Internet Sectoral Overview

Number 4
December, 2021
Year 13

Privacy and data protection during the pandemic

Personal data protection during the COVID-19 pandemic: new paradigms for data sharing and the secondary use of data in the public sector[1]

By Miriam Wimmer[2]

The spread of the novel coronavirus throughout the world has led to the rapid creation of strategies to monitor and halt it. Two important aspects can be identified in governmental initiatives to combat the pandemic: on one hand, the unprecedented intensity of use of digital technologies and mobile communication devices in detection, reporting, and investigation of the disease; on the other hand, the rapid increase in the collection, analysis, and sharing of personal data between public and private actors, as well as between different government agencies and entities.

In Brazil, such events rekindled the debate about the limits and possibilities of processing personal data in the public sector, as well as the discussion about the criteria for data sharing and secondary uses, that is, the use of personal data for purposes distinct from those that justified its original collection. The topic is controversial, because personal data protection regulations in general include the idea that data processing must be carried out according to the specific purposes informed to data subjects, without the possibility, as a rule, to carry out subsequent processing that is incompatible with the purposes initially established. Known as the principle of purpose limitation, this rationale was also acknowledged in the Brazilian legislation on personal data protection.[3]

Although the theme of personal data sharing involving the public sector had already been dealt with by the Brazilian Supreme Court (STF), 2020 was a year characterized by a more matured debate by the legal body, with the recognition of a new fundamental right to personal data protection[4] and the application of that understanding in a subsequent judgment on data sharing within the Executive branch. Given this scenario, considering the intensified use of personal data resulting from the COVID-19 pandemic and recent manifestations of the STF on the theme, this paper investigates possible criteria and parameters able to legitimately validate the sharing and the secondary use of personal data in the public sector, with reference to the interpretation of the principle of purpose limitation.

---

[1] Edited version of the article "Limites e possibilidades para o uso secundário de dados pessoais no poder público: lições da pandemia," originally published in the journal Revista Brasileira de Políticas Públicas, vol. 11, No. 1 (2021). Available at: https://www.publicacoes.uniceub.br/RBPP/article/view/7136

[2] PhD in Communications from the University of Brasília (UnB) and master's degree in Public Law from Rio de Janeiro State University (UERJ); she is a professor of the Faculty of Law at the Brazilian Institute of Education, Development, and Research (Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa – IDP) in Brasilia.

[3] According to article 6, Subparagraph I, of Law No. 13709, from 2018: "purpose: processing done for legitimate, specific and explicit purposes of which the data subject is informed, with no possibility of subsequent processing that is incompatible with these purposes." Available at: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

[4] Although the Federal Constitution already recognized and ensured the protection of intimacy and private life, in 2020 the STF acknowledged a fundamental right to personal data protection, which transcends this precept. The right to data protection does not only refer to intimate or private data, nor can be confused with the right to confidentiality. It is grounded on the idea of informational self-determination, with basis on the fundamental right to human dignity.

Photo: Diego Canabarro

Miriam Wimmer
Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP).

The COVID-19 pandemic and data sharing in the public sector: initiatives and reactions

An undisputed consequence of the COVID-19 pandemic was the increased sharing of personal data. Globally, the initiatives taken to fight the health crisis made a significant use of technological tools to monitor, halt, and mitigate the spread of the virus. Given the technical possibility of using geolocation data from mobile terminals, several countries created "heat maps" from anonymized and aggregated data, in order to identify locations with agglomeration of people, observe patterns of displacement, and estimate the level of social isolation of their populations. Other strategies were also adopted to control the observance of quarantine by infected people or those with suspected infection. Besides that, in many cases contact-tracing apps were deployed, using Bluetooth signal emissions.

This phenomenon could also be observed in Brazil. Several states of the federation entered into agreements with technology companies and telecommunications service providers to monitor social isolation rates and define strategies to combat the virus, based on the analysis of anonymized and aggregated location data. Legal challenges to such measures were ultimately not successful, because in these cases, the Judiciary branch understood there was no risk to citizen rights given that they were not individually identifiable.

However, the impacts of the global pandemic regarding the escalation in the collection, analysis, and sharing of personal data were not strictly limited to actions taken to fight COVID-19. In fact, the health crisis forced the sudden migration of numerous activities to the digital environment; and the acceleration of digital transformation projects that were already underway. Such changes intensely affected the public sector and compelled public officials to intensify efforts to digitalize public services, in order to continue carrying out legal responsibilities.

In Brazil, digital government initiatives had been developed for years. There is no doubt, nonetheless, that the pandemic imposed a new rhythm and sense of urgency to digital transformation, including on account of the need to enable the payment of the emergency aid instituted by Law No. 13982 of 2020.[5] As expected, the migration of services and processes to the digital environment was accompanied by the growing demands for collection, analysis, sharing, and merging of personal data within the public sector.

In this context, the implementation of technological solutions to fight COVID-19 was received with caution by entities dedicated to personal data protection, including many legal challenges. Data Protection Authorities from various European countries and the European Data Protection Board (EDPB)[6] indicated that there was no incompatibility between personal data protection and measures to combat the pandemic. The European normative framework was flexible enough to ensure the possibility of sharing relevant data to effectively fight the sanitary emergency. On the other hand, they stressed the importance of ensuring that the use of personal data was adequate, necessary and proportionate, in order to limit the tools adopted to their specific purpose

[5] The Law in question instituted exceptional social protection measures to be adopted during the pandemic, including the payment of financial aids, at the amount of BRL 600, for three months, to low-income citizens.

[6] In April 2020, the organization, which brings together representatives of data protection from European countries, adopted "Guidelines 4/2020 on the use of location data and means of contact tracing within the context of COVID-19." Available at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

and strictly necessary period, excluding the possibility of subsequent processing of the data collected for purposes unrelated to the health crisis management.

However, when it comes to initiatives dedicated to accelerating the migration of routine public services and processes to the digital environment – an indirect result of the pandemic –, the discussion takes on different nuances. In fact, the digital transformation of government services is usually defined as a "point of no return." Thus, elements such as the limitation of personal data processing to the pandemic period, and the use of these data only for the specific purpose of fighting COVID-19 are open to question, especially when considering that the data collected and its sharing can be useful for other public purposes, different from those that justified the original processing of data.

Renewing paradigms: a new fundamental right and the recognition of limits on personal data flows in the public sector

The demands for personal data sharing associated with the COVID-19 pandemic eventually precipitated a judicial discussion of the issue in the STF, with lasting impacts for personal data protection in Brazil. The STF had previously examined cases involving data sharing between governmental bodies, albeit more superficially. However, the most important case was certainly the decision to suspend the effects of the Provisional Measure No. 954, from 2020, which determined the sharing of data held by telecommunications service providers with the Brazilian Institute of Geography and Statistics (IBGE) for official statistical production.

Given the impossibility of conducting interviews in person due to the health crisis, IBGE decided to carry out the activities by telephone. For that reason, it needed to have access to a reliable and sufficiently representative telephone database. Thus, the referred Provisional Measure was edited, defining that, within the context of the urgent health crisis, telecommunication companies offering fixed and mobile services should provide electronically the names, phone numbers, and addresses of their consumers to IBGE, whether private individuals or legal entities. Despite several precautionary measures established by the Provisional Measure, it was promptly challenged by five Direct Unconstitutionality Actions (ADIs),[7] filed by different political parties and by the Federal Council of the Brazilian Bar Association (OAB).

The trial became paradigmatic, because, when arguing about the unconstitutionality of the Provisional Measure, the STF articulated the idea of an autonomous fundamental right to personal data protection, derived from the right to human dignity and based on the idea of informational self-determination (Mendes, 2020). The discussions held throughout the trial also addressed the fact that the new purpose of the personal data processing had not been sufficiently specified. As can be seen in the Decision, the STF understood that, by not appropriately defining how and for which purposes the collected data from telecommunication operators would be used, the Provisional Measure did not allow the consideration of the adequacy and necessity of the sharing of the

The demands for personal data sharing associated with the COVID-19 pandemic eventually precipitated a judicial discussion of the issue in the STF, with lasting impacts for personal data protection in Brazil.

[7] Legal action that seeks a decision declaring the incompatibility of certain legislation with the Federal Constitution. The competence to judge such actions rests with the STF.

(...) despite the generally meritorious and legitimate objectives for the sharing and secondary use of personal data in the public sector, the concrete form of (re)use of data can give rise to negative consequences (...)

data in question. In other words, STF stated that it was not possible to assess "the compatibility of data processing with the informed purposes and their limitation to what is strictly necessary to reach its purposes".[8]

Although the STF highlighted the insufficient specification of the purpose of data sharing in the Provisional Measure, the court decision did not further develop the analysis regarding a possible incompatibility of purposes arising from the secondary use of data. Even so, by stating that violations to rights associated to the protection of personal data are enforceable in view of the Federal Constitution, the court laid the foundations for a more detailed assessment of the theme in a subsequent trial that involved sharing the National Traffic Department (Denatran) databases with the Brazilian Intelligence Agency (ABIN).

