international human rights frameworks ratified by Brazil.

I. The adoption of government norms and practices of respect for encryption and online anonymity as factors important to the exercise of human rights, as well as the guarantee of protection for those denouncing human rights violations, known as “whistleblowers”, through the drafting of specific legislation on the subject.

J. The creation of public policies and appropriate measures for combating all forms of gender-based violence, both online and offline.

K. The adoption of measures to combat the financing of disinformation campaigns with public resources, taking into account international human rights obligations and principles.

L. The rejection of abusive laws regulating content on social networks and messaging platforms that promote the liability of intermediaries, infringing the principles established in international human rights documents and the Brazilian Civil Rights Framework for the Internet. It is also recommended that the necessary regulation of large digital platforms be the product of broad-based, multi-sector debate, with all stakeholders, and which respects international human rights standards.

M. The adoption of measures to ensure respect for existing legislation regulating access to public information, without exploiting data protection to impede this access. Analysis of observance of the principles of legality, necessity and proportionality in restricting the right to privacy is also necessary for assessing public interest for information under state control.

V. REFERENCES

1. Cetic.br, 2020. Executive Summary: ICT Household Survey 2020. Available at: https://www.cetic.br/media/docs/publicacoes/2/20211124201635/executive_summary_ict_households_2020.pdf
2. Cetic.br, 2020. ICT Household Survey 2020. Available at: https://cetic.br/pt/tics/domicilios/2020/individuos/B1/.
3. Cetic.br, 2020. ICT Household Survey 2020. Available at: https://cetic.br/pt/tics/domicilios/2020/individuos/C16A/
4. Cetic.br, 2020. ICT Household Survey 2020. Available at: https://cetic.br/pt/tics/domicilios/2020/domicilios/A4/.
5. Marco Civil da Internet no Brasil, Lei n. 12.965/2014. Available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.
6. Intervozes, 2022. Territórios Livres, Tecnologias Livres. Available at: http://territorioslivres.online/.
7. Neri, M. & Osorio, M., 2022. Retorno para Escola, Jornada e Pandemia. Available at: https://www.cps.fgv.br/cps/RetornoParaEscola/.
8. Intervozes, 2022. Territórios Livres, Tecnologias Livres. Available at: http://territorioslivres.online/.
9. Intervozes, 2022. Territórios Livres, Tecnologias Livres. Available at: http://territorioslivres.online/.
10. IPEA, 2020. Nota técnica n. 88. Acesso domiciliar à internet e ensino remoto durante a pandemia. Available at: http://repositorio.ipea.gov.br/bitstream/11058/10228/1/NT_88_Disoc_AcesDomInternEnsinoRemoPandemia.pdf.
11. Nogueira, J., 2021. Acesso à internet residencial de estudantes. Available at: https://idec.org.br/arquivos/pesquisas-acesso-internet/idec_pesquisa-acesso-internet_acesso-a-internet-residencial-dos-estudantes.pdf.
12. Venturini, J. & Souza, J. Tecnologias e Covid-19 no Brasil: vigilância e desigualdade na periferia do capitalismo. Available at: 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.
13. 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. Available at: https://www.alsur.lat/sites/default/files/2021-06/Informe%20Observatorio%20Covid-19%20del%20Consorcio%20Al%20Sur(2).pdf.
14. Hernández, L. (2021). Uso de Tecnologías para el combate de la pandemia. Datos personales en América Latina. Available at: https://globalnetworkinitiative.org/wp-content/uploads/2021/11/COVID19-LAC-SPA.pdf.
15. OKBR, 2020. Ministério da Saúde já havia deixado dados pessoais expostos no próprio sistema da Covid-19 em junho; aqui está a prova. Available at: https://ok.org.br/noticia/ministerio-da-saude-ja-havia-deixado-dados-pessoais-expostos-no-proprio-sistema-da-covid-19-em-junho-aqui-esta-a-prova/.
16. InternetLab. O Auxílio Emergencial no Brasil: desafios na implementação de uma política de proteção social datificada. (Report not yet published.)

