Internet Sectoral Overview

Number 2
July, 2023
Year 15

Personal data protection: Privacy and reliability in the digital environment

Individual's perspectives on privacy and personal data protection in Brazil

By Winston Oyadomari,[1] Ramon Silva Costa,[2] and Manuella Maia Ribeiro[3]

Introduction

Surveys on the use of the Internet in Brazil reveal an increase in the number of users accompanied by a diversification of the activities performed online. In 2022, 93% of Internet users sent instant messages, 80% used social networks, 69% shared content on the Internet, and 45% bought products and services online (Brazilian Internet Steering Committee [CGI.br], 2023). The omnipresence of the mobile phone as an access device, most of the time exclusively, suggests that a large part of these uses is accessed in Brazil through mobile phone applications, responsible for collecting an extensive range of personal data from users. Such activities also increasingly relate to the debate about how individuals' data is used and shared, with a focus both on economic and social development and on regulating and monitoring potential abuses of the indiscriminate use of such data, especially those that could generate irreparable damage to society. In this regard, one example is usages that lead to security incidents, unauthorized access, and decisions based on discriminatory biases. Given this scenario, the need for solid data governance[4] becomes increasingly important.

The activities carried out in the digital environment mobilize a wide network of actors in a data-driven ecosystem that has grown massively. In this context, recent legal standards have been established that regulate part of this ecosystem

[1] He holds a degree in Public Administration from the Fundação Getulio Vargas's São Paulo School of Business Administration (FGV EAESP) and is a researcher at the Statistics and Quantitative Methods Coordination of the Regional Center for Studies on the Development of the Information Society (Cetic.br), of the Brazilian Network Information Center (NIC.br).

[2] Doctoral candidate in Law from the Pontifical Catholic University of Rio de Janeiro (PUC-Rio) with a master's degree in Law from the Federal University of Juiz de Fora (UFJF), he is a specialist in digital law from the State University of Rio de Janeiro (UERJ) and the Institute of Technology and Society of Rio de Janeiro (ITS-Rio) with a Law degree from the Fluminense Federal University (UFF). He is a researcher at the Núcleo Legalite – Law and New Technologies at PUC-Rio and an attorney specialized in Compliance and Data Protection at NIC.br.

[3] Doctoral and a Master degree in Public Administration and Government from FGV EAESP, she is a researcher at the Survey Projects Coordination of Cetic.br|NIC.br, where she leads the ICT Electronic Government and ICT Public Access Centers surveys.

[4] For the purposes of this paper, data governance will be considered as "rules, processes, and behaviors related to the collection, management, analysis, use, sharing, and disposal of data - personal and/or non-personal" (Datasphere Initiative, 2023, p. 5).

While government organizations must act to regulate and supervise the processing of personal data, they also need to ensure the appropriate use of citizens' data to carry out their activities, such as the provision of public services.

regarding the risks of rights violations related to privacy and personal data protection, such as the General Data Protection Regulation (GDPR) in the European Union (2016), and the General Data Protection Law (Lei Geral de Proteção de Dados Pessoais [LGPD], 2018) in Brazil. The increased interest in the topic has also inspired initiatives to produce statistical data about users' perspective on their privacy and their perception of the use of their personal data by public and private actors, as the Data Protection Survey, conducted by Eurobarometer in 2015 (European Commission, 2015), and the Americans and Privacy study conducted by the Pew Research Center in 2019 (Auxier et al., 2019). Such studies also generate inputs for understanding the role of this dimension in Internet users' trust in the digital environment, pointing out that individuals' fears about the use of their personal data can impact the adoption of digital services, whether public or private (United Nations Capital Development Fund [UNCDF], 2021).

In the Brazilian context, the *Privacy and Personal Data Protection 2021: Perspectives of individuals, enterprises and public organizations in Brazil* survey (CGI.br, 2022), conducted by Cetic.br|NIC.br with Internet users, presented an innovative measurement of how the population understands the issue of privacy and data protection and their position on issues such as data collection practices and the perceived risks of these activities. In addition, the study also included indicators related to the implementation of actions aimed at the privacy and protection of personal data among enterprises and government organizations in the country. This allowed us to map the process of adaptation to the current legislation enacted in 2018, and the main challenges faced by public and private organizations.

This article presents a selection of the indicators from the *Privacy and Personal Data Protection 2021* survey (CGI.br, 2022), with emphasis on Internet users' perception of this topic. It also highlights users' perceptions of the public sector, pointing out the dual role of public authorities in ensuring rights related to privacy and data protection. While government organizations must act to regulate and supervise the processing of personal data, they also need to ensure the appropriate use of citizens' data to carry out their activities, such as the provision of public services. Thus, both in monitoring compliance with legislation, such as the LGPD, and in ensuring the security of personal data in their custody, the actions of the public sector can be a key aspect of society's trust in online activities.

Privacy and personal data protection from the perspective of the Brazilian society

PERCEPTION ABOUT THE CONCEPT

The survey explored the understanding of the concept of privacy among Internet users in the country through an open-ended question.[5] The answers were analyzed and coded automatically into broad categories, allowing us to understand which domains people refer to when they think of "privacy."

The categorization of the open-ended answers has generated six categories:

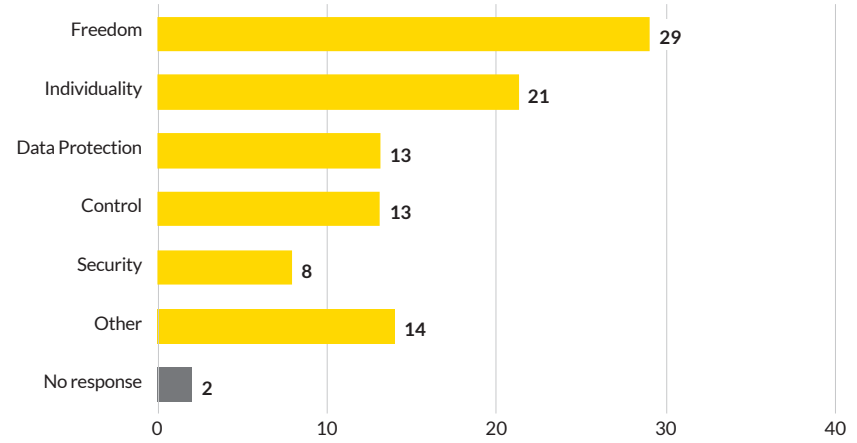
- Freedom: Guarantee of freedom in private aspects of life ("freedom" – one's own and that of others' –, "right").
- Individuality: The search for individuality, whether in places or situations ("individuality," "intimacy," "space," "private").
- Data protection: A desire to protect one's own data against third parties ("data protection against third parties," "leaks").
- Control: A desire to have control over one's own data ("control over data access," "choice over what is public," "consent").
- Security: More generic mentions of security ("security," "protection," "confidentiality," "monitoring").
- Other: Valid answers that did not fall into any of the previous categories ("peace," "tranquility," "quiet," "important," "essential," "everything" [no further explanation], "does not exist").

The results indicate that most Internet users define "privacy" based on the domains associated with freedom and individuality (Chart 1) – understood as crucial aspects of everyday life – and in some cases equated with a fundamental right. At a lower level are those that describe the data logic associated with the use of the Internet, online platforms, and social networks. Data protection is described both as a barrier to unauthorized access (controlled or configured), the perspective on who can access it (as in social network settings), as well as security against theft and leakage in the digital environment.

There is also a group of users who provided answers strictly associated with security against data invasion and theft, which reveals a concern about the risks associated with the data ecosystem. Finally, some answers could not be categorized in any of the previous groups and were grouped in the "Other" category. This plurality of perceptions reinforces the multifaceted nature of the theme among the respondents.

[5] For the analysis of the open-ended answers, a supervised machine learning method was used. In a first step, a sample of 500 responses was randomly selected and categorized manually by a group of researchers. Subsequently, topic modeling was applied (Chen et al., 2016).

Chart 1 – CATEGORIES OF THE DEFINITION OF THE CONCEPT OF PRIVACY (2021)
Total number of Internet users 16 years old or older (%)



Source: CGI.br (2022).

It is worth pointing out that the "Data Protection" category presented variations by social class (17% among users in classes AB and 8% among those in classes DE) and level of education (6% among those with up to Elementary Education and 17% among those with Secondary Education). When analyzing the responses by age groups, significant differences were also found: The answers given by the youngest were categorized in greater proportion as "Individuality" (32% for those aged 16 to 24 and 27% for those aged 25 to 34), whereas the answers given by the oldest respondents were categorized in greater proportion under "Freedom" (43% of those 60 years old or older).

REQUEST CHANNELS

The National Data Protection Authority (ANPD) was established in 2020, with responsibilities such as receiving and processing requests, complaints, or reports regarding personal data, as well as promoting sound data management practices among controlling organizations, i.e., those involved in the personal data processing. The Cetic.br|NIC.br (CGI.br, 2022) survey conducted at the end of 2021 indicates that Internet users have not fully used the opportunity to submit requests to the ANPD. It is also possible to identify that the majority of complaints are directed toward data-controlling organizations, followed by consumer rights organizations, such as the Consumer Protection and Defense Programs (Procons).

The search for consumer service channels to submit requests, complaints, or reports was made by 24% of Internet users aged 16 and older. The most frequently mentioned channel was the data-controlling enterprise or government organization (80%), followed by consumer protection agencies, such as Procon (48%). The ANPD's utilization rate, on the other hand, remains at a much lower (27%).