In this second case, even though the act authorizing data sharing was revoked before the trial, the vote of the Justice Rapporteur made numerous references to the problem of changing the purpose of data processing. The understanding that there is not an unrestricted permission in the Brazilian legal system to the free flow and sharing of data in the public sector was noted. In addition, it was highlighted that the principle of purpose limitation in these relations must consider elements such as: (i) the reasonable expectations[9] of the data subjects; (ii) the nature of the data in question; and (iii) the possible harms to be borne by the subjects.

Risks and benefits of secondary use of personal data in the public sector

The STF decisions have rekindled the debate about the benefits and risks of the collection, analysis, and sharing of personal data between the private and public sectors, as well as between different governmental bodies and entities. This discussion raises two perspectives that are difficult to reconcile. The first states that extensive data sharing allows the provision of better public services, efficiency, and reduced bureaucracy, beyond fighting frauds in the distribution of social and fiscal benefits. On the other hand, a second perspective highlights the risks resulting from these initiatives.

Through the prism of personal data protection, it must be considered that, despite the generally meritorious and legitimate objectives for the sharing and secondary use of personal data in the public sector, the concrete form of (re)use of data can give rise to negative consequences resulting from the breach of trust between data subjects and the organization that collected such data, the frustration of the expectations of subjects regarding the data processing that justified given collection, and the sense of insecurity in relation to how personal data will be used in the future (Solove, 2006).

There are even more complex issues related to institutional design, associated, on the one hand, with increased risks of moral or material damages, due to the expanded exposure and flow of data; on the other hand, due to the possibility of an undesirable imbalance of social or institutional power, given an inadequate distribution of information about individuals among public bodies with different attributions. In Brazil, there is a considerable uncertainty around the matter, since

[8] Available at: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754358567

[9] Personal data processing which individuals can reasonably expect to be conducted, considering the context of processing and the nature of the relationship between parties.

the Brazilian General Data Protection Law (LGDP)[10] merely states that the shared use of personal data by the public sector must meet the specific purposes of public policies execution and the legal attribution by bodies and entities, respecting the principles of personal data protection, established by the same Law (Article 26).

Although the LGPD does not detail how the principles of personal data protection can impact the flow of data within the State, the debate on the sharing and the secondary use of personal data is strongly linked to the interpretation of the principle of purpose limitation, fundamental to the norms of personal data protection, also present in the LGPD. As mentioned, this principle can establish important restrictions on the secondary use of personal data, given that it conditions data processing to the specific purposes informed to data subjects, without the possibility of subsequent data processing that is incompatible with those purposes.

Based on this meaningful principle, many legal scholars argue that the State must not be understood as an "informational unit," that is, an environment of unimpeded flow of information about citizens. On the contrary, data sharing between public bodies must consider the need for personal data to be processed in accordance with the responsibilities of the legal body and with the specific purpose that justified their collection (Simitis, 1987). On the other hand, the principle of purpose limitation does not mean an absolute impediment to the secondary use of personal data, but requires the new purpose to be, as a rule, compatible with the original purpose.

The idea of "compatibility" is certainly extremely broad, requiring further elaboration in the academic and legal fields in Brazil. In this line of reasoning, as indicated by Doneda and Viola (2009), in a paper published almost a decade before the approval of the LGPD, compatibility between the purpose of collection and the use of personal data can be verified through the application of the principle of proportionality. In concrete cases, this allows the assessment of whether: (i) the use of data is abusive; (ii) such secondary use exceeds the limits reasonably considered by the subjects when providing such data; and (iii) there are relevant interests that suggest the need for elasticity and tolerance in relation to wider uses of personal data.

Some additional parameters can be deduced from the European experience. The General Data Protection Regulation,[11] for example, establishes that, for archival purposes of public interest, statistical purposes, and scientific or historical research purposes, subsequent processing is not considered incompatible with the initial purposes. For other cases, it defines criteria that allow evaluating the compatibility of processing personal data for a purpose other than the original. They are: the existence of any link between the original and the new purposes; the context in which personal data were collected, especially regarding the relationship between the data subject and the organization that carries out or determines data processing; the nature of personal data; the possible consequences of further processing data for the subject; and the existence of appropriate safeguards, which may include encryption or pseudonymization.[12]

Data protection authorities have, on several occasions, stated that the compatibility of purposes is a condition for the secondary use of personal data, emphasizing the need to meet reasonable expectations of individuals as to how their personal data are processed and shared. In Brazil, Bioni (2019) uses the idea of contextual privacy to reflect on the theme. According to the author, the elasticity of the concept, supported by the legitimate expectations of the data subjects regarding the contextual characteristics of

(...) data sharing between public bodies must consider the need for personal data to be processed in accordance with the responsibilities of the legal body and with the specific purpose that justified their collection.

[10] Law No. 13709, of August 14, 2018. Available at: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

[11] Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, 2016, concerning the protection of natural persons regarding the processing of personal data and the free flow of such data, repealing Directive 95/46/CE.

[12] Techniques that make it possible to de-identify personal data in a reversible (pseudonymization) or irreversible (anonymization) manner.

(...) when it comes to the relationship between individuals and the State, the use of a legal basis of consent to support the processing of personal data can be considered problematic in some aspects, given the asymmetry of forces between the actors, which makes it difficult to obtain free, informed, and unambiguous consent.

the relationship established between the data controller[13] and data subject, provides elements to govern the secondary use of data that cannot be previously detailed or strictly verified.

Therefore, a challenge presented for the public sector as to sharing personal data between different bodies and entities is not only to verify the existence of a legal basis for data processing, but also to assess whether the new specific purpose justifying data sharing is compatible with the original purpose. Such concerns are particularly relevant in the context of the public sector because of the asymmetric, non-optional, and continuous nature of relationships between individuals and the State. Once this point has been understood, another question arises: if a certain secondary use within the State is found to be incompatible with the original purpose, would it be possible to "remedy" such incompatibility? If so, how?

Despite the controversies surrounding the topic, some consistency of understandings is seen in the international scenario. According to these understandings, the incompatibility of purposes can be overcome with the consent of data subjects or based on a specific, necessary, and proportional legal provision, observing the full respect for the other principles and rights associated with personal data protection. In this regard, the duty of transparency, an objective condition for the exercise of rights and for the possibility of challenging the new data processing, gains importance to data subjects.

It is worth recalling that, when it comes to the relationship between individuals and the State, the use of a legal basis of consent to support the processing of personal data can be considered problematic in some aspects, given the asymmetry of forces between the actors, which makes it difficult to obtain free, informed, and unambiguous consent. Moreover, as shown by international experience and the national debate on the theme, a generic normative provision to authorize personal data sharing appears to lack the necessary elements to legitimize secondary uses of personal data by the State. It is necessary to provide a sufficiently specific purpose that allows the evaluation of the public interest at stake, as well as the necessity and adequacy of such a measure.

Finally, recognition of the profound impact that the flow of personal data within the State may have on the rights of individuals requires that secondary uses of data be accompanied not only by the identification of an appropriate legal basis, but also by an assessment of the consequences of new uses of data to the rights and liberties of data subjects, established through transparent policies and adequate safeguards to mitigate any identified risks.

Conclusion: consequences for the Brazilian debate

As this article sought to demonstrate, the COVID-19 pandemic intensified and accelerated the initiatives of personal data sharing with the public sector, as well as between its bodies and entities, precipitating legal discussions that ended up establishing new paradigms. Thus, an unprecedented situation left an unexpected legacy: the definitive establishment in case law of interpretative criteria on data processing by the State, with lasting and structuring effects for the national debate. After the recognition, by the STF, of a fundamental right to personal data protection, a subsequent decision established the understanding that there is no unrestricted authorization in the Brazilian legal system for the free flow and sharing of data in the public sector. It also pointed out

[13] According to the LGPD, the data controller is the natural person or legal entity, of public or private law, in charge of making decisions regarding the processing of personal data.

that any secondary uses of personal data, resulting from data sharing among different bodies and agencies, should consider elements such as the reasonable expectations of data subjects and the nature of the processed data. These decisions are of enormous importance and impose, both for legal scholars and for the Executive branch, the need to advance the debate on the criteria that can allow legitimate data sharing within the State.

