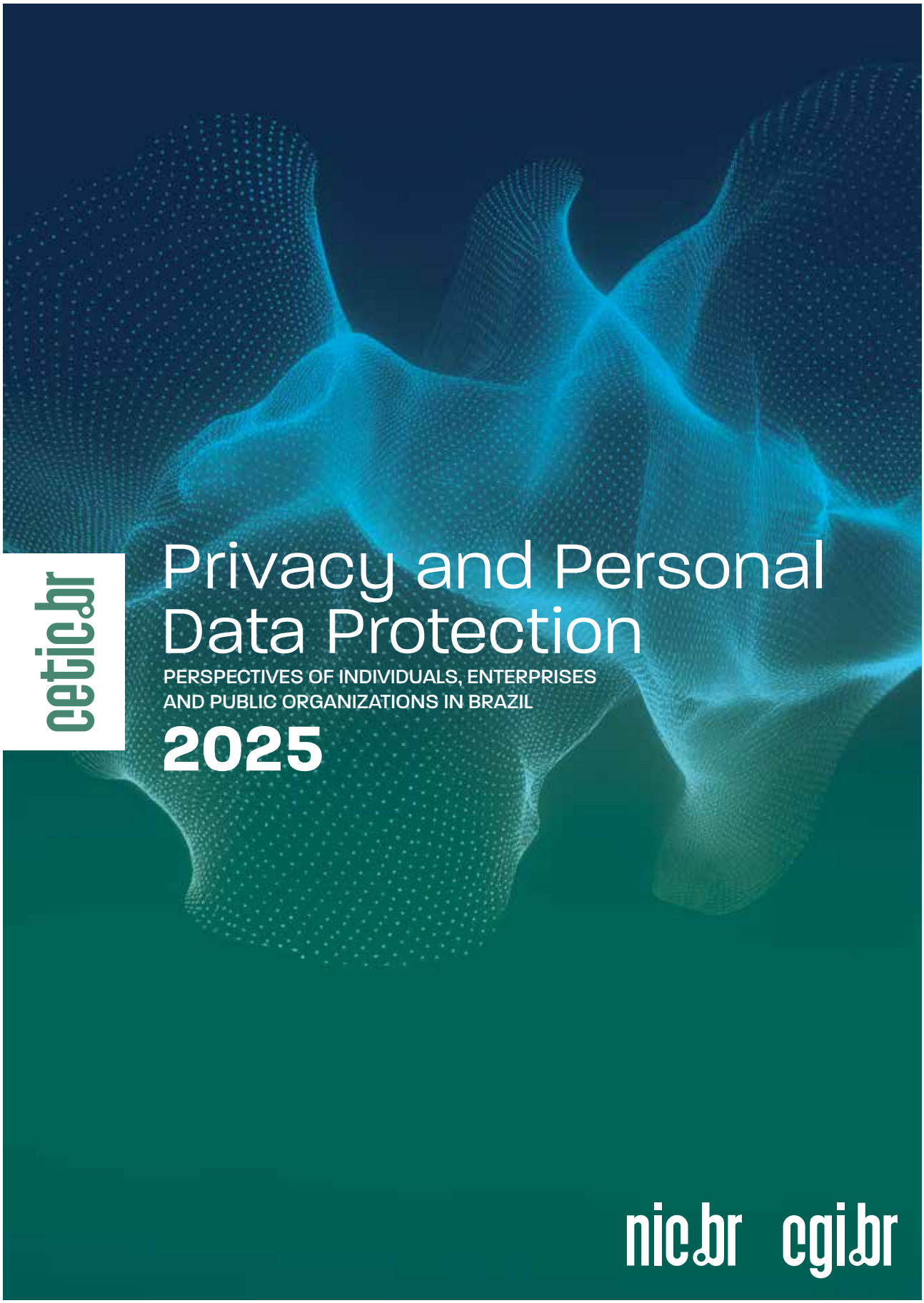


cetic.br

Privacy and Personal Data Protection

PERSPECTIVES OF INDIVIDUALS, ENTERPRISES AND PUBLIC ORGANIZATIONS IN BRAZIL

2025

nic.br cgi.br

creative commons Attribution NonCommercial 4.0 International

You are free to:

Share: Copy and redistribute the material in any medium or format.

Adapt: Remix, transform, and build upon the material.

The licensor cannot revoke these freedoms as long as you follow the license terms.

Under the following terms:

Attribution: You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

Noncommercial: You may not use this work for commercial purposes.

No additional restrictions: You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

http://creativecommons.org/licenses/by-nc/4.0/

Brazilian Network Information Center

Privacy and Personal Data Protection

PERSPECTIVES OF INDIVIDUALS, ENTERPRISES AND PUBLIC ORGANIZATIONS IN BRAZIL

2025

Brazilian Internet Steering Committee
www.cgi.br

São Paulo
2026

Brazilian Network Information Center – NIC.br

CEO : Demi Getschko
CFO : Ricardo Narchi
CTO : Frederico Neves
Director of Special Projects and Development : Milton Kaoru Kashiwakura
Chief Advisory Officer to CGI.br : Hartmut Richard Glaser

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

Executive and Editorial Coordination : Alexandre F. Barbosa
Research Coordination : Fabio Senne
Survey Project Coordination : Luciana Portilho and Manuella Maia Ribeiro (Coordinators), Ana Laura Martínez, Bernardo Ballardin, Daniela Costa, Fabio Storino, Leonardo Melo Lins, Lúcia de Toledo F. Bueno, Luísa Adib Dino, and Luiza Carvalho
Statistics and Quantitative Methods Coordination : Marcelo Pitta (Coordinator), Camila dos Reis Lima, João Claudio Miranda, Mayra Pizzott Rodrigues dos Santos, Thiago de Oliveira Meireles, and Winston Oyadomari
Sectoral Studies and Qualitative Methods Coordination : Graziela Castello (Coordinator), Javiera F. Medina Macaya, Manuela Cortez da Cunha Cruz, Mariana Galhardo Oliveira, and Rodrigo Brandão de Andrade e Silva
Process and Quality Management Coordination : Nádilla Tsuruda (Coordinator), Kayky Ferreira, Maísa Marques Cunha, and Rodrigo Gabriades Sukarie
Field management : Ipsos-Ipec: Alexandre Carvalho, Denise Dantas de Alcântara, Guilherme Militão, Ligia Amstalden Rubega, Monize Arquer, Moroni Alves, Paulo Henrique Vieira, and Rosi Rosendo (ICT in Education 2024 and 2025, ICT Enterprises 2025, ICT in Government 2025, and ICT in Health 2025); Quaest Pesquisa e Consultoria: Amábile Ochmat, Bárbara Lamounier, Bethânia Nascimento, Bruno Pinheiro, Giovani Roggia, Graziele Silotto, Guilherme Russo, João Zuquim, Maria Julia Timmers, Maria Luiza Oliveira, Matheus Moravia, Priscila Gregório, and Renata Salvo (ICT Panel)
Editing support team : Comunicação NIC.br: Carolina Carvalho, Kauã Oliveira, and Renata Barreto
Translation into English : Prioridade Consultoria Ltda.: Isabela Ayub, Lorna Simons, Luana Guedes, Luísa Caliri, and Maya Bellomo Johnson
Graphic design : Pilar Velloso
Publishing : Grappa Marketing Editorial (www.grappa.com.br)

Cetic.br Advisory Board

Carolina Botero Cabrera (Fundación Karisma), Eduardo Parajo (Durand Távola/Abranet), Guilherme Canela (UNESCO), Raúl Echeberría (ALAI), and Sonia Jorge (GDIP)

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Privacy and personal data protection 2025 [livro eletrônico] : Perspectives of individuals, enterprises and public organizations in Brazil / [editor] Núcleo de Informação e Coordenação do Ponto BR. -- São Paulo : Comitê Gestor da Internet no Brasil, 2026.
PDF

Bibliografia
ISBN 978-65-6165-031-1

1. Direito à privacidade 2. Empresas 3. Organizações públicas 4. Privacidade na Internet 5. Proteção de dados pessoais 6. Tecnologia da informação e da comunicação I. Núcleo de Informação e Coordenação do Ponto BR.

26-379004.0 CDD-004.6072081

Índices para catálogo sistemático:
1. Brasil : Privacidade e proteção de dados pessoais : Tecnologias da informação e da comunicação : Relatório de pesquisa 004.6072081

Brazilian Internet Steering Committee – CGI.br

(in August, 2026)

Coordinator
Renata Vicentini Mielli

Members
Alexandre Reis Siqueira Freire
Beatriz Costa Barbosa
Bianca Kremer
Cláudio Furtado
Cristiane Vianna Rauen
Cristiano Reis Lobato Flôres
Débora Peres Menezes
Demi Getschko
Henrique Faulhaber Barbosa
Hermano Barros Tercius
José Roberto de Moraes Rêgo Paiva Fernandes Júnior
Lisandro Zambenedetti Granville
Luanna Sant'Anna Roncaratti
Marcelo Fornazin
Marcos Adolfo Ribeiro Ferrari
Nivaldo Cleto
Pedro Helena Pontual Machado
Percival Henriques de Souza Neto
Rafael de Almeida Evangelista
Rodolfo da Silva Avelino

Executive Secretary
Hartmut Richard Glaser

Acknowledgments

The Privacy and Personal Data Protection 2025 survey relied on the support of an important group of experts, renowned for their competence, and that contributed significantly to the verification of results henceforward presented. This collaboration was instrumental for identifying new areas of investigation, improving methodological procedures and obtaining reliable data. It is worth emphasizing that the importance of new technologies for Brazilian society and the relevance of the indicators produced by the Brazilian Internet Steering Committee (CGI.br) for public policies and academic research motivated the specialists to participate in this collective effort voluntarily. The Regional Center for Studies on the Development of the Information Society (Cetic.br) would like to thank the following experts:

Alana Institute
Isabella Henriques

Brazilian Internet Steering Committee (CGI.br)
Bianca Kremer

Brazilian Network Information Center (NIC.br)
Jessica Maria dos Santos, Karen Ranieli Borges, Mariana Venancio Pereira, Nathan Paschoalini, Ramon Silva Costa, and Raquel Gatto

Brazilian Ministry of Health (MS)
Adriana Marques and Ana Estela Haddad

Center for Health Law Studies and Research (Cepedisa-FSP|USP)
Analluza Bolivar Dallari

Data Privacy Brazil
Rafael Zanatta

EducaDigital Institute
Priscila Gonsales

Federal University of Rio de Janeiro (UFRJ)
Chiara de Teffé

Getulio Vargas Foundation (FGV)
Erica Bakonyi and Walter Britto Gaspar

InternetLab
Fernanda Campagnucci

Law and Technology Research Institute of Recife (IP.rec)
Raquel Saraiva

Menke Law Firm
Fabiano Menke

National Data Protection Agency (ANPD)
Iagê Zendron Miola, Davi Teófilo Nunes Oliveira, Lucas Costa dos Anjos, Miriam Wimmer, and Waldemar Gonçalves

National Education and Research Network (RNP)
Yuri Alexandro

Pontifical Catholic University of Rio Grande do Sul (PUCRS)
Gabrielle Bezerra Sales Sarlet

Prado Vidigal
Ana Luiza Dornellas and Luis Fernando Prado

University of Virginia (UVA)
Yasmin Curzi de Mendonça

Contents

7 Acknowledgments

13 Foreword

17 Presentation

21 Introduction

23 **Executive Summary – Privacy and Personal Data Protection 2025**

31 **Methodological Report**

41 **Analysis of Results**

43 Internet users

67 Enterprises

89 Public organizations

116 List of Abbreviations

List of charts

27 Users of generative AI tools by frequency of use according to devices and level of education (2025)

27 Internet users who experienced situations involving scams, by channels where these situations occurred and access device used (2025)

29 Enterprises by whether they keep personal data of clients and users under 18 years old, size and sector (2021–2025)

29 Enterprises by origin of DPO (2021–2025)

47 Internet users by privacy concept category (2021–2025)

48 Internet users by personal data access management practices (2021–2025)

49 Internet users by personal data access management practices and access device used (2025)

51 Internet users by how often they agree with privacy policies without reading them and age group (2025)

52 Internet users by customer service channels sought out about personal data (2021–2025)

54 Internet users by level of concern about personal data, by activity carried out on the Internet (2025)

56 Internet users by level of concern about provision of sensitive personal information, by type of sensitive personal information (2025)

57 Users of generative AI tools by frequency of use according to devices and level of education (2025)

58 Users of generative AI tools by level of concern about the use of data by AI tool providers, according to devices and level of education (2025)

60 Internet users who experienced situations involving scams, by channels where these situations occurred and access device used (2025)

61 Internet users who experienced situations involving scams, by consequences of these situations and level of education (2025)

70 Enterprises by type of data kept on natural persons and size (2021–2025)

71 Enterprises by type of sensitive data kept (2021–2025)

72 Enterprises by whether they keep personal data of clients and users under 18 years old, size and sector (2021–2025)

73 Enterprises by how the personal data of customers and users is used (2021–2025)

74 Enterprises by purpose for using personal data of employees and size (2025)

75 Enterprises by whether they have carried out internal meetings to specifically address the topic of personal data protection in the last 12 months, size and sector (2021–2025)

76 Enterprises by presence of a specific area or employees responsible for personal data protection, size and sector (2021–2025)

77 Enterprises by areas or departments of the persons responsible for personal data protection (2021–2025)

78 Enterprises by whether they hire third-party services, such as consultants or advisors, to help with the topic of privacy, data protection, and compliance with the LGPD, by size and sector (2021–2025)

80 Enterprises by type of action to comply with the LGPD (2021–2025)

82 Enterprises by type of action to comply with the LGPD requirements and size (2025)

83 Enterprises by origin of the DPO (2021–2025)

84 Enterprises by resources made available on their websites (2021–2025)

92 Federal and state government organizations, by whether there are areas or persons responsible for procedures and policies for the collection, storage, or use of personal data or for the implementation of the LGPD (2021–2025)

93 Local governments, by whether there are areas or persons responsible for procedures and policies for the collection, storage, or use of personal data or for the implementation of the LGPD (2021–2025)

94 Federal and state government organizations by actions related to the LGPD (2025)

96 Local governments by actions related to the LGPD (2021–2025)

98 Public healthcare facilities with an information security policy (2023–2025)

99 Public healthcare facilities with an information security training program for employees (2023–2025)

100 Public healthcare facilities by measures adopted concerning the LGPD (2025)

103 Public schools with documents that define the information security and data protection policies of the institution (2020–2025)

104 Public school managers, by pedagogical, administrative, or financial management activities carried out through the adoption of AI (2025)

105 Public school managers by topics discussed during meetings carried out with teachers, school professionals, family members, and legal guardians about the use of digital technologies in the institution in the 12 months prior to data collection (2024–2025)

106 Public schools by target audiences of discussions or lectures on privacy and data protection held at the school in the 12 months prior to the survey (2022–2025)

Foreword

The Internet is a network built over decades through collective effort. It has established itself as an essential infrastructure for contemporary society, enabling economic activities, public policies, fundamental services, and various forms of social interaction. More than just offering a set of applications and services visible to end users, the Internet operates on an open, neutral, interoperable, and distributed technical architecture, whose integrity is a prerequisite for innovation, inclusion, and the exercise of rights in the digital environment.

Following the guiding principles of the Internet and in constant interaction with the Brazilian Internet Steering Committee (CGI.br), the Brazilian Network Information Center (NIC.br) plays its role in coordinating and strengthening the Internet in Brazil. In 2025, 20 years after its reconfiguration as a legal entity, NIC.br reaffirmed its commitment to managing critical network resources, operating stable infrastructure, and promoting a secure, accessible, and high-quality digital environment for Brazilians. This institutional milestone occurred in an equally significant context, alongside the celebration of the 30th anniversary of CGI.br—internationally recognized as a successful experiment in multistakeholder Internet governance.

One of NIC.br's various areas of activity focused on digital security is the Brazilian National Computer Emergency Response Team (CERT.br), which has played a central role in coordinating incident responses, disseminating best practices, and strengthening technical capabilities for online security, contributing to the resilience of the country's Internet infrastructure. These actions are linked to the publication of extensive awareness-raising and training material, always reinforcing the importance of a preventive and collaborative approach to security in the digital environment.[1]

Promoting a more accessible and inclusive Internet is also part of NIC.br's agenda. The Web Technologies Study Center (Ceweb.br) plays a role in this area, developing initiatives focused on digital accessibility and the standardization of web technologies.[2]

[1] More information about these actions can be found at https://internetsegura.br/

[2] Among the initiatives related to technical standards, Ceweb.br|NIC.br was part of the committee that drafted the ABNT NBR 17225 standard, focused on accessibility requirements for web content and applications. More information at https://ceweb.br/projetos/norma-abnt/

In a more technical field, the Center of Study and Research in Network Technology and Operations (Ceptro.br) works to continuously improve Brazil's Internet infrastructure through initiatives to measure connection quality, disseminate best practices for network protocols, train professionals, and provide services essential to Internet operations.[3] It was also through the actions of Ceptro.br|NIC.br that the Brazil Internet Exchange (IX.br)[4] originated and operates. It currently reaches more than 40 Tbit/s of aggregate traffic in the 38 locations where it is present, being the largest set of Internet exchange points (IXPs) in the world, with approximately 3,900 participating Autonomous Systems (AS). It should be noted that the São Paulo point is currently the world's leading IXP.

Adding to NIC.br's efforts is the creation of the Brazilian Artificial Intelligence Observatory (OBIA). It provides data and indicators that broaden understanding of the impacts and challenges of Artificial Intelligence (AI) in the country, supporting public debate and the formulation of policies aimed at its responsible use.[5]

Throughout its activities, NIC.br maintains and supports initiatives to promote the Internet and its safe, responsible, and conscious use. Annual events such as Safe Internet Day,[6] the Seminar on Privacy and Personal Data Protection,[7] and the Symposium on Children and Youth on the Internet[8] represent the ongoing effort to coordinate technical, legal, and social debates on key issues on the digital agenda. These actions highlight the importance of protecting personal data, ensuring information integrity, and safeguarding rights in the digital environment, especially for children.

In this context, the Regional Center for Studies on the Development of the Information Society (Cetic.br) is the NIC.br department responsible for regularly producing indicators and analyses on access, use, and appropriation of information and communication technologies (ICT) in Brazil. Cetic.br|NIC.br has established itself as a national and international reference in the production of reliable, comparable data aligned with internationally recognized methodological standards, which support the formulation of public policies, academic research, and multisectoral debate on the development of digital technologies.

In 2025, Cetic.br|NIC.br expanded its participation in international forums and agendas, contributing empirical evidence and methodological expertise to debates within the scope of BRICS and the Southern Common Market (Mercosur) meetings,[9] as well as other multilateral spaces. In these instances, topics such as meaningful connectivity, AI adoption, and reducing inequalities in access to and use of digital technologies took center stage, underscoring the importance of comparable, context-specific indicators to guide both regional and international cooperation.

[3] The main projects and initiatives of Ceptro.br|NIC.br can be accessed at https://ceptro.br/#projetos

[4] More information at https://ix.br/

[5] More information at https://obia.nic.br/

[6] More information at https://www.diadainternetsegura.org.br/

[7] More information at https://seminarioprivacidade.cgi.br/

[8] More information at https://criancaseadolescentesnainternet.nic.br/

[9] Publications with BRICS and Mercosur, among other international organizations, can be accessed at https://cetic.br/en/publicacoes/indice/outros/

This year, Cetic.br|NIC.br began new studies focused on strategic topics for the development of the Brazilian digital ecosystem, such as the analysis of data center infrastructure, which is now essential for data processing, storage, and sharing, as well as for the expansion of applications based on cloud computing and AI. Another strategic topic concerns information integrity, which is central to analyzing information flows and trust in data sources, as well as to addressing challenges associated with misinformation in the digital environment.

By swiftly addressing emerging and relevant topics such as connectivity quality, digital competencies, privacy, AI use, critical infrastructure, and security, Cetic.br|NIC.br's surveys help understand the multiple factors that enable effective, meaningful connectivity. Measuring access remains essential, but it is increasingly necessary to understand the conditions of use, associated risks, and capabilities required for individuals and organizations to fully benefit from digital technologies.

The financial resources generated by .br domain registrations, managed by Registro.br|NIC.br, enable continuous investment in research, security, training, and technological development, sustaining a virtuous cycle that benefits the Internet in Brazil. In a scenario of rapid technological change and growing dependence on digital infrastructure, the governance model adopted by the country since 1995 remains current and fundamental, supporting an open, secure Internet guided by the public interest.

The purpose of this publication is to contribute to the quality of public debate and strengthen the formulation, monitoring, and evaluation of evidence-based public policies. By gathering reliable data and consistent analyses, NIC.br and CGI.br reaffirm their commitment to multistakeholder governance, the promotion of rights, the reduction of inequalities, and the construction of a more inclusive, accessible, and secure digital environment, capable of responding to contemporary challenges and expanding opportunities for Brazilian society.

Enjoy your reading!

Demi Getschko
Brazilian Network Information Center – NIC.br

Presentation

Personal data protection currently occupies a central position in the digital transformation of the economy, government, and social relations. In this context, the expansion of digital platforms, the increasing circulation of information, and the rapid adoption of Artificial Intelligence (AI) systems are creating new opportunities for innovation, efficiency, and development. At the same time, they are making the challenges associated with the responsible use of personal data, information security, and privacy protection increasingly complex.

Since the enactment of the Brazilian General Data Protection Law (LGPD),[1] Brazil has been consolidating a legal and institutional framework aimed at protecting these fundamental rights and building digital relationships based on trust. This process requires not only appropriate regulations, but also institutional capacity, cooperation among different sectors, and expert knowledge about the country's reality.

In this context, the third edition of the survey *Privacy and personal data protection: Perspectives of individuals, enterprises, and public organizations in Brazil* gains particular significance. It was produced by the Regional Center for Studies on the Development of the Information Society (Cetic.br), and it brings together indicators that provide a comprehensive, comparable understanding of how personal data protection is perceived and incorporated across different segments of society.

By focusing on individuals, the study reveals Internet users' concerns, behaviors, and practices regarding privacy and the use of their personal data. Regarding the business sector, it provides evidence allowing assessment of data processing practices, compliance with the LGPD, and enterprises' preparedness to address new regulatory requirements, including those related to the protection of children in the digital environment. Regarding the public sector, indicators from the ICT in Government, ICT in Health, and ICT in Education surveys contribute to the analysis of issues such as data governance, information security, and personal data protection in the digital transformation of public services.

[1] Available at https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm (in Portuguese).

This integrated perspective is one of the publication's main contributions. By bringing together citizens' perspectives and the practices of enterprises and government organizations, the indicators help identify progress, gaps, and inequalities, while also supporting the definition of priorities, improvements in regulations, and the formulation of policies better aligned with society's needs.

The systematic production of evidence is essential for the National Data Protection Agency (ANPD) to fulfill its responsibilities for regulation, guidance, oversight, and the promotion of a data protection culture. In a context marked by the expansion of AI and emerging regulatory agendas, such as the protection of children under the Brazilian Digital Statute of the Child and Adolescent (ECA Digital),[2] data-driven decision-making contributes to more effective and proportionate public action that can keep pace with technological developments.

This publication also reflects the importance of institutional cooperation. The partnership between ANPD and the Brazilian Network Information Center (NIC.br) has contributed to expanding knowledge, disseminating good practices, and strengthening public debate about privacy, data protection, and security in the digital environment. The Seminar on Privacy and Personal Data Protection,[3] promoted by the Brazilian Internet Steering Committee (CGI.br) and NIC.br, is a significant example of this joint effort and has become an established forum for dialogue among government, the private sector, the scientific community, and civil society.

With the release of this third edition, Cetic.br|NIC.br reaffirms its commitment to producing reliable information for the development of the information society in Brazil. It is therefore a pleasure to present a publication that helps transform evidence into knowledge and knowledge into better decisions. May its indicators support new research, policies, and initiatives that ensure technological innovation advances in a manner consistent with fundamental rights, public trust, and the development of a safer, more inclusive, and more responsible digital environment.

Waldemar Gonçalves Ortunho Junior
National Data Protection Agency – ANPD

[2] Available at https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/l15211.htm (in Portuguese).

[3] More information available at https://seminarioprivacidade.cgi.br/en/

Introduction

The expansion of the digitalization of economic activities, public services, and social relations has significantly increased the collection, use, and sharing of personal data worldwide. While data has become an essential resource for innovation, public policy implementation, and the development of more personalized products and services, its intensive use also increases the risk of unauthorized access, discrimination, fraud, and other practices that may compromise the protection and exercise of human rights. In this context, ensuring privacy and protecting personal data are necessary conditions for developing a digital environment that is both safe and responsible.

It was against this backdrop of the expanding use of personal data and the consolidation of privacy and data protection as a central issue for society that, in 2021, the Regional Center for Studies on the Development of the Information Society (Cetic.br) launched the first edition of the biennial Privacy and Personal Data Protection survey. Since then, the study has produced indicators on Internet users' perceptions and the practices adopted by enterprises and public organizations, making it possible to monitor the implementation of the Brazilian General Data Protection Law (LGPD)[1] and developments in this area in the country.

Compared with the previous edition, for which data was collected in 2023, Brazil's data protection landscape has undergone significant institutional, policy, and regulatory changes. The period was marked by the expansion of the responsibilities of the National Data Protection Authority, which was renamed the National Data Protection Agency (ANPD). New frameworks related to the use of digital technologies were also established, with implications for the processing of personal data, such as the Brazilian Artificial Intelligence Plan (PBIA) 2024–2028,[2] which incorporates privacy and security into its principles, and the Brazilian Digital Statute of the Child and Adolescent (ECA Digital),[3] which establishes specific rules for protecting this population in digital environments and assigns new regulatory and oversight responsibilities to the ANPD.

[1] Available at https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm (in Portuguese).

[2] Available at https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/plano-brasileiro-de-inteligencia-artificial (in Portuguese).

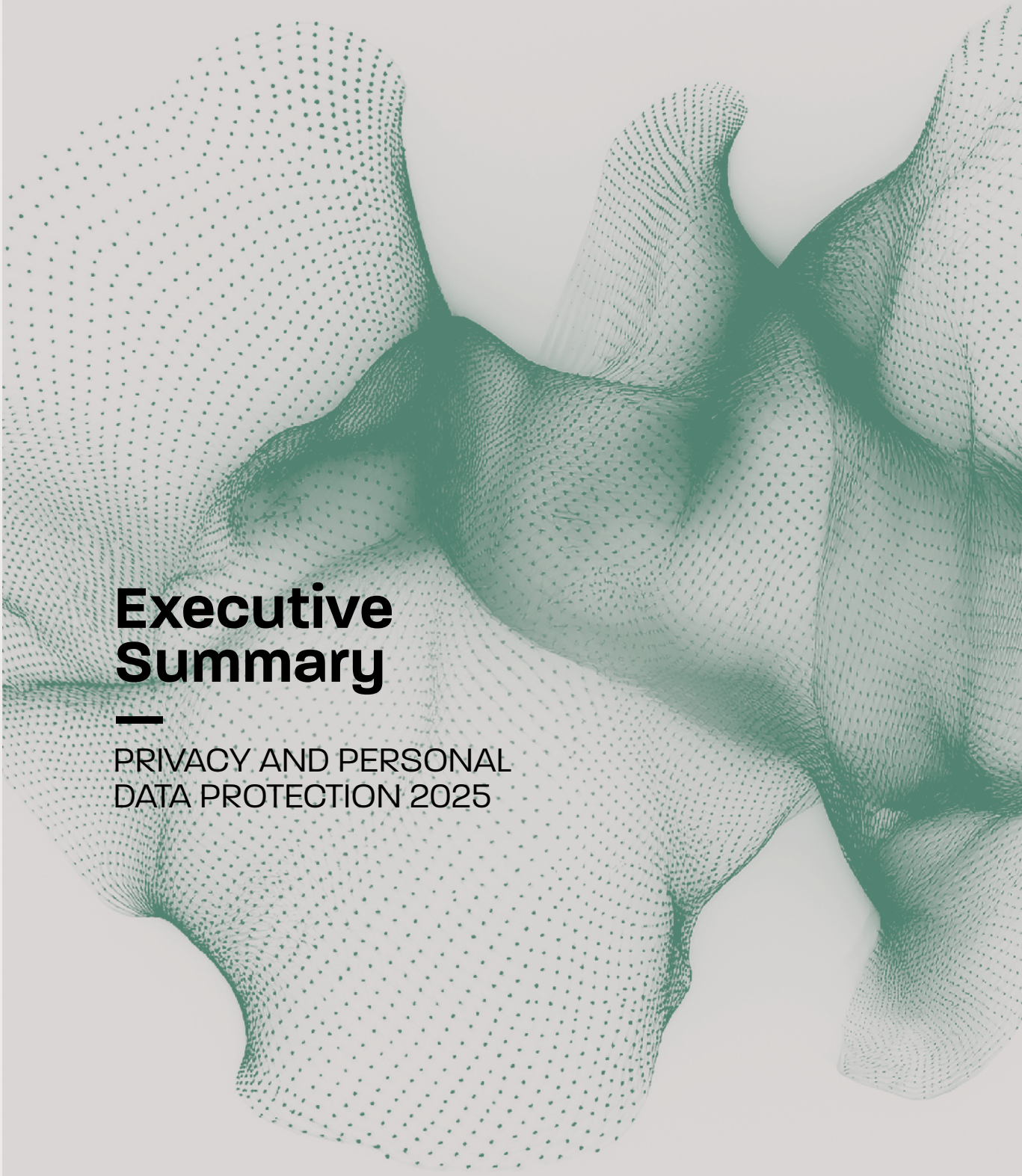
[3] Available at https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/l15211.htm (in Portuguese).

At the same time, Artificial Intelligence (AI) systems, such as generative AI, digital platforms, and other data-intensive technologies, are rapidly spreading, affecting individuals and both public and private organizations. In addition to creating opportunities, these applications introduce challenges related to transparency, security, the accountability of data processing agents, and the protection of more vulnerable groups, as they increase individuals' exposure to scams and fraud. In this context, producing evidence on public perceptions and the practices adopted by public and private organizations is essential for monitoring the implementation of the LGPD and other related legislation and policies, supporting regulatory activities, and guiding policies and strategies aimed at consolidating a culture of data protection in Brazil.