For those who did not seek consumer service channels to submit requests, complaints, or reports, the most mentioned channels for future needs were Procon (79%), followed by the data-controlling enterprise or government organization (74%), the police (65%), and the ANPD (62%). Therefore, the ANPD is not yet perceived as one of the main channels to seek assistance in cases of potential privacy violations or personal data protection, unlike consumer protection agencies that have been established since the creation of the Consumer Defense Code (CDC, 1990). Thus, complainants often associate their complaints or requests with a consumer-related, or even directly to a crime, opting to file complaints with the police authorities.

PERCEPTIONS CONCERNING SENSITIVE PERSONAL DATA PROCESSING

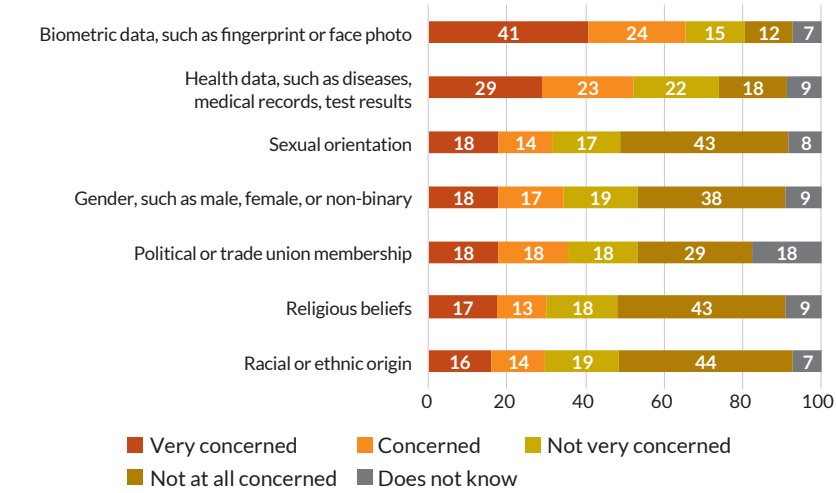
Governments handle massive volumes of citizens' personal data in their regular activities, such as security, taxation, and the provision of public services. Furthermore, they are able to relate data of different origins and nature, including sensitive data. Within this context, 40% of Internet users report that they are very concerned and 29% are concerned regarding the government's use of their data. Concern levels are somewhat lower with regard to data usage by enterprises: 47% reported being very concerned and 28% reported being concerned about such use.

The data also reveal a difference in the level of concern regarding data usage by enterprises based on the respondents' color or race. Black individuals (52%) and Brown individuals (49%) report being very concerned compared to White (43%) individuals, suggesting a perceived potential for discriminatory use of such data by enterprises against these populations. The differences are also observed in the context of government data usage: 47% of Black individuals express strong worries, while the percentages are lower among Brown individuals (41%) and White individuals (37%).

Internet users report a high level of concern regarding the provision of biometric data, surpassing concerns related to other types of sensitive personal data: 41% said they were very concerned and 24% concerned (Chart 2). Health data also emerges as a significant category data: 29% of respondents said they are very concerned and 23% said they are concerned.

(...) 40% of Internet users report that they are very concerned and 29% are concerned regarding the government's use of their data.

Chart 2 –LEVEL OF CONCERN ABOUT PROVISION OF SENSITIVE PERSONAL INFORMATION (2021)
Total number of Internet users 16 years old or older (%)



Source: CGI.br (2022).

The advancement of biometrics data in various aspects of everyday life, such as fingerprint and facial recognition, coupled with the intimate, tangible, and material nature of this data and its high potential for damage if compromised, may help to understand these results. The use of biometric data in Brazilian elections, starting with a pilot test in the 2008 election, and reaching approximately 120 million registrations in 2020, intends to cover all voters by 2026.[6] We can also observe the use of biometrics data by the private sector in banks, pharmacies, gyms, and private condominiums, leading to a series of legal questions regarding the collection and use of this type of data in specific contexts.

Furthermore, the processing of biometric data for security and public surveillance purposes has provoked extensive debate in the Brazilian context. Particularly, the automated processing of sensitive personal data through the use of facial recognition technologies equipped with Artificial Intelligence (AI) stands out. The implementation of such technologies faces criticism and resistance from some sectors, considering that facial recognition has been the hallmark of great promise in public safety, while socially vulnerable populations have been constantly subjected to automated harassment and violence, including improper police approaches, and false criminal attributions, the black population being the most affected in this scenario (Costa & Kremer, 2022).[7]

[6] In 2022, Brazil had 156 million eligible voters, according to the Superior Electoral Court (TSE). Details on the use of biometric information in elections can be found at: https://www.tse.jus.br/eleicoes/biometria/biometria

[7] On racism and the use of facial recognition technologies: https://www.brasildefato.com.br/2019/11/27/cerca-de-90-das-pessoas-presas-com-uso-de-reconhecimento-facial-sao-negras

Although the LGPD does not directly regulate cases of data use for public security and criminal prosecution purposes, it does stipulate the need for specific legislation (Article 4, section III). In 2019, the Brazilian House of Representatives took the initiative to create a Commission of Jurists to draft a preliminary document of the so-called "Criminal LGPD," and a draft bill was presented to the Brazilian House Presidency one year later. The document is in the Brazilian House of Representatives currently awaiting formal presentation by a congressman to become a bill (Costa & Kremer, 2022).

However, facial recognition-related data collection is not a practice that is restricted to or problematic solely in the public sector. ViaQuatro, the company responsible for the concession of the São Paulo subway line 4-yellow, was fined R$500,000 by the São Paulo Court of Justice for conducting facial recognition through cameras without the passengers' consent. The cameras installed in the subway captured facial expressions and even identified emotions for commercial and advertising purposes. The ruling resulted from a public civil action in defense of subway's service consumers.[8]

The indicators on the level of concern regarding sensitive personal data reveal an important debate about this special category of personal data. The LGPD defines sensitive personal data in its Article 5, section II, created due to the discriminatory and harmful potential associated with the improper treatment of certain types of data. Among these data, the law expressly includes information such as race, ethnicity, religion, political opinion, membership in a union or religious, philosophical, or political organization, data concerning health or sex life, and genetic or biometric data when linked to a natural person.

According to Doneda (2019), the selection of data that is deemed sensitive demonstrates that the circulation of certain information can lead to greater potential harm for its holders in a specific social context. He adds that the discriminatory effects lie not in the data itself, but in how it is utilized. Based on this assumption, understanding the mechanisms employed in the protection of sensitive data requires comprehension of the discriminatory dynamics present in society. Such understanding contributes to the interpretation of users' concerns about the handling of sensitive data by government organizations, especially when addressing health, race, and biometric data.

In this sense, the rigorous protection of sensitive data becomes an indispensable tool for promoting equality and freedom of individuals within an information context characterized by the implementation of advanced technologies and power asymmetries between personal data owners and controllers (Mulholland, 2020). Therefore, enterprises and public organizations must recognize that the LGPD imposes a higher standard of protection and security for sensitive personal data, which encourages organizations to undertake adaptation processes that involve the creation of internal regulations aligned with the legislation, such as strengthening codes of ethics and conduct, specifying values and

(...) understanding the mechanisms employed in the protection of sensitive data requires comprehension of the discriminatory dynamics present in society.

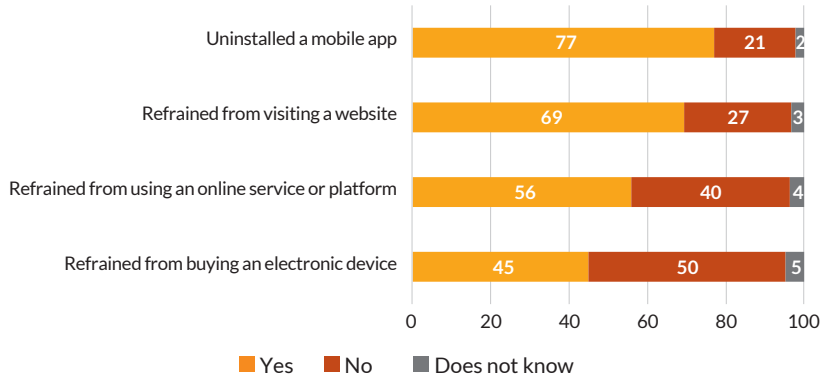
[8] Find out more: https://idec.org.br/noticia/idec-vence-acao-contra-uso-de-reconhecimento-facial-e-viaquatro-e-condenada-pagar

principles related to fundamental rights in order to curb initiatives that violate the personality and dignity of data subjects. In this regard, actions, such as multisectoral dialogues among stakeholders, are important for sharing and developing best practices (Teffé, 2022).

USAGE RESTRICTIONS

In addition to risk prevention strategies and control over the privacy settings within applications and services, the survey also revealed that Internet users may adopt usage restrictions due to concerns related to the handling of their personal data. Motivated by this concern, 77% of Internet users aged 16 and older have already uninstalled applications, 69% have refrained from visiting certain websites, 56% have refrained from using specific Internet services, and 45% have refrained from buying some electronic device (Chart 3).

Chart 3 – MEASURES TAKEN DUE TO CONCERNS ABOUT PERSONAL DATA (2021)
Total number of Internet users 16 years old or older (%)



Source: CGI.br (2022).

This indicator reveals, therefore, that a large portion of Internet users in Brazil have already restricted their activities on the Internet in some way due to concerns related to personal data. The lack of trust about the use, sharing, or leakage of personal data affects the adoption of services, application usage, and website visits. Consequently, this perception of risk in online environments can diminish access to the opportunities offered by the Internet and represents a relevant message for the development of services and applications within the digital environment, especially in the context of data governance.