Based on international experience and considering the LGDP text, it is possible to anticipate that there would be no a priori impediments for data sharing between public bodies when there is compatibility of purposes and observance of procedural rules and data processing principles, such as necessity, adequacy, and transparency. On the other hand, the concept of "compatibility" is certainly broad and open to different interpretations. It is therefore urgent to develop more objective parameters to assess compatibility of purposes.

Within government, when addressing the secondary uses of data that are incompatible with the original purposes, the question raised is whether this entails the definite exclusion of the possibility of the processing initially desired, or if new legal bases may be invoked to overcome such incompatibility. Although this is a controversial topic, international experience suggests that a new authorization by data subjects or specific legal provisions may support further data processing, under the condition that the principles of personal data protection are guaranteed, and adequate information is provided to the affected individuals. In the case of secondary uses within the public sector, the asymmetry of forces and the non-voluntary nature of the relationship between citizens and the State require additional caution in using the legal basis of consent to legitimize new processing.

With regard to both Supreme Court decisions described above, it is possible to conclude that even when personal data sharing in the public sector takes place with a change of purposes that justified their initial collection, which may be admitted under certain circumstances, it does not suffice to merely confer a legal appearance that formally supports such secondary use. Given the protective parameters conferred by the constitutional principles that ensure individual freedom, privacy, and the free development of personality, it is necessary to establish substantive and procedural protection mechanisms, as well as to observe the entire set of rights and principles associated with personal data protection, clearly identifying the specific public interest to be achieved. Defining the concrete way in which this balancing exercise can be carried out safely and legitimately, in light of the provisions of the LGPD and the Brazilian Federal Constitution, is a task still to be faced.

(...) any secondary uses of personal data, resulting from data sharing among different bodies and agencies, should consider elements such as the reasonable expectations of data subjects and the nature of the processed data.

References

Bioni, B. R. (2019). *Proteção de dados pessoais: A função e os limites do consentimento*. Forense.

Doneda, D., & Viola, M. (2009). Risco e informação pessoal: O princípio da finalidade e a proteção de dados no ordenamento brasileiro. *Revista Brasileira de Risco e Seguro*, *5*(10), 85–102.

Mendes, L. S. (2020, May 10). Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais. *Portal Jota*.

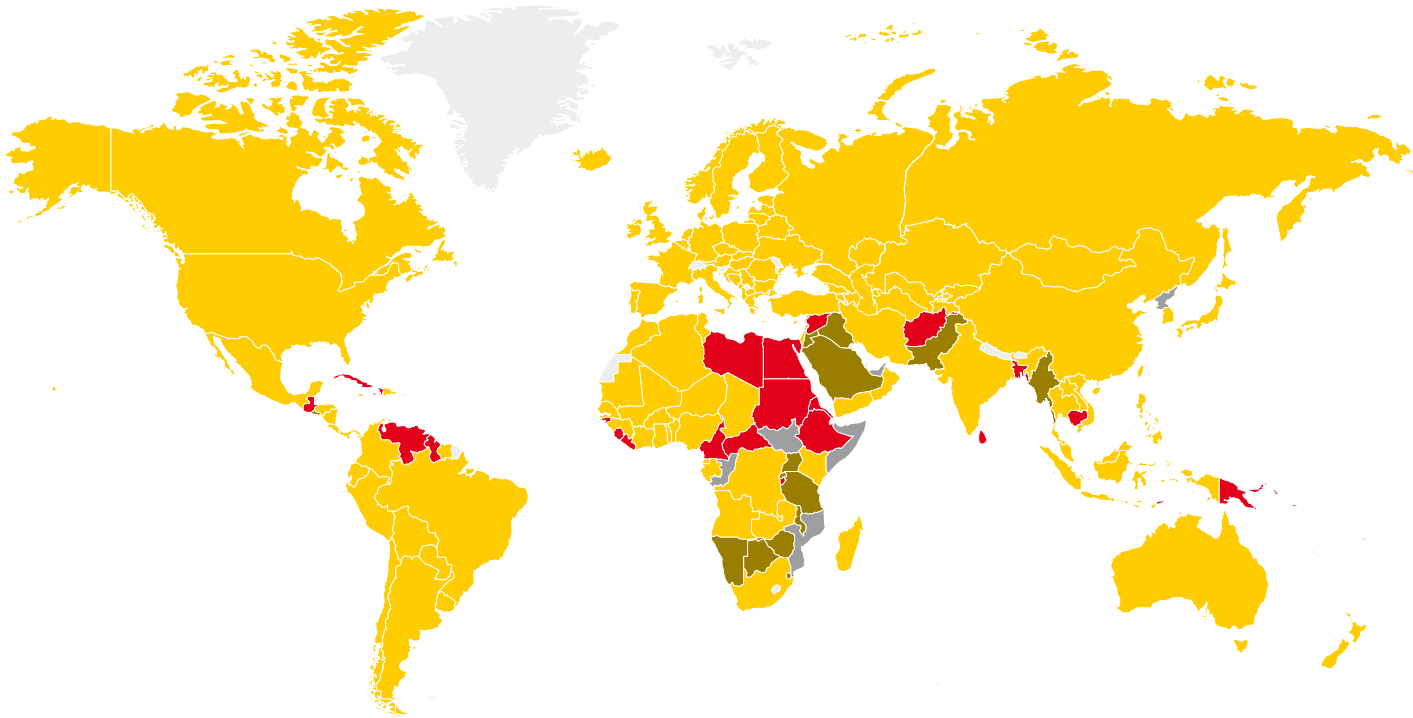
Simitis, S. (1987). Reviewing privacy in an information society. *University of Pennsylvania Law Review*, *135*, 707–46.

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, *154*(3), 477–560.

BOX 1

Data Protection and Privacy Legislation Worldwide[14]

As digitalization and the intensive use of technologies grow, the importance of privacy and data protection is increasingly recognized globally. The existence of specific legislations to deal with such issues is an indication of the adoption of regulatory measures in each country. Below is a map of the existence of data protection and privacy legislation worldwide.



Total countries (%)

- Countries with legislation – 66%
- Countries with draft legislation – 10%
- Countries with no legislation – 19%
- Countries with no data – 5%

[14] Adapted from text prepared by UNCTAD. Available at: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide. Last update on November 25, 2021.

Interview I

Bertrand de La Chapelle is the executive director of the Internet & Jurisdiction Policy Network (I&JPN), a multistakeholder organization which addresses the tensions between cross-border Internet and national jurisdictions. In this interview, he discusses reconciling data protection with the use of digital technologies to fight the pandemic, explains what data governance is, and how to promote this international agenda.

Bertrand de La Chapelle
Executive Director of the Internet & Jurisdiction Policy Network (I&JPN).

Internet Sectoral Overview (I.S.O.)_ Digital technologies adopted to fight the COVID-19 pandemic have intensively expanded the collection and use of personal data. How can concerns regarding data protection be reconciled with the benefits of the data collected for contagion prevention policies?

Bertrand de La Chapelle (B.C.)_ Different applications were developed and implemented by multiple countries in the context of the COVID-19 pandemic, and there were probably variations in their use within nations. Also, local populations have had different attitudes towards these tools, depending mostly on their trust in the authorities. Some governments were able to have their applications endorsed and adopted by citizens because their process was very transparent, and they were probably more efficient than countries with a bad track record with their population and where there was concern about surveillance and misuse of data. In sum, when reconciling competing objectives, the reputation and trust earned by public actors greatly contribute to the implementation of an innovation that requires an effort, but that has visible and clear benefits.
Privacy protection is not an absolute right. There are cases where limitations are acceptable, provided they are necessary, and that privacy protection is being considered in the overall framework. Therefore, I believe that reconciliation should consider the proportionality and circumstances that justify the limitations of this right. I often refer to the idea of reconciling apparently conflicting objectives, so that it is not understood as a zero-sum game; there are situations where you can protect privacy and fight the pandemic at the same time, without necessarily having to sacrifice one for the other.

(I.S.O.)_ What measures could be taken to mitigate risks related to privacy and data protection in the use of digital technologies to fight the pandemic?

B.C._ There is a wide range of concrete measures that can be adopted in terms of the amount of data collected, the anonymization of data, the granularity of the data that is communicated, among others. In that regard, in April 2020, I&JPN produced a short framing document[15] with a list of criteria to evaluate when an application is functioning correctly or how to implement tools that abide by defined principles.
The first measure is to evaluate who creates the application and for what beneficiaries: is it mainly for the state, the health sector or the users themselves? These are very different situations. The second question is: what is the purpose of the data sharing? Is it to track the movement of large populations, do contact tracing, verify if people are respecting a lockdown, or to receive alerts in situations where they have been exposed?

[15] Available at: https://www.internetjurisdiction.net/uploads/pdfs/Internet-Jurisdiction-Policy-Network-20-103-User-Data-Access-COVID-19.pdf

"Data location seems to be a fundamental issue, but we must pay even more attention to those who collect such data, whom they collect them from, who has access to them and for what purpose they are processed."