17. Fernanda Bruno, Paula Cardoso e Paulo Fatay. Sistema Nacional de Emprego e a gestão automatizada do desemprego. Available at: https://ia.derechosdigitales.org/wp-content/uploads/2021/04/CPC_informe_BRASIL.pdf.
18. Cetic.br, 2020. Executive Summary: ICT Household Survey 2020. Disponível em: https://www.cetic.br/media/docs/publicacoes/2/20211124201635/executive_summary_ict_households_2020.pdf
19. Cetic.br, 2020. Executive Summary: ICT Household Survey 2020. Available at: https://www.cetic.br/media/docs/publicacoes/2/20211124201635/executive_summary_ict_households_2020.pdf
20. Idec & Locomotiva, 2021. Barreiras e limitações no acesso à internet e hábitos de uso e navegação na rede nas classes C, D e E. Available at: https://idec.org.br/sites/default/files/versao_revisada_pesquisa_locomotiva.pdf.
21. Souza, M. R. & Zanatta, R. A. F., 2021 The Problem of Automated Facial Recognition Technologies in Brazil: Social Countermovements and the New Frontiers of Fundamental Rights. Available at: https://revistas.ufg.br/lahrs/article/view/69423.
22. Silva, Mariah Rafaela, 2022. Orbitando telas: Tecnopolíticas de segurança, o paradigma smart e o vigilantismo de gênero em tempos de acumulação de dados. Available at: https://sur.conectas.org/orbitando-telas/; Coding Rights, 2021. Reconhecimento Facial no Setor Público e Identidades Trans. Available at: https://codingrights.org/docs/rec-facial-id-trans.pdf.
23. Reis, C. et al, 2021. Relatório sobre o uso de tecnologias de reconhecimento facial e câmeras de vigilância pela administração pública no Brasil: versão resumida. Available at: https://lapin.org.br//download/4141/.
24. Biblioteca Digital do Ministério da Justiça e Segurança Pública. Portaria nº 793, of October 24, 2019. Available at: <https://dspace.mj.gov.br/handle/1/1380>; Portaria nº 630, of November 27, 2020. Available at: <https://dspace.mj.gov.br/handle/1/2367>.
25. Coalizão Direitos na Rede, 2021. OFÍCIO PARA ANPD | Entidades solicitam medidas contra solução automatizada de identificação biométrica da Polícia Federal. Available at: https://direitosnarede.org.br/2021/07/19/oficio-para-anpd-entidades-solicitam-medidas-contra-solucao-automatizada-de-identificacao-biometrica-da-policia-federal/.
26. Lei 13675/2018. Available at: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13675.htm.
27. Folha de S. Paulo. Sob críticas por viés racial, reconhecimento facial chega a 20 estados. Available at: https://www1.folha.uol.com.br/cotidiano/2021/07/sob-criticas-por-vies-racial-reconhecimento-facial-chega-a-20-estados.shtml.
28. Consórcio Al Sur. Reconocimiento facial en América Latina Tendencias en la implementación de una tecnología perversa. Available at: https://estudio.reconocimientofacial.info/reports/ALSUR-Reconocimiento_facial_en_Latam-ES.pdf.
29. Revista Piauí, 2021. Nos erros do reconhecimento facial, um “caso isolado” atrás do outro. Available at: https://piaui.folha.uol.com.br/nos-erros-de-reconhecimento-facial-um-caso-isolado-atras-do-outro/.
30. Monitor do reconhecimento facial no Brasil. Available at: https://opanoptico.com.br/.
31. Folha de S. Paulo, 2019. 151 pessoas são presas por reconhecimento facial no país; 90% são negras. Available at: https://www1.folha.uol.com.br/cotidiano/2019/11/151-pessoas-sao-presas-por-reconhecimento-facial-no-pais-90-sao-negras.shtml.
32. INFRAERO. Aeroporto de Congonhas testa embarque por reconhecimento facial com tripulantes. Available at: https://www4.infraero.gov.br/imprensa/noticias/aeroporto-de-con-

gonhas-testa-embarque-por-reconhecimento-facial-com-tripulantes/; SERPRO. Embarque nos aeroportos brasileiros poderá ser realizado sem apresentação de documentos. Available at: https://www.serpro.gov.br/menu/noticias/noticias-2020/embarque-biometria-serpro-1.