Final remarks

Data governance plays a key role in effective information management by establishing policies and practices to ensure data quality, compliance, and appropriate use. Within this context, the protection of personal data takes on a central importance, as it aims to preserve the confidentiality, integrity, and availability of information, mitigating risks such as unauthorized access, loss, or misuse.

The Cetic.br|NIC.br survey (CGI.br, 2022) demonstrated that Internet users in Brazil are wary regarding the use of their personal data, especially sensitive data, such as biometric information. Furthermore, the perception of the concept of privacy is associated with online practices for a portion of respondents. Such findings raise several implications for society's trust in the digital environment, including access to online activities and services.

Regarding contacting organizations to report or exercise their rights to data protection, in addition to the entities that control their data, Internet users most often cite consumer protection bodies and police authorities as the entity to approach for reporting or lodging complaints. Generally, the ANPD is not yet recognized as a venue for interaction on this topic among Internet users. Thus, strategies to disseminate the roles and activities of these different organizations can guide citizens as to the most appropriate entity to deal with requests related to the theme, in order to bring more security to the channels used to safeguard these rights.

Biometric data were the most mentioned among the respondents as a type of sensitive information that concerns Internet users. This also demands a reflection from public and private organizations regarding the strategies employed for the collection and processing of such data. It is also important to emphasize the difference in the results concerning the themes of discrimination mentioned by black individuals, which reflects a scenario of fear experienced by a segment of the population that faces daily vulnerability in relation to the intensification of discriminatory practices. Thus, it can be noted that these concerns are embedded in the daily life of Brazilian Internet users and are related to the need for greater legality in the treatment of sensitive personal data in view of the potentially harmful and discriminatory undue processing of these types of personal data.

A surprising outcome of this survey is the restraint demonstrated by Internet users on their own behavior, motivated by concern about data usage. This indicates that users may opt not to perform services through digital channels due to fear of their data being collected and used, impacting the delivery of public information and services through digital media. Furthermore, concerns regarding cyberattacks, fraud, security, and lack of transparency in data usage, among other factors, can erode trust in government services and affect their adoption by society (United Nations Department of Economic and Social Affairs [UN DESA], 2022).

(...) users may opt not to perform services through digital channels due to fear of their data being collected and used, impacting the delivery of public information and services through digital media.

(...) the adoption of practices aimed at generating greater confidence in the use of digital applications becomes fundamental to the data governance strategies and models adopted by public organizations.

When evaluating, for example, the adoption of government contact tracing apps[9] during the pandemic, studies suggest that providing transparency and trust in the security of their data use in these services also increases the propensity to use them (Hermosilla & Lapostol, 2022; Lin et al., 2020; European Council, 2020). Therefore, the adoption of practices aimed at generating greater confidence in the use of digital applications becomes fundamental to the data governance strategies and models adopted by public organizations. In this sense, the results help reinforce the importance of the topic for public debate and raise new questions that should be addressed by future studies on privacy and personal data protection in the country, especially for the promotion of good data governance.

References

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019). *Americans and privacy: Concerned, confused and feeling lack of control over their personal information (American Trends Panel Wave 49).* Pew Research Center. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Brazilian Internet Steering Committee (2023). *Survey on the use of Information and Communication Technologies in Brazilian households - ICT Households 2022*. São Paulo: CGI.br. https://cetic.br/en/tics/domicilios/2022/individuos/

Brazilian Internet Steering Committee (2022). *Privacy and personal data protection 2021: perspectives of individuals, companies and public organizations in Brazil*. São Paulo: CGI.br. https://cetic.br/en/publicacao/privacidade-e-protecao-de-dados-2021/

Chen, Q., Yao, L., & Yang, J. (2016). Short text classification based on LDA topic model. *2016 International Conference on Audio, Language and Image Processing (ICALIP)*, 749-753. https://doi.org/10.1109/ICALIP.2016.7846525

Consumer Defense Code. (1990). *Law n. 8.078, of September 11, 1990. Provides for consumer protection and makes other provisions.* Brasília: Presidency of the Republic. https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm

Costa, R., & Kremer, B. (2022, October). Inteligência Artificial e Discriminação: desafios e perspectivas para a proteção de grupos vulneráveis diante das tecnologias de reconhecimento facial. *Direitos Fundamentais & Justiça,* year 16, special issue, p. 145-167. https://dfj.emnuvens.com.br/dfj/article/view/1316/1065

Datasphere Initiative. (2023). Data governance and the Datasphere: Review of the literature. *Internet Sectorial Overview, 15*(1). https://cetic.br/en/publicacao/year-xv-n-5-data-production-and-ecosystem/

Doneda, D. (2019). *Da privacidade à proteção de dados pessoais*. São Paulo: Revista dos Tribunais.

European Commission. (2015). *Special Eurobarometer 431: Data Protection* (Special Eurobarometer 431 / Wave EB83.1). European Commission, Directorate-General for Justice and Consumers. https://doi.org/10.2838/552336

[9] Contact tracing includes activities to identify, assess, and guide people exposed to a disease to prevent further transmission, and may adopt the support of digital technologies in this process (World Health Organization [WHO], 2020).

European Council. (2020). *2020 Data protection report.* https://rm.coe.int/prems-120820-gbr2051-digital-solutions-to-fight-covid-19-texta4-web-/16809fe49c

European Union. (2016, April 27). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

General Data Protection Law. (2018). *Law n. 13,709, of August 14, 2018. Provides on the processing of personal data, including in digital media, by natural persons or legal entities of public or private law, in order to protect the fundamental rights of freedom and privacy and the free development of the personality of individuals.* https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Hermosilla, M. P., & Lapostol, P. (2022). Limits to algorithmic transparency. In Brazilian Internet Steering Committee. *Survey on the use of information and communication technologies in the Brazilian public sector: ICT eGovernment 2021* (pp. 131-137). São Paulo: CGI.br. https://cetic.br/en/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-no-setor-publico-brasileiro-tic-governo-eletronico-2021/

Lin, J., Carter, L., & Liu, D. (2021). Privacy concerns and digital government: Exploring citizen willingness to adopt the COVIDSafe app. *European Journal of Information Systems, 30*(4), 389-402. https://pesquisa.bvsalud.org/global-literature-on-novel-coronavirus-2019-ncov/resource/en/covid-who-1232104

Mulholland, C. (2020). The processing of sensitive personal data. In C. Mulholland (Org.). *The LGPD and the new regulatory framework in Brazil* (pp. 121-156). Porto Alegre: Arquipélago.

Office of the Privacy Commissioner of Canada. (2021). *2020 Survey of Canadians on Privacy-Related Issues: Final Report*. Prepared by Phoenix SPI for the Office of the Privacy Commissioner of Canada. Office of the Privacy Commissioner of Canada. https://publications.gc.ca/collections/collection_2021/cpvp-opc/IP54-109-2021-eng.pdf

Teffé, C. S. (2022). *Dados pessoais sensíveis: qualificação, tratamento e boas práticas*. Indaiatuba: Foco.

United Nations Department of Economic and Social Affairs. (2022). *E-Government Survey 2022: The future of digital government.* https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2022

United Nations Capital Development Fund. (2021, November). *The role of data protection in the digital economy.* https://static1.squarespace.com/static/5f2d7a54b7f75718fa4d2eef/t/61c39ac52e86d360a8301fd6/1640210452857/EN-UNCDFBrief-Data-Protection-2021.pdf

World Health Organization. (2020). *Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing: Interim guidance.* https://apps.who.int/iris/bitstream/handle/10665/332200/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1-eng.pdf

Interview I

Photo: Personal archive

Rafael Zanatta
Director of Data Privacy Brazil Research Association. Ph.D. from the Institute for Energy and the Environment at the University of Sao Paulo (USP).

Data privacy and security in Brazil: Today's challenges

In this interview, Rafael Zanatta, director of Data Privacy Brazil, discusses the aspects of data governance necessary for personal data protection, the impact of socioeconomic inequalities on individual privacy experiences, how the concept of feedback loop of injustice relates to surveillance issues by the public and private sectors and also addresses the main risks associated with the collection of biometric data in Brazil.

Internet Sectoral Overview (I.S.O.)_ What aspects should be covered in data governance policies to ensure the protection of personal data?

Rafael Zanatta (R.Z.)_ Data governance is an umbrella term that encompasses understanding why personal data is used in an organization and the intention of its throughout its lifecycle. Many organizations handle vast amounts of personal data but lack internal awareness regarding the necessity of such data, why it should be used, the limitations on extracting economic value from it, with whom such data can be shared, and what must be done to ensure that the basic rights of data subjects are respected.

Data governance can be viewed from a very broad and holistic perspective, as it encompasses the individuals, the processes, and the necessary tools to ensure a consistent and appropriate handling of personal data within an organization, be it public or private.

The Organisation for Economic Co-operation and Development (OECD) defines data governance policies as diverse arrangements and technical and institutional predictions that affect data' lifecycle, such as creation, collection, storage, use, protection, access, sharing, and deletion. Moreover, these polices are guided by the balance between innovation and the respect for fundamental rights; therefore, when thinking about data governance policies, it is essential to incorporate measures that respect the basic rights of data subjects and mitigate risks in the event of unlawful or security incidents that could impact individuals and society.

Each organization has its own contexts and peculiarities, so a single, definitive definition of "what data governance is" is limited. For example, when collaborating with the Public Defender Offices of São Paulo and Rio de Janeiro to reflect on the data governance, we started by reflecting on the core functions of the Public Defender Offices, the type of public service provided, the different types of data treatment, the technological tools employed, and the central role of data sharing for research and promoting access to justice. Thus, the development of the data governance policy was incorporated as

something strategic, involving the entire executive and management team of these organizations. This is an element that I believe is central: It should be viewed as something strategic rather than peripheral and outsourceable.