Two other elements that should be considered are the types of data collected and the collection modalities. Are the data on geolocation, on the proximity of users? Who provides the data? Is it the infrastructure provider or the actual user? What is the degree of data aggregation, anonymization, and granularity? Regarding protections, for how long can these data be accessed? Is this limited to the emergency period? Is there a degree of consent? If so, which one? And lastly, what are the oversight mechanisms to ensure that there are no violations?

(I.S.O.)_ What is data governance and what are the main aspects of this agenda at the international level?

B.C._ There are numerous definitions for data governance. We know that data today not only underpins most human activities, but also reflects them in many regards. Individuals, companies, and governments leave traces, and a large collection of data is emerging and growing at an amazing pace. The question of how we create both social and economic value from such data is of utmost importance and that is precisely what data governance is about.
There are many situations where it is possible to increase both social and economic values. However, there are circumstances where an attempt to increase economic value creates negative externalities in the social sphere, or vice-versa, which in fact diminishes value overall. Thus, data governance is about maximizing value creation in both dimensions in a way that is sufficiently equitable and reduces inequalities or, at least, does not increase them. This would be an overall definition of data governance in terms of objectives.
Furthermore, many international debates – especially among governments – revolve around the location of data storage and processing. Data location seems to be a fundamental issue, but we must pay even more attention to those who collect such data, whom they collect them from, who has access to them and for what purpose they are processed. In terms of data governance, these issues are certainly more important than where data is located. In sum, data governance is about maximizing the creation of value from data and focusing on the mechanisms that allow people to collect, process, and use them, irrespective of location.

(I.S.O.)_ How can we establish a balanced debate between the free flow of data, data sovereignty and data protection?

B.C._ There is extensive debate about the free flow of data on international agendas. On the one hand, it is well known that the technical infrastructure of the Internet is based on indiscriminate free flow of data – it just conveys packets, which is why this architecture is so flexible. That being said, it would be unrealistic to ignore the legitimate concerns about the consequences of unmitigated free flow of data. In the economic sphere, the concentration of wealth and power in the data economy creates a rapidly growing unequal environment. There are also security issues which justify restricting access to or removing certain data from a territory. In terms of human rights, there are legitimate concerns, such as privacy protection.
The key question is: how can we address these concerns and build trust? Is the concept of data sovereignty the appropriate response? It is certainly not the panacea that many actors suggest. First, because there is a range of different challenges, which cannot all be solved with just one measure. For instance, the focus on data storage – one of the key elements of data sovereignty – is a very limited tool to address the variety of issues mentioned. Besides, there is a fundamental connection between sovereignty and the territory of nation states. The problem is

that, for data and most digital policy issues, things are transnational. Not only do interactions take place across borders, but national measures regarding data sovereignty often impact other countries. In this way, extraterritoriality becomes an element of the exercise of data sovereignty; if a state exercises extraterritoriality, it is unavoidably infringing on the sovereignty of another country.
Therefore, data sovereignty is most likely to strengthen the imbalances of power between the different actors because those who can impose their norms across borders will endorse data sovereignty, whereas for those in the receiving end of the data sovereignty of another country, that is a different story. Moreover, many of the proposed measures – which again focus primarily on data location and not on what the data is used for – have large implementation pitfalls and unintended consequences. Therefore, when analyzing the free flow of data and data sovereignty, the underpinning element is that none of these should be considered as absolute. Unrestricted free flow of data is not the solution for everything, but we need to enable data sharing because that is how value can be created. On the other hand, a response based on a short-term territorial solution would be completely contrary to the objectives of data sharing, which could worsen the problem we are trying to solve. The data ecosystem involves a plethora of actors, which is why no single country can alone enact measures that will solve its problem, let alone the problem that we all have in common.

(I.S.O.)_ What are the key recommendations for advancing the agenda of data governance and promoting international cooperation toward a common Datasphere?

B.C._ The primary recommendation is that we need a global discussion about data.[16] Many voices are not heard in this debate, particularly countries in the South, smaller companies, and unrepresented communities. It should also be a multi-stakeholder discussion since a debate conducted only among states will not solve the problem – national government efforts are generally not coordinated and at the moment the trend towards international intergovernmental cooperation is not strong. The third element is that most of those issues are being addressed in silos. There are many organizations that legitimately address this topic, but from very particular angles (such as data protection, trade, cybersecurity), and from an economic or human rights perspective. Therefore, the first recommendation is that the debate be global, multi-stakeholder, cross-sectoral and transdisciplinary, because there are interdependencies between these areas: if we address only one dimension, there may be negative impacts in another.
These issues are new because of their scale and transnational dimension. In this regard, the most important element in the recommendation is the need to innovate the tools, the types of frameworks that we develop, and the concepts we use. The tools can be technical tools, new structures, data fiduciaries, data trusts, among others. Frameworks are relevant because these issues cannot be solved only by self-regulation or by international treaties that take years to be developed. We need governmental initiatives and new instruments to organize the mutual commitments of the different actors. More important, however, is the need for new concepts, which is precisely why we introduced the notion of the Datasphere. A shift in perspective is needed to address data governance challenges in a way that is transnational and trans-sectoral, and that looks at data governance from the Datasphere itself and not from territories.

"The primary recommendation is that we need a global discussion about data. Many voices are not heard in this debate, particularly countries in the South, smaller companies, and unrepresented communities."

[16] Find out more: https://www.internetjurisdiction.net/uploads/pdfs/We-Need-to-Talk-About-Data-Framing-the-Debate-Around-the-Free-Flow-of-Data-and-Data-Sovereignty-Report-2021.pdf

The Datasphere corresponds to the triangle of interactions between: the entire collection of data and datasets produced; the multiplicity of human groups up to humanity as a whole; and the rules and contracts regarding accessing, processing, or using such data. This is not only a conceptual shift of perspective, but also in attitudes, geared at the positive objective of building a Datasphere governance regime that maximizes well-being for all. This is absolutely necessary, because the way in which we organize the governance of the Datasphere is going to be critical for addressing most of the major problems we are confronted with – the COVID-19 pandemic, climate change, inequalities – and for achieving the Sustainable Development Goals (SDGs). It is therefore a fundamental challenge that can only be addressed through cooperation. This discussion has led to the creation of the Datasphere Initiative, which the Internet & Jurisdiction Policy Network (I&JPN) is incubating now.[17]

Article II

Between urgency and surveillance: an analysis on the use of technologies during the COVID-19 pandemic in Latin America[18]

By Jamila Venturini[19]

Since the COVID-19 pandemic was announced by the World Health Organization (WHO) on March 11, 2020, the attempts to use digital technologies to help stop the coronavirus from spreading have multiplied. Among other goals, such initiatives promised to deliver reliable information to the public and to support the monitoring of the evolution of cases and the patterns of population mobility during periods of social isolation, as well as to improve contact tracing in compliance with quarantine rules. This required the collection and processing of a large amount of personal and sensitive data, which has raised concerns among human rights activists and experts from all over the world.

[17] The Datasphere Initiative is a global network which promotes dialogues for awareness-raising, research and a lab oriented towards identifying innovative initiatives that propose normative and technological measures to data governance. Find out more: https://www.thedatasphere.org

[18] Edited version of the report "Informe Observatorio COVID-19 del Consorcio Al Sur: un análisis crítico de las tecnologías desplegadas en América Latina contra la pandemia," published by the Al Sur Coalition in 2021. It was authored by Jamila Venturini and Maria Paz Canales (Derechos Digitales), Morena Schatzky and Agustina del Campo (Centro de Estudios en Libertad de Expresión y Acceso a la Información – CELE), Olga Lucía Camacho and Carolina Botero (Fundación Karisma), and Bárbara Simão (InternetLab). Available at: https://www.alsur.lat/reporte/informe-observatorio-covid-19-consorcio-al-sur-un-analisis-critico-tecnologias-desplegadas

[19] A journalist from the University of São Paulo (USP) with a master's degree in Social Sciences focused on Education from the Latin American Faculty of Social Sciences (FLACSO Argentina), PhD student at the Social Sciences Program of the State University of Campinas (Unicamp), and member of the Latin American Network of Surveillance, Technology, and Society Studies (Lavits). She is the executive director of Derechos Digitales, a Latin American organization for the defense and protection of human rights in the digital environment.

Jamila Venturini
Derechos Digitales.

In Latin America, such measures have been promoted by public and private agents since the arrival of the new coronavirus in the region,[20] following the global trend. They were mostly based on mobile apps and chatbots, sometimes accompanied or complemented by web portals. The speed at which these systems were implemented generated unease regarding the criteria used for security and privacy, in a region where many countries lack regulatory frameworks and robust institutions for proper personal data protection.