In its third edition, the Privacy and Personal Data Protection survey updates indicators collected in previous editions while also introducing a set of new data for 2025. Following the presentation of the methodological aspects that guided the study, the analysis of the publication's results is organized into the following chapters:

- **Internet users:** Presents the results of the ICT Panel, conducted in 2025 among Internet users 16 years old or older, which investigates users' perceptions of the processing and protection of their personal data. This edition also addresses new topics related to the use of AI and to scams and fraud.
- **Enterprises:** Identifies how small, medium-sized, and large Brazilian enterprises process personal data in the course of their activities, based on a specific module included in the ICT Enterprises 2025 survey.
- **Public organizations:** Presents results from the ICT in Government 2025, ICT in Health 2025, and ICT in Education 2024 and 2025 surveys, detailing data protection and privacy initiatives adopted, respectively, by federal and state government organizations and local governments, public healthcare facilities, and public primary and secondary schools.

With this publication, Cetic.br|NIC.br reinforces its commitment to producing and disseminating reliable and up-to-date statistics on the development of the information society in Brazil. By bringing together indicators from different sectors, this edition expands the evidence available to inform public policies, governance initiatives, and regulatory strategies related to privacy and personal data protection. Consolidating the survey's historical series makes it possible to monitor the evolution of this agenda in the country, providing evidence to track progress and challenges in implementing the LGPD and other regulatory frameworks that guide digital transformation in Brazil.



Executive Summary

—

PRIVACY AND PERSONAL DATA PROTECTION 2025

Executive Summary Privacy and Personal Data Protection 2025

Privacy and personal data protection have taken on an increasingly central role in international agendas, driven by the growing digitalization of processes and the adoption of Artificial Intelligence (AI) by public and private organizations. In this context, given the need for up-to-date information on the topic and the challenges associated with consolidating the Brazilian General Data Protection Law (LGPD)[1] in Brazil, since 2021, the Privacy and Personal Data Protection survey has brought together indicators on the practices and perceptions of individuals, enterprises, and public organizations related to fostering a data protection culture in the country. The third edition of the survey provides evidence for understanding how this topic has been perceived and incorporated into individuals' daily lives, while also identifying trends in the adoption of data protection compliance practices among public and private organizations and highlighting areas requiring attention in future initiatives.

MESSAGING APPLICATIONS (84%) AND PHONE CALLS (79%) ARE THE MAIN CHANNELS FOR SCAMS INVOLVING PERSONAL DATA

Internet users

PERCEPTIONS OF RISKS

The survey investigated Internet users' levels of concern regarding the exposure of their personal data in different online activities. The highest levels of concern were reported for making purchases online (35% were very concerned) and accessing banking services (32%), indicating that concerns are concentrated in situations that may result in financial losses. Differences were observed by age group and social class. Among younger users (16 to 24 years old), most reported being slightly or not at all concerned about the use of social media, whereas concern was greater among those 45 to 59 years old. Similarly, concern about government services was greater among individuals in classes AB (27%) than among those in classes DE (13%).

Despite this perceived risk, everyday personal data management practices showed no significant changes, revealing a gap between perception and behavior. This context provides a backdrop for analyzing emerging issues, such as the use of AI and the growing sophistication of digital scams and fraud, which introduce new challenges for data protection and increasingly affect the daily lives of Internet users in Brazil.

GENERATIVE AI

The 2025 edition introduces new indicators on the use of generative AI, including frequency of use, types of information provided, and levels of concern. Daily use was more frequent among users of this technology who accessed it through both mobile phones and computers, and among those with higher levels of education, suggesting that these tools have become part of the routine of certain segments of the population (Chart 1).

[1] Available at https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm (in Portuguese).

Among the types of information shared, the most common were work or study topics (73%), personal preferences and tastes (58%), feelings and emotions (54%), health data (52%), and photos of themselves or people they know (50%).

The use of generative AI has also expanded to activities involving advice, emotional support, and companionship. This type of interaction tends to encourage users to share intimate information and images. Most users (66%) reported being concerned or very concerned about how enterprises using these tools handle their data, suggesting they recognize the risks associated with these technologies.

SCAMS INVOLVING PERSONAL DATA

For the first time, the survey investigated scams involving personal data. In 2025, 32% of users experienced scam attempts involving their personal data, while 20% were actually victims of scams. The most frequently mentioned channels were messaging applications (84%) and phone calls (79%), followed by fake websites or apps (71%), SMS (71%), e-mails (69%), and social networks (67%). The results show that these scams occur through multiple communication channels, combining digital and traditional means to reach potential victims. This scenario demonstrates that exposure to fraudulent situations can affect even individuals who do not use the Internet, since scam attempts by phone and SMS are also common.

Significant differences were observed by devices used: Mentions of fake websites or applications were more frequent among users who accessed the Internet only through mobile phones, illustrating that limited connectivity may make security verification more difficult (Chart 2). In addition, the consequences of scams extend beyond financial losses, including emotional impacts and effects on well-being, with differences according to level of education.

Enterprises

STORAGE OF PERSONAL DATA

As in previous editions of the survey, in 2025, the type of personal data most frequently stored by Brazilian enterprises came from clients and users: 69% of enterprises reported storing this type of data, while 58% stored data from partners and suppliers. The same pattern was observed by enterprise size, with a higher proportion of large enterprises storing personal data from clients and users (73%). Regarding the types of sensitive personal data stored and investigated by the survey, biometric data remained the most frequently stored type of sensitive data (31%). This was followed by sensitive health data, stored by 26% of enterprises, a proportion that remained stable compared with the previous edition.

Among enterprises that stored personal data from clients and users, 9% reported storing personal data from individuals under 18 years old, with higher proportions among large enterprises (21%) and those in the accommodation and food service sector (19%) (Chart 3). Within this same group, 63% reported using this data to contact clients and users directly, while 39% used it for credit checks, a pattern that has remained unchanged since the first edition of the survey. Regarding internally generated data, 35% of enterprises used employees' personal data for performance evaluations, and the same proportion used it to monitor entry to and exit from workplaces.

69% OF ENTERPRISES STORE PERSONAL DATA FROM CLIENTS AND USERS

INTERNAL CAPACITIES

In 2025, 40% of enterprises held meetings specifically to address personal data protection, remaining stable compared with previous editions of the survey. As observed for other indicators, large enterprises held these meetings in a higher proportion (66%) than small enterprises (38%), with this pattern remaining stable throughout the historical series.

CHART 1

—

Users of generative AI tools by frequency of use according to devices and level of education (2025)

Total number of Internet users 16 years old or older who used generative AI tools (%)

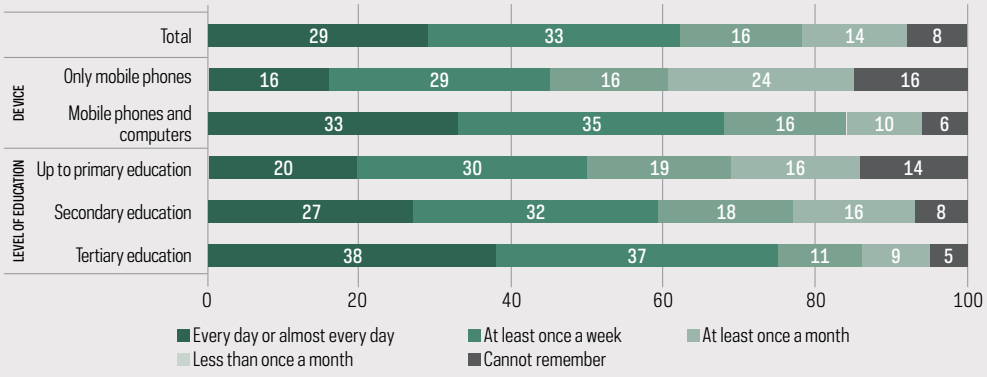
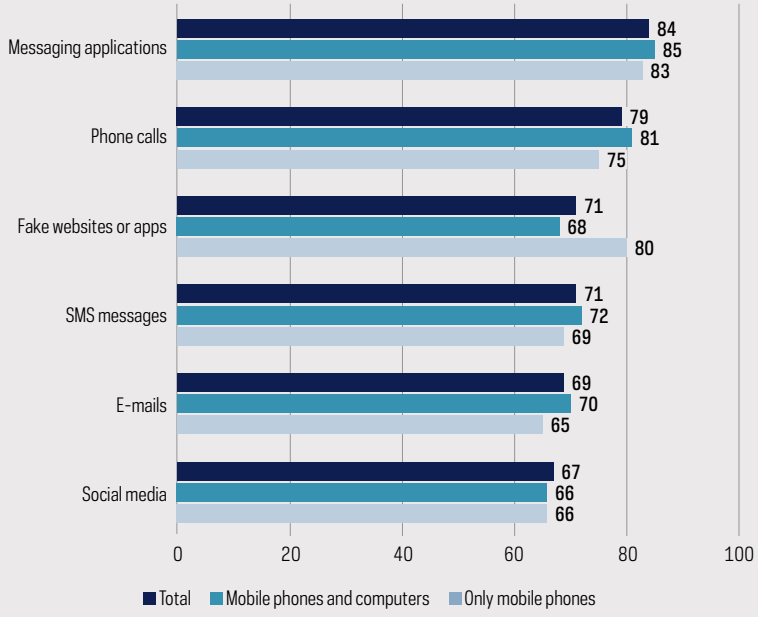


CHART 2

—

Internet users who experienced situations involving scams, by channels where these situations occurred and access device used (2025)

Total number of Internet users 16 years old or older who experienced an attempted scam or were victims of a scam using personal data (%)



Regarding organizational structure, 20% of enterprises had departments or employees responsible for privacy and personal data protection activities, a proportion that remained stable compared with previous years. By enterprise profile, large enterprises (55%) and those in the information and communication sector (39%) mobilized the most human resources specifically to address personal data protection.

COMPLIANCE WITH THE LGPD

In 2025, the measure most frequently adopted by enterprises was making changes to ongoing contracts to comply with the LGPD, reported by 30% of enterprises, maintaining the pattern observed in the previous edition of the survey. This was followed by formulating policies for the use of employees' personal data (29%) and formulating privacy policies (28%). Appointing data protection officers (DPO) was reported by 14% of enterprises. Among these enterprises, 28% reported that these professionals came from information technology (IT) departments, while 19% indicated they came from enterprises' administrative departments, a result consistent with the greater presence of organizational structures dedicated to privacy and personal data protection (Chart 4).

Survey methodology and access to data

The Privacy and Personal Data Protection 2025 survey gathered unpublished data collected by different surveys conducted by the Regional Center for Studies on the Development of the Information Society (Cetic.br) with individuals, enterprises, and public organizations in Brazil. The ICT Panel 2025 survey interviewed, via an online questionnaire, 2,500 Internet users 16 years old or older in December 2025. The ICT Enterprises 2025 survey included a specific module on the processing of personal data in the private sector. Interviews were conducted with 1,775 enterprises, which answered the module's questions, between February 2025 and January 2026. In addition to these unprecedented results, an analysis of Brazilian public organizations was carried out based on indicators related to privacy and personal data protection from the ICT in Government 2025, ICT in Health 2025, and ICT in Education 2024 and 2025 surveys. The survey results presented in this publication are available on the Cetic.br|NIC.br website (https://cetic.br). The "Methodological Report" is available in both the printed publication and on the website.

BOX 1

—

PRIVACY AND PERSONAL DATA PROTECTION IN THE PUBLIC SECTOR

As in previous editions, the third edition of the Privacy and Personal Data Protection survey includes a chapter on the public sector, based on indicators from the ICT in Government 2025, ICT in Health 2025, and ICT in Education 2024 and 2025 surveys. The analysis covers federal and state government organizations and local governments, public healthcare facilities, and public primary and secondary schools.

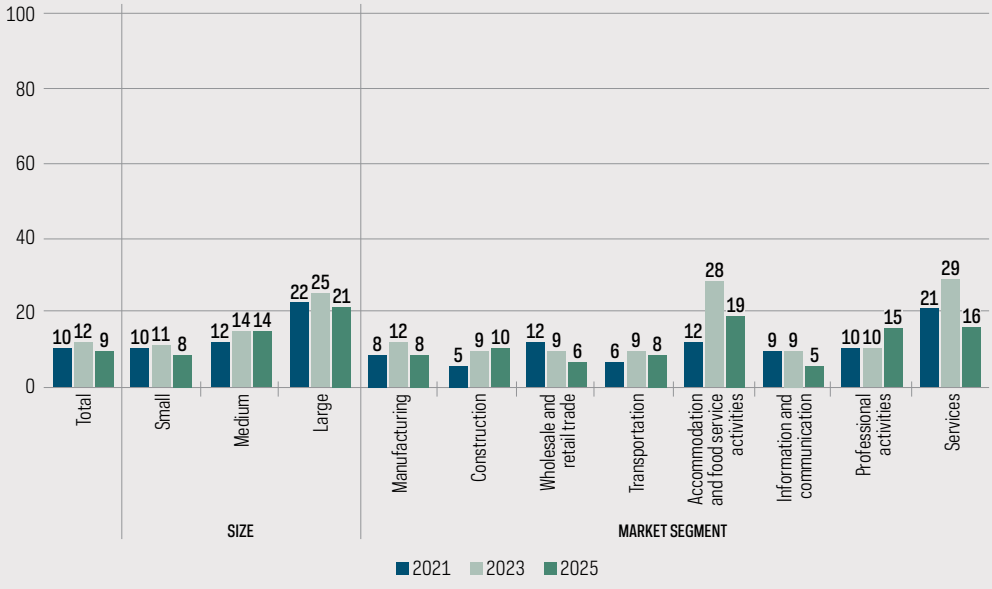
The increasing digitalization of public services and the adoption of AI applications are transforming how public organizations collect, process, share, and use personal data, creating new challenges for information security, data protection, and data governance. The results of this edition show progress in the adoption of information security policies, the designation of departments or individuals responsible for LGPD implementation, and training and awareness-raising initiatives. However, challenges remain in implementing specific measures to comply with the LGPD, such as consolidating governance structures and defining institutional responsibilities. The data also reveals inequalities across organization types, indicating that institutional capacity remains central to ensuring a safe and ethical digital transformation that can keep pace with the digitalization of public services.

CHART 3

–

Enterprises by whether they keep personal data of clients and users under 18 years old, size and sector (2021–2025)

Total number of enterprises that keep personal data of clients and users (%)



Sensitive data stored by enterprises in 2025:

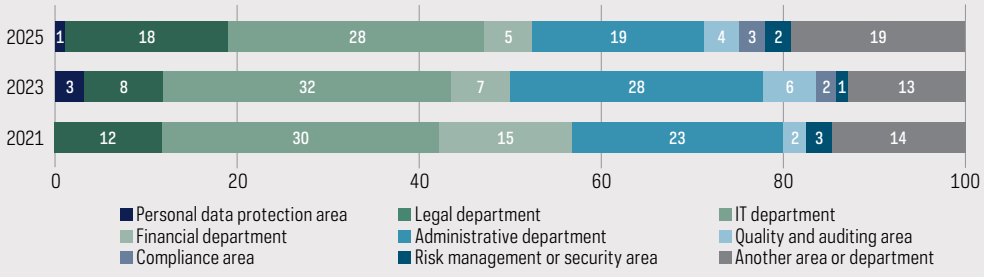
31%	26%	16%	12%
stored biometric data	stored health data	stored data on race or color	stored data on sexual orientation

CHART 4

–

Enterprises by origin of DPO (2021–2025)

Total number of enterprises whose DPO came from inside the enterprises (%)



Access the full survey data!

In addition to the results presented in this publication, tables of indicators, questionnaires, information on how to access the microdata, and the presentation of the results of the launch event are available on the Cetic.br|NIC.br website, as well as other publications on the topic of the survey.

The tables of results (https://cetic.br/en/pesquisa/privacidade-e-protecao-de-dados-pessoais/indicadores/), available for download in Portuguese, English, and Spanish, present the statistics produced, including information on the data collected and cross-referencing for the variables investigated in the study. The information available in the tables follows the example below:

Code and indicator name

Population to which the results refer

PR9C - INTERNET USERS BY HOW OFTEN THEY AGREE WITH PRIVACY POLICIES WITHOUT READING WHAT THEY SAY

Total number of Internet users 16 years old or older

PERCENTAGE (%)		ALWAYS	ALMOST ALWAYS	SOMETIMES	RARELY	NEVER
TOTAL		23	29	25	14	10
SEX	Male	25	30	25	12	8
	Female	21	28	24	16	11
LEVEL OF EDUCATION	Up to primary education	24	23	25	15	13
	Secondary education	23	30	24	14	9
	Tertiary education	22	31	26	13	8
AGE GROUP	16 to 24 years old	25	29	23	13	10
	25 to 34 years old	27	27	21	16	9
	35 to 44 years old	22	34	24	11	8
	45 to 59 years old	23	28	25	15	8
	60 years old or older	13	24	32	13	18

Indicator responses

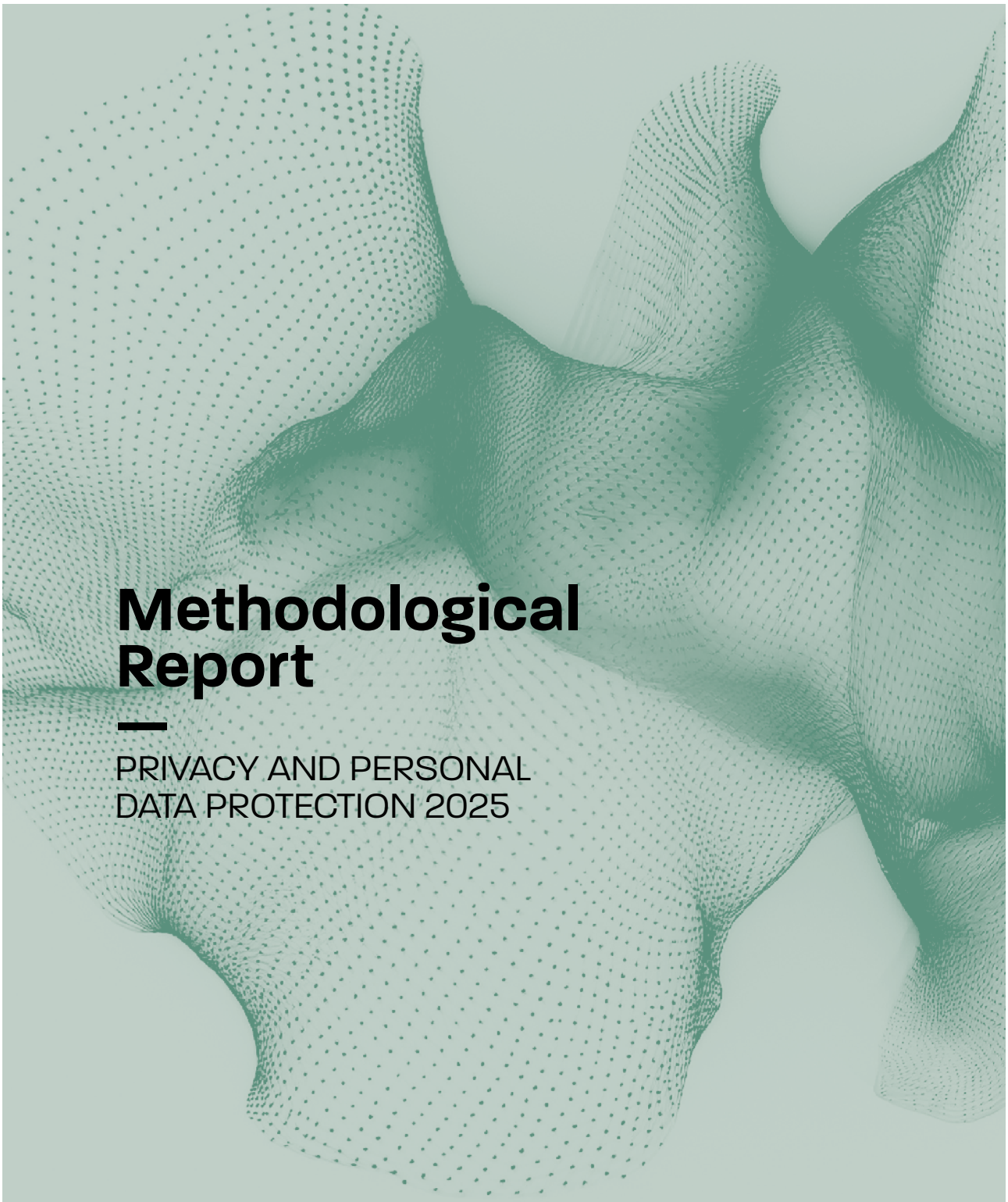
Results tabulation breakdowns: total (population as a whole) and characteristics of analysis (region, age group, etc.), different in each survey

Results: can be in % or totals

Source: Brazilian Network Information Center (2026). *ICT Panel 2025: Web survey with Internet users in Brazil: Privacy and data protection* [Tables].

How to reference the tables of indicators

This publication is also available in Portuguese on the Cetic.br|NIC.br website.



Methodological Report

—

PRIVACY AND PERSONAL DATA PROTECTION 2025

Methodological Report
Privacy and Personal Data Protection 2025

The Regional Center for Studies on the Development of the Information Society (Cetic.br), a department of the Brazilian Network Information Center (NIC.br) linked to the Brazilian Internet Steering Committee (CGI.br), presents the methodological aspects of the publication *Privacy and personal data protection 2025: Perspectives of individuals, enterprises and public organizations in Brazil*. The aim of the survey was to ascertain the current scenario and understand the main challenges to building a digital ecosystem that guarantees respect for privacy and the protection of personal data in the country. The information gathered was based on the collection and processing of quantitative data obtained through surveys conducted regularly by Cetic.br|NIC.br.

From the perspective of individuals, the information includes Internet users' perceptions of their rights and how their personal data is processed. Regarding organizations, the publication shows how enterprises and public organizations have been adapting to the topic of privacy and personal data protection since the Brazilian General Data Protection Law ([LGPD], Law No. 13.709/2018) came into force.

The project has three specific objectives:

- to investigate the perceptions of the population of Internet users about the use and protection of their personal data;
- to understand how small, medium, and large enterprises process the personal data of their clients/consumers, in addition to relevant issues associated with the implementation of the LGPD in Brazil;
- to outline a scenario of data protection in the context of public policies, including the adoption of practices by government agencies, healthcare facilities, and public schools.

Presented below are the main methodological aspects of the surveys carried out to collect indicators and the references for comprehensive access to the "Methodological Report" and the "Data Collection Report" of each survey.

ICT Panel – Internet users (2025)

The ICT Panel was created to collect information about Internet use during the pandemic caused by the novel coronavirus. Carried out via online questionnaires, the survey was developed as an alternative to in-person data collection, which was affected by social distancing measures imposed during this period. Since then, the Panel methodology has been adopted to collect data about other topics relevant to the discussion about digital transformation.

In 2021, a new module of the ICT Panel was developed to investigate the perceptions of the population of Internet users about the processing and protection of their personal data (CGI.br, 2021). Creating a specific module about privacy among Internet users was based on various previous surveys with converging objectives. One of the first data collections identified was *Special Eurobarometer 431: Data Protection*, of 2015, requested by the European Commission. Another relevant source was the June 2019 edition of the *American Trends Panel* of the Pew Research Center. Among official surveys produced by national statistics institutes, we considered the *Survey of Canadians on Privacy-Related Issues*, carried out in 2020 by the Office of the Privacy Commissioner of Canada.

The second edition of the ICT Panel COVID-19 survey of Cetic.br|NIC.br was also considered, which included a privacy module. This module was part of a regional effort led by the Inter-American Development Bank (IDB) to measure attitudes and perceptions related to personal data protection, considering the use of information and communication technologies (ICT) in pandemic containment measures (CGI.br, 2020).

The 2025 survey followed the objectives and references of the 2021 study. The target population was made up of individual Internet users 16 years old or older in Brazil, considering that users are people who used the Internet in the three months prior to the survey, following the methodological recommendation of the International Telecommunication Union (ITU, 2020).

For its sampling design, the survey used as a basis an online panel of individuals maintained by Quaest Consulting & Research (Quaest Consultoria e Pesquisa), with approximately 153,000 panelists. A quota sampling plan was employed to obtain the sample of respondents, considering the variables sex, age group, level of education, macro-region, social class, and propensity to be an Internet user. The data collection for the survey was carried out in December 2025; in all, 2,500 interviews were obtained.

With the objective of minimizing the selection biases found in quota approaches, a weighting structure was constructed for the ICT Panel, in which the reference was a probabilistic survey, ICT Households 2025.[1] First, the results were recalibrated to the population of the Continuous National Household Sample Survey (Continuous PNAD) (Brazilian Institute of Geography and Statistics [IBGE], n.d.), using the most recently published quarter.

[1] More information available at https://www.cetic.br/en/pesquisa/domicilios/

Subsequently, with the objective of estimating the contingent of the population represented by the respondents of the ICT Panel, a propensity score estimation procedure was adopted.[2] In this methodology, initially, the propensity scores for being an Internet user were calculated according to socioeconomic variables based on the last available edition of the ICT Households survey.[3] Next, this same model was used to estimate propensity scores for respondents of the ICT Panel.

Comparing the distribution of propensity scores for the ICT Panel with those verified in the last ICT Households survey, it was possible to determine which part of the last survey's population could be represented by the respondents of the Panel, including whether this representation covers the entire population. This is the equivalent of estimating the coverage error of the ICT Panel in relation to the target population initially considered for the survey. In the present edition of the ICT Panel, the represented audience is equivalent to the entire target audience of the survey: Internet users 16 years old or older.

ICT Enterprises – Small, medium, and large enterprises (2025)

Carried out since 2005, the main objective of the ICT Enterprises survey is to measure Brazilian enterprises' ownership and use of ICT. The survey presents indicators that translate the reality of Brazilian enterprises on various topics into numbers, such as access to ICT; Internet use; electronic commerce; ICT skills; software; and digital security and new technologies.

The universe covered by the survey consists of all active Brazilian enterprises with 10 or more employed persons[4] that are registered with the Central Register of Enterprises (*Cadastro Central de Empresas* [Cempre]) of IBGE and belong to the National Classification of Economic Activities (*Classificação Nacional das Atividades Econômicas* [CNAE 2.0]) market segments of interest to the ICT Enterprises survey and meet the definition of Legal Nature Type 2 – business entities, except for public enterprises (Legal Nature 201-1).

The surveyed enterprises operate in the following segments:

C – Manufacturing;

F – Construction;

G – Wholesale and retail trade; repair of motor vehicles and motorcycles;

H – Transportation and storage;

[2] Different from estimates based on a traditional sample design, the probabilities of selection in the Panel are unknown and undefined because it is a pseudo-sampling design. Pseudo-probability is the estimated probability of belonging to the non-probability sample used instead of a known probability. More information available in Baker et al. (2013).

[3] For this edition of the ICT Panel, the ICT Households 2025 (CGI.br, 2026) was used.

[4] The ICT Enterprises survey considers small, medium, and large enterprises with 10 to 49 employed persons, 50 to 249 employed persons, and 250 or more employed persons, respectively. Microenterprises, those with 1 to 9 employed persons, were not within the scope of the survey.

I – Accommodation and food service activities;

J – Information and communication;

L – Real estate activities;

M – Professional, scientific, and technical activities;

N – Administrative and support service activities;

R – Arts, entertainment, and recreation;

S – Other service activities.

The ICT Enterprises survey is developed to maintain international comparability. It uses the methodological standards proposed in the manual from the UN Trade and Development (UNCTAD, 2021), which was prepared in partnership with the Organisation for Economic Co-operation and Development (OECD), the Statistical Office of the European Union (Eurostat), and the Partnership on Measuring ICT for Development—a coalition formed by various international organizations that seeks to harmonize key indicators in ICT surveys.

The sampling plan for the present survey was stratified in two steps, and the enterprises were selected randomly within each stratum. The first step covered the definition of natural strata by correlating the variables geographic region and activity segment (CNAE 2.0). The final strata were defined from each natural stratum, which considered the division of natural strata by enterprise size.[5] In 2025, the survey interviewed 4,174 enterprises, of which 1,775 answered specific questions from the module about privacy and personal data protection.

Enterprises were contacted for interviews using the computer-assisted telephone interview (CATI) technique. In all enterprises, the survey sought to interview the persons in charge of information technology (IT), computer network management, or similar areas, which corresponded to positions such as:

- Information and technology directors;
- Business managers (senior vice presidents, business vice presidents, directors);
- Technology managers or buyers;
- Technology influencers (employed persons in commercial or IT operations departments who influenced decisions on technology issues);
- Project or system coordinators;
- Directors of other departments or divisions (excluding IT);
- System development managers;
- IT managers;

[5] The sizes considered were 10 to 19 employed persons; 20 to 49 employed persons; 50 to 249 employed persons; and 250 employed persons or more.

- Project managers;
- Enterprise owners or partners.

In large enterprises (250 or more employed persons), the strategy employed was to interview a second professional, preferably the accounting or finance manager. If neither professional was available, the next option was the person in charge of the administrative, legal, or government relations area, who responded only to questions about e-commerce and activities carried out on the Internet.

In 2025, to meet the demand for data about emerging topics, such as how small, medium, and large enterprises process the personal data of their clients/consumers, in addition to relevant issues associated with the implementation of the LGPD in Brazil, the ICT Enterprises survey began to collect data in three rounds. In each, specific modules for topics of interest were administered. In this edition, the privacy module was administered in two of the round: the second, between July and November 2025, and the third, between October 2025 and January 2026. The person within the enterprise most familiar with the topic was identified; this could be either the initial respondent or a person or department designated by the respondent. In all, 1,775 enterprises answered the survey.

ICT in Government – Federal and state government organizations and local governments (2025)

Carried out every two years since 2013, the survey on the use of ICT in the Brazilian public sector, ICT in Government, investigates the incorporation of digital technologies in public organizations and their use to offer public services. The study also measures the presence of initiatives that promote access to public information and society's participation through new technologies. Starting in 2021, new modules related to the adoption of new technologies and indicators about privacy and personal data protection were included.

The survey is carried out nationwide and includes two units of analysis: federal and state government organizations from all branches of power (Executive, Legislative, Judicial, and the Public Prosecutor's Office) and local governments. A census is conducted for all populations of interest, except State executive organizations, for which a sample of approximately 400 public entities is selected. The interviews are carried out using a structured questionnaire with the CATI technique. The indicators analyzed for this publication were collected between July 2025 and April 2026 from 576 federal and state government organizations and 3,253 local governments.