I.S.O._ Within the Brazilian context, to what extent do social and economic inequalities interfere with individual perceptions and experiences regarding privacy and data protection?

R.Z._ Social and economic conditions result in asymmetrical positions when comparing citizens in absolutely different contexts. For example, for highly-educated and financially-privileged individuals, the possibilities for protecting their personal data are numerous. As a privileged individual in Brazil, you can afford to pay for encryption services and Virtual Private Networks (VPN). You can subscribe to Spotify and YouTube accounts and be less subject to massive data collection for behavioral advertising. You can pay for specialized services for masking personal information when registering a domain on the Internet. You can use paid email services, such as ProtonMail, which are secure and not very dependent on profiling and behavioral modulation. You can also choose not to rely on social networks, due to your economic status, and not be exposed to Instagram and TikTok. Furthermore, you do not need to use public policies and share your data with the Federal Government when participating in programs like the University for All Program (Programa Universidade de Todos [Prouni]) or the *Bolsa Família* (Brazilian federal cash transfer program).

Now, let's consider the opposite situation. As a vulnerable, precarious, and socially and economically marginalized person, you may only have access to the Internet through your mobile phone and will be subjected to massive extraction of personal data. You will use *freemium* accounts that will turn you into a product by modulating your behavior through profiling and behavioral advertising. You will not be able to afford any masking services when registering a domain for your small business website. When registering as an Individual Microentrepreneur (Microempreendedor Individual [MEI]), your personal data will be widely available. As a beneficiary of the Bolsa Família and Prouni programs, your personal data may be collected and shared through the Citizen's Base Register (Cadastro Base do Cidadão [CBC]). In short, your social relationships and exposure to what we refer to as "digital extractivism" will be entirely different from that of individuals from the upper or upper-middle class.

This is why, at Data Privacy Brasil, we say that a culture of personal data protection must be built considering power asymmetries and structural injustices in Brazil. A national personal data protection policy should not treat all Brazilians as equals, as mere "data subjects". While the principle of equality before the law is crucial, we need to enhance the discussion with a profound analysis of our inequalities and recognize how different social contexts give rise to different social dynamics, as well as processes of datafication and threats to rights that are also deeply different.

"Basically, the feedback loop mechanism of injustice operates as follows: If you are a user of public welfare policies, you become the target of massive data collection and an intense surveillance process by the State."

I.S.O._ What is the feedback loop of injustice? How does this process relate to the discussions about surveillance by the public and private sectors?

R.Z._ This is a great question. This concept has been used by the political scientist Virginia Eubanks to describe a situation of vulnerability of populations that rely on public policies in the United States of America. Basically, the feedback loop mechanism of injustice operates as follows: If you are a user of public welfare policies, you become the target of massive data collection and an intense surveillance process by the State. For instance, individuals receiving maternity benefits in marginalized communities are catalogued, with their digital footprints, such as the number of hospital visits, purchases from local pharmacies, and other types of data being recorded and consolidated into integrated databases.

Eubanks has demonstrated that many of these individuals who are beneficiaries of public policies and undergo intensified surveillance and data treatment, later face disadvantages in automated processes of analysis and decision-making, such as automated systems for job allocation, because the hyper-surveillance places that individual in a discriminated category in the subsequent automated analysis process. For example, automated systems for job allocation take into account if a person having been a user of public health services for a long period of time and can be considered an input to assess a higher degree of risk for that person in terms of stability. Consequently, these actions create a system that perpetuates automated and deeply invisible injustices.

Another very important philosopher who has reflected on this is Professor Anita Allen. She has even coined new concepts, which go beyond the notion of *panopticon* devised by Jeremy Bentham. For her, besides the *panopticon* as a surveillance architecture (those who are being watched cannot see who is watching), today we have a “complicated situation” for black people in the United States of America, who are also submitted to a hyper-surveillance, which gives rise to a form of *banopticon* (entry barriers, data-driven automated turnstiles, and profile-based exclusion situations) and *conopticon* (these same hyper-surveillance people are more susceptible to scams, frauds, harmful schemes, etc.). Both Allen and Eubanks are concerned about criticizing how contemporary societies can exacerbate inequalities and racism when using Artificial Intelligence (AI) and automated decision systems.

I.S.O._ What is the current debate regarding the biometric data collection in Brazil? What are the main risks associated with this practice?

R.Z._ Currently, we are faced with a dilemma driven by public security. There is a seductive belief regarding the promises that technologies will solve our social problems and the issues of violence and public safety. We are experiencing a naive technosolutionism.

Many mayors have embraced facial recognition as the main solution for public safety in open spaces as if it were a magical solution for combating crime. Brazilian cities like Salvador (Bahia) and Maringá (Paraná) are celebrating the use of modern systems to identify criminals at public events, such as carnivals or São João parties. However, this has been done with little consideration of the multiple risks associated with normalizing automated facial recognition in public places. There is a celebration of the "magical results achieved" through the automation of visual tasks that should be performed by police officers. However, these actions do very little to address the problems and its root causes.

This normalization is dangerous because it creates a false sense that the problems will be solved. It also creates a perverse stimulus for local governments to invest millions of Brazilian reals in facial recognition solutions, diverting already scarce resources from other public policies such as adequate food, healthcare, and professional training for young people in marginalized schools. The ones benefiting greatly from this are a few companies that charge inflated and artificial prices.

There are important counter-movements. The public civil action we conducted in 2018 against the improper treatment of biometric passenger data in the São Paulo subway, during the time I was at the Brazilian Institute of Consumer Protection (Idec) — the "Idec *vs*. Viaquatro" case, judged by the São Paulo Court of Justice [TJSP]), is an important example of the limits imposed by the judiciary. In this case, the justice system clearly stated that individuals cannot be treated as objects and have their emotions extracted from their faces without transparency, necessity, and respect for basic rights.

I believe this is an important remedy for the discussion on biometrics in Brazil. We are talking about its basic aspects. First, a simple conception, inspired by Kant: We are subjects in law, not things or lab rats that can be used. We have dignity and personality rights. Second, some essential questions: Do we really need it? Is it beneficial? Does it actually solve anything? That is why we insist on impact assessments and public debates that demonstrate that there are valid reasons behind these decisions.

"(...) this has been done with little consideration of the multiple risks associated with normalizing automated facial recognition in public places. (...) This normalization is dangerous because it creates a false sense that the problems will be solved."

Article II

Emerging privacy-enhancing technologies: Current regulatory and policy approaches[10]

By the Organisation for Economic Co-operation and Development[11]

This article examines privacy-enhancing technologies (PET), which are digital solutions that allow information to be collected, processed, analyzed, and shared while protecting data confidentiality and privacy. The text reviews recent technological advancements and evaluates the effectiveness of different types of PET, as well as the challenges and opportunities they present. It also outlines current regulatory and policy approaches to PET to help privacy enforcement authorities (PEA) and policymakers better understand how they can be used to enhance privacy and data protection and to improve overall data governance.

In particular, PET enables a relatively high level of utility from data, while minimizing the need for data collection and processing. PET are not new but the latest advances in connectivity and computation capacity have led to a fundamental shift in how data can be processed and shared. While still in their infancy, these developments hold immense potential to move society closer to the continuing process and practice of privacy by design, and thereby to foster trust in data sharing and reuse.

A growing number of policymakers and privacy enforcement authorities are considering how to incorporate PET in their domestic privacy and data protection frameworks. However, the highly technical and fast-evolving nature of these technologies often presents a barrier to implementation by organizations and to their consideration in policy and legal frameworks applicable to data.

[10] This material builds on the Organisation for Economic Co-operation and Development (OECD) work titled: OECD. (2023). Emerging privacy-enhancing technologies: Current regulatory and policy approaches, OECD Digital Economy Papers, No. 351. Paris: OECD Publishing, available at: https://doi.org/10.1787/bf121be4-en. The opinions expressed and arguments employed herein are entirely those of the authors and should not be attributed in any manner to the OECD or its Member countries.

[11] This report was drafted to OECD by Christian Reimsbach-Kounatze (Digital Economy Policy Division) together with an external consultant, Taylor Reynolds (Technology Policy Director of MIT's Internet Policy Research Initiative), under the supervision of Clarisse Girot (Digital Economy Policy Division).

The emergence of privacy-enhancing technologies

The collection and processing of personal data have changed in ways that could enable a more privacy-protective use of personal data at a technical level, moving society closer to the process and practice of privacy by design. A broad set of approaches is emerging based on new cryptographic techniques and structural changes to how data are processed. These approaches are introducing new privacy and digital security protections into data collection and processing.

While not fundamentally new,[12] these digital technologies and techniques provide novel and approaches to accountability and data protection while they are in use. They may also slightly alter the data while allowing them to be processed for certain uses without disclosing the information they contain. These approaches are often grouped together under the term "privacy-enhancing technologies" or PET. However, that term understates the essential role these disruptive technologies and approaches may have in data governance more broadly.

PET alters how organizations gather, access, and process data, particularly personal data. PET are promising because they expand access to data analytics while increasing digital security and privacy and data protection. For example, PET support collaborative analysis over data that would otherwise be too sensitive to disclose, combine, and use across individuals or entities.

Governments and regulators, most notably privacy enforcement authorities (PEA), have identified and emphasized these types of technologies as prominent solutions for privacy and personal data protection (European Data Protection Board [EDPB], 2020; European Union Agency for Cybersecurity [ENISA], 2021; Office of the Privacy Commissioner of Canada [OCP], 2021; White House [United States], 2022; Information Commissioner's Office [ICO], 2022).