Some governments used this pandemic to ease their responsibilities related to the delivery of public information and to advance in the collection of sensitive data without proper protection guarantees. Based on this diagnosis, the AI Sur Coalition – consisting of 11 Latin American organizations for digital rights protection[21] – concentrated efforts on mapping and analyzing how initiatives that use technology to fight the health crisis in the region complied with international human rights criteria.[22] The results were published in the COVID-19 Observatory of the AI Sur Coalition (OCCA), a public and open-access repository which contains detailed data sheets on 16 systems (14 applications and two chatbots) from 14 countries.[23]

This article seeks to summarize the main trends observed in the analysis of these initiatives. Although their launch and use were more pronounced in 2020, new strategies of digitalization associated with the context of the pandemic are now presented with a focus on vaccination. The data and reflections described herein are intended to serve as reminders for future discussions on the potential impacts of this type of technology on the exercise of fundamental rights.

Regional trends

The responses of authorities to COVID-19 varied significantly from country to country in Latin America, which influenced how each government employed technology to fight the pandemic. In Argentina and Chile, where strict quarantine measures were implemented for long periods, these tools played an important role in controlling the mobility of the population. In Uruguay, the national app was part of a broader strategy for identifying and tracing cases.

The technologies identified in the region have been implemented by public and private agents or, in most cases, by an association between both. In countries such as Costa Rica, pre-existing solutions have been adapted or extended to new uses. While some countries have focused on promoting a main tool of national reach, in others – such as Bolivia, Brazil and Mexico – local initiatives have multiplied. The situation was similar regarding applications: some of the countries sought to concentrate a number of functionalities in a single application or portal, while others – such as Brazil, for example – provided different solutions according to the area of implementation. The various experiences have in common the dependence on access and data processing for their operations – whether by direct collection via applications or by prior availability in public or private databases whose use has been redirected. The former is more common, but there is little transparency regarding how this information collected by apps can be linked to other data.

[20] The Uruguayan application was launched in February 2020, when the first case of COVID-19 was recorded in Latin America. By April of that same year, most countries already had at least one national application.

[21] Namely Asociación por los Derechos Civiles (Argentina), CELE (Argentina), Coding Rights (Brazil), Derechos Digitales (Latin America), Fundación Karisma (Colombia), Hiperderecho (Peru), Instituto Brasileiro de Defesa do Consumidor – Idec (Brazil), Instituto Panameño de Derecho y Nuevas Tecnologías (Panama), InternetLab (Brazil), Red en Defensa de los Derechos Digitales (Mexico), and TEDIC (Paraguay). More information available at: https://www.alsur.lat/

[22] The study is based on a standardized methodology that allowed the comparative analysis of mobile apps and chatbots investigated. The information collected refers to contextual data on the country of implementation (including on Internet access); characteristics of the initiative; terms of use and privacy policies; security characteristics, transparency, financing, and effectiveness. This data collection was based on interviews, requests for access to information, official releases or news published in the press, among other sources. The study also included an analysis of the legal framework of each country and of the changes conducted during the pandemic.

[23] Detailed data for each country is available at: https://covid.alsur.lat/en/

The implementation strategies of the initiatives were very heterogenous. In some cases, technology promotion was shy, such as in Bolivia and Brazil. Other discourses were marked by a technological optimism that overestimated the role of the tools in the health strategy, as in Colombia and Ecuador, where they were presented as capable of "saving lives." In addition to the use for citizenship, there were also arguments related to public management: data collection through the functionality of self-diagnosis would help to map cases and guide policies to fight the pandemic. This rhetoric is situated in a scenario of testing shortages that has severely affected the region.

It is undeniable that the use of personal data has a relevant public interest in contexts such as the COVID-19 pandemic and that digital technologies can help governments design response strategies. However, the effectiveness of these tools and the risks associated with potential misuse or abuse depend on the regulatory, technical, and governance frameworks behind their operations. As highlighted by United Nations (UN) experts, states must respect human rights in their efforts to fight the health crisis, which in any case must be proportionate, necessary, and non-discriminatory.[24]

The Inter-American Commission on Human Rights (IACHR) is even more specific in its guidelines. According to Resolution 1/2020, the use of digital surveillance tools in response to the pandemic must be strictly limited in terms of purpose and timing and must protect strictly individual rights, the principle of non-discrimination, and fundamental freedoms.[25] Furthermore, states must be transparent in relation to the surveillance technologies used and their purpose, and also implement independent oversight mechanisms to review their use, and secure channels for receiving reports and complaints.

Below is an analysis of how guidelines of international human rights organizations have or have not been observed in the implementation of technologies to fight COVID-19 in Latin America, with a focus on aspects of legality, necessity, proportionality, and transparency.

Table 1 – INITIATIVES ANALYZED AND MAIN FEATURES

NAME	COUNTRY	VOLUNTARY ADOPTION	ADOPTION RATE (POPULATION%)[26]	LEGAL NATURE	COLLECTED DATA	FREE, SPECIFIC, AND INFORMED CONSENT
Cuidar	Argentina	Yes	22.12	Public-private	Identity document, name, age, gender, address, location, symptoms, pre-existing conditions	Yes
Bolivia Segura	Bolivia	Yes	0.43	Public	Identity document, name, age, address, location, symptoms	No
Salud en Cochabamba	Bolivia	Yes	Not applicable	Public-private	Identity document, name, age, gender, address, location, symptoms, pre-existing conditions	Yes

[24] "COVID-19: States should not abuse emergency measures to suppress human rights," March 16, 2020. Available at: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25722&LangID=E

[25] Available at: https://www.oas.org/pt/cidh/decisiones/pdf/Resolucao-1-20-pt.pdf

[26] Data calculated from official sources or information available regarding downloads in app stores until December 2020. Considers only apps for mobile devices and initiatives of national reach (does not apply to chatbots or to the Bolivian app Salud en Cochabamba).

NAME	COUNTRY	VOLUNTARY ADOPTION	ADOPTION RATE (POPULATION%)	LEGAL NATURE	COLLECTED DATA	FREE, SPECIFIC, AND INFORMED CONSENT
Dr. Sammy Bot	Bolivia	Yes	Not applicable	Public-private	Identity document, location, symptoms, pre-existing conditions	No
Coronavírus-SUS	Brazil	Yes	0.47	Public	Location, symptoms	No
CoronApp	Chile	Yes	0.52	Public	Identity document, name, age, gender, address, location, symptoms, pre-existing conditions	Yes
CoronApp	Colombia	Yes	21.62	Public	Identity document, name, location, symptoms	No
EDUS	Costa Rica	Yes	10.27	Public	Identity document, name, age, gender, address, location, symptoms, pre-existing conditions	No
ASÍ Ecuador	Ecuador	Yes	2.83	Public-private	Age, gender, location	No
SIVI	El Salvador	Yes	Not applicable (chatbot)	Public-private	Name, age, symptoms	No
Alerta Guate	Guatemala	Yes	1.68	Public-private	Location	No
COVID-19MX	Mexico	Yes	0.4	Public	Name, age, gender, address, location, symptoms, pre-existing conditions	Yes
Protégete con salud	Panama	Yes, except for foreigners arriving in the country	0.06	Public-private	Identity document, name, age, gender, address, location, symptoms, pre-existing conditions, picture	No
Covid-19 PY	Paraguay	Yes	0.08	Public	Identity document, name, age, gender, address, location, symptoms, pre-existing conditions	No
Perú en tus manos	Peru	Yes	3.03	Public-private	Identity document, name, age, gender, location, symptoms, pre-existing conditions	Yes
Coronavirus UY	Uruguay	Yes, but certain groups were instructed to use it, such as people arriving in the country	17.73	Public-private	Identity document, name, age, gender, address, symptoms, pre-existing conditions	Yes

Source: Prepared by the author based on data from the COVID-19 Observatory of AI Sur Coalition (OCCA).

(...) without sufficient information about the conditions of collection and processing of data, the possibility of informed consent is seriously compromised.

Urgency, opacity, and surveillance

All initiatives analyzed were implemented administratively, without going through legislative discussions before or after their release. With rare exceptions, no specific standards were found establishing frameworks to guide their operation, whether in relation to the potential impact on fundamental rights that are distinct from the right to health, or regarding the creation of control mechanisms, targets, or goals to assess their efficiency. Most tools were the result of public-private initiatives arising from direct interactions between governments and businesses.

Although cooperation from different sectors is welcome, especially in extreme contexts such as the COVID-19 pandemic, it must be transparent. However, the cases analyzed show the opposite: disclosure, if any, was made after alliances had been built, without the public knowing or having a say in the terms and access conditions that companies would have to the population's personal or sensitive data.