ICT in Health – Public healthcare facilities (2025)

Carried out annually since 2013, the ICT in Health survey has the objective of understanding the stage of ICT adoption in public and private healthcare facilities and its appropriation by nurses and physicians. To this end, it identifies the available technological infrastructure and investigates the use of systems and applications designed to support healthcare services and the management of healthcare facilities. In addition, it produces indicators on the activities carried out by professionals using these technologies, as well as on the motivations and barriers to their adoption and use.

In 2021, the survey began to examine how healthcare facilities were adapting to certain measures outlined in the LGPD. In 2022, the survey included indicators related to information security training, considering both training offered by healthcare facilities and training undertaken by professionals. The survey also includes information on whether healthcare facilities have information security policies and the information security tools they use.

The ICT in Health survey has national coverage and collects data from healthcare facilities at the three levels of care. The facilities were selected based on the National Registry of Healthcare Facilities (CNES), maintained by the Brazilian Ministry of Health. The interviews were carried out using the CATI technique, and the questionnaire was also made available for self-completion online via a specific platform. Data for the 2025 edition was collected between February and November of that same year from 3,270 managers, representing a total of approximately 129,000 Brazilian healthcare facilities.

ICT in Education – Public schools (2024 and 2025)

Carried out since 2010, the ICT in Education survey investigates access to, use, and appropriation of ICT by the educational community, especially students and teachers, in teaching, learning, and school management activities. Carried out nationwide, the survey is administered every year in Basic Education schools, both public and private, that are located in urban and rural areas and offer regular primary and secondary education classes. In the 2020 edition, the inclusion of a specific module on privacy, with questions about digital security and the collection and protection of personal data, allowed for a better understanding of the perceptions and experiences of different school players on this topic.

The data analyzed in this publication is based primarily on the indicators for the 2024 and 2025 editions of the ICT in Education surveys. The 2024 edition was carried out between August 2024 and March 2025, in person, via the computer-assisted personal interviewing (CAPI) technique, in 1,023 schools. In all, 7,476 students from the 4th year of primary education through the 3rd year of secondary education, 1,462 teachers, 864 directors of studies, and 954 school managers were interviewed. The data from the 2025 survey was collected between August 2025 and April 2026, via CATI, with 2,404 school managers.

Data dissemination

The results of the surveys mentioned above are presented according to the variables described in the "Methodological Report" for each survey, in the item "Domains of interest for analysis and dissemination."

Rounding made it so that in some results, the sum of the partial categories differed from 100% for single-answer questions. The sum of frequencies on multiple-answer questions is usually different from 100%. It is worth noting that, in cases with no response to the item, a hyphen (-) was used. Since results are presented without decimal places, cells displayed as zero indicate that there were responses to the item, but the underlying value is greater than zero and less than one.

The survey results are published on the Cetic.br|NIC.br website (https://cetic.br/). The tables of proportions, totals, and margins of error for each indicator are available for download in Portuguese, English, and Spanish. More information about the survey's documentation, metadata, and microdata datasets is available on the microdata page (https://cetic.br/microdados/).

References

Baker, R., Brick, J. M., Bates, N. A., Battaglia, M., Couper, M. P., Dever, J. A., Gile, K. J., & Tourangeau, R. (2013). *Report of the AAPOR Task Force on non-probability sampling*. https://aapor.org/wp-content/uploads/2022/11/NPS_TF_Report_Final_7_revised_FNL_6_22_13-1.pdf

Brazilian General Data Protection Law. Law No. 13.709, of August 14, 2018. (2018). Brazilian General Data Protection Law (LGPD). https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Brazilian Institute of Geography and Statistics. (n.d.). *Pesquisa nacional por amostra de domicílios contínua (Pnad Contínua)*. https://www.ibge.gov.br/estatisticas/sociais/trabalho/9173-pesquisa-nacional-por-amostra-de-domicilios-continua-trimestral.html

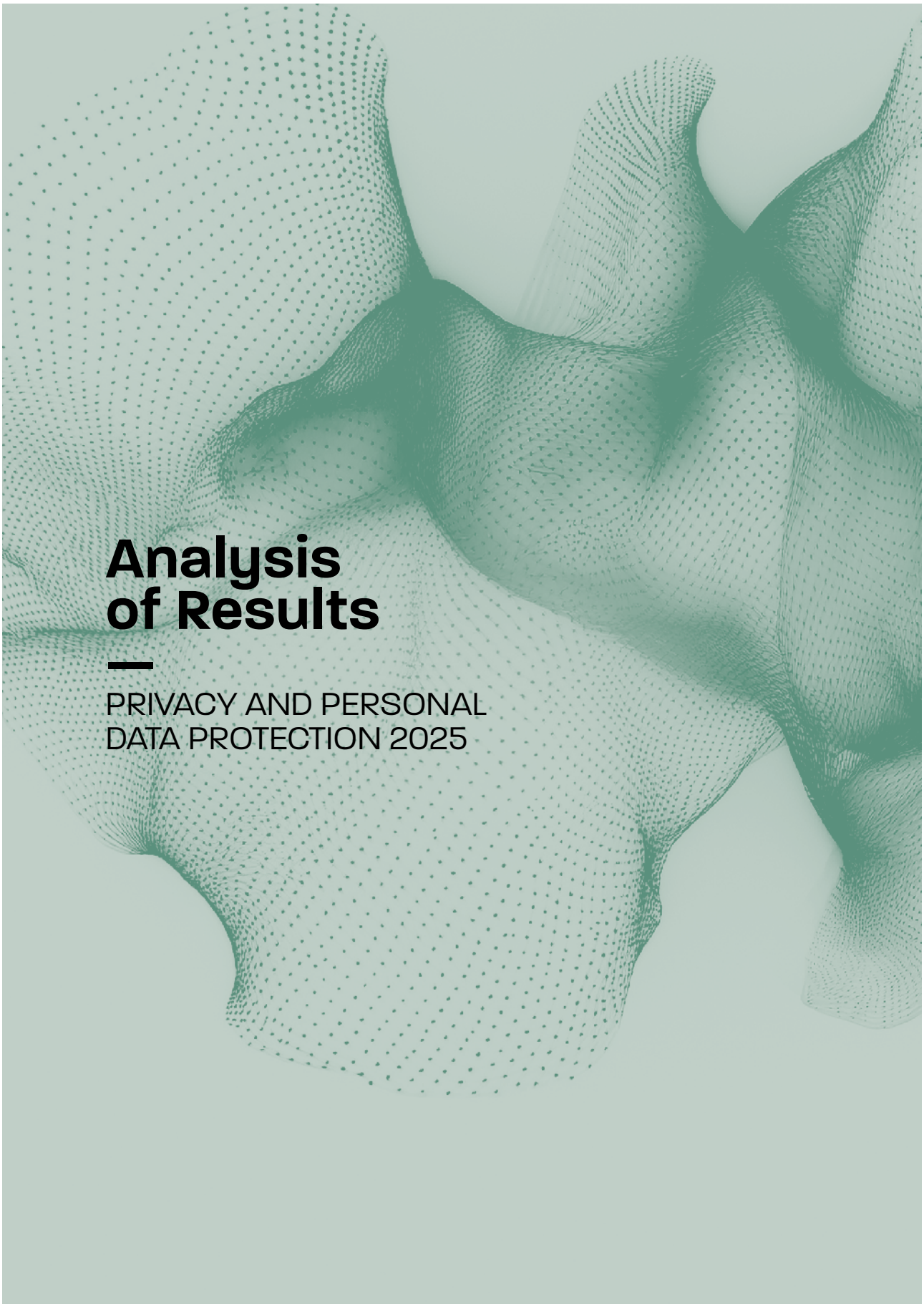
Brazilian Internet Steering Committee. (2020). *ICT Panel COVID-19: Survey on the use of Internet in Brazil during the new coronavirus pandemic - 2nd edition: Public online services, telehealth, and privacy*. https://cetic.br/en/publicacao/painel-tic-covid-19-pesquisa-sobre-o-uso-da-internet-no-brasil-durante-a-pandemia-do-novo-coronavirus-2-edicao-servicos-publicos-on-line-telessaude-e-privacidade/

Brazilian Internet Steering Committee. (2021). *Web survey on the use of Internet in Brazil during the new coronavirus pandemic: ICT Panel COVID-19*. https://cetic.br/en/publicacao/pesquisa-web-sobre-o-uso-da-internet-no-brasil-durante-a-pandemia-do-novo-coronavirus-painel-tic-covid-19/

Brazilian Internet Steering Committee. (2026). *Survey on the use of information and communication technologies in Brazilian households: ICT Households 2025*. https://cetic.br/en/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-nos-domicilios-brasileiros-tic-domicilios-2025/

International Telecommunication Union. (2020). *Manual for measuring ICT access and use by households and individuals, 2020 edition*. https://www.itu.int/en/ITU-D/Statistics/Pages/publications/manual.aspx

UN Trade and Development. (2021). *Manual for the production of statistics on the information economy 2020*. https://unctad.org/system/files/official-document/dtlstict2021d2_en.pdf



Analysis of Results

—

PRIVACY AND PERSONAL DATA PROTECTION 2025

Analysis of Results
Privacy and Personal Data Protection 2025
Internet users

In recent years, the increased availability of digital services, the intensification of the use of Artificial Intelligence (AI), the expansion of biometric data collection, and the growing incidence of scams and fraud involving personal data have made it even more essential to understand how individuals perceive the risks associated with the digital environment and what strategies they adopt to protect their information.

Increasing digitalization of Brazilian society has brought to light complex challenges related to privacy and the protection of personal data. In this scenario, the Brazilian General Data Protection Law ([LGPD], Law No. 13.709/2018) established an essential regulatory framework by defining fundamental rights for data subjects, such as access, correction, and deletion of personal information, in addition to fostering a data protection culture that involves both organizations and citizens. The National Data Protection Agency (ANPD), which is responsible for the regulation, implementation, and oversight of compliance with the LGPD, is part of this arrangement. Its transformation into a regulatory agency introduces changes to the institutional structure of Brazilian personal data protection policy, with implications for its autonomy and the exercise of its regulatory and supervisory duties.

To understand how these regulatory advances resonate in the daily lives of Brazilians, it is essential to investigate the perceptions, practices, and concerns of the population regarding the use of their data in the digital environment. In this context, the survey conducted by the Regional Center for Studies on the Development of the Information Society (Cetic.br), in its third edition, expands the scope of the investigation initiated in 2021. By consolidating this historical series, the survey allows us to track the evolution of Internet users' perceptions and practices over time, helping to identify changes in individual behavior in the face of technological and regulatory transformations.

This edition of the Privacy and Personal Data Protection survey presents the results of an online survey conducted with Internet users 16 years old and older that was dedicated to mapping the behavior and perceptions of individuals on central themes of the contemporary digital agenda. The questionnaire, developed based on international experiences from similar investigations in the United States (Auxier et al., 2019) and the European Union (European Commission, 2015), has been improved to incorporate new indicators that reflect emerging trends. In addition to delving deeper into topics

covered in previous editions—such as reading privacy policies and concerns about the use of biometric data—the survey introduces new questions about the use of AI and the growing exposure to scams and frauds that exploit personal data, topics that have grown in importance in the public debate in recent years.

By bringing these issues to light, this publication seeks not only to contribute to knowledge on the subject, but also to support the formulation and evaluation of public policies, awareness campaigns, and organizational strategies, in order to offer relevant information for researchers, organizations that process personal data, and others interested in promoting a safer and more transparent digital experience for all Brazilian citizens. This analysis is organized into the following themes:

- **Concepts of privacy:** Internet users' perceptions of what privacy means, collected through an open-ended question;
- **Data protection practices:** measures adopted by individuals to protect their data and seek support channels for requests, complaints, or reports;
- **Risk perception:** levels of concern regarding activities performed on the Internet and main perceived risks regarding personal data;
- **Sensitive data and biometric data:** levels of concern regarding the provision of various types of biometric data;
- **Generative AI:** frequency of use of generative AI tools, types of information provided, and associated levels of concern;
- **Scams involving personal data:** situations involving such scams, the channels through which they occurred, and the consequences of these episodes.

Concepts of privacy

To understand perceptions and practices related to privacy, the survey began the questionnaire with an open-ended question, which allowed for the unstructured capture of the different meanings of the concept attributed by users. This methodological approach aimed to avoid restricting responses to definitions previously established by the researchers, offering evidence of individuals' understanding of the term. The responses were analyzed and coded into broad categories, which made it possible to identify which domains people refer to when they think of "privacy," revealing how Internet users perceive the protection of their personal data.

METHODOLOGY

The approach revisits the classification methodology developed for the 2021 edition of the Privacy and Personal Data Protection survey (Brazilian Internet Steering Committee [CGI.br], 2022), reapplied and updated in the current edition (2025), with a new sample of manually classified responses and a readjusted predictive model. Initially, 500 responses were randomly selected and grouped into the six categories defined in the previous

publication[1]: freedom, individuality, data protection, control, security, and other. The classification strategy in 2021 had gone through three stages of development: (i) approximation with the categories of Auxier et al. (2019), from the Pew Research Center; (ii) creation of categories specific to the Brazilian context; and (iii) selection of the ideal number of categories by topic modeling, described in CGI.br (2022).

To begin the statistical analysis, the most frequently used words in the Portuguese language (stop words), accents, and special characters were removed, and only the roots of the remaining words were retained (stemming). From the new texts, descriptive analyses were performed to identify possible terms common to several categories without substantive meaning (also removed).

Given the limited number of responses, a cross-validation model was used to regularize the results, to prevent the model from being overfitted, that is, learning too much from only the manually classified responses and not being able to generalize to the other responses. The LASSO model with hyperparameterization of the penalty term (Friedman et al., 2010; Tibshirani, 1996) was applied, which identifies the best parameter to regularize the results. In this process, the texts were divided into five groups for cross-validation, repeated in ten different ways, to increase the reliability of the validation of the training data—that is, the ability to classify the 500 randomly selected responses.

Before deciding whether the model trained with the 2021 sample remained adequate to classify the 2025 responses or whether it would be necessary to train a new model, two validation scenarios were tested. The tests reproduce step-by-step the tokenization, modeling, and confusion matrices of each scenario:

- **New-Old:** The model trained in 2021 was applied directly, without retraining, to the 500 manually classified responses from 2025.
- **New-New:** The model was trained and evaluated by cross-validation (five groups, ten repetitions) exclusively for the 2025 sample.

The 2021 edition model applied directly to the new dataset (New-Old) performed considerably worse than retraining with 2025 data (New-New). For this reason, it was decided to train a new model with the 500 responses from the 2025 survey to generate population estimates for this edition, replicating the same architecture (LASSO with hyperparameterization of the penalty term and cross-validation).

To define the model adjusted to the present edition of the survey and applied to the new sample, two additional steps were carried out. In the first, the point estimate for the proportions of each category was calculated, adjusting their respective weights within the 2,500 responses (of which 500 were manually classified and the remaining 2,000 predicted by the model). In the second, 200 different subsamples were used in a bootstrap process, a resampling method, with updated weights for each of them. From this, an additional 200-point estimates were generated, allowing for the estimation of confidence intervals for the category portions. This made it possible to incorporate the uncertainty of the response classification process, considering the survey's sampling plan.

[1] The categories were not redefined in this edition as there were no significant differences in the context of the responses obtained.

To verify the robustness of these population estimates to different model specification choices, six alternative cross-validation specifications were tested, varying the number of groups, the metric used to choose the hyperparameter, and the selection rule. The selected option adopts the hyperparameter with the highest accuracy in absolute value, following the same selection rule as the 2021 edition, but now with ten groups and ten repetitions for cross-validation, instead of five and ten. The strategy combines a greater number of repetitions and a less conservative selection rule.

CLASSIFICATION OF RESPONSES

Six categories were created to represent different dimensions of the concept of privacy as expressed in the respondents' answers, and these categories were used to classify the 500 manually coded responses so that the model could assign them to the remaining responses, as follows:

- **Freedom:** guarantee of freedom in private aspects of life ("freedom" [one's own and others'], "right," "expression," "opinion," and "interference");
- **Individuality:** the pursuit of individuality, whether in spaces or situations ("individuality," "intimacy," "space," "private," "respect," "moment," and "alone");
- **Data protection:** the desire to protect your data from third parties ("data protection against third parties," "leaks," "information," and "confidentiality");
- **Control (of data):** desire to have control over one's own data ("control over data access," "choice of what is public," "consent," "access," "information," and "sharing");
- **Security:** more generic mentions of security ("security," "protection," "confidentiality," "monitoring," "keeping," and "trust");
- **Other:** valid responses not fitting into the other categories ("peace," "tranquility," "quiet," "important," "essential," "everything" [not elaborated], and "does not exist").

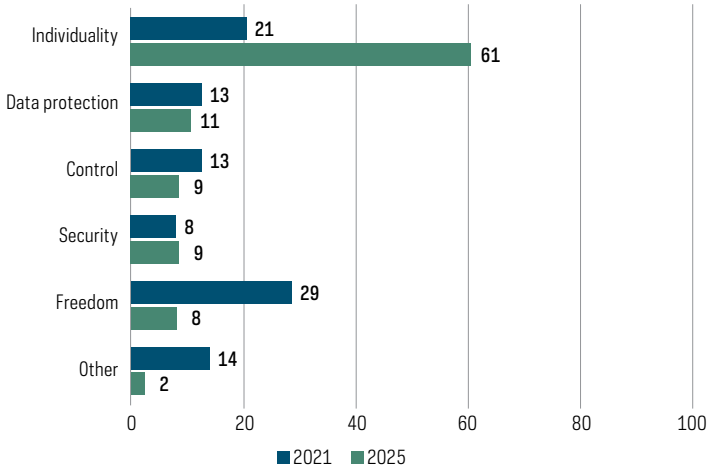
Compared to 2021, the 2025 results showed some changes in how Internet users associated different concepts with privacy. The category "Individuality," which remained the most frequent, showed an increase compared to the previous edition, while associations with "Freedom" decreased. "Data protection", "Control", and "Security" showed greater stability between the two editions (Chart 1).

CHART 1

—

Internet users by privacy concept category (2021–2025)

Total number of Internet users 16 years old or older (%)



Some categories showed conceptual proximity, which should be considered when interpreting the results. In some cases, there are subtle distinctions between "Individuality" and "Freedom." Similarly, "Control" is close to "Data Protection," since both categories refer to what third parties can do with the personal data or information of respondents, differing mainly in emphasis. While "Control" is associated with possession and control over information, "Data Protection" emphasizes protection against potential harm. The "Other" category, in turn, brings together heterogeneous responses that did not constitute meaningful groupings for disaggregation, including mentions ranging from "important" and "essential" to "does not exist."

In general, the results highlighted the diversity of how Internet users understand the concept of privacy and pointed to changes in relation to 2021. The increase in associations with "Individuality" and the reduction in mentions of "Freedom" may indicate stronger links between the idea of privacy and the protection of private life and intimacy, to the detriment of an understanding more tied to individual freedom. These changes are occurring in the context of an increasing digitalization of social relations and expansion of the collection, use, and sharing of personal data, so privacy is becoming increasingly related to the possibilities of defining limits on third-party access to personal information.

Data protection practices

The theme about these practices investigates how Internet users protect their personal data, what precautions they take in the daily use of the network and platforms, and how they proceed if there is a problem related to this issue. The analysis of these practices allows us to understand to what extent the growing concern with privacy and data protection translates into concrete user behaviors in the digital environment.

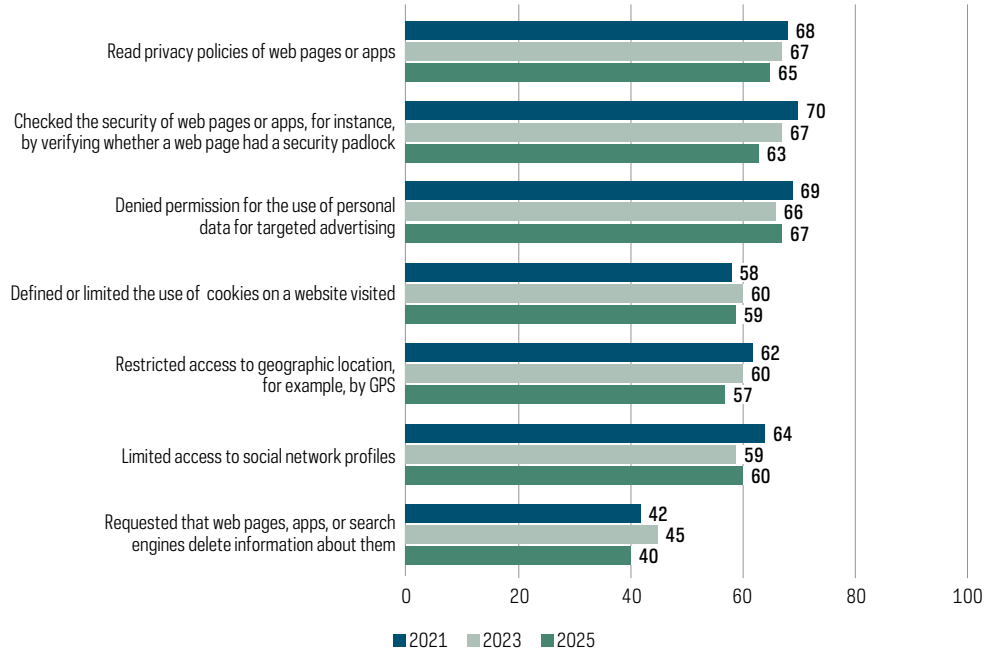
According to the survey, Internet users 16 years old or older most frequently reported denying permission for the use of their personal data for targeted advertising (67%), followed by reading the privacy policies of web pages or apps (65%), and checking the security of those sites or apps (63%). The least frequently mentioned activity was requesting that web pages, apps, or search engines delete information about them (40%), an action that requires knowledge about the possibility of data deletion and the contact channel to make the request. The survey estimates for all categories investigated remained stable in both 2021 and 2023 (Chart 2), indicating that transformations in the regulatory and technological context do not always translate, in the short term, into changes in the daily behavior of individuals.

CHART 2

—

Internet users by personal data access management practices (2021–2025)

Total number of Internet users 16 years old or older (%)



In 2025, 65% of Internet users accessed the Internet exclusively via mobile phones, while 34% also used computers. The distinction between these groups is relevant because the device used can affect browsing conditions, information viewing, and the performance of procedures related to the management and protection of personal data. As in previous editions of the survey, exclusive mobile phone users showed lower proportions of activities related to management of personal data than those who combined mobile phone and computer use (Chart 3). The largest difference in percentage points occurred in page security verification: While 70% of those using both devices stated that they checked the security of web pages or apps by verifying whether they had security padlocks, among those using only mobile phones, this proportion was 48%.

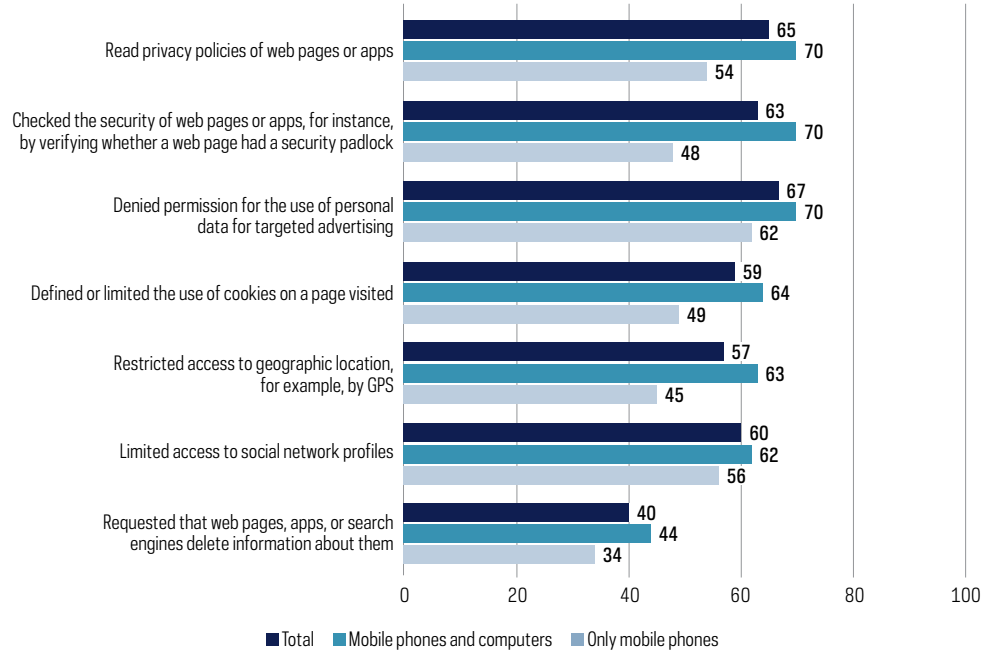
The three categories most mentioned by users who combined mobile phone and computer use were reading privacy policies, checking security, and denying permission for personalized advertising (all at 70%). Among exclusive mobile phone users, the category most mentioned was denying permission for personalized advertising (62%). These results reinforce that access conditions and available devices constitute significant dimensions of meaningful connectivity and can influence users' ability to adopt data protection practices in the digital environment.

CHART 3

—

Internet users by personal data access management practices and access device used (2025)

Total number of Internet users 16 years old or older (%)



Regarding personal data management practices, the survey supplemented the indicators with a question that reduces the possible effect of socially desired responses. Following the same hypotheses described in the previous study (that there may be a socially desired response effect or that there may be a heterogeneous understanding of what privacy policies are) (CGI.br, 2024b), in the 2025 edition, questions were repeated with formulations aimed at reducing these problems. The question about the frequency with which Internet users agreed to privacy policies without reading what they said indicated that the proportion of Internet users who always agreed was 23%, while another 29% stated that they almost always did so and 25% sometimes agreed without reading. In addition, only 14% rarely agree without reading, and another 10% never do.

As in 2023, the breakdown by age group showed significant differences. Among Internet users 25 to 34 years old, 27% stated that they always agreed with privacy policies without reading their content, a proportion that decreased to 13% among those 60 years old or older. Differences were also identified for the "rarely" and "never" alternatives in the 60 years old and older age group (Chart 4), which showed the highest proportions of individuals who rarely agreed with privacy policies without reading them (32%) and who never agreed (18%).

The data presented above suggests a relationship between the age group of users and their practices related to privacy and the protection of personal data, which may reflect differences in both the intensity of technology use and how different generations deal with digital risks and consent mechanisms. This phenomenon suggests a need for further investigation to understand to what extent and why this occurs. Furthermore, it also points to the importance of considering generational perspectives when formulating public policies aimed at strengthening the culture of data protection in the country.

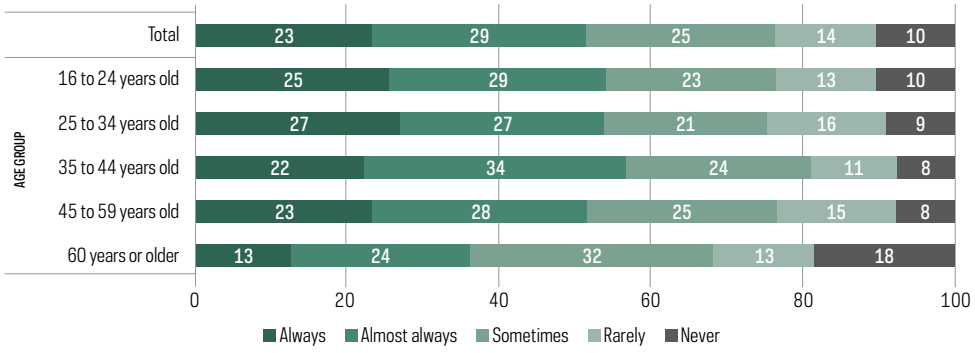
This hypothesis is corroborated by data from the ICT Households 2025 survey, which revealed significant differences in Internet use patterns between generations: While 95% of individuals 25 to 34 years old were Internet users, this proportion dropped to 54% among those 60 years old or older (CGI.br, 2026). This disparity in digital engagement paves the way for new survey questions about the influence of different patterns of technological appropriation on risk perceptions and self-protection attitudes in the online environment.

CHART 4

—

Internet users by how often they agree with privacy policies without reading them and age group (2025)

Total number of Internet users 16 years old or older (%)



Taken together, the two questions about privacy-policy reading practices suggest that individuals read them only occasionally (or only information they consider equivalent to them), but frequently accept the terms without reading them and do not consult these policies on all occasions when they are required to do so. Collectively, these results suggest that the growing concern about privacy and the protection of personal data does not necessarily translate into consistent practices of reading privacy policies, highlighting a mismatch between risk perception and behavior.

SEARCH FOR CUSTOMER SERVICE CHANNELS

According to the survey, in 2025, 26% of Internet users 16 years old or older sought some kind of customer service channel to make requests, complaints, or reports related to their personal data, a stable result compared to the two previous editions. The proportion was higher among male users (29%) than among female users (24%), and among those with tertiary education (29%) than among those with Primary (25%) and Secondary (26%) Education. Finally, it was also lower among Internet users aged 60 or older (17%) than among those 25 to 34 years old and 35 to 44 years old (29% each).

The understanding of what it means to seek customer service regarding personal data can be broad. The question explicitly states "requests, complaints, or reports," which may evoke a wide variety of situations in the respondent's memory. It is possible, for example, that some users consider searching for information about their personal data as seeking customer service.

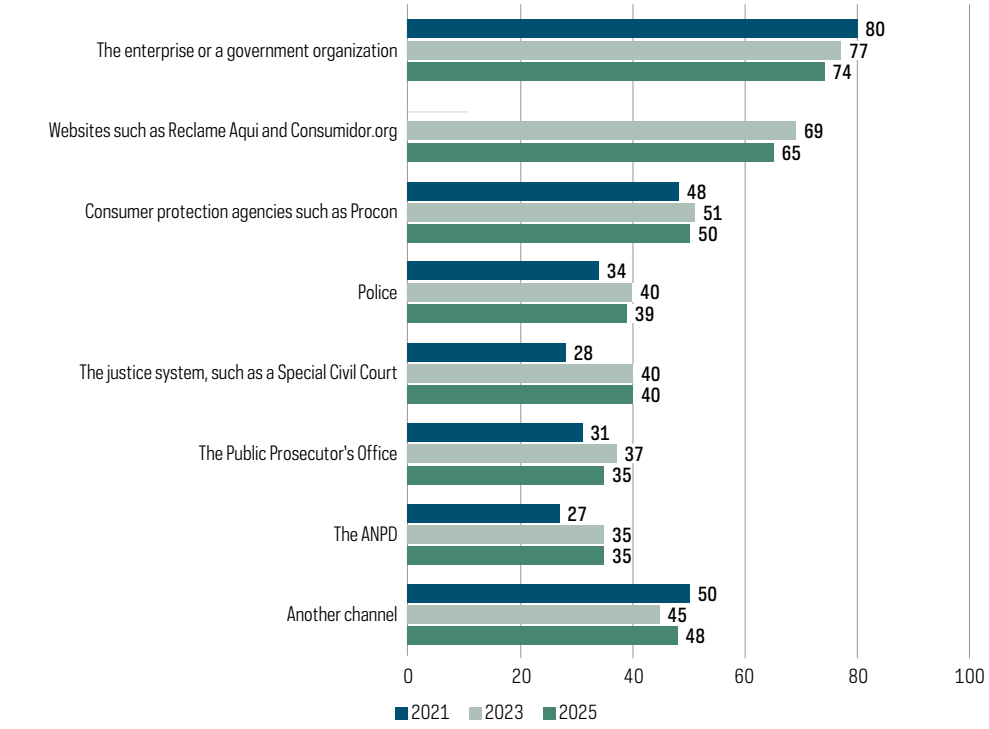
Among those who sought customer service channels, the most frequently mentioned methods were to contact the enterprise itself or the government organization that controls the data (74%), and websites for consumer complaints (65%). Chart 5 shows the comparison between the results observed in 2021 and 2025.