The 2022 Communiqué Promoting Data Free Flow with Trust and knowledge sharing about the Prospects for International Data Spaces from the Roundtable of G7 Data Protection and Privacy Authorities (G7, 2022) recognizes that

> [t]he use of PET can facilitate safe, lawful, and economically valuable data sharing that may otherwise not be possible, unlocking significant benefits to innovators, governments, and the wider public. In recognition of these benefits … the G7 data protection and privacy authorities … will seek to promote the responsible and innovative use of PET to facilitate data sharing, supported by appropriate technical and organizational measures. (G7, 2022)

PET alters how organizations gather, access, and process data, particularly personal data (…) are promising because they expand access to data analytics while increasing digital security (…).

[12] The OECD held a ministerial conference in Ottawa, Canada in 1998 on realizing the potential of global electronic commerce. In international policy circles, the conference represented one of the first large-scale conferences devoted to Internet policy. The conference conclusions produced nearly 25 years ago in 1998 specifically called on governments to "encourage the use of privacy-enhancing technologies" (OECD, 1998).

The review of the implementation of the OECD (2013) *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (OECD Privacy Guidelines) highlighted the need to examine PET and their application to transborder data flows:

> Responding countries also agreed that further guidance is needed on available technical and organizational safeguards. Specifically, responding countries and experts pointed to the need for an in-depth examination of opportunities and barriers in the use of emerging new privacy-enhancing technologies (PET), including their application to transborder data flows. (OECD, 2021)

While some of these technologies are not new, many are evolving and may ultimately warrant a re-evaluation of regulations on data collection and processing. As one key challenge, these technologies often fall outside the radar of policymakers and regulators given their highly innovative nature of the technologies themselves and their application areas. In addition, the technologies are highly technical, creating a significant "language barrier" between engineers building these systems and the policymakers and regulators who will ultimately determine how to use them. These technologies, which are at different stages of development and maturity, will likely need to be part of broader data governance frameworks. This should ensure they are used in line with associated risks, including privacy risks, and that data are secure. Governments and PEA will increasingly need to consider how personal data are collected and processed with PET and how these technologies fit into their privacy and data protection frameworks.

Evolving paradigms

The evolution of paradigms for protection of confidentiality, integrity, and availability of data (data security) offers a good way to contextualize the changing landscape of privacy and data protection with respect to the new approaches to PET. Data security is undergoing a significant evolution. Initially, security sought to protect data at the perimeter of the organization. It is now moving to a new "zero trust" paradigm where the bad actors are already assumed to be inside the organization. Digital security, then, is accomplished by locking down all data except for specific approved uses by authorized people. Zero-trust approaches in digital security have helped mitigate the risk of damage that a bad actor can cause if they can gain access to internal digital resources.

A similar evolution could be seen as emerging in privacy and data protection. Today, privacy and data protection still primarily rely on rules for how data can be collected, processed, and used. Once the data are collected and/or transferred, "individuals then lose their capabilities to control how their data are re-used and to object to or (technically) oppose such uses and can rely solely on law en-

forcement and redress. The risks of loss of control are multiplied where the data are further shared downstream across multiple tiers, in particular when these tiers are located across multiple jurisdictions" (OECD, 2019). This increases the risk for large-scale data breaches and misuse such as in the case of Cambridge Analytica (Isaak & Hanna, 2018).

The evolving data governance paradigm enabled by PET follows a similar trajectory to the zero-trust approach in digital security: Trust is no longer assumed and personal data must remain protected in an adversarial environment. In this sense, PET can help ensure the continuity of privacy and data protection through technical means, even after data have been collected and eventually transferred to other entities, possibly including where these entities may be located out of the original jurisdiction. In so doing, they can effectively complement protection offered mainly by legal or contractual measures for such transfers. Therefore, PET should not be regarded as a "silver bullet" solution to all privacy and data protection challenges. PET, for example, do not necessarily help address issues related to undue biases which may be reflected in the original data. Their use can also not guarantee the security of the entire information technology (IT) systems that rely on the data for which PET are used. Consequently, PET cannot substitute legal frameworks but operate within them, so their applications will need to be combined with legally binding and enforceable obligations to protect privacy and data protection rights.

The evolving data governance paradigm enabled by PET follows a similar trajectory to the zero-trust approach in digital security: Trust is no longer assumed and personal data must remain protected in an adversarial environment.

Current definitions and categorizations of PET

TOWARDS A COMMON UNDERSTANDING OF PRIVACY-ENHANCING TECHNOLOGIES

Although the concept of PET is far from new and their use is spreading, it has never had a universally accepted definition. Over the years, different organizations have come up with definitions of PET and the categorizations of the corresponding technologies. Each one has its own merits and deserves consideration. However, these definitions and categorizations were also influenced by the context in which they were developed. They reflect the state of technology at any given time or the purpose of a study or project that the PET came to support.

The absence of a stable definition in this field can hinder a concerted analysis by policymakers, and privacy enforcement authorities in particular, of the potential impacts of PET on data protection and privacy assessments.

For this article, PET are understood as a collection of digital technologies, approaches, and tools that permit data processing and analysis while protecting the confidentiality, and in some cases also the integrity and availability, of the data and thus the privacy of the data subjects and commercial interests of data controllers.

PET typically are not stand-alone tools. Rather, they can be used in concert with other organizational and legal tools to implement data governance objectives. PET may rely on each other to function. In the same way that chefs use a variety of ingredients to form a recipe for a dish, PET are the ingredients that can be combined to achieve certain privacy and data protection objectives.

CATEGORIES OF PRIVACY-ENHANCING TECHNOLOGIES

Building on definitions and categorization of PET, this section proposes a new taxonomy for classifying PET. It assigns each PET (whether old, emerging, or eventual) to a category of technologies that addresses specific Basic Principle(s) of the OECD Privacy Guidelines. These categories are: (i) Data obfuscation, (ii) encrypted data processing, (iii) federated and distributed analytics, and (iv) data accountability tools.

- **Data obfuscation tools** include zero-knowledge proofs (ZKP), differential privacy, synthetic data, and anonymization and pseudonymization tools. These tools increase privacy protections by altering the data, by adding "noise" or by removing identifying details. Obfuscating data enables privacy-preserving machine learning and allows information verification (e.g., age verification) without requiring sensitive data disclosure. Data obfuscation tools can leak information if not implemented carefully, however. Anonymized data for instance can be re-identified with the help of data analytics and complementary data sets.
- **Encrypted data processing tools** include homomorphic encryption, multi-party computation including private set intersection, as well as trusted execution environments. Encrypted data processing PET allow data to remain encrypted while in use (in-use encryption) and thus avoiding the need to decrypt the data before processing. For example, encrypted data processing tools were widely deployed in COVID-19 tracing applications. These tools have limitations, however. For instance, their computation costs tend to be high although tools are emerging that address this limitation.
- **Federated and distributed analytics** allow executing analytical tasks upon data that are not visible or accessible to those executing the tasks. In federated learning, for example, a technique gaining increased attention, data are pre-processed at the data source. In this way, only the summary statistics/results are transferred to those executing the tasks. Federated learning models are deployed at scale, for instance, in predictive text applications on mobile operating systems to avoid sending sensitive keystroke data back to the data controller. Federated and distributed analytics require reliable connectivity to operate, however.

- **Data accountability tools** include accountable systems, threshold secret sharing, and personal data stores. These tools do not primarily aim to protect the confidentiality of personal data at a technical level and are therefore often not considered PET in the strict sense. However, these tools seek to enhance privacy and data protection by enabling data subjects' control over their own data, and by enabling them to set and enforce rules for when data can be accessed. Most tools are in their early stages of development, have narrow sets of use cases, and lack stand-alone applications.

Table 1 presents 14 PET, which were identified based on research and development in the private sector, including academic institutions such as the Massachusetts Institute of Technology (MIT). The PET are divided into the following four broad categories introduced above: (i) Data obfuscation, (ii) encrypted data processing, (iii) federated and distributed analytics, and (iv) data accountability tools. Some of the 14 PET can fit in more than one category; in which case they are assigned to a main category. It should also be noted that most PET, as discussed in this report, do not address the risk of group harm that would result from the potential misuse of insights gained from analyzing data that are made available through PET.[13] Table 1 also gives an overview of the major opportunities and challenges of PET.

[13] For discussion on the risk of group harm see (Hausman, 2007; Hausman, 2008; Harmon, 2010; Cargill et al., 2016).

Table 1 – OVERVIEW OF MAJOR TYPES OF PET, THEIR OPPORTUNITIES, AND CHALLENGES

TYPES OF PET	KEY TECHNOLOGIES	CURRENT AND POTENTIAL APPLICATIONS*	CHALLENGES AND LIMITATIONS
Data obfuscation tools	Anonymization / Pseudonymization	Secure storage	• Ensuring that information does not leak (risk of re-identification). • Amplified bias in particular for synthetic data. • Insufficient skills and competences.
	Synthetic data	Privacy-preserving machine learning	
	Differential privacy	Expanding research opportunities	
	Zero-knowledge proofs	Verifying information without requiring disclosure (e.g., age verification)	• Applications are still in their early stages.
Encrypted data processing tools	Homomorphic encryption	Computing on encrypted data within the same organization Computing on private data that is too sensitive to disclose Contact tracing/discovery	• Data cleaning challenges. • Ensuring that information does not leak. • Higher computation costs.
	Multi-party computation (including private set intersection)		
	Trusted execution environments	Computing using models that need to remain private	• Higher computation costs. • Digital security challenges.
Federated and distributed analytics	Federated learning	Privacy-preserving machine learning	• Reliable connectivity needed. • Information on data models needs to be made available to the data processor.
	Distributed analytics		
Data accountability tools	Accountable systems	Setting and enforcing rules regarding when data can be accessed Immutable tracking of data access by data controllers	• Narrow use cases and lack stand-alone applications • Configuration complexity • Privacy and data protection compliance risks where distributed ledger technologies are used • Digital security challenges • Not considered PET in the strict sense
	Threshold secret sharing		
	Personal data stores/ Personal Information Management Systems	Providing data subjects control over their own data	

Note: (*) Only one application has been included for the sake of readability.