The absence of public debate regarding the adoption of technological systems designed to help fight COVID-19 has reproduced a trend observed in the procurement of surveillance systems in Latin America. Likewise, no evidence was found that the implemented technologies have undergone prior assessment regarding any effects on the exercise of rights and, specifically, on privacy. The practice goes against the IACHR recommendation which states that, when hiring private systems, the state must ensure that an external and independent audit be carried out to identify any potential impacts on human rights.[27]

Among the functionalities offered by technologies are the delivery of public interest information, self-diagnosis, coronavirus exposure notifications, telemedicine, as well as mobility and work passports, which involve the collection of sensitive personal data on gender, health condition, and location. The processing of these and other data allows the inference of a series of additional information about private and equally sensitive habits, such as political and religious preferences. Their handling must be subject to the highest protection, security, and transparency criteria.

In this context, transparency must be understood not only from the perspective of access to public information on the characteristics of the initiatives – which, as pointed out, has been seriously restricted – but also in relation to the processing and use of personal data collected by each system. This relates to a fundamental principle for the exercise of autonomy by the users on how their data will be utilized, as established by international standards and different national data protection standards. In other words, without sufficient information about the conditions of collection and processing of data, the possibility of informed consent is seriously compromised.

This aspect involves several problems. As shown in Table 1, less than half of the initiatives comply with the criteria established for express, free, and informed consent, and this flaw is due to several reasons. In the case of the

[27] Avaliable at: https://www.oas.org/es/cidh/decisiones/pdf/Resolucion-4-20-es.pdf

Brazilian app Coronavirus-SUS, for example, inconsistencies were identified between the information included in the Privacy Policy and the data in fact collected. While most of the tools actively requests consent, three of them assume it has been provided through its use. Also, seven tools (referring to Bolivia, Brazil, Colombia, Guatemala, and Panama) do not specify in their policies the mechanisms for removing consent after it has been granted.

Many of the analyzed systems allow access from other government institutions to the collected data. Some initiatives state this possibility in their adhesion contracts, while in others it is only possible to understand what happens when reviewing the applicable standards and any changes in force during the pandemic. Because of that, it is not always easy to understand which agencies have permission and conditions to access the data. The Privacy Policy of the Brazilian app, for example, states that consent only covers data processing by the Ministry of Health, but the legislation provides for a series of hypotheses for sharing.[28] In the case of Panama, data can be accessed by a task force created in the context of the pandemic which includes the national police – similar to the Paraguayan app.

None of the analyzed initiatives – mobile apps or chatbots embedded in other applications – offer detailed information about the security strategies adopted. At most, they indicate the commitment to ensure the security of the data collected or the adoption of "appropriate" measures for that. Only in the Argentine case a web page associated with the app mentions compliance with specific ISO standards. Only half of the systems enables the effective control of the use of data by subjects which is reflected in the rights of access, correction, deletion, and opposition to data processing. Still, in many cases it is not explicit how these rights can be exercised, especially in countries that do not have an established data protection authority.

Beyond technological solutionism

The analysis carried out by the Al Sur Coalition points out several risks to the exercise of fundamental rights posed by the use of technologies for citizenship in the context of fighting the COVID-19 pandemic. In addition to the aforementioned weaknesses regarding transparency, security, and privacy, the situation worsens when we take into consideration that not all countries of Latin America have adequate and up-to-date regulatory frameworks for access to information and data protection, or independent institutions duly trained to oversee the implementation of this type of technology.

It should be noted that, in facing the pandemic, several countries eased their data protection rules, expanding the possibility of accessing and sharing health data without the need for consent by data subjects. In some cases, the already precarious control structures had their operation limited due to quarantine restrictions. The same happened in relation to transparency

Many of the analyzed systems allow access from other government institutions to the collected data.

[28] The assumptions on the sharing of sensitive data (such as those related to health) are provided for in Decree No. 10046/2019 and in the following articles of the Brazilian General Data Protection Law (LGPD): Article 11, Item II; Article 13; and Article 26. Available at: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm and http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

(...) in facing the pandemic, several countries eased their data protection rules, expanding the possibility of accessing and sharing health data without the need for consent by data subjects.

standards, although in countries such as Brazil the attempts to reduce state liability in the delivery of public information have been challenged.[29]

In addition to the huge discriminatory potential of this type of information, contexts marked by authoritarianism, polarization, and political persecution brought additional concerns about how the data collected by the so-called "COVID apps" could be used. An example of this is Bolivia, which went through the first months of the pandemic under an interim government that tried to criminalize in an ambiguous and unsettling manner the dissemination of information that could affect public health. It led to the prosecution of at least 781 people and 273 criminal cases in April 2020 alone, according to local civil society organizations.[30]

As stated in the assessment carried out by the Al Sur Coalition, the right to data protection is the most affected by the identified initiatives, followed by the right to privacy, which is directly connected to the former. While data protection refers to the informational self-determination capacity of data subjects – that is, the ability to exercise effective control over the use of their personal information –, privacy concerns the right of non-intrusion in private matters by third parties or public authorities. Privacy abuses can lead to the violation of several other rights, such as to freedom of expression, freedom of association and non-discrimination.

It is true that no right is absolute, and a pandemic context requires measures that benefit the health of the population. Nonetheless, the criteria of legality, necessity, proportionality, and transparency are crucial for a balanced intervention, as well as to differentiate responsible public policies from mere technological solutionism, which has marked the use of technologies by the Latin American States. Therefore, it is worth analyzing whether these initiatives in fact fulfill their goals. As we have seen, governments were not careful about setting goals and evaluation mechanisms, which seems to be symptomatic of blind trust in the power of technologies. What we do know is that adoption by the population was extremely limited due to the profound inequalities in the access to technologies, which became even more evident during the pandemic.

It is important to highlight that digital inclusion is not restricted to access to devices or connectivity; it also concerns the ability to use technologies and the quality of connection. Therefore, the barriers imposed by accessing the Internet mostly through mobile devices and limited data plans impact application penetration and, consequently, their effectiveness. For coronavirus exposure notifications, for example, studies indicate that the efficacy of this functionality relies on an adoption by 40%

[29] Find out more: https://ok.org.br/noticia/so-venceremos-a-pandemia-com-transparencia/

[30] Find out more: https://www.derechosdigitales.org/14611/in-support-of-freedom-of-expression-in-bolivia-we-request-the-abrogation-of-the-ds-4231/

to 60% of the population.[31] In Latin America, in 2020, only Argentina, Colombia, and Uruguay were close to 20%, locations where the use of apps was associated with access to certain services, and with mobility or work permissions. In other countries, the rate was around 3%.

It is a concern that, in the search for technological solutions to help fight the pandemic, states fail to offer a comprehensive perspective that observes human rights – as instructed by international organizations – and do not comply with their obligations to protect these rights, making them more fragile in most cases. As noted, in general terms, factors such as inequalities of access, impact analysis, and evidence of effectiveness were not taken into consideration in the planning of the analyzed initiatives. The trend is that governments remain passive to technologies that pose real risks of restriction to the rights of the population.

Whether in the context of the COVID-19 pandemic or in other circumstances, the use of technologies by states must be accompanied by strict transparency, participation, and accountability measures. It is unacceptable that initiatives with great potential for abuse of rights do not have solid justifications for their implementation. On behalf of the Al Sur Coalition, we hope that this analysis serves as a starting point for opportunities to improve technology use practices in addressing the pandemic, as well as for a collective reflection on the role they may play in the future.

Whether in the context of the COVID-19 pandemic or in other circumstances, the use of technologies by states must be accompanied by strict transparency, participation, and accountability measures.

[31] Luca Ferretti et al., "Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing," *Science* (2020). Available at: https://science.sciencemag.org/content/early/2020/03/30/science.abb6936/tab-pdf. See also Patrick Howell O'Neill, "No, coronavirus apps don't need 60% adoption to be effective," *MIT Technology Review* (2020). Available at: https://www.technologyreview.com/2020/06/05/1002775/covid-apps-effective-at-less-than-60-percent-download/

BOX 2

UNDP Guidance on privacy, data protection and broader human rights dimensions of using digital technologies to combat COVID-19[32]

Considering the ample digital response to the COVID-19 pandemic and the related challenges concerning privacy rights, the United Nations Development Programme (UNDP) proposed the following set of principles and practical orientations for their country offices.

Key privacy and data protection challenges in the COVID-19 digital response

- Lack of opportunity for public deliberation during crisis;
- Lack of general privacy and data protection regulations.