CHART 5

—

Internet users by customer service channels sought out about personal data (2021–2025)

Total number of Internet users 16 years old or older who sought customer service channels about their personal data (%)



Note: *Response category included from 2023 onwards.

Among users who did not seek customer service channels for requests, complaints, or reports, the most frequently mentioned channels for any eventual need were the enterprise or government organization controlling the data (74%), consumer protection agencies such as Procon (74%), and consumer complaint websites (65%).

It is possible to state that most users seek the organization controlling the data, such as the enterprise, government organization, platform, or app, that registers and holds the data related to the request. In a second tier are consumer protection agencies, such as Procon, or consumer complaint websites. Consumer service and complaint channels are the primary points of contact; in third place are police authorities and the justice system, in addition to the ANPD.

As verified in previous editions of the survey, Internet users demonstrated that they treated requests for personal data with the same logic as a consumer relationship or police reports (Oyadomari et al., 2023). This scenario indicates that the protection of personal data as a specific field of rights is still in the process of being appropriated by citizens. It will be important for the future research agenda to better characterize these requests and broaden the understanding of what is being requested, how, and through which channel.

The challenge of implementing effective and specific channels for service requests related to personal data is also present in public administration. The 2023 ICT Electronic Government survey showed a wide range of generic service channels among Brazilian government organizations; however, less than half of local governments offered channels for requests regarding personal data (CGI.br, 2024a). Therefore, as the supply of digital services grows and the volume of personal data processed by public and private organizations increases, it will become increasingly important to broaden the population's knowledge about the channels available for exercising their rights provided for in the LGPD.

Risk perception

The perceptions of Internet users regarding the risks related to the use of their personal data allow to understand how they assess different situations of exposure in the digital environment. The survey investigated the levels of concern about the recording of their activities and the main risks perceived in the processing of their personal data.

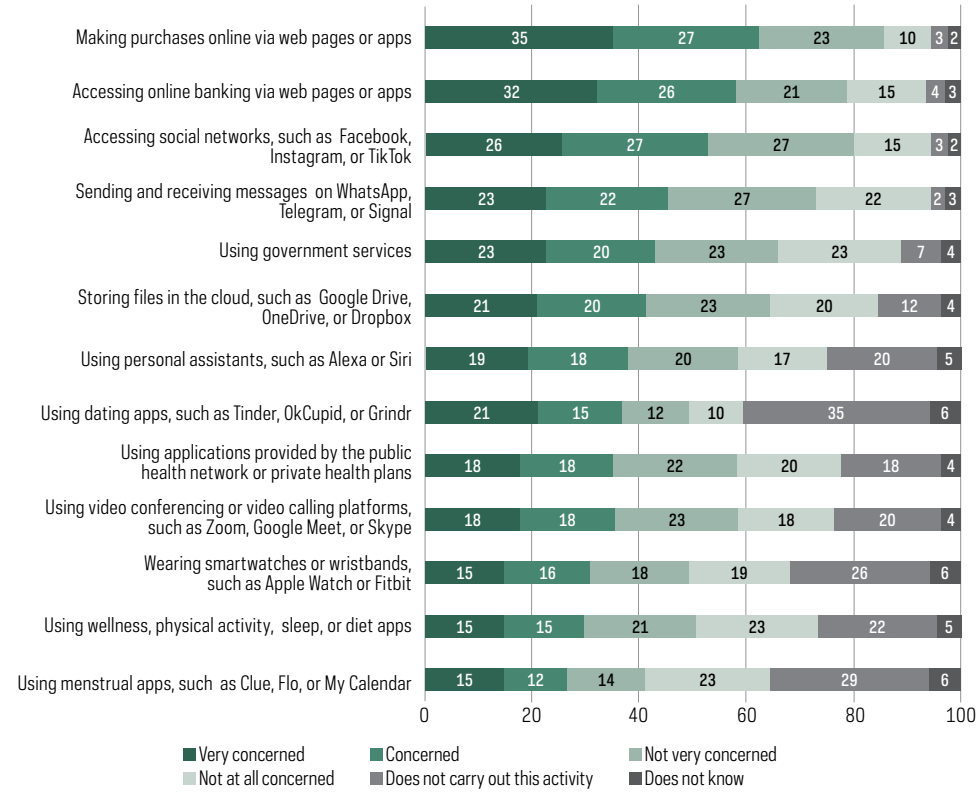
Regarding activities performed on the Internet (Chart 6), the highest level of concern was identified about making purchases online via web pages or apps (35% very concerned and 27% concerned), followed by accessing online banking via web pages or apps (32% very concerned and 26% concerned).

CHART 6

—

Internet users by level of concern about personal data, by activity carried out on the Internet (2025)

Total number of Internet users 16 years old or older (%)



Note: *Only considers female Internet users.

In the case of "using social media," there was noticeable variation among younger Internet users: While 23% of users 16 to 24 years old said they were very concerned and 18% were concerned, most were not very concerned (32%) or not concerned at all (19%). In contrast, among users aged 45 to 59, 25% said they were very concerned, 36% concerned, 24% not very concerned, and 12% not at all concerned.

Regarding concerns about using government services, there were marked differences by social class: 27% of Internet users in classes AB said they were concerned, while among those in classes DE, this proportion was 13%. When questioned about their level of concern regarding potential uses of personal data, the most frequent categories were sharing with third parties without consent and financial losses due to fraud. The results point to a perception of risk focused primarily on situations involving the exchange of personal data that could cause financial losses and impact individuals' daily lives.

The perceptions of risk regarding personal data explain cautious attitudes towards online activities, especially abstaining from activities on apps or pages, with no significant variations in this indicator compared to the 2023 survey. According to the survey, 69% of Internet users aged 16 years old or older stated that concern about personal data led them to uninstall apps, 68% to refrain from visiting a web page, 54% to refrain from using an online service or platform, 43% to refrain from buying an electronic device, and 47% to refrain from buying another type of product.

Users' perception of the insecurity of the digital environment, doubts about the veracity of information, pages, services, and applications, and doubts about how personal data will be used, stored, or shared, are a limiting factor for the adoption of digital transactional services. Despite this persistent pattern across all editions of the survey, there have been no significant changes in daily practices for managing personal data among Internet users. This apparent mismatch between perceptions and behavior shows that awareness of risks may not be sufficient to promote more consistent practices for protecting personal data. This context serves as a backdrop for analyzing emerging themes, such as the use of AI and the increasing sophistication of digital scams and frauds, which bring new challenges to the protection of personal data and interfere daily in the lives of Internet users in Brazil.

Sensitive data and biometric data

Since its first edition, the survey has investigated the level of concern among Brazilian Internet users regarding their sensitive personal data. In 2023, new indicators were incorporated to deepen the understanding of the topic, considering the different types of sensitive personal data indicated in the literature (Teffé, 2022). This topic was investigated again in the 2025 edition, given that the increasing use of biometric data, in both public and private organizations, and its incorporation into authentication and digital identification mechanisms, are especially relevant to understanding how users perceive the collection and processing of this information.

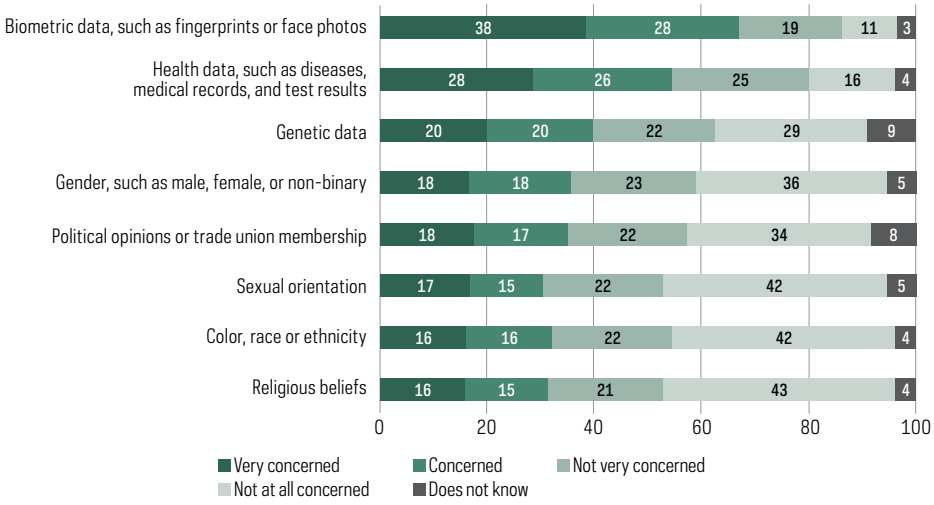
According to the survey, Internet users declared a higher level of concern about providing biometric data than about the other types of personal data investigated: 38% said they were very concerned and 28% concerned (Chart 7). Another category that stood out was health data: 28% declared themselves very concerned and 26% concerned. Among the other types of sensitive data investigated, the proportions of "very concerned" did not exceed 20%. The high level of concern regarding health data may be due to its highly personal nature and the potential for discrimination or undue exposure if used without the consent of the data subjects.

CHART 7

—

Internet users by level of concern about provision of sensitive personal information, by type of sensitive personal information (2025)

Total number of Internet users 16 years old or older (%)



Regarding the type of biometric data provided, the highest levels of concern were shown for types of biometric data commonly encountered in everyday life, such as fingerprints and facial recognition: The sum of concerned and very concerned users was 83% and 81%, respectively. A significant portion of Internet users showed high levels of concern about all types of biometric data investigated, even those less present in daily life. The lowest level of concern occurred in relation to the category "Walking, writing, or typing pattern," but even in this case, 63% of Internet users stated that they were concerned or very concerned, which reinforces the understanding that the collection of biometric data is considered worrying as a whole. This result suggests that users show greater concern about information that can uniquely identify the individual and that, unlike passwords, cannot be replaced.

Generative AI

According to the ICT Households 2025 survey, 32% of Internet users employed some type of generative AI tool, with the highest proportions among individuals with tertiary education, those with a higher income, those belonging to higher socioeconomic classes, and younger people (CGI.br, 2026). The survey also found that the most frequently mentioned reasons for not using this type of tool were lack of need or interest (76%) and concerns about security and privacy (63%).

Considering the widespread use of these tools and their potential to involve the sharing of personal information, there was a need to broaden the understanding of Internet users' perceptions on this topic in Brazil. Therefore, the Privacy and Personal Data Protection 2025 survey presents three new indicators on the use of generative AI. First, to distinguish intensity, the frequency of use of these tools was investigated. Then, to focus on personal data in the context of generative AI, respondents were asked what types of information they provided to these tools. Finally, the survey investigated their levels of concern when using them.

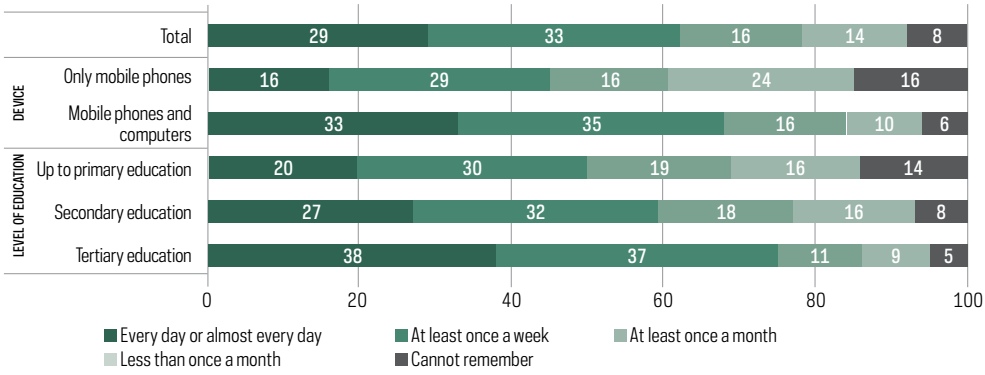
Among AI users, frequency of use showed significant differences according to device combination and education level: Daily use was more frequent among those who combined mobile phone and computer use than among those who used mobile phones exclusively, and was also higher as the level of education increased (Chart 8). The results indicate that generative AI is part of the routine of a portion of Internet users, since most users reported using these tools at least weekly.

CHART 8

–

Users of generative AI tools by frequency of use according to devices and level of education (2025)

Total number of Internet users 16 years old or older who used generative AI tools (%)



To better characterize the nature of this use, the survey investigated the types of information provided to generative AI tools. Of the categories investigated, "work or study topics" was the most mentioned (73%). In a second, lower tier, but with similar proportions, were: "personal preferences and tastes, such as movies or music" (58%), "feelings and emotions" (54%), "health data, such as symptoms and tests" (52%), and "photos of yourself or of people you know" (50%). Finally, the least mentioned categories were "personal finances, such as budgets and investments" (41%) and "personal data, such as name, address, date of birth or Individual Taxpayer Registry (CPF)" (37%).

In line with recent research conducted in several countries, the survey found that the use of generative AI has expanded beyond professional and academic purposes, increasingly encompassing activities related to counseling, emotional support, and companionship (International Telecommunication Union [ITU], 2025; Lira et al., 2026). This type of interaction tends to encourage users to share intimate and, in some cases, sensitive information, such as feelings, tastes, and health data. Images created or edited by AI tools have also become popular on social media, enabling the sharing of personal and third-party photographs on these platforms, which creates new challenges related to privacy and the protection of personal data.

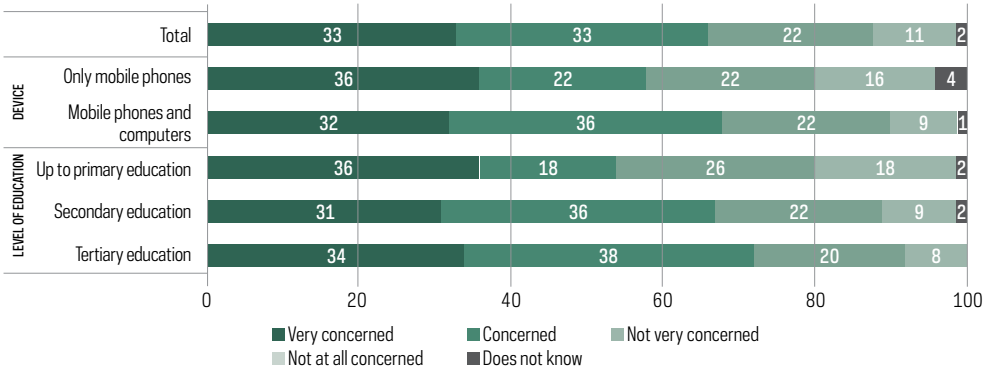
Most users of generative AI tools stated that they were very concerned or concerned about the use of their data by the enterprises providing the tools (Chart 9). These results indicate that, although they shared different types of personal information with these tools, levels of concern remained high regarding the processing of this data, suggesting that they recognized the potential risks associated with these technologies.

CHART 9

—

Users of generative AI tools by level of concern about the use of data by AI tool providers, according to devices and level of education (2025)

Total number of Internet users 16 years old or older who used generative AI tools (%)



Similar to the frequency of use indicator, the level of concern was also higher among those who combined devices and among those with higher levels of education. Given this scenario, the differences observed among users, along with the diversity of information shared with these tools, reinforce the importance of monitoring the impacts of generative AI use on privacy and the protection of personal data.

Scams involving personal data

There is growing debate about crime statistics and their intersection with the digital environment, driven by recent global diagnoses. As pointed out in the *Global Financial Fraud Threat Assessment* report by the International Criminal Police Organization (Interpol, 2026), empirical data on the evolution of new forms of digital financial fraud and scams support governments and private entities in anticipating complex social engineering trends. Similarly, reports published by the United Nations Office on Drugs and Crime (UNODC, 2025) reinforce the idea that the production of statistics is indispensable for monitoring the real economic harm inflicted on families and improving institutional cybersecurity mechanisms.

Internationally, the main reference for these statistics from citizens' perspectives is the *Victimization Survey Atlas*, developed by the UNODC–INEGI Centre of Excellence for Statistical Information on Government, Public Security, Victimization and Justice (UNODC–INEGI Centre of Excellence, 2025). This tool standardizes methodologies used globally to give visibility to the so-called "dark figure": the proportion of crimes suffered by society that do not get reported to the authorities. In the current scenario, cybercrimes and online scams represent the main frontier of this underreporting, since most victims of digital fraud fail to file complaints because they do not believe the criminals will be identified or their money recovered.

In addition to measuring the real extent of digital fraud and identifying the channels through which it occurs, these indicators allow mapping the demographic profile of the most vulnerable groups. This diagnosis generates fundamental evidence to both raise citizen awareness and strengthen the preventive capacities of the institutions involved.

The need for accurate data is urgent in Latin America and the Caribbean, regions that have experienced accelerated digitalization in recent years, accompanied by an exponential increase in rates of online fraud. To standardize this regional diagnosis and integrate cybercrime into security metrics, the United Nations (UN) has been promoting the Latin American and Caribbean Victimization Survey Initiative (Lacsi) since 2013. Through standardized questionnaires, the initiative seeks to measure, in a comparable way, the real impact of electronic fraud in different countries of the region (UNODC-INEGI Centre of Excellence, 2013).

Although the Privacy and Personal Data Protection 2025 survey does not include a complete questionnaire dedicated to the topic, a preliminary approach was taken through the inclusion of three indicators on fraud involving personal data. Before the questions were administered, respondents were presented with a brief explanatory text to contextualize the topic.

The research identified that, in 2025,[2] 32% of Internet users experienced scam attempts with use of their personal data, while 20% were victims of successful scams in which their personal data was used. Among those who experienced these situations, when asked about the channels through which they occurred (both attempted and successful scams), the most frequently mentioned categories were messaging applications (84%) and phone calls (79%). Other channels investigated included fake websites or apps (71%), SMS (71%), e-mail (69%), and social media (67%). The results showed that scams involving personal data occurred through multiple communication channels, combining digital and traditional means, with the aim of reaching potential victims. This scenario demonstrates that exposure to fraudulent situations has the potential to reach even individuals who are not Internet users, since attempts via telephone and SMS are also common.

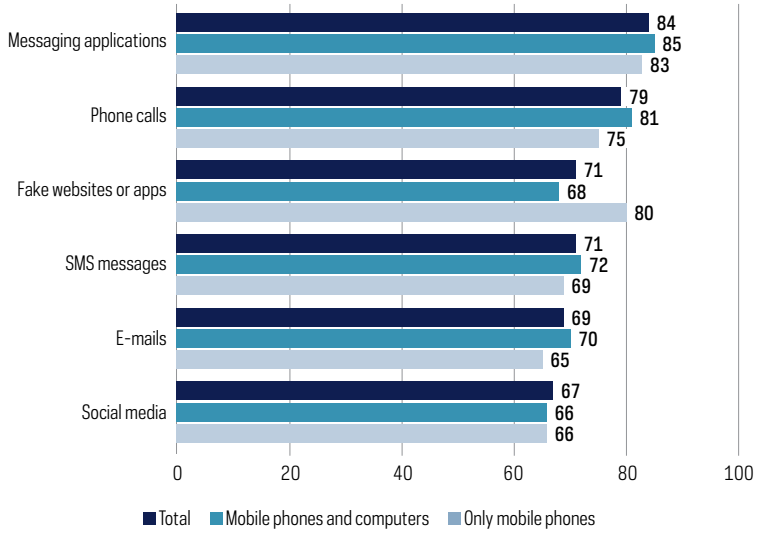
The device used to access the Internet showed significant variation for the fake website or app response category, being more frequently mentioned among individuals who only used mobile phones (Chart 10). This difference illustrates how significant connectivity dimensions relate to data security and protection, since individuals in more restricted usage contexts may have more difficulty performing security verification practices.

CHART 10

—

Internet users who experienced situations involving scams, by channels where these situations occurred and access device used (2025)

Total number of Internet users 16 years old or older who experienced an attempted scam or were victims of a scam using personal data (%)



[2] Unlike other activities investigated in the survey that used "the last three months" as a reference, this set of questions considered "the year 2025," in an attempt to reduce possible seasonality and broaden the scope of the investigation to 12 months. Since the data collection took place entirely during a fortnight in December 2025, the formulation made it easier for respondents to correctly situate any events they remember within or outside the current year.

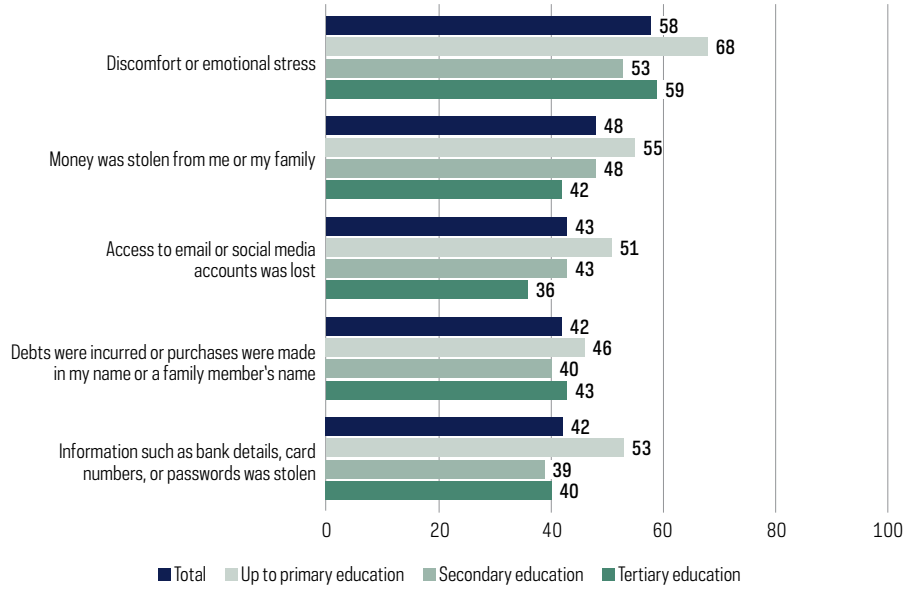
When asked about the consequences of situations involving scams with personal data, respondents mentioned consequences that went beyond financial damage and effects directly related to the data, including emotional impacts and broader repercussions on well-being. In addition, significant variations were observed according to the level of education: All categories were more frequently mentioned by individuals who completed up to primary education (Chart 11).

CHART 11

—

Internet users who experienced situations involving scams, by consequences of these situations and level of education (2025)

Total number of Internet users 16 years old or older who experienced an attempted scam or were victims of a scam using personal data (%)



Given this scenario, it is observed that fraud involving personal data represents a significant dimension of the risks associated with the use of digital technologies. Beyond the frequency of attempts and the diversity of channels used, their consequences can extend beyond financial losses, highlighting the importance of monitoring this issue.

Final considerations: Agenda for public policies

The analysis of Internet users' perspectives on personal data protection issues offers valuable insights for improving public policies in Brazil. Since the enactment of the LGPD and the subsequent role of the ANPD, there has been significant progress in the legal and regulatory coverage of the topic, especially within public and private organizations. However, for this agenda to be consolidated and disseminated in the daily lives of citizens, it is essential to understand how Brazilians perceive, experience, and respond to the challenges of privacy in the digital environment.

Investigating everyday data-protection practices allows comparison between individuals' perceptions of privacy and their actual behaviors when using digital technologies. In this edition, the survey delved deeper into the analysis of reading privacy policies, a topic intrinsically linked to informed consent. The results indicated a mismatch between the behaviors declared by users and their actual practices, with users exhibiting socially expected behaviors (such as stating that they read the terms of use) that were not confirmed in practice or were not consistently adopted on all occasions. Furthermore, notable differences associated with the individuals' age group were identified, pointing to the need for public policies that consider generational differences in promoting a data protection culture.

Another important aspect concerns the distinction between users who access the Internet exclusively via mobile phones and those who combine computer and phone use. This difference highlights the importance of considering the various realities of access and connectivity in the debate on data protection, especially regarding the ability of users in situations of greater digital vulnerability to adopt good security practices. The concept of meaningful connectivity (Brazilian Network Information Center [NIC.br], 2024), which considers dimensions such as cost, device, quality, and digital skills, has gained ground in the field of digital inclusion; in this scenario, the results of this survey suggest that security and data protection should be incorporated as qualifiers of these connectivity levels.

As observed in the previous edition, the risks perceived by Internet users remain mostly associated with financial losses and fraud, followed by concerns such as surveillance in public spaces, risk of discrimination, and the inherent sensitivity of personal health and biometric data. This pattern highlights the prevalence of concern among Brazilians about data theft for the purpose of committing fraud, reinforcing the urgency of improving security in the national digital environment.

In this edition, the survey also delved deeper into measuring aspects related to biometric data, continuing the discussion initiated in the previous study. The results confirmed that this topic is particularly sensitive for users, given the high potential for perceived risk, especially in relation to the most commonly used categories, such as facial recognition and fingerprinting. The perception of risk is significantly higher when data collection is carried out by public organizations and the banking sector, suggesting that users associate this information with the risk of identity theft for fraud. There is less concern regarding smaller private organizations, indicating that the multiplication of biometric data collection points and their consequent storage worries users less than providing this information to larger and more important institutions. This hypothesis, as well as the results that support it, presents a challenge to society regarding the regulation of the collection, storage, and use of biometric information for identification purposes.

The survey findings point to the convergence of two trends that are proving particularly challenging for the data protection agenda in Brazil: the increasing use of generative AI by users and the rise in scams and frauds that exploit personal data. This diagnosis is corroborated by the *20th Brazilian Yearbook of Public Security* (Brazilian Forum on Public Security [FBSP], 2026), which recorded 2.2 million cases of fraud in Brazil in 2025, a number more than four times higher than that recorded in 2018. The Forum's research also revealed that 26.3 million Brazilians were victims of Internet scams, highlighting significant underreporting that is not fully captured by official records.

Although the LGPD and the actions of the ANPD have established important regulatory frameworks, the rapid dissemination of AI tools introduces new levels of complexity into the debate about privacy. The Privacy and Personal Data Protection 2025 survey showed that users share increasingly intimate and sensitive information with these platforms, such as feelings, health data, and personal preferences.

Simultaneously, concern about the use of data for fraud and scams remains the main fear of Brazilians, reflecting an international scenario described by UNODC (2025) and the *Victimisation Survey Atlas,* from the UNODC-INEGI Centre of Excellence (2025), which documents the global expansion of fraud centers and the increasing use of AI by criminal organizations. This diagnosis suggests that public data protection policies should not be restricted to the corporate environment and consumer relations, as they need to incorporate strategies for raising awareness and increasing the digital empowerment of the population, as well as specific governance mechanisms for the use of AI that consider the risks of manipulation, discrimination, and fraud. Coordination between the ANPD, the public sector, the private sector, and civil society will therefore be fundamental to facing these challenges.

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.* 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 Forum on Public Security. (2026). *20th Brazilian Yearbook of Public Security: Data from 2025.* https://forumseguranca.org.br/publicacoes/anuario-brasileiro-de-seguranca-publica/

Brazilian General Data Protection Law. Law No. 13.709, of August 14, 2018. (2018). Brazilian General Data Protection Law (LGPD). https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Brazilian Internet Steering Committee. (2022). *Privacy and personal data protection 2021: Perspectives of individuals, enterprises and public organizations in Brazil.* https://cetic.br/en/publicacao/privacidade-e-protecao-de-dados-pessoais-2021-perspectivas-de-individuos-empresas-e-organizacoes-publicas-no-brasil/

Brazilian Internet Steering Committee. (2024a). *Survey on the use of information and communication technologies in the Brazilian public sector: ICT Electronic Government 2023.* https://cetic.br/en/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-no-setor-publico-brasileiro-tic-governo-eletronico-2023/

Brazilian Internet Steering Committee. (2024b). *Privacy and protection of personal data 2023: Perspectives of individuals, enterprises and public organizations in Brazil.* https://cetic.br/en/publicacao/privacidade-e-protecao-de-dados-pessoais-2023-perspectivas-de-individuos-empresas-e-organizacoes-publicas-no-brasil/

Brazilian Internet Steering Committee. (2026). *Survey on the use of information and communication technologies in Brazilian households: ICT Households 2025.* https://cetic.br/en/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-nos-domicilios-brasileiros-tic-domicilios-2025/

Brazilian Network Information Center. (2024). *Meaningful connectivity: Measurement proposals and the portrait of the population in Brazil* (NIC.br Sectoral Studies). https://cetic.br/en/publicacao/conectividade-significativa-propostas-para-medicao-e-o-retrato-da-populacao-no-brasil/

European Commission. (2015). *Special Eurobarometer 431: Data protection* (Special Eurobarometer 431 / Wave EB83.1). https://doi.org/10.2838/552336

Friedman, J., Hastie, T., & Tibshirani, R. (2010). Regularization paths for generalized linear models via coordinate descent. *Journal of Statistical Software, 33*(1), 1–22. https://doi.org/10.18637/jss.v033.i01

International Criminal Police Organization. (2026). *Global financial fraud threat assessment.* https://www.interpol.int/News-and-Events/News/2026/INTERPOL-report-warns-of-increasingly-sophisticated-global-financial-fraud-threat

International Telecommunication Union. (2025). *Report of the EGH subgroup on measuring artificial intelligence (AI) through household surveys*. https://www.itu.int/dms_pub/itu-d/md/22/egh.ai.2025/r/D22-EGH.AI.2025-R-0001!!PDF-E.pdf

Lira, B., Folk, D., Ungar, L., & Duckworth, A. L. (2026). How Gen Z uses Gen AI – and why it worries them. *Harvard Business Review*. https://hbr.org/2026/01/how-gen-z-uses-gen-ai-and-why-it-worries-them

Oyadomari, W., Costa, R. S., & Ribeiro, M. M. (2023). Individual's perspectives on privacy and personal data protection in Brazil. *Internet Sectoral Overview, 15* (2), 1–11. https://cetic.br/en/publicacao/ano-xv-n-2-protecao-de-dados-pessoais-privacidade-e-confianca-no-ambiente-digital/

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

Tibshirani, R. (1996). Regression shrinkage and selection by the LASSO. *Journal of the Royal Statistical Society: Series B (Methodological), 58*(1), 267–288. https://academic.oup.com/jrsssb/article/58/1/267/7027929

United Nations Office on Drugs and Crime. (2025). *What to know about cybercrime in 2026*. https://www.unodc.org/unodc/frontpage/2025/October/what-to-know-about-cybercrime-in-2025.html

UNODC–INEGI Centre of Excellence for Statistical Information on Government, Public Security, Victimization and Justice. (2013). *Iniciativa de Pesquisas de Vitimização na América Latina e Caribe (LACSI)*. https://www.cdeunodc.inegi.org.mx/unodc/index.php/lacsi-initiative/index.htm

UNODC–INEGI Centre of Excellence for Statistical Information on Government, Public Security, Victimization and Justice. (2025). *Victimisation Survey Atlas*. https://www.cdeunodc.inegi.org.mx/unodc/index.php/atlas-on-cvs/index.htm

Analysis of Results
Privacy and Personal Data Protection 2025
Enterprises

The increasing digitalization of economic activities has expanded the volume and diversity of personal data processed by Brazilian enterprises. Relationships with customers, suppliers, and employees; hiring processes; e-commerce; digital marketing; and, more recently, the use of Artificial Intelligence (AI)-based systems are causing organizations of all sizes to increasingly handle personal information in their operations. In this context, monitoring how enterprises have incorporated privacy and data protection practices has become fundamental to understanding the stage of implementation of the Brazilian General Data Protection Law (LGPD, Law No. 13.709/2018) and the opportunities and challenges for strengthening a transparent and secure digital economy.