33. G1, 2017. Escolas municipais de Jaboatão adotam reconhecimento facial para controlar frequência de alunos. Available at: https://g1.globo.com/pernambuco/noticia/escolas-municipais-de-jaboatao-adotam-reconhecimento-facial-para-controlar-frequencia-de-alunos.ghtml.
34. See: https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session48/Documents/A_HRC_48_31_AdvanceEditedVersion.docx
35. Lapin, 2021. Histórico da LGPD Penal: o que foi feito até aqui e quais são os próximos passos? Available at: https://lapin.org.br/2021/04/16/lgpd-penal-o-que-foi-feito-ate-aqui-e-quais-sao-os-proximos-passos/.
36. Coalizão Direitos na Rede. A Internet e as propostas de Lei de Defesa do Estado Democrático de Direito. Available at: https://direitosnarede.org.br/2021/04/16/a-internet-e-as-propostas-de-lei-de-defesa-do-estado-democratico-de-direito/.
37. Access Now, 2021. La persecución de la comunidad infosec en América Latina. Available at: https://www.accessnow.org/cms/assets/uploads/2021/08/persecusion-latam-seguridad-digital.pdf.
38. Artigo 19, 2015. Criptografia e anonimato são essenciais para liberdade de expressão. Available at: https://artigo19.org/2015/06/01/criptografia-e-anonimato-sao-essenciais-para-liberdade-de-expressao/.
39. UOL. "TCU suspende pregão para a compra de sistema espião pelo governo Bolsonaro." Available at: https://noticias.uol.com.br/politica/ultimas-noticias/2021/11/11/tcu-suspensao-compra-governo.htm. Accessed March 2022.
40. IstoÉ, 2021. Além do Pegasus, Carlos Bolsonaro queria outra ferramenta para espionagem dentro do governo. Available at: https://istoe.com.br/alem-do-pegasus-carlos-bolsonaro-queria-outra-ferramenta-para-espionagem-dentro-do-governo.
41. UOL, 2022. Gabinete do ódio busca comprar nova ferramenta espiã intitulada DarkMatter. Available at: https://noticias.uol.com.br/politica/ultimas-noticias/2022/01/17/gabinete-do-odio-usou-viagem-de-bolsonaro-para-negociar-sistema-espiao.htmOSINT/
42. MPPE. Curso de Inteligência e Investigação em Fontes Abertas - OSINT. Available at: https://www.mppe.mp.br/mppe/institucional/escola-superior/ultimas-noticias-escola-superior/15370-curso-de-inteligencia-e-investigacao-em-fontes-abertas-osint; Twitter.MPF. Available at: https://twitter.com/oea_cyber/status/1174752582583181313.
43. The Intercept, 2021. Governo Bolsonaro deturpou edital de Dilma para fichar 'detratores' na internet. Available at: https://theintercept.com/2021/07/07/governo-bolsonaro-deturpou-edital-de-dilma-para-fichar-detratores-na-internet/.
44. G1, 2021. Jovem é preso em flagrante após publicação sobre visita de Bolsonaro a Uberlândia. Available at: https://g1.globo.com/mg/triangulo-mineiro/noticia/2021/03/04/jovem-e-preso-apos-publicacao-sobre-vinda-de-bolsonaro-a-uberlandia.ghtml.
45. G1, 2020. Ministério entrega a comissão do Congresso material com suposto dossiê de opositores do governo. Available at: https://g1.globo.com/politica/noticia/2020/08/11/ministerio-entrega-a-comissao-do-congresso-material-com-suposto-dossie-de-opositores-do-governo.ghtml.
46. Conjur, 2020. Dossiê de antifascistas entregue aos EUA cita jornalistas e professores. Available at: https://www.conjur.com.br/2020-ago-17/dossie-antifascistas-entregue-aos-eua-cita-jornalistas-professores.

47. G1, 2020. STF decide suspender produção de dossiê sobre antifascistas pelo Ministério da Justiça. Available at: https://g1.globo.com/politica/noticia/2020/08/20/stf-forma-maioria-para-proibir-ministerio-da-justica-de-produzir-dossie-contra-antifascistas.ghtml.
48. Coding Rights; InternetLab, 2017. Violências contra mulher na internet: diagnóstico, soluções e desafios. Contribuição conjunta do Brasil para a relatora especial da ONU sobre violência contra a mulher. Available at: https://www.internetlab.org.br/wp-content/uploads/2017/11/Relatorio_ViolenciaGenero_ONU.pdf.
49. Perifericas; Gig@ UFBA, 2021. Diálogos feministas sobre a violência digital de gênero no Brasil durante a pandemia de COVID-19 no ano de 2020. Available at: https://perifericas.netlify.app/posts/lancamento-de-publicacao-sobre-violencia-digital-de-genero-e-covid-19-no-brasil-em-2020/.
50. See: https://indicadores.safernet.org.br/
51. The Media Today. Brazil's Bolsonaro smears reports investigating his son. March 12, 2019. Available at: https://www.cjr.org/the_media_today/bolsonaro_twitter_press_threats.php.
52. Folha de S. Paulo, 2018. Folha pede que Polícia Federal investigue ameaças a profissionais. Available at: https://www1.folha.uol.com.br/poder/2018/10/folha-pede-que-policia-federal-investigue-ameacas-a-profissionais.shtml.
53. Intervozes, 2020. Governo Bolsonaro promove desinformação e acusa organizações da sociedade civil de censura na CIDH. Available at: https://intervozes.org.br/violencia-e-divergencia-de-opiniao-e-desinformacao-e-liberdade-de-expressao-afirma-governo-na-cidh/.
54. El País, 2018. Grupo "Mulheres contra Bolsonaro" no Facebook sofre ataque cibernético. Available at: https://brasil.elpais.com/brasil/2018/09/14/politica/1536941007_569454.html.
55. See: https://www.tretaqui.org.
56. Intervozes, 2020. Governo Bolsonaro promove desinformação e acusa organizações da sociedade civil de censura na CIDH. Available at: https://intervozes.org.br/violencia-e-divergencia-de-opiniao-e-desinformacao-e-liberdade-de-expressao-afirma-governo-na-cidh/; Carta Capital, 2021. PF sugere que Bolsonaro seja investigado por desinformação sobre urna eletrônica. Available at: https://www.cartacapital.com.br/politica/pf-sugere-que-bolsonaro-seja-investigado-por-desinformacao-sobre-urna-eletronica/.
57. Carta Capital, 2019. Jair Bolsonaro traz discurso de ódio como fala oficial da Presidência. Available at: https://www.cartacapital.com.br/opiniao/jair-bolsonaro-traz-discurso-de-odio-como-fala-oficial-da-presidencia/; Brasil de Fato, 2020. Bolsonaro pratica xenofobia ideológica com o veto à Sinovac. Available at: https://www.brasildefato.com.br/2020/10/25/bolsonaro-pratica-xenofobia-ideologica-com-o-veto-a-sinovac; Folha de S. Paulo, 2019. Termo 'paraíba' usado por Bolsonaro reflete preconceito ao Nordeste, e cabe punição. Available at: https://www1.folha.uol.com.br/poder/2019/07/termo-paraiba-usado-por-bolsonaro-reflete-preconceito-ao-nordeste-e-cabe-punicao.shtml.
58. UOL, 2021. Facebook e Instagram publican un aviso de información falsa en la publicación de Bolsonaro. Available at: https://www.uol.com.br/tilt/noticias/redacao/2021/04/29/facebook-instagram-informacao-falsa-bolsonaro.htm; UOL, 2020. Instagram oculta publicación de Bolsonaro sobre covid-19: 'Información falsa'. Available at: https://noticias.uol.com.br/saude/ultimas-noticias/redacao/2020/05/11/instagram-tira-do-ar-post-de-bolsonaro-sobre-covid-19-informacao-falsa.htm; EXAME, 2020. Após Twitter, Facebook e Instagram eliminan publicaciones de Bolsonaro. Available at: https://exame.com/brasil/apos-twitter-facebook-e-instagram-removem-posts-de-bolsonaro/; G1, 2021. YouTube remove live de Bolsonaro com mentira sobre vacina da Covid e Aids