COVID-19-specific digital guidance

GENERAL PRINCIPLES THAT SHOULD BE CONSIDERED

- Human-rights-based approach;
- Participatory approach;
- User consent;
- Anonymization/pseudonymization of personal data;
- Temporary nature of digital 'tracking' and surveillance measures;
- Guidelines for the collection, use and duration of storage of data;
- Protection from gender-based privacy infringements;
- Protection of vulnerable populations;
- Right of redress from harm caused by the collection, processing and use of personal data.

RECOMMENDATIONS WHEN USING OR CREATING TECHNOLOGY FOR COVID-19-RELATED WORK

- In the absence of general data protection regulations, use regional or other international frameworks, as well as health data privacy regulations;
- Create a data authorization framework to establish clear rules about who can gather, access, and use what data, when and for what purpose;
- Set purpose limitation and data minimization practices in place;
- Include privacy and participation at the design stage;
- Ensure best practice through the procurement process of digital technologies and services;
- Emphasize privacy codes of conduct for commercial holders of data;
- Carry out careful licensing of private sector digital innovations;
- Conduct mandatory human rights and privacy due diligence processes for every partnership and public procurement;
- Start a conversation about the need for general data protection regulation;
- Look beyond digital tracking and surveillance.

[32] Adapted from text prepared by UNDP. Available at: https://www.sdg16hub.org/content/covid-19-guidance-undp-country-offices-privacy-data-protection-and-digital-technologies

Interview II

Nina da Hora
CTS/FGV Researcher and Digital Security Advisor at TikTok Brazil.

Nina da Hora is a researcher at the Centre for Technology and Society of the Law School of the Getulio Vargas Foundation (CTS/FGV) and Digital Security Advisor at TikTok Brazil. In this interview, she talks about digital security and privacy risks, implications of collecting biometric data and ways to ensure more accessible digital rights.

Internet Sectoral Overview (I.S.O.) _ In the current context of intensified adoption of digital technologies to face the COVID-19 pandemic, what are the main risks associated with privacy? How can they be mitigated?

Nina da Hora (N.H.)_ In Brazil, even before COVID-19, digital technologies were already used to tackle structural problems in society, such as in Health and other areas. The pandemic intensified their use, as well as privacy-related risks, which contributed to the digital surveillance that has been going on for a long time. In this context, people hand over their data to have access to fundamental rights. At the same time, they do not read the privacy terms on the use of technologies because they are long and difficult to understand. However, there are significant issues when we relate data and artificial intelligence (AI), and today, with the idea that we need to be connected to everything and everyone, we face more and more challenges regarding digital security. On the other hand, emblematic cases of data security failures involving hacker attacks, application cloning, and data leakage – widely covered by the press – raised awareness among people about data sharing, whether digitally or not (for example, when they start to question the reason for providing their SSN for purchases). The concern with protection thus appears because of the flaws found in the digital environment. Not that these threats did not occur before the pandemic, but this issue that was previously restricted to specialists and scholars has gained visibility and greater attention. There is a long way ahead of us, but we need to rethink the entire data structure. I see digital education as a pillar that allows society to generate information and questions regarding the tools that are being used.

I.S.O._ Considering the existing inequalities in Brazilian society, how can we guarantee the right to privacy and personal data protection for the most vulnerable populations?

N.H._ Within the current system, thinking about ensuring the right to privacy and data protection is hard, since we are increasingly linked to databases that are intensively used for various purposes. Brazil still has a large portion of the population with no access to the Internet or digital services, and we need to identify how to protect their data as well. There are, for example, many homeless people who are undocumented, and we do not know how many of them have had their data hacked for misuse.
When using digital technologies, we provide and store our data in private companies, without transparency of conditions and processing of these information. In addition to the anonymization of sensitive data, defining transparency rules is of fundamental

"In addition to the anonymization of sensitive data, defining transparency rules is of fundamental importance, in the sense of explaining to users what is collected, for which purposes and use, which must be adapted to each context."

importance, in the sense of explaining to users what is collected, for which purposes and use, which must be adapted to each context. The adoption of free software digital tools could also contribute to digital education and the development of critical thinking about technologies, since the opening of these tools presupposes the understanding and documentation of what happens with the data, how the collection and processing take place, as well as their possible uses and results, including ethical issues. In my opinion, these are possible ways to build a more accessible right to privacy and data protection for the population.

I.S.O._ What are the possible implications of collecting sensitive data through technological solutions adopted in emergency aid actions during the pandemic, such as the collection of biometric data for facial recognition?

N.H._ The collection of biometric data is not new, as we have been using digital biometrics for a long time. This practice was naturalized as the safest method, but it has not necessarily prevented fraud. The problem with using facial recognition and other remote biometric recognitions is that they allow for mass, discriminatory, and biased surveillance. Facial recognition is even more harmful because it identifies the person, allowing for individualized tracking. Many non-white citizens are being directly affected by these tools, which can identify, follow, single out, and track people everywhere. This undermines basic human rights, such as the rights to privacy and data protection, equality, and non-discrimination, or even freedom of expression (leading to the criminalization of protests, for example).
Each technological innovation generates vulnerabilities to be discovered along the way, which are less linked to the tools themselves than to the strategies and contexts of use. There are several potential problems in accelerating the use of AI, such as the techniques developed to clone faces and to create deepfake technology. When faces are stored and we do not know what will be done with such information, there are risks. Although some facial recognition and biometric apps are promoted as a mechanism to increase digital security and encourage their greater adoption in society, there are alternative ways to ensure privacy and security. In all these situations, the damage to these rights occurs regardless of the anonymization of data, which, in my opinion, goes against what is understood by human rights and democracy.

I.S.O._ What strategies can be adopted to increase the population's knowledge and engagement in the debate on the possible negative impacts of digital technologies, especially in relation to the collection and processing of personal data?

N.H._ I always start with education. First, we need to make these themes accessible and rethink the examples used to explain them, so that they adapt to different Brazilian contexts. The debate on diversity and inclusion thus needs to take place, especially in groups that currently promote discussion on these themes. Another aspect is to carry out this process gradually. Internet and technology are connected to all areas and all people, because even those who

do not have access are “tracked” in the system. Therefore, this is a long-term process. In my opinion, the answer is not in technological solutionism, that is, the tendency to use technology to solve problems – including technological – that will not be solved with more technology. Racial, gender, or any other type of bias, for example, will not be resolved with more data, but with reflection and critical thinking, as they are human biases found in society.

How is it possible to solve the issue of democracy in Brazil and in the world using technologies that are monitored, designed, and created by only a social group, usually by private companies, to which civil society does not have access? It is necessary to foster public policies and a more open and plural debate among several sectors, not only the public sector, but also the private sector and civil society, including organizations and activists related to different agendas and contexts. Decision-making must be accessible to the population so that it can participate in this process. This truly refers to a comprehensive approach to education and information for leveraging the understanding regarding these themes.

"It is necessary to foster public policies and a more open and plural debate among several sectors, not only the public sector, but also the private sector and civil society (...)"

Domain Report

Domain registration dynamics in Brazil and around the world

The Regional Center for Studies on the Development of the Information Society (Cetic.br), department of the Brazilian Network Information Center (NIC.br), carries out monthly monitoring of the number of country code top-level domains (ccTLD) registered in countries that are part of the Organisation for Economic Co-operation and Development (OECD) and the G20.[33] Considering members from both blocs, the 20 nations with highest activity sum more than 89.75 million registrations. In November 2021, domains registered under .de (Germany) reached 17.10 million, followed by China (.cn), the United Kingdom (.uk) and Netherlands (.nl), with 9.83 million, 9.70 million and 6.21 million registrations, respectively. Brazil had 4.85 million registrations under .br, occupying 6th place on the list, as shown in Table 1.[34]

[33] Group composed by the 19 largest economies in the world and the European Union. More information available at: https://g20.org/

[34] The table presents the number of ccTLD domains according to the indicated sources. The figures correspond to the record published by each country, considering members from the OECD and G20. For countries that do not provide official statistics supplied by the domain name registration authority, the figures were obtained from: https://research.domaintools.com/statistics/tld-counts. It is important to note that there are variations among the date of reference, although the most up-to-date data for each country is compiled. The comparative analysis for domain name performance should also consider the different management models for ccTLD registration. In addition, when observing rankings, it is important to consider the diversity of existing business models.