At the same time, this environment of increasing digitalization and technological transformation may contrast with the pace of dissemination of privacy and personal data protection practices in Brazilian enterprises. In this regard, there are still significant challenges for enterprises in their pursuit of compliance with the LGPD. For example, if, on the one hand, AI amplifies the challenges related to the legitimate processing of personal data,[1] on the other, new rules have emerged to complement or specify aspects addressed in the law, focusing on specific audiences or situations.[2]

Thus, the scenario presented to enterprises is outlined by challenges stemming from technological advancement and the growing demand for the adoption of advanced technologies, such as AI, coupled with the need to seek compliance with regulations that guide and establish parameters for their performance in the digital environment. In this context, regardless of enterprise size, adopting good privacy and personal data protection practices can represent not only a means to avoid sanctions and damage to their public image but also an increasingly important asset for differentiating the enterprise from competitors, strengthening its reputation and the trust of customers and partners, especially in the face of leaks or misuse of their personal data.

[1] The increasing use of generative AI poses challenges regarding the processing of personal data, whether due to the possibility of abuse or indiscriminate use for training (National Data Protection Agency [ANPD], 2024). According to the ICT Households 2025 survey, 32% of Internet users in Brazil used generative AI tools, with more frequent use among individuals in class A (69%) and with tertiary education (59%) (Brazilian Network Information Center [NIC.br], 2026c).

[2] One example is the debate surrounding age-verification mechanisms, in connection with the entry into force of the Brazilian Digital Statute of the Child and Adolescent (ECA Digital, Law No. 15.211/2025), and its relationship with the protection of personal data (ANPD, 2026).

Therefore, the results of the third edition of the survey on privacy and personal data protection in Brazilian enterprises should be interpreted within this context of greater technological and regulatory complexity. In this context, the 2025 edition shows few changes compared to the 2023 data, highlighting that, despite the transformations observed in other indicators of the ICT Enterprises survey, such as the greater adoption of AI across all sizes of enterprises,[3] overall, there have been no significant changes in the proportion of enterprises adopting best practices for protecting personal data, especially among small ones. Furthermore, large enterprises and enterprises in the information and communication sector continue to show higher proportions of the personal data processing practices investigated by the survey.

Between the previous edition of the survey and the present one, although there have been no sweeping changes in the regulatory framework applicable to enterprises' privacy and personal data protection practices, the period has been marked by significant institutional changes. The main change concerned the enactment of the Provisional Measure No. 1.317/2025,[4] transforming the National Data Protection Authority into an autonomous regulatory agency, the National Data Protection Agency. An example of the expanded scope of action resulting from the institutional strengthening of the regulatory body is Decree No. 12.622/2025, which designated the ANPD as the autonomous administrative authority responsible for the regulation, guidance, and oversight of legislation aimed at protecting the rights of children in the digital environment.[5]

In the case of the ECA Digital, there are implications for the online operations of enterprises, especially those with services and platforms likely to be accessed by children.[6] Among these, the need to implement effective age verification mechanisms should be considered by enterprises, which may require the development or adoption of specific technological solutions in the market. This is important because these tools must comply with the principles and rules applicable to the processing of personal data, as they aim to prevent or restrict children's access to certain applications or platforms on the Internet, such as app stores.[7]

[3] The ICT Enterprises 2025 survey showed that 17% of Brazilian enterprises used some type of AI technology, representing a five-percentage-point increase compared to 2024. Among enterprises that used AI, 44% stated that they used it for marketing or sales, which requires caution regarding the processing of personal data, especially that of minors under 18 years old (NIC.br, 2026b).

[4] Subsequently, the measure was converted into Law No. 15.352/2026, making the ANPD a special autonomous entity in the form of a regulatory agency, while maintaining its link with the Brazilian Ministry of Justice and Public Security (MJSP).

[5] One example of the activities assigned to the ANPD in this area is receiving orders to block websites that fail to comply with requirements stipulated by law.

[6] ECA Digital provides a broad definition of technology products and services, generating diverse interpretations about the scope of the law, especially regarding the concept of probable access. According to the Brazilian Internet Steering Committee (CGI.br): "The breadth of the definition demonstrates the legislator's intention to encompass different agents involved in offering digital products and services targeted at or likely accessible to children. At the same time, this scope demands interpretative criteria that allow for the adequate distinction between the different types of suppliers covered by the legal definition, considering their functions and characteristics in the digital ecosystem." (CGI.br, 2026a, p. 4).

[7] According to the ANPD, these mechanisms must align with the principles of personal data processing described in the LGPD. Still, they must also consider precepts of the Brazilian Statute of the Child and Adolescent (ECA) and the Brazilian Consumer Defense Code (CDC): "It is based on this regulatory model that one must understand the command of Article 9, caput and paragraph 1, of the ECA Digital, which determines that the age verification mechanisms adopted must be 'reliable'. In this sense, it is an obligation that stems from the general duty imposed on service and product providers to act proactively and diligently to prevent and mitigate risks to children in the digital environment. The same provision also establishes that 'effective' measures must be adopted to prevent children from accessing content, products or services whose offer or access is inappropriate, inadequate or prohibited for minors under eighteen years old." (ANPD, 2026, p. 5).

Therefore, it is essential for enterprises to monitor regulatory developments and continuously assess their compliance in light of the regulator's actions. Consequently, they must pay close attention to the processing of personal data and its relationship to related legislation, such as the ECA Digital, as well as other legal frameworks applicable to the digital environment, in order to strengthen data governance and contribute to a safer and more trustworthy digital environment.

Therefore, in an environment of increasing technical and legal complexity, it is important for enterprises to promote actions aimed at complying with legislation and strengthening good digital security practices, in order to reduce risks that can lead to financial and reputational damage. The increased online presence of enterprises amplifies their exposure to cyberattacks; when not accompanied by adequate data governance practices, it also increases the risks of noncompliance with applicable legislation. Therefore, the accountability of enterprises operating in the digital economy is expanding, which reinforces the importance of a data protection culture and information security in these organizations.

In this context, considering the data collected through interviews with small, medium, and large enterprises in Brazil, this analysis is organized into three sections:

- **Storage of personal data and purpose of use:** indicators on the types of personal data held by enterprises and the purposes for which they are used;
- **Development of internal capabilities:** indicators on actions to raise awareness and train enterprises' internal staff on the topic of privacy and personal data protection;
- **Compliance with the LGPD:** indicators on actions aimed at increasing compliance with the law and seeking to strengthen best practices for the processing of personal data within the enterprise.

Storage of personal data and purpose of use

As in previous editions of the survey, the type of personal data most retained by Brazilian enterprises comes from customers and users:[8] in 2025, 69% of enterprises stated they stored this type of data, followed by 58% that stored data from partners and suppliers (Chart 1). From a size perspective, the same pattern is observed, with large enterprises showing a higher level of retention of personal data of customers and users (73%).

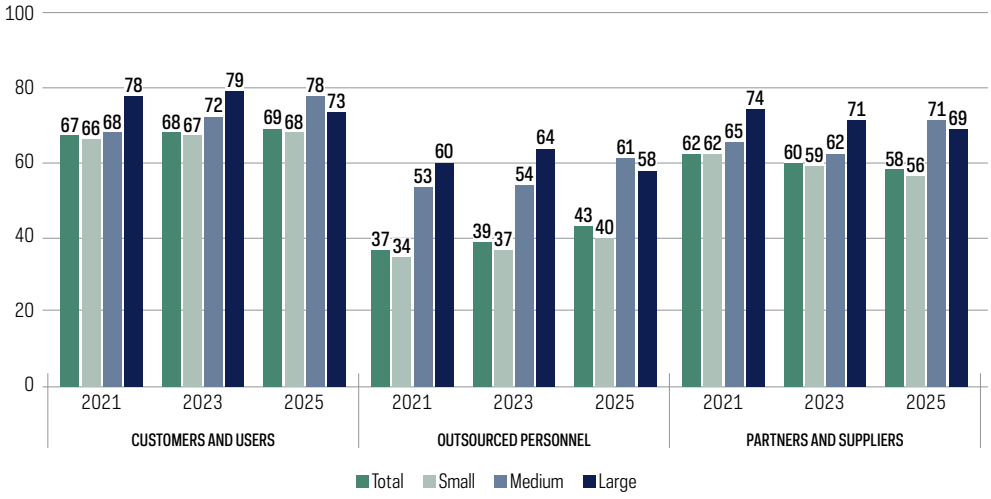
[8] The ICT Enterprises survey includes an indicator on data usage and collection sources. In 2025, 20% of Brazilian enterprises collected data internally, from processes and staff, with the proportion reaching 56% among large enterprises. In turn, 16% of enterprises collected customer and user data, reaching 37% of large enterprises (NIC.br, 2026b).

CHART 1

—

Enterprises by type of data kept on natural persons and size (2021–2025)

Total number of enterprises (%)



Among the personal data processed by enterprises, the LGPD stipulates that the processing of sensitive data requires special care.[9] In the data investigated by the survey, biometrics remained the most frequently stored data by enterprises: 31% of them stored it in 2025, a proportion that was 30% in 2023.[10] Next, sensitive health data was retained by 26% of enterprises in 2025, the same proportion as in the previous edition (Chart 2). In sectoral terms, storing health data was more frequent in the construction (35%) and professional activities (36%) sectors. As stipulated in paragraph 4 of Article 11 of the LGPD, the processing of health data has specific restrictions, especially regarding its shared use between data controllers, with the aim of gaining economic advantages.

The results therefore indicate that the storage of sensitive data by enterprises remains at the levels observed in previous editions of the survey; this reinforces the need for this handling to be carried out as specified by law.[11] This scenario demands that enterprises

[9] According to the LGPD, sensitive personal data is "personal data concerning racial or ethnic origin, religious belief, political opinion, trade union or religious, philosophical or political organization membership, data concerning health or sex life, genetic or biometric data, when related to a natural person" (Law No. 13.709/2018).

[10] It is important to mention that, according to the LGPD, sensitive data can be processed with the consent of the data subjects, but also without it in specific circumstances, as highlighted by the law in item II of Article 11.

[11] For example, in Article 38: "The national authority may determine that the controller must prepare an impact report on protection of personal data, including sensitive data, referring to its data processing operations, pursuant to regulations, subject to commercial and industrial secrecy." (Law No. 13.709/2018).

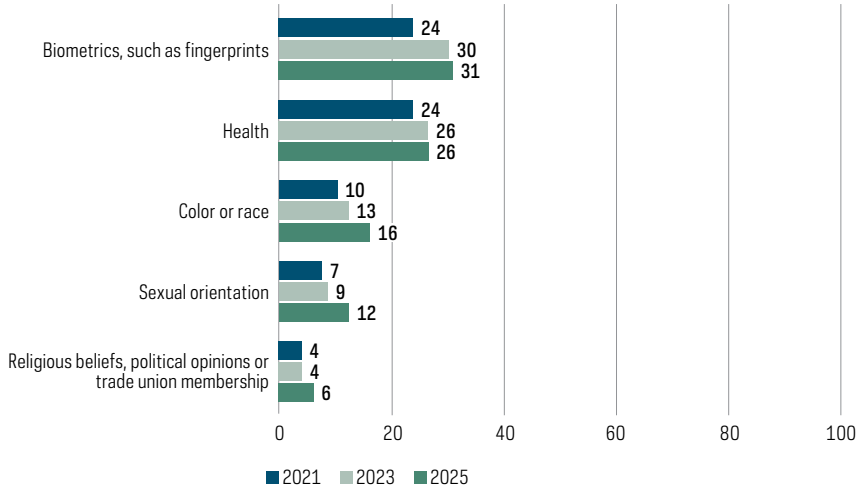
adopt appropriate practices throughout the personal data processing life cycle, especially in the case of sensitive data, in order to reduce associated risks and prevent abuses that could lead to potential sanctions and fines.[12]

CHART 2

—

Enterprises by type of sensitive data kept (2021–2025)

Total number of enterprises (%)



Among enterprises that hold personal data of customers and users, 9% stated that they stored personal data of minors under 18 years old, most frequently large enterprises (21%) and those in the accommodation and food sector (19%)[13] (Chart 3). Although the results did not show any significant changes compared with previous years, maintaining the personal data of children still requires specific safeguards under the LGPD, including requirements related to their best interests, specific and prominent consent from at least one parent or legal guardian, and public disclosure of the types of data collected and how

[12] An example of obligations regarding the processing of personal data is found in the section on data security and confidentiality (Article 46), which allows for the requirement of minimum technical standards for data protection, especially for sensitive data: "Processing agents shall adopt security, technical and administrative measures able to protect personal data from unauthorized accesses and accidental or unlawful situations of destruction, loss, alteration, communication or any type of improper or unlawful processing." (Law No. 13.709/2018).

[13] According to the ICT Kids Online Brazil 2025 survey, 20% of Internet users 9 to 17 years old said they had shopped online. Among users 11 to 17 years old, 84% reported seeing product or brand advertisements. Regarding privacy protection practices, 61% of Internet users 11 to 17 years old blocked messages from someone they did not want to talk to, while 52% changed their privacy settings so that fewer people could access their profile (NIC.br, 2026a).

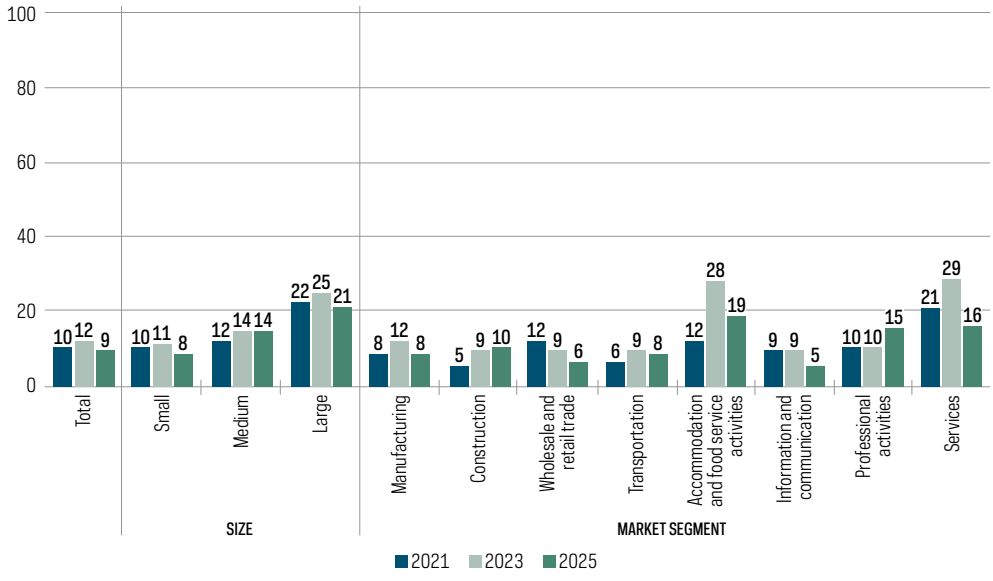
they are used (Article 14).[14] Furthermore, with the enactment of the ECA Digital in 2025, enterprises' responsibilities were expanded, especially regarding the targeting of advertising to this audience, involving greater control over this practice.[15] Therefore, the processing of personal data of minors under 18 years old requires governance mechanisms capable of ensuring greater control in the collection of this data, with more restrictions on the purpose of use and the sharing of this information.[16]

CHART 3

–

Enterprises by whether they keep personal data of clients and users under 18 years old, size and sector (2021–2025)

Total number of enterprises that keep personal data of customers and users (%)



[14] An example of the relationship between the ECA Digital and the LGPD, in terms of greater control over the processing of personal data of minors under 18 years old, is the requirement outlined in Article 16 (sole paragraph) of the ECA Digital, according to which, in the case of processing personal data for purposes that are not strictly necessary, the controller must: "I – map the risks and make efforts to mitigate them; and II – prepare a personal data protection impact, monitoring and evaluation report, to be shared upon request from the autonomous administrative authority for the protection of the rights of children in the digital environment, in accordance with the applicable regulations." (Law No. 15.211/2025).

[15] According to Chapter IV of the ECA Digital, regarding age verification mechanisms, in its Article 10: "Providers of information technology products or services directed at children or likely to be accessed by them shall adopt mechanisms to provide age-appropriate experiences, in accordance with this Chapter, respecting the evolving autonomy capacities and diversity of Brazilian socioeconomic contexts." (Law No. 15.211/2025). Therefore, enterprises that may target their products and services to an audience under 18 years old must have effective age verification mechanisms in place and use the personal data collected only for that purpose.

[16] In a publication providing guidelines for age verification mechanisms, the ANPD (2026) highlights the broad implications of processing personal data of minors under 18 years of age, considering the various regulations in force: "The protection of users' privacy, in this context, is also related to the need for the mechanisms adopted to be compatible with the constitutional guarantee of the inviolability of intimacy, private life, honor and image of users, under the terms of art. 5, X, of the Federal Constitution. Similarly, other guarantees provided for in regulations such as the Brazilian Civil Rights Framework for the Internet (Law No. 12.965/2014) must also be observed, which ensures the inviolability and confidentiality of the flow of communications carried out over the Internet, except by court order, as provided by law. Thus, age verification mechanisms cannot generate, directly or indirectly, violations of users' privacy in its various dimensions." (ANPD, 2026, p. 17).

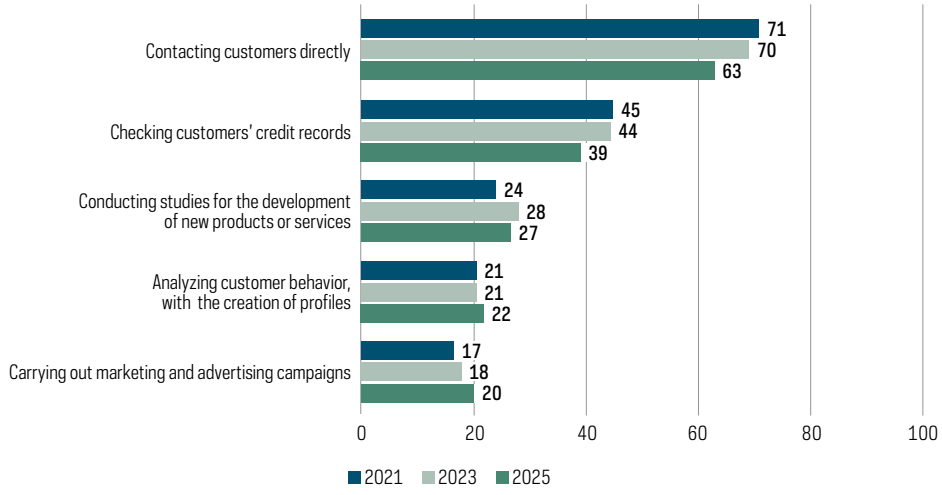
Considering the enterprises that stated they store the personal data of customers and users, in 2025, 63% reported using it to contact these audiences directly, while 39% reported using it to check credit records, a pattern maintained since the first edition of the survey (Chart 4). The ICT Enterprises 2025 survey showed that 41% of Brazilian enterprises paid for Internet advertising, with higher proportions among organizations in the accommodation and food sector (51%), information and communication sector (53%), and services sector (55%) (NIC.br, 2026b). It is important to note that these are precisely the sectors with the highest proportions of enterprises storing personal data of individuals under 18, reinforcing the need to comply with the requirements established by the LGPD and the ECA Digital for processing this data. In this regard, a study by the Regional Center for Studies on the Development of the Information Society (Cetic.br) on age verification mechanisms for various platforms shows that the strategies adopted are very diverse and not always effective in meeting legal requirements, which highlights the challenges for the implementation of these measures (CGI.br, 2026b).

CHART 4

—

Enterprises by how the personal data of customers and users is used (2021–2025)

Total number of enterprises that keep personal data of customers and users (%)



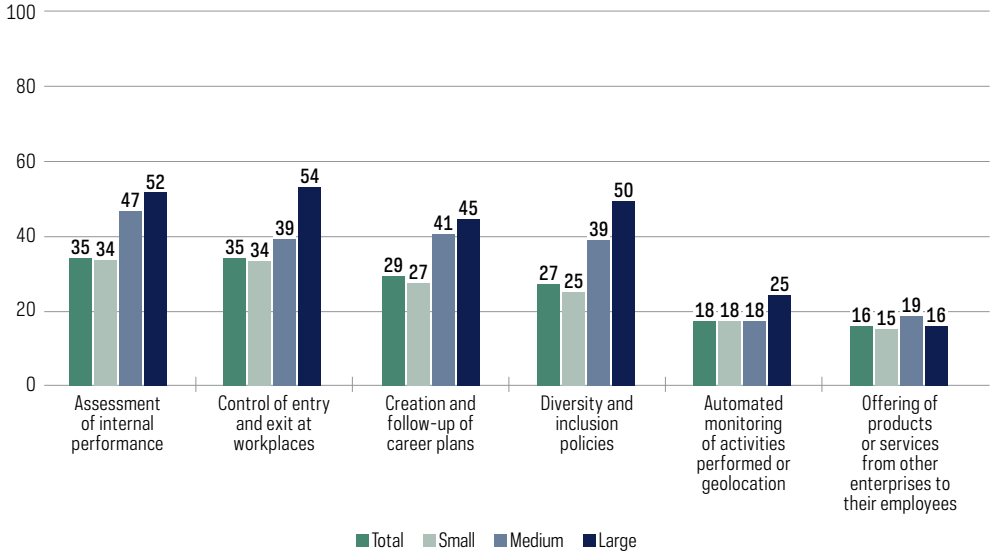
From the perspective of internally generated data processing, in 2025, 35% of enterprises used employees' personal data for performance assessment, and the same proportion used it to control entry and exit from workplaces (Chart 5).[17] It is important to mention that the purpose of using personal data may involve the collection of biometrics, which are frequently used in access control and security systems. In this case, since it is sensitive personal data, its processing must follow the provisions and requirements set out in the LGPD, especially the consent of the data subject (Article 11).

CHART 5

—

Enterprises by purpose for using personal data of employees and size (2025)

Total number of enterprises (%)



This section showed that storing personal data implies several obligations for enterprises, which become more complex when sensitive data or data concerning minors under 18 years old is involved. Furthermore, the results reinforce the need for enterprises to understand the relationship between the various regulations governing their personal data collection practices, given the specifications required based on the nature of the data and its intended use.

[17] According to the ICT Enterprises 2025 survey, 14% of enterprises used smart devices or Internet of Things (IoT) devices. In 90% of cases where these devices were used, the purpose was facility security, such as alarm systems, smoke detectors, door locks, and smart security cameras (NIC.br, 2026b).

Development of internal capacities

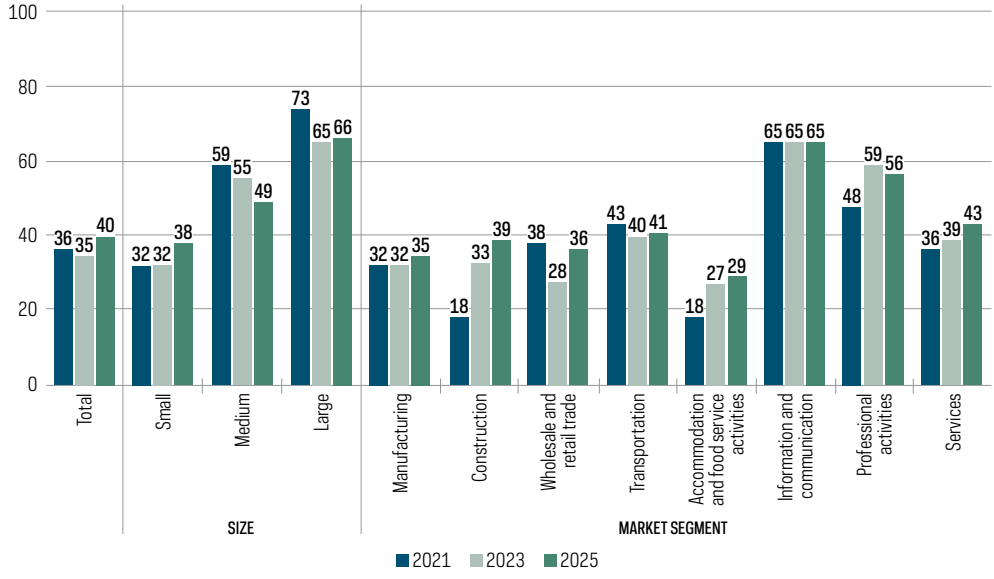
As already pointed out in the introduction section of this analysis, in a scenario of increasing digitalization and evolution of the regulatory framework for data protection, it is important that enterprises have an internal structure capable of guiding actions for the processing of personal data, in accordance with regulations. In 2025, 40% of enterprises held meetings to specifically address the topic of personal data protection, a result that remained stable compared to previous editions of the survey. As observed in other indicators associated with enterprise size, large ones held these meetings in a greater proportion (66%) than small ones (38%), levels that remained stable in both groups throughout the historical series (Chart 6).

CHART 6

—

Enterprises by whether they have carried out internal meetings to specifically address the topic of personal data protection in the last 12 months, size and sector (2021–2025)

Total number of enterprises (%)



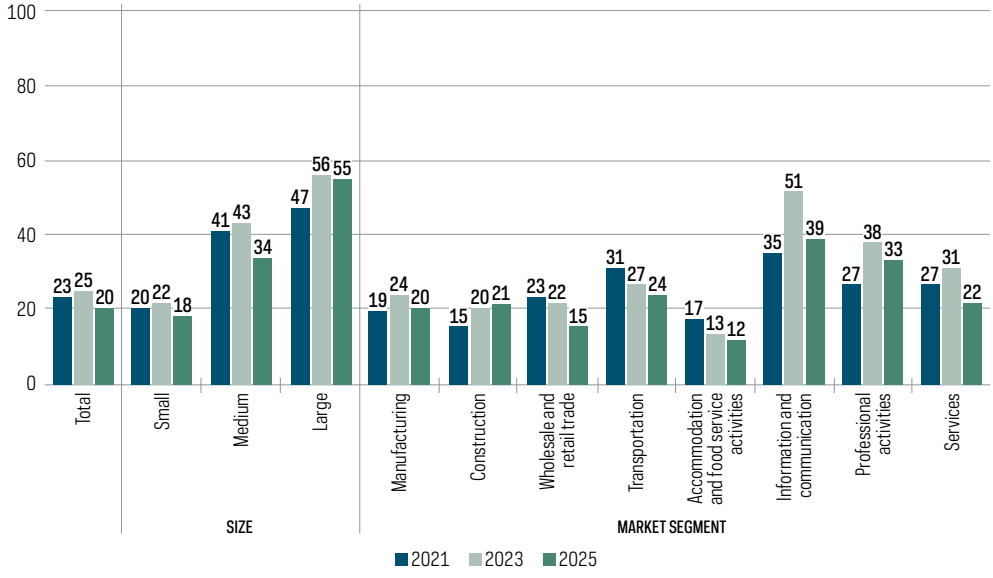
Regarding the development of internal capacities related to the protection of personal data, it is observed that the existence of organizational structures dedicated to the topic did not change in this edition of the survey. In 2025, 20% of enterprises had a department or person responsible for activities related to the topic of personal data protection, a stable level compared to previous years (Chart 7). From the perspective of enterprise profiles, large enterprises and those in the information and communication sector mobilized the most human resources specifically to address the protection of personal data.[18]

CHART 7

—

Enterprises by presence of a specific area or employees responsible for personal data protection, size and sector (2021–2025)

Total number of enterprises (%)



[18] The ANPD anticipated regulatory asymmetries depending on the size of the enterprises. There are exemptions from certain obligations for small enterprises, however, in terms of revenue and not the number of people employed, which is the criterion used in the ICT Enterprises survey. Resolution CD/ANPD No. 2/2022 establishes the differences for what is called "small-scale data processing agents" but mandates the full application of the law in cases of high-risk data processing.