e suspende canal por uma semana. Available at: https://g1.globo.com/tecnologia/noticia/2021/10/25/youtube-live-bolsonaro.ghtml.

59. Intervozes, 2021. Fake news: how platforms face disinformation. Available at: https://intervozes.org.br/publicacoes/fake-news-how-platforms-combat/.
60. Several, 2021. Declaración Latinoamericana sobre Transparencia de Plataformas de Internet. Available at: https://intervozes.org.br/wp-content/uploads/2021/11/Declaracio%CC%81n-Latinoamericana-sobre-Transparencia-de-Plataformas-de-Internet.pdf.
61. Intervozes, 2021. Fake News: como as plataformas enfrentam a desinformação. Available at: https://intervozes.org.br/publicacoes/fake-news-como-as-plataformas-enfrentam-a-desinformacao/.
62. Conjur, 2021. MP 1.068, regulação de conteúdo em redes sociais e livre iniciativa. Available at: https://www.conjur.com.br/2021-set-21/opiniao-mp-1068-regulacao-conteudo-redes-sociais.
63. Conjur, 2020. Segundo Rosa, marco civil da internet não permite que WhatsApp seja suspenso. Available at: https://www.conjur.com.br/2020-mai-27/rosa-marco-civil-internet-nao-permite-whatsapp-seja-suspenso.
64. STF, 2022. Ministro Alexandre de Moraes suspende funcionamento do Telegram no Brasil. Available at: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=483659&ori=1.
65. STF, 2022. Ministro Alexandre de Moraes revoga bloqueio após Telegram cumprir determinações do STF. Available at: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=483712&ori=1.
66. Tecmundo, 2022. TSE quer banir Telegram durante eleições para combater fake news. Available at: https://www.tecmundo.com.br/mercado/232304-tse-quer-banir-telegram-durante-eleicoes-combater-fake-news.htm.
67. Coalizão Direitos na Rede. A Internet e as propostas de Lei de Defesa do Estado Democrático de Direito. Available at: https://direitosnarede.org.br/2021/04/16/a-internet-e-as-propostas-de-lei-de-defesa-do-estado-democratico-de-direito/.
68. See: https://www.transparencia.org.br/downloads/publicacoes/lgpd_reforco_respostas_negativas_dez_2021.pdf.
69. Artigo 19, 2019. Entre vetos preocupantes, Presidência tenta derrubar proteção de dados pessoais de requerentes de informação pública. Available at: https://artigo19.org/2019/07/10/entre-vetos-preocupantes-presidencia-tenta-derrubar-protecao-de-dados-pessoais-de-requerentes-de-informacao-publica/.