Regulatory and policy approaches to PET

PET are often addressed explicitly and/or implicitly in countries' privacy and data protection laws and regulations through legal requirements for privacy and data protection by design and by default; requirements for de-identification, digital security, and accountability; and/or regulatory mandates to PEA to further promote adoption of PET.

These measures are often complemented by guidance issued by governments or PEA that help clarify the measures. However, regulators tend not to adopt definitive positions on the merits of certain PET to meet specific legal requirements, for example on cross-border data transfers, which underscores the difficulty in definitively validating specific PET solutions in a rapidly evolving landscape.

In addition, countries have adopted a wide variety of policy initiatives to promote innovation in and with PET. They do this through research and technology development, adoption of secure data processing platforms, certification of trusted PET, innovation contests, regulatory and other sandboxes, and deployment of digital identity solutions.

Conclusions

PET are at different stages of development and will likely need to be part of data governance frameworks to ensure they are used properly in line with the associated privacy risks. Many of these tools are still in their infancy and are limited to specific data processing use cases.

Given their innovative nature and high potential, PET warrant a comprehensive re-evaluation of the application of regulations on data collection and processing. It is important that this re-evaluation focuses on the effective privacy outcome that PET may contribute to rather than the processes of using a particular PET.

Policymakers, and PEA in particular, will increasingly need to consider how the use of PET may impact regulatory assessments under national privacy and data protection frameworks, taking into account the contribution of PET to privacy protective outcomes.

PET will require complementary tools, tests, and procedures to ensure they are used safely and in accordance with the law throughout the economy.

As PET mature, there will be an increasing need for awareness raising and training to better design, build, implement, use, and audit these new technologies.

Stronger cross-border and cross-sectoral regulatory cooperation will be needed to better consider technological developments on PET for privacy and data protection.

To this end, an analysis of concrete use cases of PET, including but not limited to the use of PET for facilitating cross-border data flows, may help inform policy discussions, including in respect to the privacy and economic outcomes PET promise to help achieve.

Given their innovative nature and high potential, PET warrant a comprehensive re-evaluation of the application of regulations on data collection and processing.

References

Cargill, S. S., DeBruin, D., Eder, M. M., Heitman, E., Kaberry, J. M., McCormick, J. B., Opp, J., Sharp, R., Strelnick, A. H., Winkler, S. J., Yarborough, M., & Anderson, E. E. (2016). Community-engaged research ethics review: Exploring flexibility in federal regulations. *IRB Ethics and Human Research, 38*(3), 11-19. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4997782/

European Data Protection Board (2020). *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*. European Data Protection Board, Brussels, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

European Union Agency for Cybersecurity (2021). *Data Pseudonymisation: Advanced Techniques and Use Cases*. European Union Agency for Cybersecurity, Athens, https://www.enisa.europa.eu/publications/data- pseudonymisation-advanced-techniques-and-use-cases

G7 (2022). *Communiqué Roundtable of G7 Data Protection and Privacy Authorities: Promoting Data Free Flow with Trust and knowledge sharing about the prospects for International Data Spaces.*

Harmon, A. (2010). Indian Tribe Wins Fight to Limit Research of Its DNA, *The New York Times*, https://www.nytimes.com/2010/04/22/us/22dna.html

Hausman, D. (2008). Protecting groups from genetic research, *Bioethics, 22*(3), pp. 157- 165, http://dx.doi.org/10.1111/j.1467-8519.2007.00625.x

Hausman, D. (2007). Group risks, risks to groups, and group engagement in genetics research. *Kennedy Institute of Ethics journal, 17*(4), 351-369. http://dx.doi.org/10.1353/KEN.2008.0009

Information Commisioner's Office. (2022). *Chapter 5: Privacy-enhancing technologies (PETs)*. Information Commissioner's Office, London. https://ico.org.uk/media/about-the-ico/consultations/4021464/chapter-5-anonymisation-pets.pdf

Isaak, J., & Hanna, M. J. (2018). User data privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer, 51*(8), pp. 56-59. http://dx.doi.org/10.1109/MC.2018.3191268

OECD (2021). *Report on the Implementation of the Recommendation of the Council Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD*, Paris.

OECD (2019). *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Reuse across Societies*. OECD Publishing, Paris, http://dx.doi.org/10.1787/276aaca8-en

OECD (2013). *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*. n. OECD/Legal 0188, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

OECD (1998). *Ministerial Declaration on the Protection of Privacy on Global Networks*. Abrogated on: 18/11/2016. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0301

Office of the Privacy Commissioner of Canada. (2021). *Privacy Tech-Know blog: Privacy Enhancing Technologies for Businesses*. https:// www.priv.gc.ca/en/blog/20210412/

White House [United States] (2022). *Request for Information on Advancing Privacy-Enhancing Technologies*. https://www.federalregister.gov/documents/2022/06/09/2022-12432/request-for- information-on-advancing-privacy-enhancing-technologies

Interview II

Data governance for personal data protection and digital security policies in Latin America

Photo: Personal archive

Carolina Botero Cabrera
Director of Karisma Foundation.

In this interview, Carolina Botero Cabrera, director of the Karisma Foundation, addresses the challenges for Latin America and the Caribbean (LAC) in establishing governance models that guarantee the privacy and protection of personal data, the current scenario of digital security policies in the region and the foundations of a privacy perspective based on Human Rights.

Internet Sectoral Overview (I.S.O.)_ Considering the growing demand for data use and the possible implications for ensuring privacy and personal data protection, is it possible to think of a data governance model for the Latin American and Caribbean (LAC) region? What aspects should be considered in the design of such a model?

Carolina Botero Cabrera (C.B.)_ Latin American countries have not only a similar history and experience, but also share many similarities regarding their legal framework. With regard to Human Rights, the Inter-American system has established a comprehensive legal framework that allows the region to have a reference and develop data governance models with common characteristics, which guarantee not only the right to privacy, but also the right to freedom of expression and access to information, for example.
With respect to privacy, the first problem is that data protection laws, which are necessary to think from the point of view of Human Rights and privacy guarantees, are not homogeneous in the region. On the other hand, data governance models are mainly based on the idea of facilitating exploitation models (also considering individual rights, based on individuals' consent to their management and exploitation by governments and private entities) and not based on justice (even if considered collectively). Therefore, it may be necessary to think about whether the LAC region would contemplate other types of visions regarding this governance.

I.S.O._ What is the current scenario for national digital security policies in the LAC region? What is their importance for the management of possible security incidents?

C.B._ When it comes to national digital security policies in the region, one should look to the Organization of American States (OAS), which has played an important role in the development and monitoring of these policies.

"Countries in the region are lagging behind to follow this path, to implement broader and more comprehensive visions from cybersecurity to digital security, and to invest more resources to be able to adequately respond to the challenge."

The OAS supported the development of the first generation of national digital security plans, which are currently being revised. Initially, these plans echoed the military origin of this discipline, focusing on critical infrastructure related to national security and adopting a vision in which individuals were considered passive recipients of these legal frameworks that, in addition to ensuring security, were also a way of expressing a securitization goal. The incident coordination and response function was consequently influenced by this perspective.

The OAS has conducted some evaluations (2016 and 2020) that allow us to analyze some of the impact, lessons learned, and obstacles faced by this first generation of plans. However, these evaluations are largely focused on State infrastructures, failing to analyze the impact on people in general. What is noticeable is that, in recent years, there has been a more realistic approach to the sector, which will have an impact on national policies.

Consider, for example, how ransomware, when it affects certain data systems (health systems, for example), represents a challenge for national security policies: It not only reveals weaknesses in the system but also in the State's capability to respond. It is also a challenge because it is a field that is traditionally associated with cybercrime, but which also touches on digital security – although they are different discussions, they come together in some areas.

Certainly, response structures, such as Computer Emergency Response Teams (CERT) and Computer Security Incident Response Teams (CSIRT), have provided a certain degree of reaction and mitigated the impacts somewhat. However, I realize that in very serious cases, such as Costa Rica's,[14] it was evident that such structures were not sufficient, and it was other countries and large companies that needed to provide first aid and contribute to the patient's recovery.

The OAS has carried out some additional assessments, considering, for example, the problem of labor demand and the shortage of professionals in this area. This is a global issue, but with specific numbers in the region. The data collected allows us to discuss the need to have a gender perspective for cybersecurity as well. This was a first step to recognize the need for more women working in this area.

Countries in the region are lagging behind to follow this path, to implement broader and more comprehensive visions from cybersecurity to digital security, and to invest more resources to be able to adequately respond to the challenge.

[14] Find out more: https://en.wikipedia.org/wiki/2022_Costa_Rican_ransomware_attack

I.S.O._ What are the main challenges to ensuring citizens' autonomy and self-determination over how different actors (public and private) use their personal data?