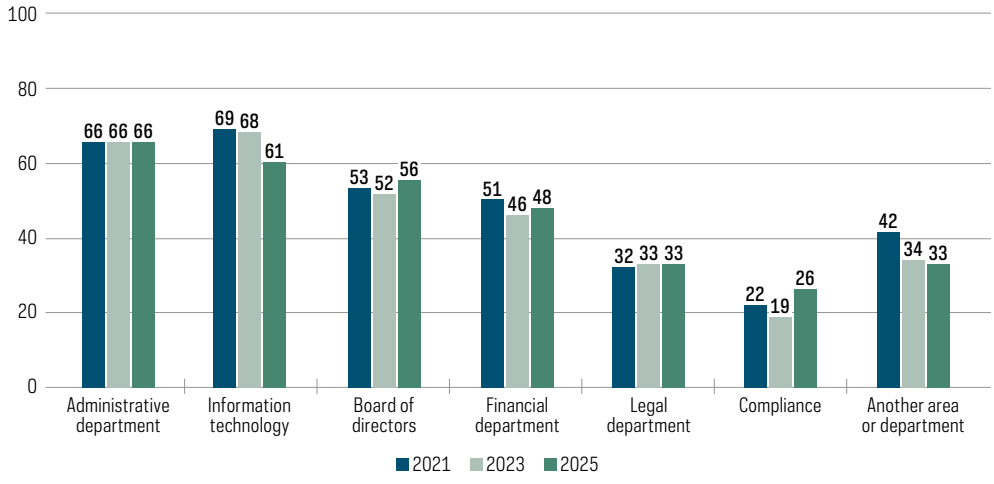
In 2025, among enterprises that had a department or person responsible for personal data protection, 66% indicated that they were linked to the administrative sector, while 61% mentioned that they came from the enterprise's information technology area, maintaining the pattern observed in recent years. There are differences according to enterprise size among the most frequently cited areas of origin: in 2025, 71% of small enterprises highlighted the administrative sector for dealing with personal data protection issues, while 82% of large enterprises directed these activities to the information technology sector (Chart 8). These results suggest that the organization of data protection-related activities varies according to the structure and complexity of enterprises, reflecting different strategies for incorporating data governance into organizational routines.

CHART 8

—

Enterprises by areas or departments of the persons responsible for personal data protection (2021–2025)

Total number of enterprises with areas or persons responsible for personal data protection (%)

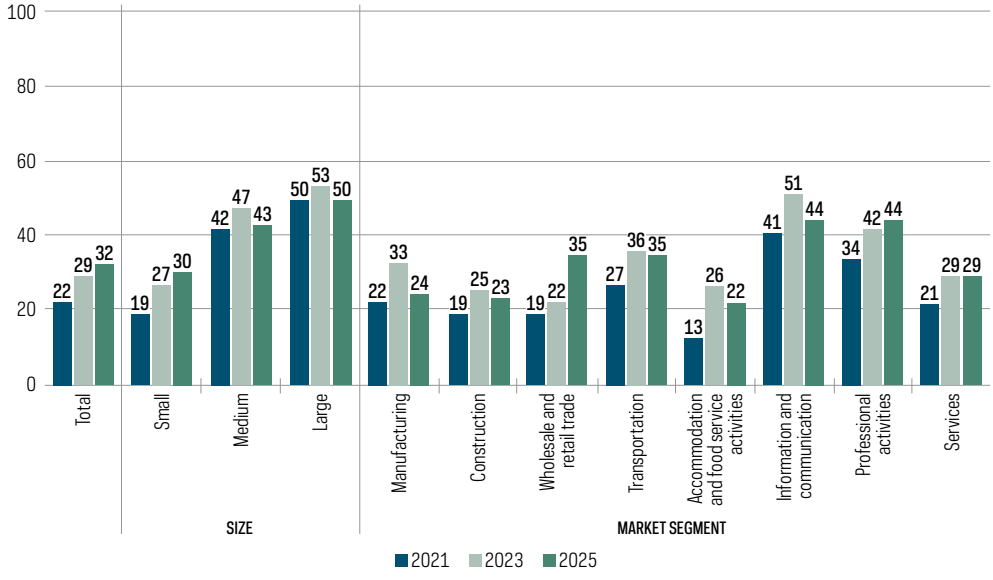


Despite having a department or person dedicated to the topic of personal data protection, enterprises can also resort to hiring specialized services to support the various aspects covered by the law. According to the results of the ICT Enterprises 2025 survey, 32% of enterprises hired third-party services, such as consulting or advisory services, to assist with privacy, data protection, and compliance with the LGPD, maintaining the level of previous editions. The pattern by size and sector follows what was observed in other indicators, with a greater presence of outsourcing of services related to the topic of personal data protection in large enterprises and in the information and communication and professional activities sectors (Chart 9).

CHART 9
—

Enterprises by whether they hire third-party services, such as consultants or advisors, to help with the topic of privacy, data protection, and compliance with the LGPD, by size and sector (2021–2025)

Total number of enterprises (%)



In summary, the indicators regarding the development of internal skills, whether through in-house teams or the contracting of specialized services, showed little change across the three editions of the survey. This stability suggests that there is still room to increase enterprises' awareness of the risks associated with the absence or low adoption of best practices in the processing of personal data, especially among smaller enterprises.

The legal and regulatory frameworks that affect how enterprises operate in the digital environment also demand attention, requiring teams to be prepared to operate in a more complex context, demanding not only one-off actions but also a continuous strengthening of institutional capacities to handle data processing. This section addressed aspects related to organizational structure and internal capacities for handling personal data processing; the next section aims to examine effective actions undertaken by enterprises to achieve compliance with the LGPD.

Compliance with the LGPD

The ICT Enterprises survey investigates how enterprises have sought to comply with the LGPD through actions foreseen by the law and the adoption of best practices in digital security and personal data protection.[19] In 2025, the most common action taken by enterprises was making changes to ongoing contracts to comply with the LGPD, as stated by 30% of enterprises, maintaining the pattern observed in the previous edition of the survey.

Next, 29% of them created a policy for the use of employees' personal data, while the development of a privacy policy was mentioned by 28% (Chart 10). Therefore, the results indicate that the practices most adopted by enterprises in relation to the law concern the establishment of internal procedures aimed at legal certainty regarding employees, with fewer initiatives related to external audiences.[20]

[19] Although not explicitly mentioned in the law, some practices listed in the indicator on compliance with the LGPD are related to principles set forth in the legislation, for example, items VI, VII, VIII, IX, and X of Article 6: "Activities of processing of personal data shall be done in good faith and be subject to the following principles: VI – transparency: guarantee to the data subjects of clear, precise and easily accessible information about the carrying out of the processing and the respective processing agents, subject to commercial and industrial secrecy; VII – security: use of technical and administrative measures which are able to protect personal data from unauthorized accesses and accidental or unlawful situations of destruction, loss, alteration, communication or dissemination; VIII – prevention: adoption of measures to prevent the occurrence of damages due to the processing of personal data; IX – nondiscrimination: impossibility of carrying out the processing for unlawful or abusive discriminatory purposes; and X – accountability: demonstration by the agent of the adoption of measures which are efficient and capable of proving the compliance with the rules of personal data protection, including the efficacy of such measures." (Law No. 13.709/2018).

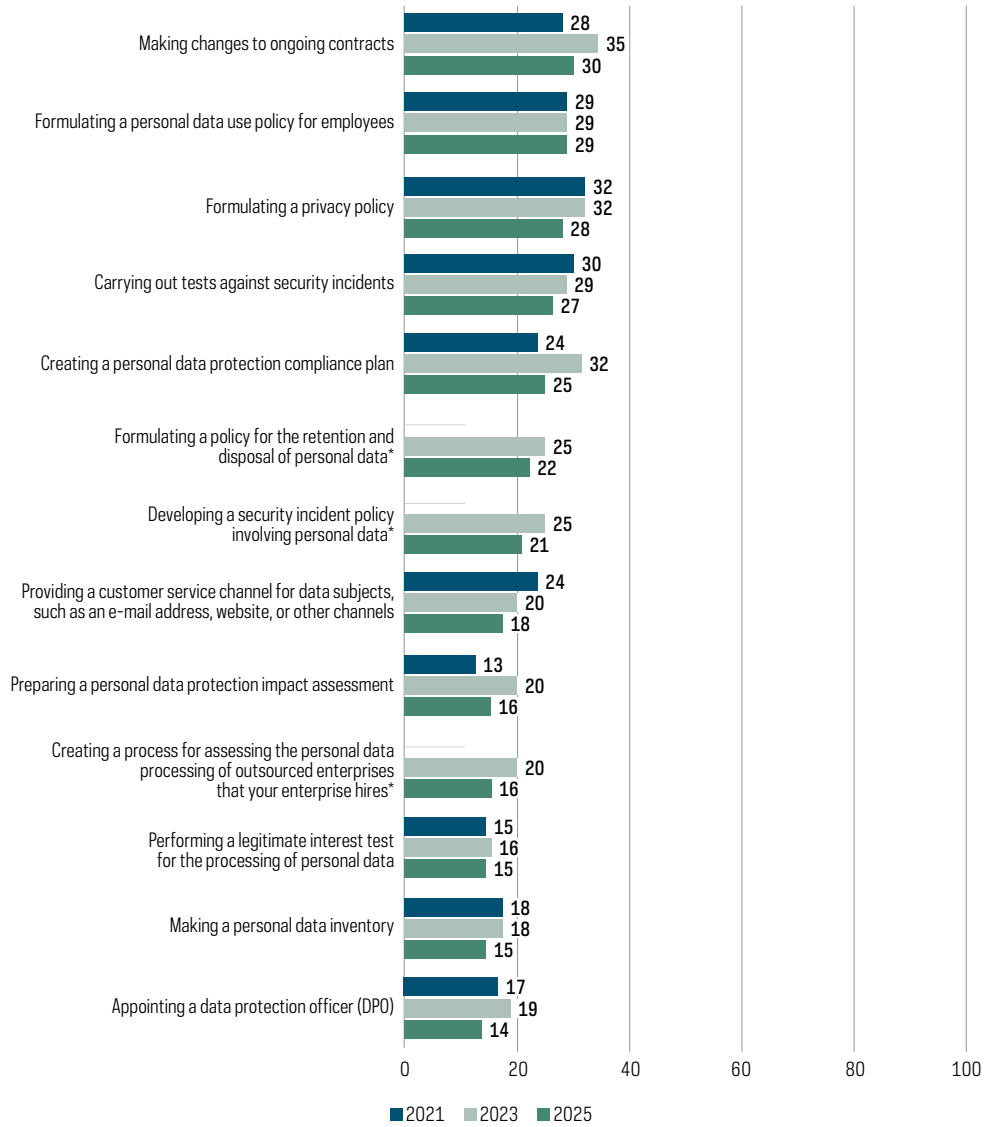
[20] The discussion mentioned in the previous section regarding the use of biometrics for access control may be related to these results, due to the need for differentiated treatment of sensitive data, in terms of explicitly stating the purpose and sharing practices, among others, in order to comply with the principles that guide the law. In this regard, the ANPD published a technological radar on the specifics of biometric data processing (Cebrian et al., 2024).

CHART 10

—

Enterprises by type of action to comply with the LGPD (2021–2025)

Total number of enterprises that keep data on natural persons (%)



Note: *Response category included starting in 2023.

As noted, some practices listed in Chart 10, although not expressly provided for in the LGPD, are consistent with the principles established by it for the processing of personal data. Among the highlighted items, four are mandated by law and constitute obligations for enterprises. In 2025, the availability of a service channel for data subjects was the most common item, reported by 18% of enterprises that store data on individuals (Chart 11).[21] The second most cited was the preparation of a personal data protection impact assessment report,[22] mentioned by 16% of enterprises, followed by conducting a legitimate interest test (15%) and appointing a DPO (14%).[23]

Finally, it is worth highlighting that there is a greater pursuit of compliance among large enterprises, which may reflect a greater availability of resources to structure personal data protection actions, as well as a likely larger volume of data processed internally.[24]

[21] As stipulated in Article 9 of the LGPD: "The data subject has the right to facilitated access to information concerning the processing of her/his data, which much be made available in a clear, adequate and ostensible manner, concerning, among other characteristics provided in regulation for complying with the principle of free access: I – the specific purpose of the processing; II – the type and duration of the processing, being observed commercial and industrial secrecy; III – identification of the controller; IV – the controller's contact information; V – information regarding the shared use of data by the controller and the purpose; VI – responsibilities of the agents that will carry out the processing; and VII – the data subject's rights, with explicit mention of the rights provided in Art. 18 of this Law." (Law No. 13.709/2018).

[22] The impact report is mentioned several times in Article 38: "The national authority may determine that the controller must prepare an impact report on protection of personal data, including sensitive data, referring to its data processing operations, pursuant to regulations, subject to commercial and industrial secrecy. Sole paragraph. Subject to the provisions of the lead sentence of this article, the report must contain at least a description of the types of data collected, the methodology used for collection and for ensuring the security of the information, and the analysis of the controller regarding the adopted measures, safeguards and mechanisms of risk mitigation." (Law No. 13.709/2018).

[23] Legitimate interest is precisely one of the requirements for processing personal data, and its specification can be included in the personal data protection impact assessment report. According to Article 10: "Controller's legitimate interest can only be grounds for processing personal data for legitimate purposes, based on particular situations, which include but are not limited to: I - support and promotion of the controller's activities; and II - protection of data subject's regular exercise of her/his rights or provision of services that benefit her/him, subject to her/his legitimate expectations and fundamental rights and freedoms, in accordance with this Law. Paragraph 1 When processing is based on the controller's legitimate interest, only the personal data which are strictly necessary for the intended purpose may be processed. Paragraph 2 The controller shall adopt measures to ensure transparency of data processing based on her/his legitimate interests. Paragraph 3 The national authority may request of the controller an impact report on protection of personal data, when processing is based on her/his legitimate interest, being observed commercial and industrial secrecy." (Law No. 13.709/2018).

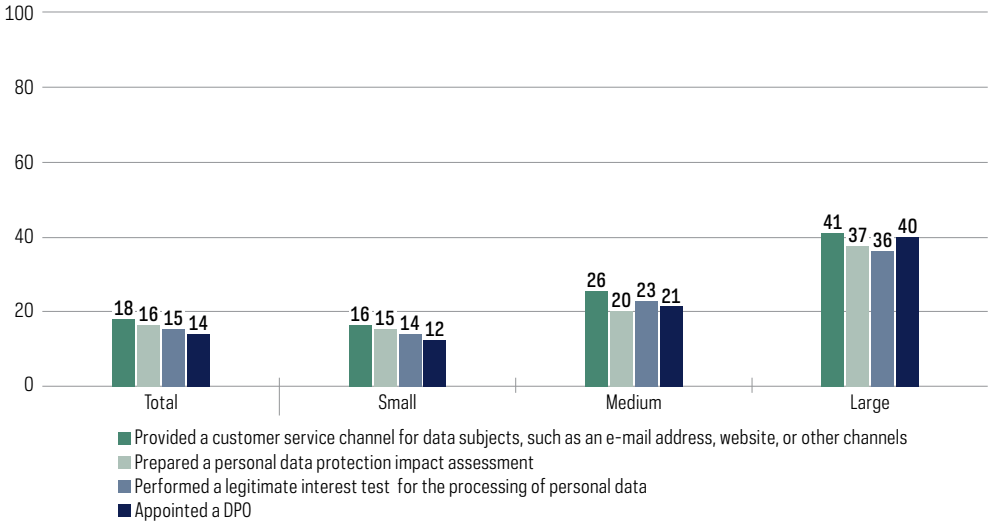
[24] The regulatory asymmetries established by CD/ANPD No. 2/2022 may influence these results, since some obligations are no longer required of small enterprises. Although, as discussed, the concept of size used in the resolution and in ICT Enterprises is not the same, there may be enterprises covered by both criteria.

CHART 11

—

Enterprises by type of action to comply with the LGPD requirements and size (2025)

Total number of enterprises that keep data on natural persons (%)



One of the practices foreseen by the LGPD is the appointment of a DPO. According to Article 41 of the LGPD, the DPO is responsible for communicating about the organization's data processing practices and acts as a focal point for data subjects and the regulatory body.[25] In addition to this function, they are also responsible for providing internal guidance on best practices for data processing, giving the position an important role in the development of internal capacities. Among enterprises with a DPO in 2025, 28% reported that this professional comes from the information technology department, and 19% reported that the source was the enterprise's administrative department, showing a relationship with the indicator on the existence of organizational structures exclusively dedicated to dealing with the subject (Chart 12).

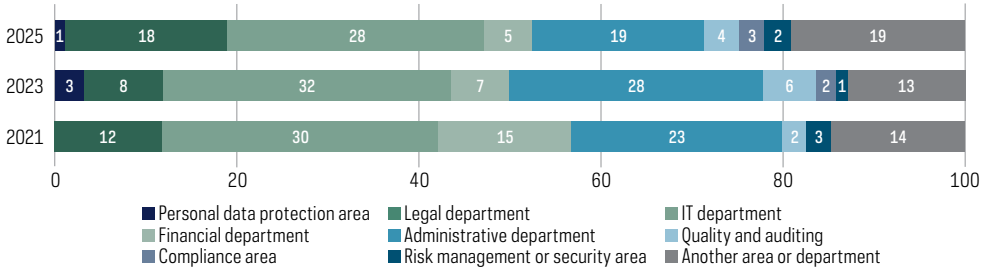
[25] In 2024, the ANPD published Resolution CD/ANPD No. 18/2024, which regulates the role of the DPO, detailing their actions in relation to Article 41 of the LGPD, especially establishing the parameters of their interaction with the regulator.

CHART 12

—

Enterprises by origin of the DPO (2021–2025)

Total number of enterprises whose DPO came from inside the enterprises (%)



Given their role in communicating with data subjects and the regulator, controllers are expected to make public the information about their DPO. Resolution CD/ANPD No. 18/2024, for example, establishes, in its Article 9, the required information about the DPO that must be made available on the data controller's website, clearly and objectively, in a prominent and easily accessible location.[26] In addition to this specific requirement, according to the LGPD, websites are the designated means for displaying various information, such as the purpose and procedures for processing personal data of the organization.

Thus, websites assume a relevant institutional role as a means of transparency and communication with data subjects, serving as a repository for information required by law and important instruments to contribute to the enterprise's reputation among customers and users, through transparency criteria such as information availability and means of communication.[27] In 2025, among enterprises with websites, 42% stated that they offered a customer service channel for data subjects, while 41% provided an information security policy (Chart 13).[28] However, it is important to note that the proportion of enterprises that made the DPO's name and contact information available on their website fell to 7% in 2025, down from 17% in 2023.

[26] "The identity and contact information of the data protection officer must be publicly disclosed, clearly and objectively, in a prominent and easily accessible location on the data processing agent's website, except in the case of paragraph 3 of this article: Paragraph 1. The disclosure of the data protection officer's identity shall include, at a minimum: I - the full name, if a natural person; or II - the company name or establishment title, as well as the full name of the responsible natural person, if a legal entity."

[27] According to the ICT Enterprises 2025 survey, 56% of Brazilian enterprises had websites, reaching 87% of large enterprises, 76% of medium enterprises, and 53% of small enterprises (NIC.br, 2026b).

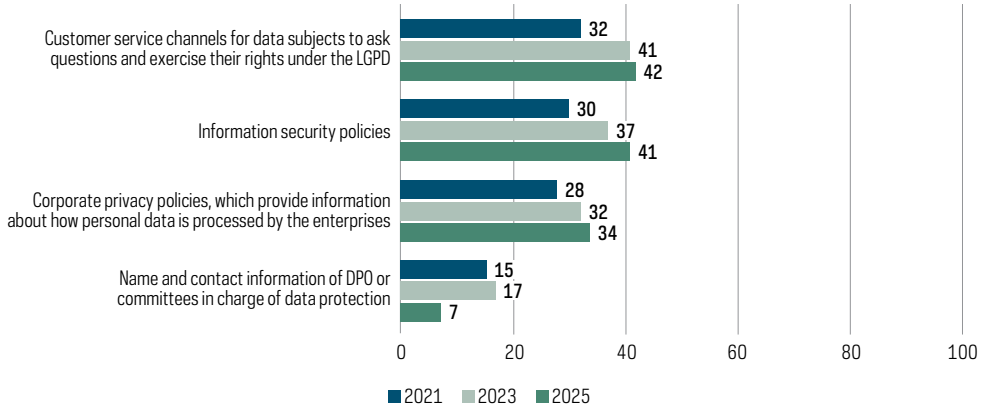
[28] The provision of information via websites is also foreseen in Article 41 of the ECA Digital, maintaining a relationship with the requirements of the LGPD, even if restricted to Internet application providers or those with probable access, with more than one million registered child users.

CHART 13

—

Enterprises by resources made available on their websites (2021–2025)

Total number of enterprises with a website (%)



Data from the historical series of research on compliance with the LGPD shows that challenges persist, both regarding the requirements demanded by law and best practices for privacy and protection of personal data. As discussed throughout this chapter, this scenario deserves attention, given the advancement of digital technologies that increases enterprises' exposure to digital security risks, as well as making the rules that guide organizational operations and, consequently, the governance of personal data processing more complex. In this context, compliance with the law tends to take on a more strategic role on enterprises' agendas, not only to meet legal requirements but also to contribute to organizational resilience, information security, and the trust of customers and users.

Final considerations: Agenda for public policies

The latest edition of the survey on privacy and personal data protection among Brazilian enterprises shows that there is still significant room to expand the adoption of best practices and strengthen compliance with the parameters established by the LGPD. Furthermore, the enactment of the ECA Digital brings new challenges, as it establishes additional obligations for enterprises related to their operations in the digital environment when children are involved.

From a technological standpoint, the increasing digitalization of production and service processes amplifies enterprises' exposure to risks related to the processing of personal data. Therefore, even though the greater availability of process automation tools can facilitate internal communication and enable a more strategic use of the digital environment, it is necessary that the use of technology is also accompanied by greater awareness of its relationship with best practices for processing personal data.

In this context, it is important for enterprises to monitor how the regulator will act in overseeing two laws that complement each other in several aspects. Throughout this chapter, ANPD documents have been referenced that highlight convergences between the LGPD and the ECA Digital, which enterprises should observe, especially the relationship between age verification mechanisms and the processing of personal data of individuals under 18 years old. Therefore, it is understood that there is a new moment of regulation of the digital economy in the country, with more defined rules on the online operation of enterprises.

In this sense, the results indicate that best practices for protecting personal data still have room to be incorporated into enterprises' processes. Most indicators showed stability compared to the first edition of the survey, conducted in 2021. There is room for progress, especially among small enterprises and across most sectors of the economy, given that virtually all enterprises process personal data in some way and are, to some extent, exposed in the digital environment.

Therefore, the results show that the advancement of digital transformation has not been accompanied by the same intensity in the consolidation of personal data protection practices among Brazilian enterprises. This scenario reveals that the adoption of these measures is still uneven, concentrated in large enterprises and in certain sectors of activity, mainly in the information and communication sector.

Finally, the results presented in this chapter reinforce the importance of public policies aimed at disseminating guidelines, tools, and best practices that support the implementation of the LGPD, especially among small and medium-sized enterprises and in sectors that showed lower adoption of the measures analyzed. In addition to contributing to regulatory compliance, training and guidance initiatives tailored to the characteristics of each segment can help strengthen data governance, broaden the culture of personal data protection, and reduce the disparities identified by the survey.

References

Brazilian Digital Statute of the Child and Adolescent. Law No. 15.211, of September 17, 2025 (2025). This law addresses the protection of children and adolescents in digital environments (Brazilian Digital Statute of the Child and Adolescent). https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/l15211.htm

Brazilian General Data Protection Law. Law no. 13.709, of August 14, 2018. (2018). Brazilian General Data Protection Law (LGPD). https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Brazilian Internet Steering Committee. (2026a, July 24). *Contribuição do CGI.br à tomada de subsídios sobre o Guia Orientativo "Mecanismos de Aferição de Idade"*. https://cgi.br/publicacao/contribuicao-do-cgi-br-a-tomada-de-subsidios-da-anpd-sobre-mecanismos-de-afericao-de-idade/

Brazilian Internet Steering Committee. (2026b). *Práticas de aferição de idade em 25 serviços digitais no Brasil*. https://cetic.br/pt/publicacao/praticas-de-afericao-de-idade-em-25-servicos-digitais-no-brasil/

Brazilian Network Information Center. (2026a). *Survey on Internet use by children in Brazil: ICT Kids Online Brazil 2025* [Tables]. https://cetic.br/en/pesquisa/kids-online/indicadores/

Brazilian Network Information Center. (2026b). *Survey on the use of information and communication technologies in Brazilian enterprises: ICT Enterprises 2025* [Tables]. https://cetic.br/en/pesquisa/empresas/indicadores/

Brazilian Network Information Center. (2026c). *Survey on the use of information and communication technologies in Brazilian households: ICT Households 2025* [Tables]. https://cetic.br/en/pesquisa/domicilios/indicadores/

Cebrian, F. S. P. F., Prudente, G. A., Guedes, M. S., Sá, M. L. D., & Thiago, G. M. (2024). *Radar tecnológico n. 2: biometria e reconhecimento facial: estudos preliminares*. National Data Protection Agency. https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/radar-tecnologico-biometria-anpd-1.pdf

Decree No. 12.622, of September 17, 2025. (2025). This decree regulates Law No. 15.211, of September 17, 2025, to designate the National Data Protection Agency as an autonomous administrative authority for the protection of children and adolescents in digital environments, and to establish competencies for the fulfillment of judicial blocking orders. https://www.in.gov.br/en/web/dou/-/decreto-n-12.622-de-17-de-setembro-de-2025-656777269

Law No. 15.352, of February 25, 2026. (2026). Transforms positions within the federal Executive Branch; amends Law No. 13.709, of August 14, 2018 (Brazilian General Data Protection Law), to provide for the National Data Protection Agency (ANPD), Law No. 10.871, of May 20, 2004, to create the Career in Regulation and Supervision of Data Protection, Law No. 15.211, of September 17, 2025 (Brazilian Digital Statute of the Child and Adolescent), to provide for the beginning of the validity of said Law; Amends Laws No. 9.008 of March 21, 1995, No. 11.890 of December 24, 2008, No. 13.326 of July 29, 2016, No. 13.848 of June 25, 2019, and No. 14.600 of June 19, 2023; revokes Provisional Measure No. 1.319 of September 17, 2025; and provides other measures. https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/lei/l15352.htm

National Data Protection Agency. (2024). *Radar tecnológico n.º 3: Inteligência artificial generativa*. Federal Government. https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/radar_tecnologico_ia_generativa_anpd.pdf

National Data Protection Agency. (2026). *Mecanismos confiáveis de aferição de idade: orientações preliminares*. https://www.gov.br/anpd/pt-br/assuntos/eca-digital/mecanismos-confiaveis-de-afericao-de-idade-orientacoes-preliminares.pdf

Provisional Measure No. 1.317, of September 17, 2025. (2025). It alters the legal nature of the National Data Protection Agency. Presidency of the Republic. https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/mpv/mpv1317.htm

Resolution CD/ANPD No. 2, of January 27, 2022. (2022). Approves the Regulation for the application of Law No. 13.709, of August 14, 2018 (Brazilian General Data Protection Law – LGPD), for small-scale data processing agents. https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no-2-de-27-de-janeiro-de-2022

Resolution CD/ANPD No. 18, of July 16, 2024. (2024). Approves the Regulation on the role of the data protection officer. https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-18-de-16-de-julho-de-2024-572632074

Analysis of Results
Privacy and Personal Data Protection 2025
Public organizations

Digital transformation has intensified the adoption of digital technologies in public administration, healthcare facilities, and educational institutions. This process ranges from the digitalization of public services to the adoption of electronic systems to support administrative, care, pedagogical, and management processes. It contributes to expanded public access to these services, increased administrative efficiency, and improved public policy formulation and implementation. Furthermore, this shift has been increasingly associated with the incorporation of advanced technologies such as Artificial Intelligence (AI) to redesign processes, improve decision-making, and offer more efficient, responsive services focused on the needs of society (United Nations Department of Economic and Social Affairs [UN DESA], 2024; United Nations Educational, Scientific and Cultural Organization [UNESCO], 2022).

In this context, data use and sharing have become central to implementing public policies and providing digital services in public organizations worldwide. One example is the dissemination of digital identification systems: The 2025 edition of the World Bank's *ID4D Global Dataset 2025: Trends in Identification for Development* report indicated that more than one hundred countries had already implemented some form of digital identity (Ansar et al., 2026). Sharing information between public organizations and electronic systems can also reduce the need for repeated document submission and enable proactive or "zero-click" services,[1] which are offered based on information already available in the public sector (Maia, 2026).

Despite recognizing these benefits, the challenges and risks of using and sharing data in public administration are also increasing. One of these challenges is the need to ensure the right to privacy and the protection of personal data, so that digital transformation initiatives in the public sector are accompanied by data governance measures that promote these rights.

[1] Proactivity in this context refers to the ability of governments to anticipate citizens' needs and offer services before they are explicitly requested, based on the once-only principle, data analysis, AI, and predictive tools, in order to promote a shift from a reactive to an anticipatory model of government action (Organisation for Economic Co-operation and Development [OECD], 2026).

The importance of the topic is also reflected in the Regulatory Agenda of the National Data Protection Agency (ANPD) for the 2025–2026 biennium (Resolution CD/ANPD No. 31/2025), which included the shared use of personal data by the public sector as a priority. In 2025, the ANPD submitted a proposed regulation for public consultation and a public hearing, highlighting the need to establish clearer parameters for the sharing of information between public organizations and, in certain situations, between the public sector and private entities.[2]

The adoption of protective measures has special significance for handling sensitive personal data or information about groups subject to specific protection. In healthcare facilities, both public and private, medical records, test results, diagnoses, and other information about patients' health conditions are identified as sensitive personal data under the Brazilian General Data Protection Law (LGPD). While using and sharing this information is essential for continuity of care, healthcare system management, and public policy formulation, it can also lead to harm to data subjects if it is accessed without authorization, leaked, or used for purposes incompatible with its intended use.

Educational institutions, especially in Basic Education, increasingly adopt educational platforms, management systems, applications, and other digital resources that process children's data, including information on performance, behavior, attendance, and personal and family circumstances (Brazilian Internet Steering Committee [CGI.br], 2025). In addition to the protection provided by the LGPD, this area has recently been regulated by the Digital Statute of the Child and Adolescent (ECA Digital), established by Law No. 15.211 of September 17, 2025, which sets out rules for the protection of children in digital environments, including measures for the prevention and mitigation of risks and obligations related to the protection of their rights.