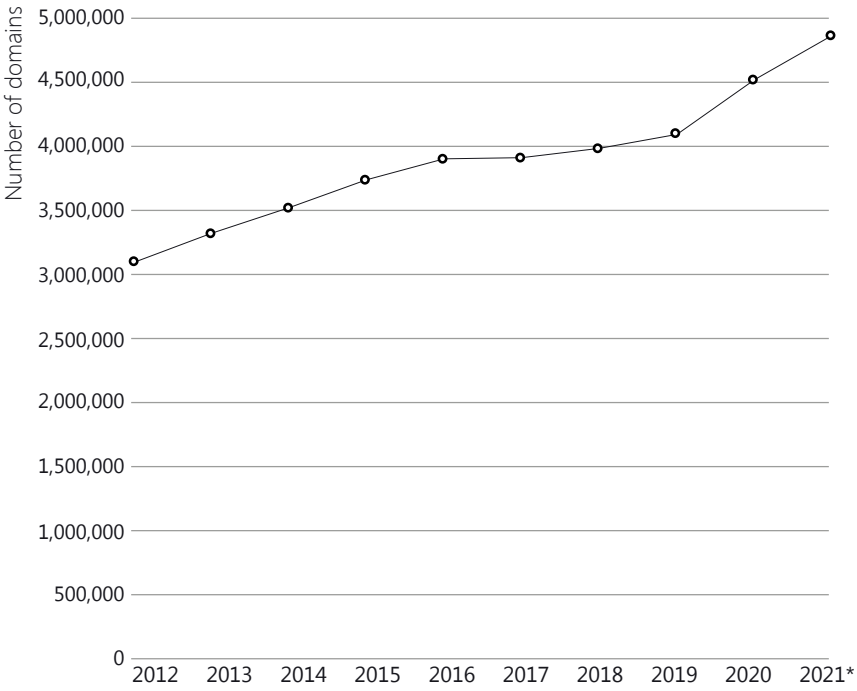
Table 1 – TOTAL REGISTRATION OF DOMAIN NAMES AMONG OECD AND G20 COUNTRIES

Position	Countries	Number of domains	Date of reference	Source (website)
1	Germany (.de)	17,109,697	30/11/2021	https://www.denic.de
2	China (.cn)	9,837,644	30/11/2021	https://research.domaintools.com/statistics/tld-counts/
3	United Kingdom (.uk)	9,703,171	01/06/2021	https://www.nominet.uk/news/reports-statistics/uk-register-statistics-2021/
4	Netherlands (.nl)	6,219,806	30/11/2021	https://api.sidn.nl/rest/counters/domains
5	Russia (.ru)	5,025,335	30/11/2021	https://cctld.ru
6	**Brazil (.br)**	**4,858,768**	**30/11/2021**	**https://registro.br/dominio/estatisticas/**
7	France (.fr)	3,874,717	30/11/2021	https://www.afnic.fr/en/observatory-and-resources/statistics/
8	European Union (.eu)	3,666,151	30/11/2021	https://research.domaintools.com/statistics/tld-counts/
9	Italy (.it)	3,456,471	30/11/2021	http://nic.it
10	Australia (.au)	3,401,599	30/11/2021	https://www.auda.org.au/
11	Canada (.ca)	3,214,548	30/11/2021	https://www.cira.ca
12	Colombia (.co)	3,186,901	30/11/2021	https://research.domaintools.com/statistics/tld-counts/
13	India (.in)	2,586,097	30/11/2021	https://research.domaintools.com/statistics/tld-counts/
14	Poland (.pl)	2,521,965	30/11/2021	https://www.dns.pl/en/
15	Switzerland (.ch)	2,459,804	15/11/2021	https://www.nic.ch/statistics-data/domains_ch_monthly.csv
16	Spain (.es)	1,980,363	25/10/2021	https://www.dominios.es/dominios/en
17	Belgium (.be)	1,735,833	30/11/2021	https://www.dnsbelgium.be/en
18	United States (.us)	1,735,153	30/11/2021	https://research.domaintools.com/statistics/tld-counts/
19	Japan (.jp)	1,674,481	30/11/2021	https://jprs.co.jp/en/stat/
20	Sweden (.se)	1,508,386	30/11/2021	https://internetstiftelsen.se/en/domain-statistics/growth-se/?chart=active

Collection date: November 30, 2021.

Graph 1 shows the performance of .br since 2012.

Graph 1 – TOTAL NUMBER OF DOMAIN REGISTRATIONS FOR .BR – 2012 to 2021*



*Collection date: November 30, 2021.
Source: Registro.br
Retrieved from: https://registro.br/dominio/estatisticas/

In November 2021, the five generic Top-Level Domains (gTLD) totaled more than 189.52 million registrations. With 158.41 million registrations, .com ranked first, as shown in Table 2.

Table 2 – TOTAL NUMBER OF DOMAINS AMONG MAIN gTLD

Position	gTLD	Number of domains
1	**.com**	158,418,426
2	**.net**	13,289,632
3	**.org**	10,523,459
4	**.info**	3,828,293
5	**.xyz**	3,467,440

Collection date: November 30, 2021.
Source: DomainTools.com
Retrieved from: research.domaintools.com/statistics/tld-counts

APPLICATIONS AND PERSONAL DATA DURING THE COVID-19 PANDEMIC: WHAT IS THE OPINION OF THE BRAZILIAN POPULATION?

Strategies for adopting digital technologies to fight the pandemic have expanded the collection and use of personal data. Below are data[35] on the likelihood of Internet users[36] in Brazil to download applications related to COVID-19, as well as their perceptions about the benefits and risks of sharing personal data.

DOWNLOADING GOVERNMENT APPS WITH INFORMATION ABOUT SYMPTOMS AND TREATMENTS

Among Internet users aged 16 and over

20% DOWNLOADED IT

19% WOULD NOT DOWNLOAD IT

REASONS FOR NOT DOWNLOADING APPS[37]

Among those who would not download apps

42%

- Do not think apps help to control the pandemic
- Concern with government surveillance after the pandemic

39%

- Do not want the government to access their geolocation data
- Do not believe apps prevent identification

PERCEPTION OF RISKS AND BENEFITS OF PROVIDING PERSONAL DATA TO GOVERNMENTS OR ENTERPRISES

Among Internet users aged 16 and over

54% More risks than benefits

16% Neither benefits nor risks

13% More benefits than risks

17% Does not know

The Brazilian Network Information Center (NIC.br) and the Brazilian Internet Steering Committee (CGI.br) produce debates and informative materials concerning privacy and personal data protection, such as:

· INTERNET SECURITY BOOKLET:

PRIVACY FASCICLE (2020)

DATA PROTECTION FASCICLE (2021)

cartilha.cert.br/fasciculos/#privacidade | cartilha.cert.br/fasciculos/#protecao-de-dados

· PRIVACY AND PERSONAL DATA PROTECTION SEMINARS:

seminarioprivacidade.cgi.br

[35] Data from the ICT Panel COVID-19, web survey on the use of the Internet in Brazil during the new coronavirus pandemic, by Cetic.br|NIC.br. Available at: https://www.cetic.br/pt/tics/tic-covid-19/painel-covid-19/2-edicao/

[36] A "user" is a person who has used the Internet at least once in the three months prior to the interview.

[37] Refers to apps that inform symptoms and how to get treatment for COVID-19 or that notifies of contact with people diagnosed with the disease.

/Credits

TEXT

ARTICLE I

Miriam Wimmer
(Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa – IDP)

ARTICLE II

Jamila Venturini
(Derechos Digitales)

DOMAIN REPORT

José Márcio Martins Júnior
(Cetic.br|NIC.br)

GRAPHIC DESIGN AND PUBLISHING

Giuliano Galves,
Klezer Uehara and
Maricy Rabelo
(Comunicação|NIC.br)

ENGLISH REVISION AND TRANSLATION

Letralia

PORTUGUESE PROOFREADING AND REVISION

Mariana Tavares

EDITORIAL COORDINATION

Alexandre F. Barbosa,
Tatiana Jereissati,
Javiera F. M. Macaya and
Luciana P. B. Lima
(Cetic.br|NIC.br)

ACKNOWLEDGMENTS

Bertrand de la Chapelle and
Lorrayne Porciuncula
(Internet & Jurisdiction Policy Network)
Jamila Venturini
(Derechos Digitales)
Miriam Wimmer (IDP)
Nina da Hora (CTS/FGV)
Scarlett Fondeur Gil and
Torbjorn Fredriksson (Unctad)

*The ideas and opinions expressed in the texts of this publication are those of the respective authors and do not necessarily reflect those of NIC.br and CGI.br.

United Nations Educational, Scientific and Cultural Organization

cetic.br
Regional Center for Studies on the Development of the Information Society under the auspices of UNESCO

nic.br
Brazilian Network Information Center

cgi.br
Brazilian Internet Steering Committee

POR UMA INTERNET CADA VEZ MELHOR NO BRASIL

CGI.BR, MODELO DE GOVERNANÇA MULTISSETORIAL

www.cgi.br

nic.br cgi.br

FOTOS: RICARDO MATSUKAWA E SHUTTERSTOCK