C.B._ It is a multi-stakeholder field, not all of whom have the same capacity to participate in the discussion or the same resources to implement what is decided. It is therefore problematic to start thinking about ensuring autonomy and determination as a level playing field for all actors except for the citizens.

As I said, there is no real commitment to privacy, as this would imply changing the economic model (which is not discussed); while in relation to existing data protection legislation, the opacity is worrying.

Although data protection laws have increased in the region, when we seek information on how our data is used, the rights we have or the responsibility for misuse, the policies of the entities are poor, confusing, general, if not non-existent. It is not possible to understand whether good or bad data management is done and, when incidents occur, nothing happens.

In the sectors that we have been monitoring, there is no information about data leakage (when it happens), and less about when incidents occur. In addition, incidents are not reported to response groups, there are no routes to report them, nor recommendations on how to deal with them. Now, in the current scenario, it is hard to think that the solution is to mandate incident reporting since there is not the trust needed for this to really strengthen the ecosystem. Perhaps, in this case, it is important to start with recommendations and responses that serve as an incentive.

"Although data protection laws have increased in the region, when we seek information on how our data is used, the rights we have or the responsibility for misuse, the policies of the entities are poor, confusing, general, if not non-existent."

I.S.O._ How can a Human Rights-based perspective on privacy contribute to the formulation of policies that mitigate the reproduction of social and economic inequalities?

C.B._ Promoting a Human Rights perspective where people are at the center means caring about what happens to people's data, seeking to reduce their risks and empowering them to make decisions about it. These kinds of perspectives change the landscape. For example, if we adopted this perspective, permissions for an app would be opt-in rather than opt-out, and we would ask for explanations of privacy and digital security risks.

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.[15] Considering members from both blocs, the 20 nations with highest activity sum more than 90.39 million registrations. In June 2023, domains registered under .de (Germany) reached 17.56 million, followed by China (.cn), the United Kingdom (.uk) and Netherlands (.nl), with 9.58 million, 7.45 million and 6.30 million registrations, respectively. Brazil had 5.16 million registrations under .br, occupying 5th place on the list, as shown in Table 1.[16]

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

[16] 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.

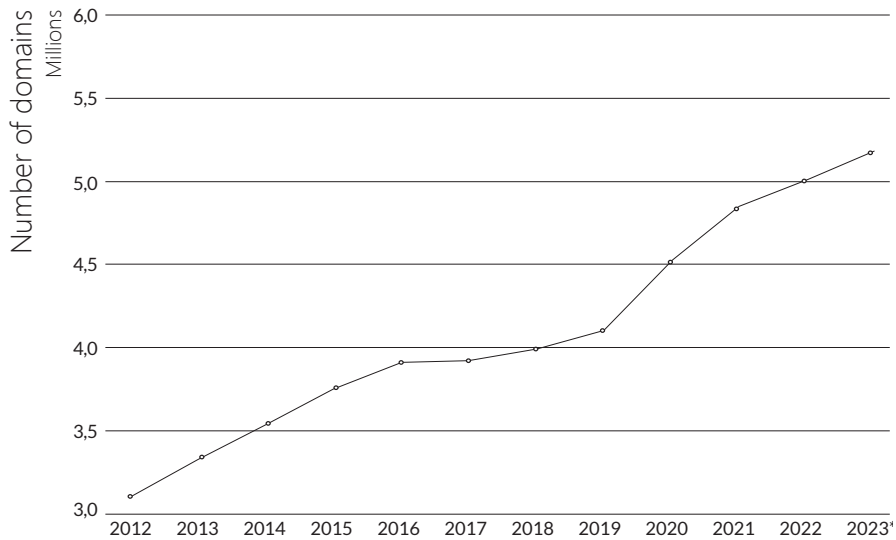
Table 1 – TOTAL REGISTRATION OF DOMAIN NAMES AMONG OECD AND G20 COUNTRIES

Position	Country	Number of domains	Date of reference	Source (website)
1	Germany (.de)	17,562,869	03/07/2023	https://www.denic.de
2	United Kingdom (.uk)	9,583,168	31/05/2023	https://www.nominet.uk/news/reports-statistics/uk-register--statistics-2023
3	China (.cn)	7,452,014	03/07/2023	https://research.domaintools.com/statistics/tld-counts
4	Netherlands (.nl)	6,306,044	03/07/2023	https://stats.sidnlabs.nl/en/registration.html
5	**Brazil (.br)**	**5,169,143**	**30/06/2023**	**https://registro.br/dominio/estatisticas**
6	Russia (.ru)	5,009,209	03/07/2023	https://cctld.ru
7	Australia (.au)	4,240,809	03/07/2023	https://www.auda.org.au
8	France (.fr)	4,065,102	01/07/2023	https://www.afnic.fr/en/observatory-and-resources/statistics
9	European Union (.eu)	3,660,646	03/07/2023	https://research.domaintools.com/statistics/tld-counts
10	Italy (.it)	3,493,525	04/07/2023	http://nic.it
11	Canada (.ca)	3,357,415	03/07/2023	https://www.cira.ca
12	Colombia (.co)	3,350,767	03/07/2023	https://research.domaintools.com/statistics/tld-counts
13	India (.in)	2,920,842	03/07/2023	https://research.domaintools.com/statistics/tld-counts
14	Switzerland (.ch)	2,549,083	15/06/2023	https://www.nic.ch/statistics/domains
15	Poland (.pl)	2,518,070	03/07/2023	https://www.dns.pl/en
16	Spain (.es)	2,059,470	28/06/2023	https://www.dominios.es/dominios/en
17	United States (.us)	1,900,711	03/07/2023	https://research.domaintools.com/statistics/tld-counts
18	Japan (.jp)	1,742,261	01/07/2023	https://jprs.co.jp/en/stat
19	Belgium (.be)	1,741,657	03/07/2023	https://www.dnsbelgium.be/en
20	Portugal (.pt)	1,714,217	03/07/2023	https://www.dns.pt/en/statistics

Collection date: July 3, 2023.

Chart 1 shows the performance of .br since 2012.

Chart 1 – TOTAL NUMBER OF DOMAIN REGISTRATIONS FOR .BR – 2012 to 2023*



* Collection date: June 30, 2023.
Source: Registro.br
Retrieved from: https://registro.br/dominio/estatisticas

In June 2023, the five generic Top-Level Domains (gTLD) totaled more than 190.32 million registrations. With 159.57 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**	159,570,312
2	**.net**	12,907,966
3	**.org**	10,760,810
4	**.info**	3,766,205
5	**.xyz**	3,318,500

* Collection date: July 3, 2023.
Source: DomainTools.com
Retrieved from: research.domaintools.com/statistics/tld-counts

Internet markers in Brazil

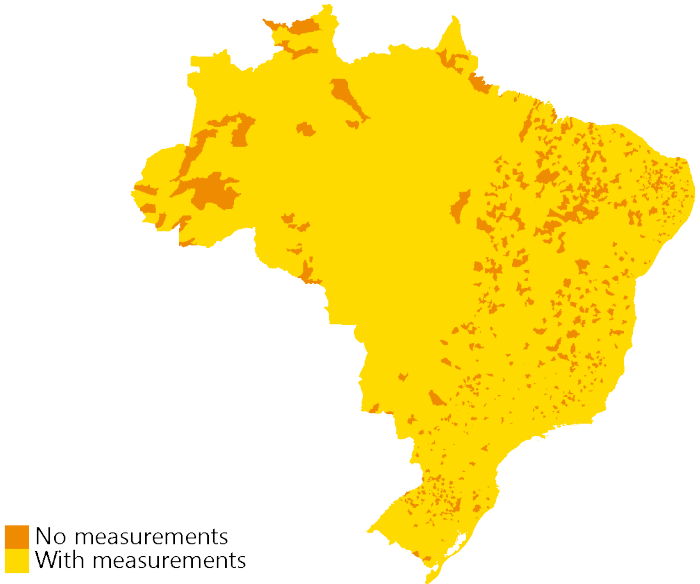
Indicators of the Internet Traffic Measurement System (SIMET)[17]

The Center of Study and Research in Network Technology and Operations (Ceptro.br)[18], a department of the Brazilian Network Information Center (NIC.br), is responsible for SIMET, a tool used to assess the quality of the Internet. The tests, conducted by users in real-time, collect various metrics, including latency, jitter, packet loss, and download and upload speeds.

The advantage of using SIMET is how the quality of the Internet is measured. Based on a methodology that aims to ensure unbiased and neutral measurements, the tests are primarily performed outside the network of the Internet service provider (ISP) or operator, to collect data with the highest possible quality of information.

Measurements can be carried using the Web (browser on any device with network access) or through the Mobile (application available for mobile devices). Over the last six months, 666,626 measurements were conducted across both modalities. Chart 1 illustrates the extent of voluntary measurements using SIMET: out of the 5,568 municipalities in Brazil, 4,676 (84%) had at least one measurement recorded during this period, while Chart 2 shows the number of measurements conducted per municipality.