The ECA Digital also expanded the institutional responsibilities of the ANPD, which was designated as an autonomous administrative authority responsible for ensuring the implementation of the new legislation (Decree No. 12.622/2025). This mandate adds to the functions already exercised by the agency under the LGPD and reinforces the relationship between the comprehensive protection of this population and the guarantee of the rights to privacy and the protection of personal data. In the school context, although many requirements of the ECA Digital apply to providers of digital products and services, the new legislation increases the importance of evaluating how technologies used by schools handle student data and incorporate measures appropriate to each age group and the best interests of this population.

In the Brazilian context, instruments related to public-sector digital transformation, such as the Brazilian Artificial Intelligence Plan (PBIA) (Brazilian Ministry of Science, Technology and Innovation [MCTI] & Center for Management and Strategic Studies [CGEE], 2025) and the National Digital Government Strategy (ENGD) (Brazilian Ministry of Management and Innovation in Public Services [MGI], n.d.), identify privacy and data protection as guiding principles for their implementation. Likewise, Law No. 14.129/2021, which establishes principles, rules, and measures for digital government,

[2] More information is available at https://www.gov.br/participamaisbrasil/regulamento-sobre-o-uso-compartilhado-de-dadospessoais-pelo-poder-publico

includes the protection of personal data among its guidelines. Therefore, as digital services expand, government databases become more integrated, and data-intensive technologies such as AI are adopted, it is essential to assess the extent to which public organizations incorporate privacy and personal data protection rights into their practices.

To this end, this chapter presents indicators produced by the Regional Center for Studies on the Development of the Information Society (Cetic.br), a department of the Brazilian Network Information Center (NIC.br), on privacy and protection of personal data in various public organizations. The chapter is organized as follows:

- **Federal and state government organizations and local governments:** The first section presents the results of the ICT in Government 2025 survey (CGI.br, 2026b) and analyzes the main measures adopted by the organizations surveyed regarding privacy and the protection of personal data.
- **Public healthcare facilities:** The second section addresses initiatives to promote digital security, privacy, and data protection in public healthcare facilities, based on indicators from the ICT in Health 2025 survey (CGI.br, 2026c), including comparisons with private facilities.
- **Public Basic Education institutions:** The third section analyzes the main challenges for consolidating a data protection culture in these institutions, from the perspective of different members of the school community surveyed in the 2024 and 2025 editions of the ICT in Education survey (CGI.br, 2025, 2026a).

Federal and state government organizations and local governments

In 2025, the biennial ICT in Government survey included, for the third time, Module G – "Privacy and protection of personal data". This set of indicators makes it possible to monitor how Brazilian government organizations are adopting actions related to data protection and to identify the challenges to consolidating a data protection culture across the public sector, including federal and state government organizations in the executive, legislative, and judicial branches, the Public Prosecutor's Office, and local governments.

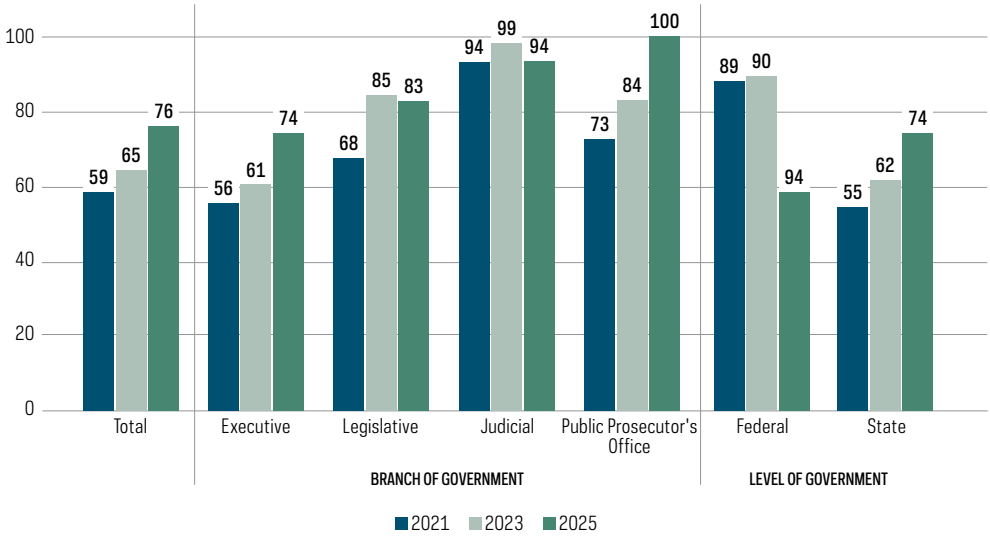
In the set of actions related to privacy and the protection of personal data investigated by ICT in Government, one change observed in relation to the 2023 edition was an increase in the proportion of government organizations that had areas or persons responsible for procedures and policies governing the collection, storage, and use of personal data. In federal and state government organizations, having persons or institutional structures focused on this issue remained higher in the Public Prosecutor's Office (100%) and the judicial (94%), and legislative branches (83%) compared to the executive branch (74%), and in federal government organizations (94%) compared to state government organizations (74%). Chart 1 shows that there was significant growth compared to 2023 in organizations that had areas or persons focused on the LGPD in the Public Prosecutor's Office, with an increase of 16 percentage points, and in the executive branch and state government organizations, both with growth of 13 percentage points.

CHART 1

—

Federal and state government organizations, by whether there are areas or persons responsible for procedures and policies for the collection, storage, or use of personal data or for the implementation of the LGPD (2021–2025)

Total number of federal and state government organizations (%)



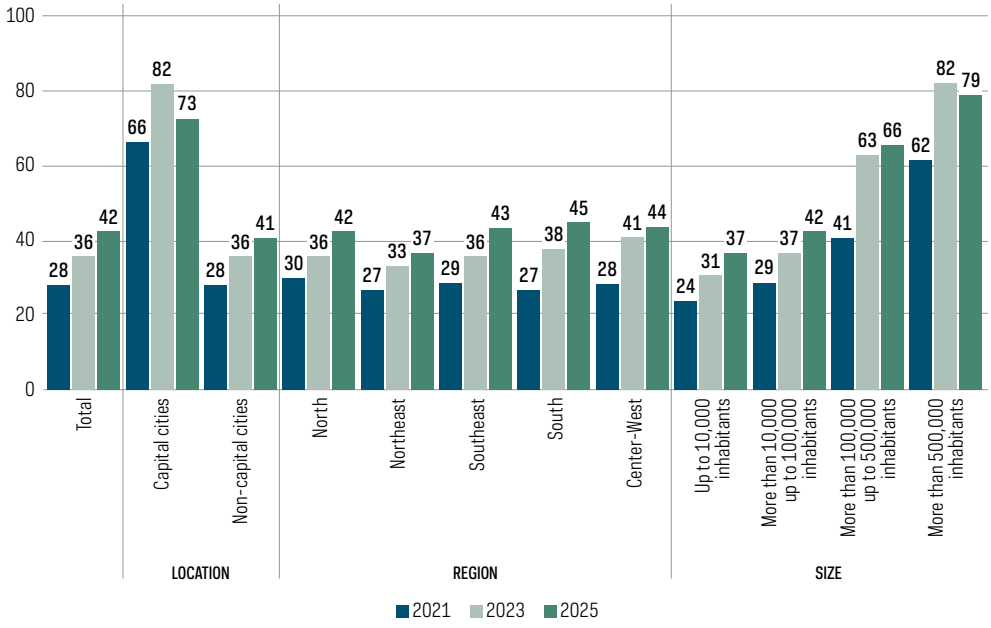
An increase was also identified at the local level in having structures or persons responsible for privacy and data protection, rising from 36% in 2023 to 42% in 2025. This change can be attributed to the growth among local governments of municipalities with up to 10,000 inhabitants: Having areas or persons responsible for personal data was mentioned by less than a third of these local governments in 2023 and reached 37% in 2025 (Chart 2).

CHART 2

—

Local governments, by whether there are areas or persons responsible for procedures and policies for the collection, storage, or use of personal data or for the implementation of the LGPD (2021–2025)

Total number of local governments (%)



In addition to having areas or persons responsible for data protection, internal training is fundamental to consolidating a data protection culture in the public sector. Within the scope of Objective 4, Privacy and Security (MGI, n.d.), the ENGD recommends awareness-raising, sensitization, and training actions for public agents, government leaders, and society on privacy, personal data protection, information security, and cybersecurity.

The ICT in Government survey investigates the provision of LGPD training, courses, and workshops for information technology (IT) professionals.[3] In 2025, 95% of organizations in the judicial branch, 83% of the Public Prosecutor's Office, and 75% of the legislative branch promoted these initiatives. The proportions were lower in the executive branch (61%) and in state government organizations (62%), compared to federal organizations (85%). Among local governments with IT departments, 35% trained at least one employee in the sector, with a higher proportion in capital cities (72%), in local governments of municipalities with more than 100,000 and up to 500,000 inhabitants (51%), and in those with more than 500,000 inhabitants (82%).

[3] The ICT in Government 2025 survey found that 86% of federal and state government organizations had IT departments, which was more prevalent in the judicial (100%) and legislative (96%) branches, the Public Prosecutor's Office (96%), and federal-level organizations (99%). Among state organizations, 85% had areas dedicated to technology; at the municipal level, 49% of local governments had IT areas or departments in 2025 (CGI.br, 2026b).

The ICT in Government survey also measures specific actions for the implementation of the LGPD, such as the appointment of data protection officers (DPO) and the provision of online channels for citizens to send messages about the use of their data. The survey investigated five actions in federal and state government organizations. More than half had already appointed DPO (62%), made online customer service channels available for citizens regarding the use of their personal data (57%), and posted privacy policies on the Internet (52%). In smaller proportions, respondents mentioned implementing response plans for information security incidents related to personal data (43%) and having governance programs for privacy and personal data protection (44%).

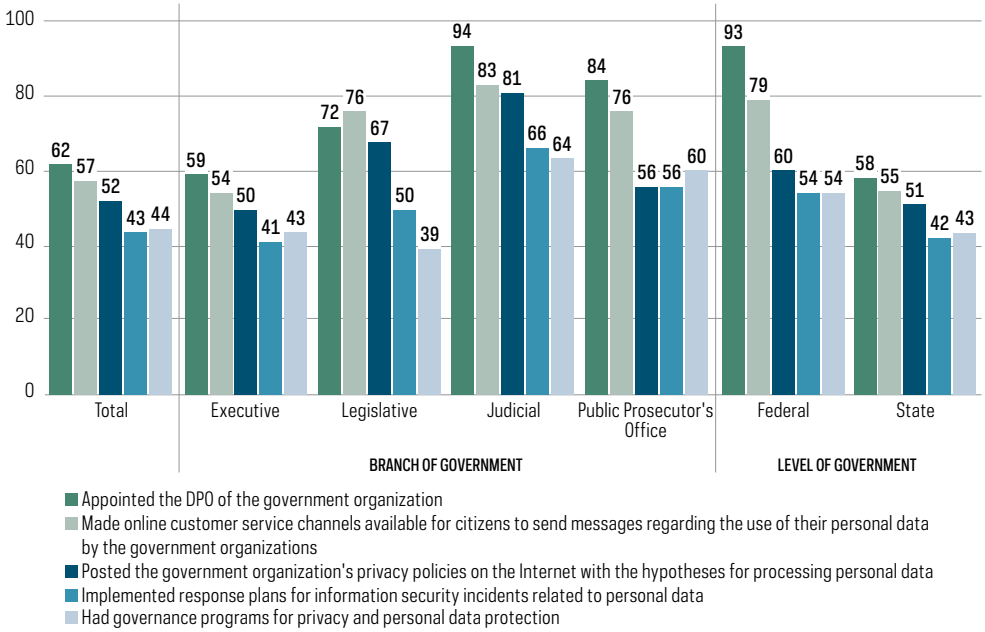
Between 2023 and 2025, there was an increase in the adoption of measures related to the LGPD, especially among state government organizations. More than half of the organizations at this level of government had appointed DPO (going from 46% in 2023 to 58% in 2025), while the implementation of incident response plans increased from 30% to 42%. However, these proportions remained lower compared to the federal level, where 93% had appointed DPO and 54% had incident response plans in 2025. As in previous editions, the judicial branch was notable for the highest proportion of the investigated actions (Chart 3). In 2025, more than 80% of its organizations had appointed DPO, made online customer service channels available, and posted privacy policies on the Internet.

CHART 3

—

Federal and state government organizations by actions related to the LGPD (2025)

Total number of federal and state government organizations (%)



In 2025, the survey began investigating the presence of governance programs for privacy and data protection in federal and state government organizations. Like incident response plans, this was one of the least-mentioned initiatives. These programs were present in 54% of federal government organizations and in 43% of state organizations. Among the branches of government, the highest proportions were observed in the judicial branch (64%) and the Public Prosecutor's Office (60%), followed by the executive (43%) and the legislative (39%) branches.

Article 50 of the LGPD addresses privacy governance programs in the section on best practices and governance, establishing minimum requirements for their implementation. This type of program can be defined as an "instrument capable of demonstrating the integrity and commitment of the data controller in adopting internal processes and policies that ensure comprehensive compliance with standards and best practices related to the protection of personal data" (ANPD, 2024, p. 33). Some government organizations already have specific regulations on the subject, such as Resolution No. 281/2023 of the National Council of the Public Prosecutor's Office (CNMP); a guide has also been developed to support the implementation of privacy governance programs at the federal level (MGI, 2024).

The inclusion of the "Rules of Good Practices and Governance" initiative among the priorities of the ANPD Regulatory Agenda for the 2025–2026 biennium (Resolution CD/ANPD No. 31/2025) reinforces the importance of this issue. The Call for Contributions on the regulatory agenda also highlighted the role of these programs in ensuring compliance with the LGPD in the adoption of AI tools (ANPD, 2025). Despite growing normative and regulatory support, the data from the ICT in Government 2025 survey indicate that the adoption of governance programs for privacy and data protection is not yet widespread among federal and state government organizations. This data further reinforces the importance of monitoring the development of these policies in future editions of the survey, considering their strategic role in institutionalizing practices to comply with the LGPD and promoting the responsible use of personal data and advanced technologies such as AI.

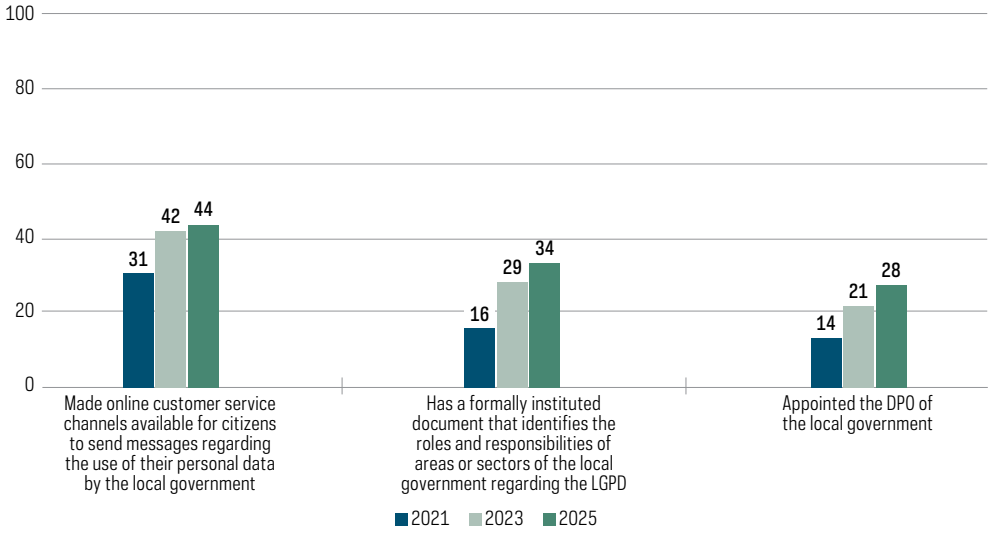
Among local governments, the survey measures three actions related to the LGPD. Between 2023 and 2025, there was significant growth in the appointment of DPO and in having formal documents defining the roles and responsibilities of local governments' areas or sectors related to the LGPD (Chart 4). This progress was mainly due to changes observed in municipalities with up to 10,000 inhabitants, where the appointment of DPO increased from 17% to 24%, and having a formal document increased from 27% to 32%. The appointment of DPO also rose from 21% to 34% among municipalities with more than 10,000 and up to 100,000 inhabitants.

CHART 4

—

Local governments by actions related to the LGPD (2021–2025)

Total number of local governments (%)



Online customer service channels for citizens to send messages regarding the use of their personal data remained the most frequently mentioned initiative, although less than half of the local governments (44%) had them. The actions investigated were also cited more frequently in larger local governments and capital cities. For example, seven out of ten municipalities with more than 500,000 inhabitants and 62% of capital cities mentioned having formal documents defining the roles and responsibilities of their areas in relation to the LGPD. Despite the progress observed during the period, especially among smaller local governments, inequalities remain among municipalities in the adoption of measures related to privacy and the protection of personal data.

Public healthcare facilities

Digital transformation has brought about profound changes in the organization of healthcare systems and the delivery of healthcare services. In this scenario, the increasing incorporation of digital technologies into clinical and administrative processes has expanded the computerization of healthcare facilities and the offer of digital services, such as electronic health records, electronic prescriptions for medications, requesting and sharing of exams, clinical decision support systems, telehealth platforms, and other applications focused on patient management and care. This process not only expands opportunities to improve care quality, care coordination, and healthcare system efficiency, but also reinforces the importance of information security in systems that store and process personal health data, which are identified as sensitive personal data under the

LGPD. The increasing digitalization of health care has intensified the volume, circulation, and use of sensitive data, making the protection of this information one of the main challenges to developing ethical and responsible digital health care aligned with the guarantee of fundamental rights (Aith et al., 2025).

The ICT in Health survey results highlight progress in this digitalization process in Brazilian public healthcare facilities. In 2025, considering all three levels of care, 91% of public facilities used electronic systems to record patient information, 35% made test results available online, 32% offered online booking of consultations, and 34% conducted teleconsultations. Furthermore, 11% of public facilities used AI applications, a technology whose adoption has been uneven across different levels of care, with proportions reaching 10% in outpatient facilities and 23% in public hospitals with more than 50 inpatient beds (CGI.br, 2026c). This pattern suggests that the use of these tools, in addition to expanding the potential for data analysis and sharing, automating processes, and supporting clinical and managerial decisions, also introduces new challenges related to information security, data governance, and the protection of patient privacy.

International organizations emphasize that the digital healthcare transformation must be accompanied by stronger data governance and information security. In its guiding principles for the digital transformation of the health sector, the Pan American Health Organization (PAHO) highlights that trust in digital systems depends on adopting policies and mechanisms capable of ensuring the confidentiality, integrity, availability, and ethical use of health data (PAHO, 2021). Similarly, the OECD emphasizes that expanding the use of health data for care, management, research, and public policy formulation requires robust governance, privacy, and information security structures that strengthen public trust and ensure responsible use of this data (OECD, 2022).

In line with these recommendations, the World Health Organization (WHO), in its Global Digital Health Strategy 2020–2025, highlights that the maturity of digital health security depends on adopting technological solutions and implementing governance structures, institutional policies, professional training, and risk-management and incident-response mechanisms (WHO, 2021).

At the national level, this agenda is supported by the ANPD's guidelines that are focused on the processing of personal data by public authorities and designed to guide public bodies and entities in complying with the LGPD (ANPD, 2023). From this perspective, the indicators presented in this section allow for the analysis of the degree of institutionalization of these capabilities in Brazilian public healthcare facilities, offering an overview of the implementation of information security policies, training actions, system protection tools, and measures related to LGPD compliance.

An information security policy is one of the main governance instruments for protecting organizations' informational assets. In addition to defining rules for the use and protection of data, it establishes responsibilities, procedures, and guidelines to prevent security incidents and promote a culture of data protection. The 2025 survey results show that the institutionalization of these policies remains limited, with no significant change among Brazilian healthcare facilities: less than half (42%) said they had defined information security policies, compared to 40% in 2023 (CGI.br, 2024). Furthermore, there was a gap between public (28%) and private (54%) facilities, with public facilities showing a 4 percentage point increase and private facilities remaining stable.

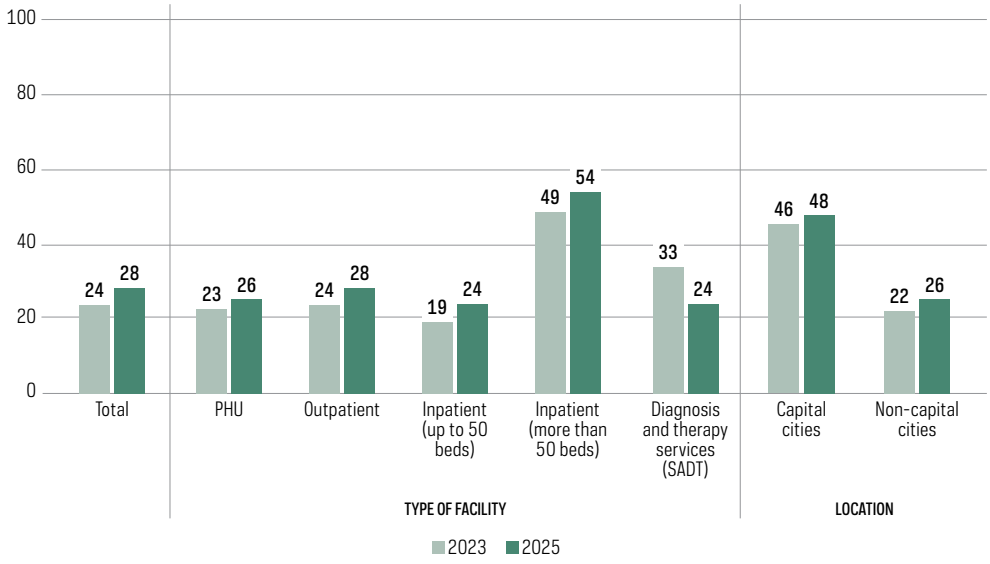
When looking specifically at public facilities, the main difference is related to the size and complexity of services: While 54% of public hospitals with more than 50 beds had information security policies, this percentage was around 25% in other types of facilities (Chart 5). There were also differences according to the location of the facilities. The proportion was 48% for facilities in capital cities, a percentage notably higher than that recorded in non-capital cities (26%).

CHART 5

—

Public healthcare facilities with an information security policy (2023–2025)

Total number of public healthcare facilities with Internet access (%)



Professional training is another fundamental component of information security. Although institutional policies establish data protection guidelines, their effectiveness depends on incorporating these practices into the routines of the professionals who use information systems and handle patients' personal data.

The data indicates that 47% of healthcare facilities offered information security training to their professionals in 2025, which represents an improvement compared to 2023, when that proportion was 31% of facilities. This increase occurred both in public facilities, going from 16% to 32% in the analyzed period, and in private facilities, which went from 44% to 60%.

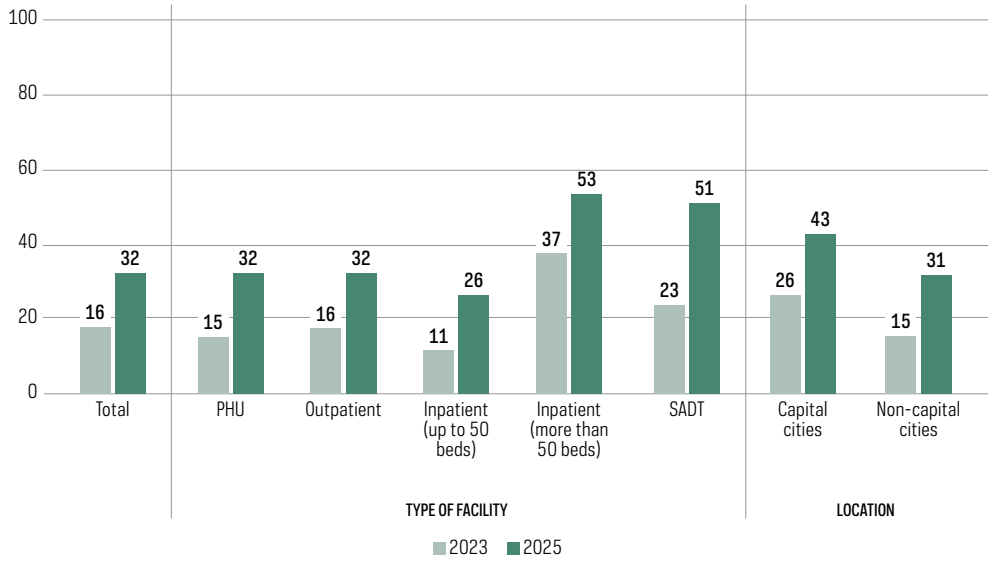
Despite this change, the provision of training remains less frequent in the public sector. Hospitals with more than 50 beds (53%) and diagnosis and therapy services (SADT, as per its acronym in Portuguese) (51%) showed the highest percentages, while other types of facilities showed significantly lower proportions (Chart 6). There were also differences according to the location of the facilities: In capital cities, 43% of the facilities offered this training, while that figure was 31% in the non-capital cities.

CHART 6

—

Public healthcare facilities with an information security training program for employees (2023–2025)

Total number of public healthcare facilities with Internet access (%)



In addition to information security policies and professional training, the survey examined the adoption of measures related to implementing the LGPD. Initiatives focused on data governance were analyzed, such as the appointment of DPO and the implementation of security incident response plans, as well as actions related to transparency and institutional awareness, including the provision of service channels for data subjects, the publication of privacy policies, and the implementation of internal awareness campaigns about the LGPD.

Comparison between 2023 and 2025 shows that the implementation of these measures remained relatively stable during the period. Across all healthcare facilities, there was a slight increase in internal awareness campaigns about the LGPD (from 43% to 46%), in the publication of privacy policies (from 30% to 32%), and in the provision of customer service channels for data subjects (from 28% to 30%). In contrast, the proportion of facilities that had appointed a DPO remained stable at 30%, while the implementation of incident response plans changed only slightly, from 31% to 30%.

A similar pattern emerged when public and private facilities were analyzed separately. In public facilities, the implementation of internal campaigns about the LGPD increased from 28% in 2023 to 30% in 2025. The publication of privacy policies rose from 25% to 29%, while the availability of customer service channels for data subjects increased from 16% to 19%. There was a reduction in the proportion of institutions that had designated DPO (from 16% to 13%) and implemented security incident response plans (from 17% to 15%). Among private facilities, the variations were also small, maintaining higher levels than those observed in the public sector for all indicators analyzed.

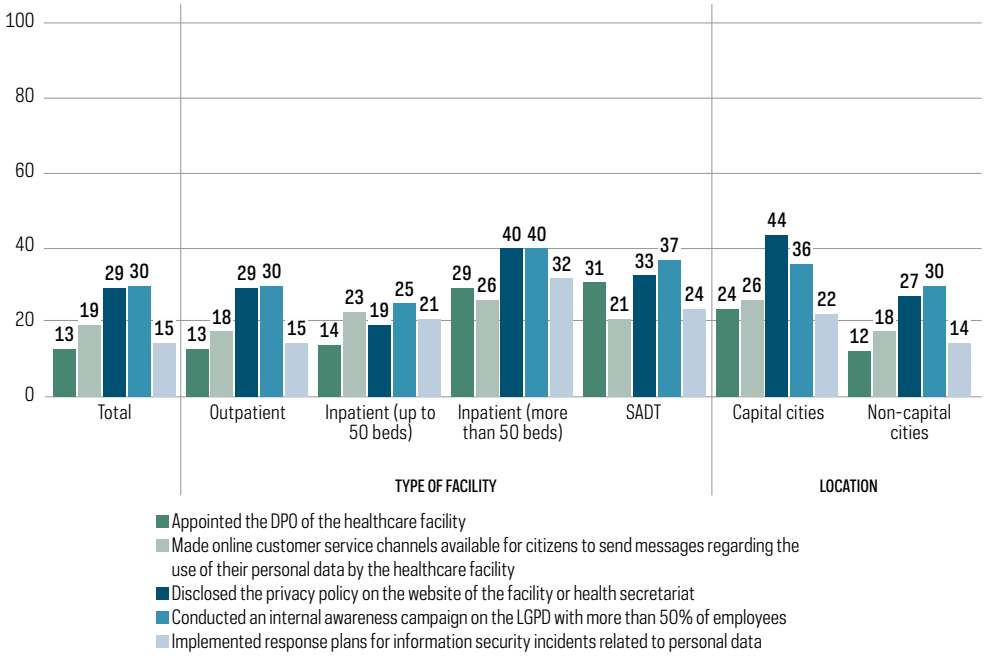
Therefore, the analysis of public facilities in 2025 reveals important differences in the adoption of LGPD-related measures by type of facility and location (Chart 7). In general, hospitals with more than 50 beds and SADT showed higher percentages across most indicators, while outpatient facilities, hospitals with up to 50 beds, and primary healthcare units (PHU) registered lower implementation levels.

CHART 7

—

Public healthcare facilities by measures adopted concerning the LGPD (2025)

Total number of public healthcare facilities with Internet access (%)



Public hospitals with more than 50 beds were notable mainly for the publication of privacy policies (40%), carrying out internal awareness campaigns about the LGPD (40%), and implementing response plans for information security incidents related to personal data (32%). SADT showed the highest percentage for facilities that had designated the DPO (31%), and also showed high adoption of privacy policies (33%) and internal awareness campaigns (37%).

In contrast, outpatient facilities, hospitals with up to 50 beds, and PHU show lower percentages for most indicators, especially having designated DPO and implementing incident response plans, which remained below 25% of the units. This suggests that measures related to data governance and preparedness for security incidents are still not widespread in smaller public facilities with lower levels of care complexity.

There were also differences according to the locations of the facilities. For all indicators analyzed, units located in capital cities showed higher percentages than those observed in non-capital cities. The greatest differences were concentrated in the publication of privacy policies (44% in capital cities and 27% in non-capital cities), designation of DPO (24% and 12%, respectively), and the implementation of incident response plans (22% and 14%).

These results show that the adoption of information security and personal data protection practices in healthcare facilities is directly associated with institutional capacity and complexity of care. Consistently, public hospitals with more than 50 beds, SADT, and facilities located in capital cities showed higher levels of institutionalization of information governance practices, likely due to their more complex organizational structures, greater availability of technical resources, more robust infrastructure and specialized teams, and responsibility for larger volumes of data and systems.

The results also suggest that the different dimensions of information security do not progress homogeneously. While there was an increase in the adoption of information security policies and in the provision of training to professionals, measures directly related to the implementation of the LGPD generally remained stable between 2023 and 2025, especially those that require a larger organizational structure, such as designating DPO and implementing incident response plans. This scenario indicates that the strengthening of information security is not always accompanied by the consolidation of formal governance and compliance mechanisms.