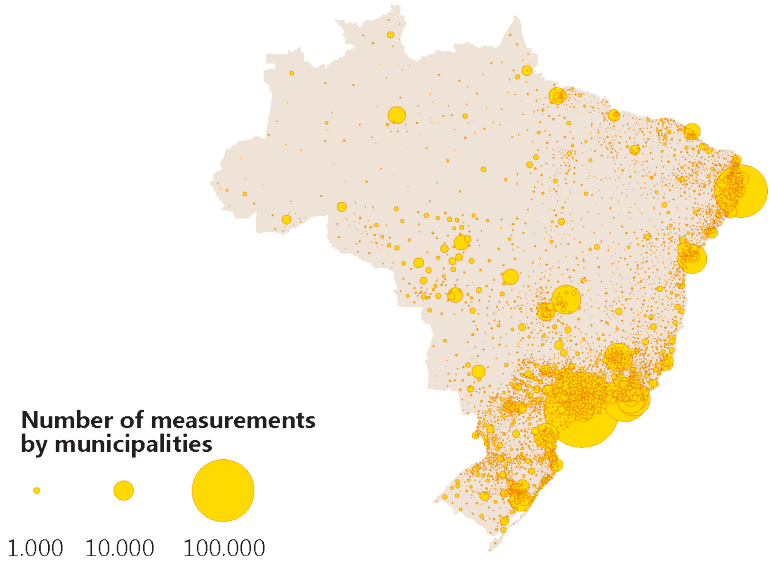
Chart 1 - MUNICIPALITIES WITH MEASUREMENT RECORDING FROM WEB AND MOBILE METERS



Collection Period: December 2022 to May 2023.
Source: Ceptro.br|NIC.br

[17] Find out more: https://medicoes.nic.br/
[18] Find out more: https://ceptro.br/

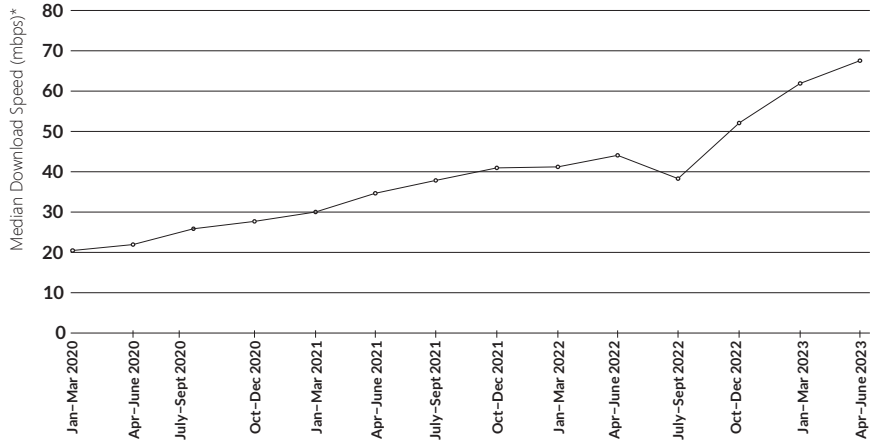
Chart 2 - NUMBER OF WEB AND MOBILE METER MEASUREMENTS, BY MUNICIPALITY



Collection Period: December 2022 to May 2023.
Source: Ceptro.br | NIC.br

Download speed, one of the metrics for analyzing the quality of the Internet, refers to the data transmission rate or speed at which transactions take place between the measuring servers and the measured device. The higher the speed, the better the connection. Chart 3 presents the median of total download speed measurements per quarter since 2020, while Chart 4 shows the median download speed for the last six months for each Federation Unit (FU).

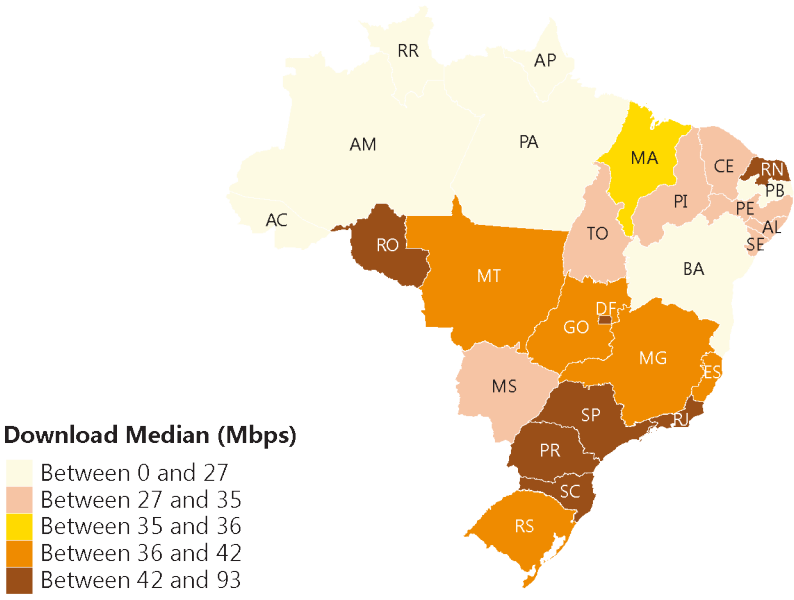
Chart 3 - DOWNLOAD SPEED MEDIAN BY QUARTER - 2020 TO 2023[19]



Collection Period: January 2020 to May 2023.
Source: Ceptro.br | NIC.br

[19] The fluctuations observed reflect existing variations in the proportion of measurements performed by mobile and web meters in each quarter. Despite this, there is a clear general trend toward an increase in download speed over time.

Chart 4 - DOWNLOAD SPEED MEDIAN BY FEDERATIVE UNIT



Collection Period: December 2022 to May 2023.
Source: Ceptro.br | NIC.br

Measurements are an essential subsidy to foster studies, generate analysis, and propose actions for a better Internet. The more measurements are taken in all Brazilian municipalities, the better the estimates of Internet quality will be.

Enterprises and the protection of personal data

Data from the ICT Households 2022[20] survey show that about 41 million Internet users in Brazil cited concerns about sharing personal information[21] as one of the reasons for not making online purchases.

In 2021, 78% of enterprises in Brazil reported retaining personal data: 67% indicate retaining data from clients and users, 62% retain data from partners and suppliers, and 37% from outsourced employees. The following indicators[22] show the actions[23] taken by these enterprises to comply with the Brazilian General Data Protection Law (Lei Geral de Proteção de Dados Pessoais [LGPD]).

ENTERPRISES BY TYPES OF ACTIONS TO COMPLY WITH THE LGPD (2021)

Total number of enterprises that keep individuals' data (%)

32% of enterprises have formulated a privacy policy that outlines how personal data is processed by the enterprise;

30% have conducted data leakage security tests;

24% have provided customer service channels for data holders, such as an email address, website, or other channels;

17% have appointed a Data Protection Officer (DPO), who is responsible for the communication between data subjects and the National Data Protection Authority (Autoridade Nacional de Proteção de Dados [ANPD]).

[20] Data from the ICT Households survey conducted by Cetic.br|NIC.br. Available at: https://cetic.br/pt/pesquisa/domicilios/

[21] Additional reasons for not making online purchases, as collected by *ICT Households survey* can be found at: https://cetic.br/pt/tics/domicilios/2022/individuos/H6/

[22] Data from the Privacy and Personal Data Protection *2021 survey: perspectives of individuals, enterprises and public organizations in Brazil*. Available at: https://cetic.br/pt/publicacao/privacidade-e-protecao-de-dados-2021/

[23] Additional types of actions related to LGPD compliance, as collected by the *Privacy and Personal Data Protection 2021* survey, can be found at: https://cetic.br/pt/publicacao/privacidade-e-protecao-de-dados-2021/

/Credits

TEXT

DOMAIN REPORT

Thiago Meireles (Cetic.br|NIC.br)

INTERNET MARKERS IN BRAZIL

Paulo Kuester, Solimary García, Cristiane Millan, and Gabriela Marin (Ceptro.br|NIC.br)

GRAPHIC DESIGN

Giuliano Galves, Larissa Paschoal, and Maricy Rabelo (Comunicação|NIC.br)

PUBLISHING

Grappa Marketing Editorial (www.grappa.com.br)

ENGLISH REVISION AND TRANSLATION

Ana Zuleika Pinheiro Machado and Robert Dinham

EDITORIAL COORDINATION

Alexandre F. Barbosa, Graziela Castello, Javiera F. M. Macaya, and Mariana Galhardo Oliveira (Cetic.br|NIC.br)

ACKNOWLEDGMENTS

Carolina Botero Cabrera (Karisma Foundation)

Christian Reimsbach-Kounatze (OCDE)

Manuella Maia Ribeiro, Ramon Silva Costa, and Winston Oyadomari (NIC.br)

Organisation for Economic Co-operation and Development

Rafael Zanatta (Data Privacy Brasil)

ABOUT CETIC.br

The Regional Center for Studies on the Development of the Information Society – Cetic.br (https://www.cetic.br/en/), a department of NIC.br, is responsible for producing studies and statistics on the access and use of the Internet in Brazil, disseminating analyzes and periodic information on the Internet development in the country. Cetic.br acts under the auspices of UNESCO.

ABOUT NIC.br

The Brazilian Network Information Center – NIC.br (http://www.nic.br/about-nic-br/) is a non-profit civil Entity in charge of operating the .br domain, distributing IP numbers, and registering Autonomous Systems in the country. It conducts initiatives and projects that bring benefits to the Internet infrastructure in Brazil.

ABOUT CGI.br

The Brazilian Internet Steering Committee – CGI.br (https://cgi.br/about/), responsible for establishing strategic guidelines related to the use and development of the Internet in Brazil, coordinates and integrates all Internet service initiatives in the country, promoting technical quality, innovation, and dissemination of the services offered.

*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.

unesco
Centre under the auspices of UNESCO

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

nic.br
Brazilian Network information Center

cgi.br
Brazilian Internet Steering Committee

STRIVING FOR A BETTER INTERNET IN BRAZIL

CGI.BR, MODEL OF MULTISTAKEHOLDER GOVERNANCE

https://cgi.br

nic.br cgi.br

FOTOS: RICARDO MATSUKAWA E SHUTTERSTOCK