Furthermore, the results suggest gradual implementation of these measures. Actions focused on raising awareness among professionals and promoting transparency, such as internal campaigns about the LGPD and the publication of privacy policies, are more widespread among public institutions. Mechanisms that require greater institutional capacity and definition of responsibilities, such as designating DPO and implementing incident response plans, remain less frequent. This pattern is consistent with international models of digital security maturity, which indicate that the consolidation of information governance depends on the integration of institutional policies, training, technical protection mechanisms, and formal risk management and response structures.

Public Basic education schools

In 2026, the National Education Plan (PNE) (Law No. 15.388, of April 14, 2026) was approved, establishing the objectives, goals, and strategies that will guide the country's provision of Basic Education during the 2026–2036 decade. Objective 7 presents specific goals related to school connectivity, media literacy, and the integration of digital information and communication technologies (DICT) into teaching and learning processes and school management activities. Five of the 20 strategies included in this objective refer directly to transparency, security, privacy, and data protection in the provision of digital education in schools, which demonstrates the importance acquired by these themes in educational policies in recent years.

In addition to being equitable, accessible, and of high quality, the interaction of children with digital environments must occur through actions that promote respect for the developmental levels of this population, in order to protect them against direct and indirect risks in the use of digital resources, and to preserve rights such as privacy and the protection of personal data. These measures should guide the adoption of digital services by family members and guardians, caregivers, educators, policymakers, and other actors.

The approval of ECA Digital, which took effect in March 2026 (Decree No. 12.880, of March 18, 2026), made the debate about the LGPD even more significant by broadening the role of multiple sectors of society in its implementation. Individuals and organizations were assigned responsibility for the comprehensive protection of children in digital environments, including consideration of their well-being, the effects of system design on their development, and the creation of opportunities for safe and beneficial use of digital technologies while preventing potential risks (Oliveira et al., 2026).

The implementation of the ECA Digital extends beyond the digital resources and services currently intended for use by children—such as games, educational platforms, and playful applications—and also includes resources that are likely to be used by or of interest to these individuals, such as "Internet applications, computer programs, software, terminal operating systems, Internet application stores, and electronic and similar games connected to the Internet or another communications network" (Law No. 15.211/2025). Therefore, the responsibility for adopting security, privacy, and monitoring measures to prevent risks to the well-being of children is now shared with providers of digital products and services, including platforms and solutions contracted by educational institutions.

Data from the ICT in Education survey on the school community shows how these themes are shared across educational institutions. For example, 39% of managers of public schools (municipal, state, and federal) at the primary and secondary education levels cited concerns about privacy risks and the protection of personal data as some of the main challenges schools face when using digital programs, systems, and platforms for school management. This concern was mentioned by 36% of municipal school managers and 58% of state school managers.

Concerns about the privacy and protection of student data were also cited by 25% of managers as a reason for not adopting digital educational devices, platforms, or other resources. Concerns that the digital resources could lead to data leaks or theft of student information (16%), and that their terms of use did not clearly state how student data would be handled (15%), were among the reasons most frequently cited by public school managers.

The choice not to adopt digital educational devices, platforms, or other resources due to concerns about privacy risks and the protection of personal data was more frequent among managers of private schools (41%) than among managers of public schools—municipal schools (23%) and state schools (27%)—which may be related to the greater autonomy enjoyed by private school teams in selecting and adopting educational resources. According to data collected in the ICT in Education 2024 survey, 40% of directors of studies reported always participating in the selection of digital educational resources used in the schools, a proportion that was 32% among directors of studies of municipal schools, 42% among directors of studies of state schools, and 61% among those working in the private school system. The centralization of decisions regarding

digital services used in teaching, learning, and school management activities in public administration bodies heightens the importance of these school systems' attention to digital rights, such as privacy and the protection of personal data.

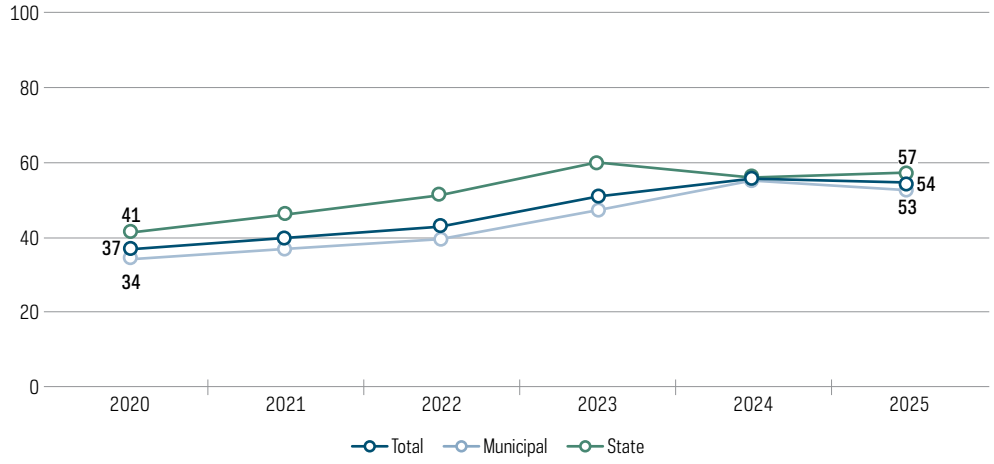
Regarding the presence of data protection and information security policies, in 2020, 37% of all public primary and secondary education schools had them, a proportion that reached 54% in the 2025 edition of the survey. Chart 8 shows the gradual increase in these policies in public schools, although further action is needed to broaden awareness of the topic, since just over half of the school managers stated that their institutions had such guidelines.

CHART 8

–

Public schools with documents that define the information security and data protection policies of the institution (2020–2025)

Total number of public primary and secondary education schools (%)



Regarding support from school networks, 73% of public school managers said they had received guidance on the handling of personal data of students, teachers, and school employees, a proportion that was 71% among municipal schools and 71% among state schools.

The widespread use of emerging technologies, such as predictive or generative AI-based systems in teaching, learning, and school management activities, makes the discussion of privacy and the protection of personal data in educational institutions even more critical, especially in the public education system (Brazilian Ministry of Education [MEC], 2026a). In the 2025 edition of the survey, 14% of public schools located in the South region reported having student facial recognition identification systems, a proportion of 1% among schools located in the North region, 4% in the Southeast region, 5% in the Northeast region, and 7% in the Center-West region. Notably, the use of systems based on biometric data is considered high-risk because of the sensitivity of the data collected, stored, and processed by the enterprises that provide these types of services (InternetLab, 2025; MEC, 2026b).

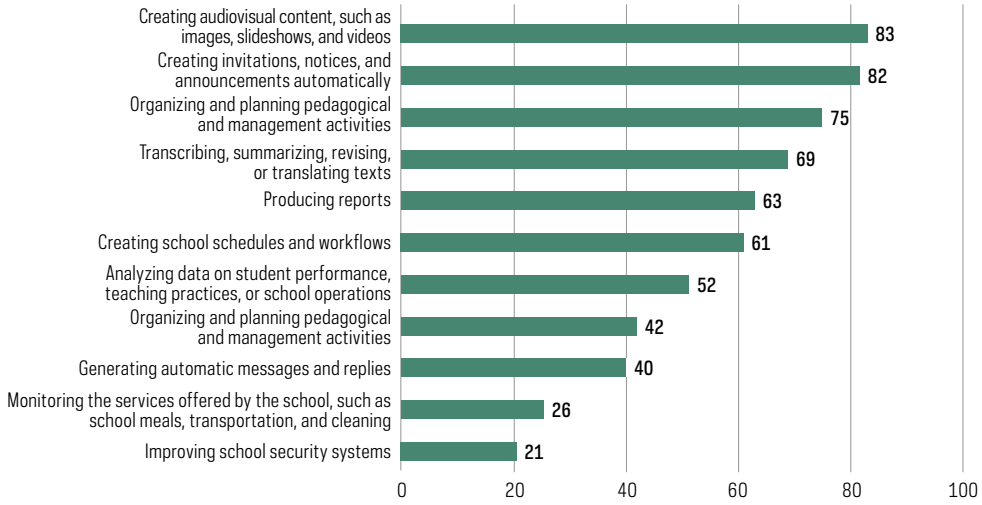
Regarding the use of generative AI in school management activities, 53% of school managers (51% among managers of municipal schools and 58% among those of state schools) mentioned this type of technology. A large proportion of public school managers said they adopted these digital resources in the production of visual or communication content, such as images, slide presentations, videos (83%); invitations, notices, and announcements (82%); and transcription, summarization, revision, and translation of texts (69%). Furthermore, half of the managers stated that they adopted these resources in the analysis of data on student performance, pedagogical practices, and school functioning to support management decisions (52%), activities that could be considered more complex in terms of digital skills and more critical in relation to privacy and data protection (Chart 9).

CHART 9

—

Public school managers, by pedagogical, administrative, or financial management activities carried out through the adoption of AI (2025)

Total number of public primary and secondary education school managers who adopt AI in management activities (%)



Although a large proportion of schools still lacked systematized guidelines on the use of these resources in management activities (22%), a significant proportion of public school managers (60%) mentioned having discussed the use of AI-based systems by students and teachers with educators, school professionals, family members, and legal guardians—57% among municipal school managers and 57% among state school managers.

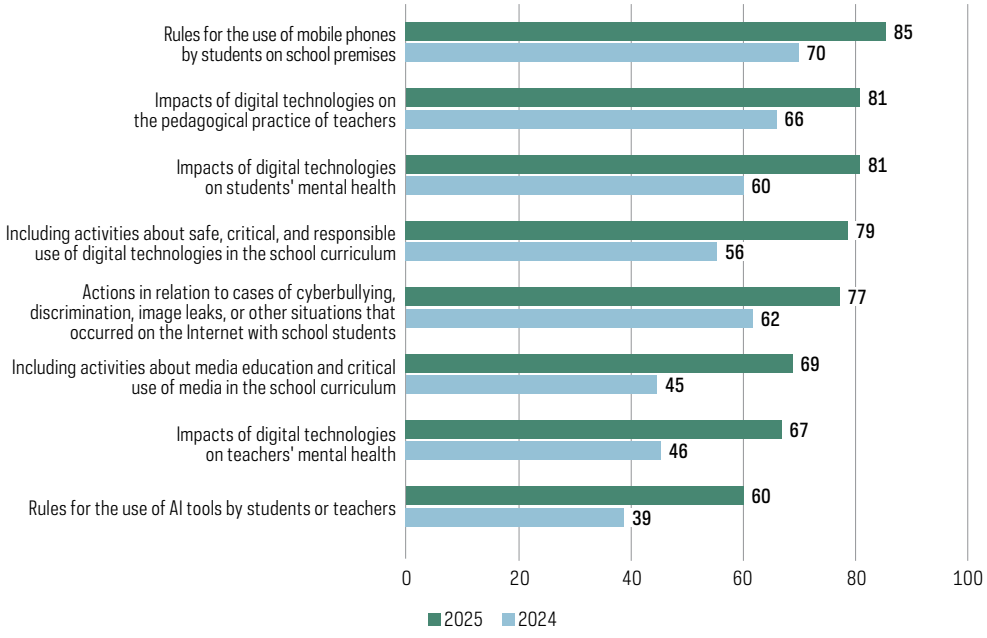
The 2024 and 2025 editions showed differences in the data about holding meetings with teachers and other professionals (in the 12 months before the survey) to discuss the use of digital technologies in schools (from 66% to 87%), and meetings with parents and legal guardians (from 60% to 78%). The possible influence of the discussions surrounding the approval of Law No. 15.100/2025, which restricts the use of mobile phones by students in school environments, and the ECA Digital, can also be seen in the topics raised by school managers in meetings with educators, school professionals, family members, and legal guardians. The 2024 and 2025 editions of the survey saw increases in a number of indicators: Debate about the impacts of digital technologies on students' mental health increased from 60% to 81%; the inclusion of activities related to the safe, critical, and responsible use of digital technologies in the school curriculum increased from 56% to 79%; and the inclusion of activities on media literacy increased from 45% to 69% (Chart 10).

CHART 10

—

Public school managers by topics discussed during meetings carried out with teachers, school professionals, family members, and legal guardians about the use of digital technologies in the institution in the 12 months prior to data collection (2024–2025)

Total number of public primary and secondary education school managers with Internet access (%)



The comparison between the 2023 and 2025 editions of the survey shows a positive increase in the proportion of institutions that held debates or lectures specifically on privacy and personal data protection in the 12 months before the survey, rising from 32% to 46% among public schools, with even greater variation among municipal schools (from 27% to 45%).

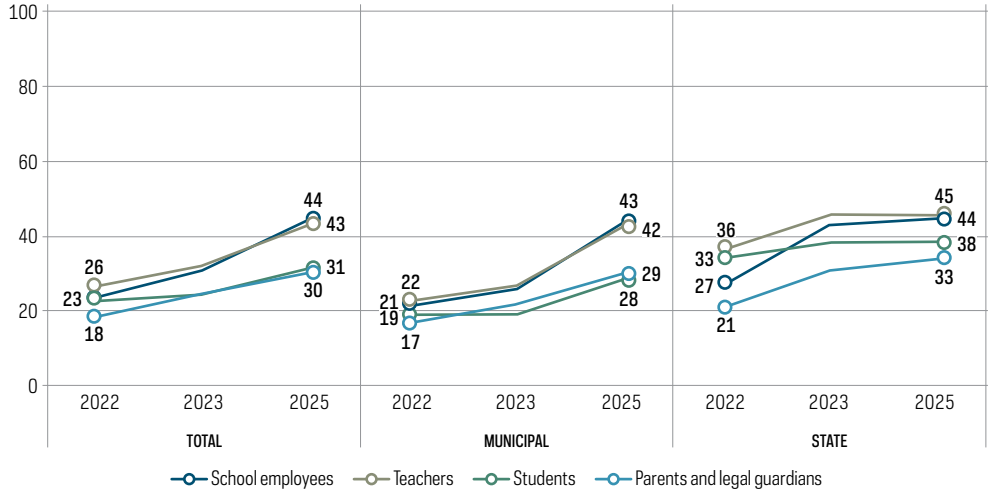
Overall, internal teams, such as teachers (44%) and other professionals working at the institutions (43%), were the main target audience of the initiatives carried out in schools on privacy and data protection. In addition to the higher proportion of managers reporting the offer of debates and lectures for these professionals in the latest edition of the study, the comparison of the data with the 2023 edition also shows an increase, as shown in Chart 11.

CHART 11

–

Public schools by target audiences of discussions or lectures on privacy and data protection held at the school in the 12 months prior to the survey (2022–2025)

Total number of public primary and secondary education schools (%)



Among public schools, 24% offered activities on the topic for students, a proportion that reached a higher level among state schools (33%); even so, only one third of the institutions included students in the initiatives developed in schools. However, students are the primary focus of the policies outlined in the regulations and guiding documents on digital and media education, such as the National Digital Education Policy (Pned) (Law No. 14.533, of January 11, 2023), the Brazilian Media Education Strategy (Ebem) (Secretariat of Social Communication of the Presidency of the Republic [Secom], 2023), the operational guidelines of the National Education Council (CNE) (Resolution CNE/CEB No. 2/2025), the ECA Digital, and the PNE 2026–2036.

The analyzed data reveals progress in the discussion of rights, privacy, and data protection in public schools. During the approval process for Law No. 15.100/2025 and the ECA Digital, public debate focused on the risks children face in digital environments and on the role of schools in the network of protection and psychosocial support for students, which may have helped drive these discussions. However, transforming these debates into effective initiatives will require greater attention from the school community and from public educational policies, especially to ensure that students receive guidance and learning on how to engage with digital environments in an ethical, safe, critical, creative, and responsible manner.

Final considerations: Agenda for public policies

This chapter presents results that allow for an integrated analysis of how public organizations from different areas have structured initiatives focused on privacy and the protection of personal data in a context of increasing digitalization. Although the three analyzed surveys reveal important advances, they also highlight persistent challenges related to the consolidation of these institutional capacities and the reduction of asymmetries between different types of public organizations.

The three editions of the ICT in Government survey that investigated privacy and personal data protection indicators show progress in the creation of institutional structures and the implementation of actions related to the topic in Brazilian public organizations. In 2025, there were significant increases in the adoption of these initiatives, especially among groups that, in previous editions, showed lower proportions, such as state government organizations and smaller local governments.

Despite these results, the scenario of disparities between public organizations that was identified in 2021 and 2023 remains. In general, the analyzed initiatives continue to be more present in federal organizations and the judicial branch, as well as in capitals and larger municipalities. The designation of DPO illustrates these differences. Although required in Article 41 of the LGPD and regulated by Resolution CD/ANPD No. 18/2024, it was reported by only 28% of local governments. Therefore, the findings indicate that the consolidation of governance structures in privacy and data protection still occurs unevenly across levels of government and different sizes of municipalities.

This scenario contrasts with the progress in digital transformation identified in other modules of the ICT in Government 2025 survey. The provision of digital public services is widespread, while the use of AI technologies is growing, especially among federal and state organizations, capital cities, and larger municipalities. Since these initiatives often involve the intensive processing of personal data and may include automated decisions affecting citizens, their expansion must be accompanied by strengthening privacy, data protection, and information security structures.

The results of the ICT in Health 2025 survey show that the expansion of digitalization in healthcare facilities has been accompanied by advances in the institutionalization of information security practices, such as the adoption of formal policies and the provision of training for professionals. However, measures directly related to the implementation of the LGPD remain less widespread and have shown little progress compared to previous editions of the survey, especially among public outpatient facilities and PHU. The results also reveal inequalities in the institutional capacity of the facilities, with a greater presence of information governance practices in hospitals with more than 50 beds, SADT, and facilities located in capital cities.

This scenario occurs within a context of rapid digital transformation in the healthcare sector, marked by the expansion of electronic health records, interoperability between systems, telehealth, and the incorporation of AI applications to support clinical, administrative, and digital security processes. As these technologies expand the processing and sharing of sensitive personal data, it becomes increasingly necessary to strengthen data governance, information security, and the protection of patient privacy. The survey results suggest that consolidating these institutional capabilities is an essential element for promoting the responsible use of health data, strengthening trust in digital health services, and ensuring that technological innovation advances in line with the protection of patients' rights.

Regarding educational institutions, the results of the ICT in Education survey show that the incorporation of digital technologies in public schools continues to advance, supporting both school management and teaching and learning processes. However, the consolidation of practices focused on protecting personal data and information security is still uneven among educational institutions. Although there has been progress in some of the initiatives investigated, significant challenges remain regarding the institutionalization of these practices, especially in a context of increasing use of digital platforms, virtual learning environments, and other systems that process data on students, teachers, and other members of the school community.

Given the expansion of AI applications in education and the growing adoption of digital resources for teaching and learning, these challenges become even more pressing. While these technologies expand the possibilities for supporting pedagogical activities and school management, they also reinforce the need to ensure the protection of personal data, especially that of children. In this context, strengthening data governance, improving information security, and training school teams are essential to ensure that the digital transformation of education occurs ethically, securely, and in alignment with LGPD and ECA Digital.

Taken together, the results of the ICT in Government, ICT in Health, and ICT in Education surveys show that the digital transformation of Brazilian public organizations continues to advance in different ways. The expansion of the supply of digital public services, the advancement in the computerization of healthcare facilities, the incorporation of digital technologies into teaching and learning activities, and the growing use of AI tools point to a process of intensified data use in the Brazilian public sector. This shift expands the possibilities for innovation, efficiency, and improvements in public management; however, it also enhances the challenges related to data governance, information security, and the protection of personal data.

In this context, the consolidation of the LGPD and the implementation of the ECA Digital reinforce the need to strengthen the institutional capacities of public organizations. The results of the three surveys show that, despite advances in initiatives related to information security and the creation of governance structures, these actions are still unevenly distributed among different levels of government, healthcare facilities, and educational institutions.

Finally, the results presented in this chapter reinforce that, beyond the consolidation of regulatory frameworks, the implementation of data protection measures in public organizations depends on the development of institutional capacities. This makes it essential to expand public policies that disseminate best practices, provide continuous training for civil servants and professionals, and strengthen the institutionalization of data governance so that digital transformation occurs in a secure, ethical, and transparent manner, aligned with the protection of citizens' rights.

References

Aith, F., Santana, S., & Dallari, S. G. (2025). A proteção do direito à saúde na era digital: saúde digital, inteligência artificial e direito. *Revista de Direito Sanitário, 25*, e0025. https://doi.org/10.11606/issn.2316-9044.rdisan.2025.240814

Ansar, S., Clark, J. M., & Wolff, J. M. (2026). *ID4D Global Dataset 2025: Trends in identification for development.* World Bank Group. http://documents.worldbank.org/curated/en/099061526195037307

Brazilian General Data Protection Law. Law No. 13.709, of August 14, 2018. (2018). Brazilian General Data Protection Law (LGPD). http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

Brazilian Internet Steering Committee. (2024). *Survey on the use of information and communication technologies in Brazilian healthcare facilities: ICT in Health 2023.* https://cetic.br/en/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-nos-estabelecimentos-de-saude-brasileiros-tic-saude-2023/

Brazilian Internet Steering Committee. (2025). *Survey on the use of information and communication technologies in Brazilian schools: ICT in Education 2024.* https://cetic.br/en/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-nas-escolas-brasileiras-tic-educacao-2024/

Brazilian Internet Steering Committee. (2026a). *Survey on the use of information and communication technologies in Brazilian schools: ICT in Education 2025.* https://cetic.br/en/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-nas-escolas-brasileiras-tic-educacao-2025/

Brazilian Internet Steering Committee. (2026b). *Survey on the use of information and communication technologies in the Brazilian public sector: ICT in Government 2025.* https://cetic.br/en/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-no-setor-publico-brasileiro-tic-governo-eletronico-2025/

Brazilian Internet Steering Committee. (2026c). *Survey on the use of information and communication technologies in Brazilian healthcare facilities: ICT in Health 2025.* https://cetic.br/en/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-nos-estabelecimentos-de-saude-brasileiros-tic-saude-2025/

Brazilian Ministry of Education. (2026a). *Inteligência Artificial na Educação Básica: documento orientador sobre caminhos curriculares e práticas éticas de uso de IA nas escolas*. https://www.gov.br/mec/pt-br/escolas-conectadas/arquivos/ia-basica.pdf

Brazilian Ministry of Education. (2026b). *Referencial para desenvolvimento e uso responsáveis de inteligência artificial na educação*. https://www.gov.br/mec/pt-br/referencial-de-ia-na-educacao/referencial-ia-na-educacao

Brazilian Ministry of Management and Innovation in Public Services. (n.d.). *Estratégia Nacional de Governo Digital*. https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/estrategianacional/

Brazilian Ministry of Management and Innovation in Public Services. (2024). *Guia de elaboração de Programa de Governança em Privacidade* (Versão 2.3). https://tce.pb.gov.br/wp-content/uploads/2025/09/11guia_programa_governanca_privacidade.pdf

Brazilian Ministry of Science, Technology and Innovation & Center for Management and Strategic Studies. (2025). *IA para o bem de todos: Plano Brasileiro de Inteligência Artificial*. https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/plano-brasileiro-de-inteligencia-artificial-pbia-_vf.pdf

Decree No. 12.622, of September 17, 2025. (2025). Regulates Law No. 15.211, of September 17, 2025, to designate the National Data Protection Agency as an autonomous administrative authority for the protection of children and adolescents in digital environments, and to establish competencies for the fulfillment of judicial blocking orders. https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/d12622.htm

Decree No. 12.880, of March 18, 2026. (2026). Regulates Law No. 15.211, of September 17, 2025, which provides for the protection of children and adolescents in digital environments and establishes the National Policy for the Promotion and Protection of the Rights of Children and Adolescents in the Digital Environment. https://www.in.gov.br/en/web/dou/-/decreto-n-12.880-de-18-de-marco-de-2026-693683613

Digital Statute of the Child and Adolescent. Law No. 15.211, of September 17, 2025. (2025). Provides for the protection of children and adolescents in digital environments (Digital Statute of the Child and Adolescent). https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/L15211.htm

InternetLab. (2025). *Tecnologias de vigilância e inteligência artificial na educação: promessas de modernização, realidades de opacidade*. https://internetlab.org.br/pt/biblioteca/relatorio-completo-tecnologias-de-vigilancia-e-inteligencia-artificial-na-educacao-promessas-de-modernizacao-realidades-de-opacidade/

Law No. 14.129, of March 29, 2021. (2021). Establishes principles, rules, and instruments for Digital Government and for increasing public efficiency, and amends Law No. 7.116 of August 29, 1983, Law No. 12.527 of November 18, 2011 (Access to Information Law), Law No. 12.682 of July 9, 2012, and Law No. 13.460 of June 26, 2017. https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14129.htm

Law No. 15.100, of January 13, 2025. (2025). Regulates the use of personal portable electronic devices by students in public and private basic education facilities. https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/l15100.htm

Law No. 15.388, of April 14, 2026. (2026). Approves the National Education Plan (PNE). https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/lei/l15388.htm

Maia, G. (March 6, 2026). *Zero-click government: Why it's time to rethink when and how the state acts*. World Economic Forum. https://www.weforum.org/stories/all/digital-government-ai-zero-click/

National Data Protection Agency. (2023). *Guia orientativo: tratamento de dados pessoais pelo Poder Público*. https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_lgpd_final.pdf

National Data Protection Agency. (2024). *Glossário de proteção de dados pessoais e privacidade*. https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/glossario-anpd-protecao-de-dados-pessoais-e-privacidade.pdf

National Data Protection Agency. (2025). *Nota Técnica n. 12/2025/CON1/CGN/ANPD*. https://www.gov.br/anpd/pt-br/acesso-a-informacao/participacao-social/outras-acoes/documentos/ts-06-2024-nt-12-2025-consolidacao-das-contribuicoes.pdf/@@display-file/file

National Digital Education Policy. Law No. 14.533, of January 11, 2023. (2023). Establishes the National Digital Education Policy and amends Law No. 9.394, of December 20, 1996 (National Education Guidelines and Bases Law), Law No. 9.448 of March 14, 1997, Law No. 10.260 of July 12, 2001, and Law No. 10.753 of October 30, 2003. https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/lei/l14533.htm

Oliveira, D. T. N., Machado, D. C., Barbosa, J. D., & Carvalho, L. B. (2026). *Mecanismos confiáveis de aferição de idade: orientações preliminares*. http://www.gov.br/anpd/pt-br/assuntos/eca-digital/mecanismos-confiaveis-de-afericao-de-idade-orientacoes-preliminares.pdf

Organisation for Economic Co-operation and Development. (2022). *Health data governance for the digital age: Implementing the OECD recommendation on health data governance*. OECD Publishing. https://doi.org/10.1787/68b60796-en

Organisation for Economic Co-operation and Development. (2026). *Digital Government Outlook 2026: From foundations to transformational impact*. OECD Publishing. https://doi.org/10.1787/0496b2bc-en

Pan American Health Organization. (2021). *Eight guiding principles of digital transformation of the health sector. A call to Pan American action* (OPAS/EIH/IS/21-0004). https://iris.paho.org/handle/10665.2/54669

Resolution CD/ANPD No. 18 of July 16, 2024. (2024). Approves the Regulation on the role of the data protection officer. https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-18-de-16-de-julho-de-2024-572632074

Resolution CD/ANPD No. 31, of December 22, 2025. (2025). Amends the Regulatory Agenda for the biennium 2025-2026. https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-31-de-22-de-dezembro-de-2025-677950080

Resolution CNE/CEB No. 2, of March 21, 2025. (2025). Establishes the National Operational Guidelines on the use of digital devices in school spaces and curricular integration of digital and media education. National Education Council, Basic Education Chamber. https://www.gov.br/mec/pt-br/cne/2025/marco/rceb002_25.pdf

Resolution No. 281, of December 12, 2023. (2023). Establishes the National Policy for the Protection of Personal Data and the National System for the Protection of Personal Data in the Public Prosecutor's Office and provides other measures. National Council of the Public Prosecutor's Office. https://www.cnmp.mp.br/portal/images/CALJ/resolucoes/Resoluo-281-de-2023.pdf

Secretariat of Social Communication of the Presidency of the Republic. (2023). *Estratégia Brasileira de Educação Midiática.* https://www.gov.br/secom/pt-br/arquivos/2023_secom-spdigi_estrategia-brasileira-de-educacao-midiatica.pdf

United Nations Department of Economic and Social Affairs. (2024). *E-Government Survey 2024: Accelerating digital transformation for sustainable development: With the addendum on Artificial Intelligence.* https://publicadministration.un.org/egovkb/en-us/reports/un-e-government-survey-2024

United Nations Educational, Scientific and Cultural Organization. (2022). *Artificial intelligence and digital transformation: competencies for civil servants.* https://unesdoc.unesco.org/ark:/48223/pf0000383325

World Health Organization. (2021). *Global strategy on digital health 2020-2025.* https://www.who.int/publications/i/item/9789240020924

List of Abbreviations

AI – Artificial Intelligence

ANPD – National Data Protection Agency

CAPI – computer-assisted personal interviewing

CATI – computer-assisted telephone interviewing

CDC – Brazilian Consumer Defense Code

Cempre – Central Register of Enterprises

Ceptro.br – Center of Study and Research in Network Technology and Operations

CERT.br – Brazilian National Computer Emergency Response Team

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

Ceweb.br – Web Technologies Study Center

CGEE – Center for Management and Strategic Studies

CGI.br – Brazilian Internet Steering Committee

CNAE – National Classification of Economic Activities

CNE – National Education Council

CNES – National Registry of Healthcare Facilities

CNMP – National Council of the Public Prosecutor's Office

Continuous Pnad – Continuous National Household Sample Survey

DICT - digital information and communication technologies

Ebem – Brazilian Media Education Strategy

ECA – Statute of the Child and Adolescent

ECA Digital – Digital Statute of the Child and Adolescent

ENGD – National Digital Government Strategy

Eurostat – Statistical Office of the European Union

FBSP – Brazilian Forum on Public Security

IBGE – Brazilian Institute of Geography and Statistics

ICT – information and communication technologies

IDB – Inter-American Development Bank

Interpol – International Criminal Police Organization

IoT – Internet of Things

IT – information technology

ITU – International Telecommunication Union

IX.br – Brazil Internet Exchange

IXP – Internet Exchange Point

Lacsi – Latin American and Caribbean Victimization Survey Initiative

LGPD – Brazilian General Data Protection Law

MCTI – Brazilian Ministry of Science, Technology and Innovation

MEC – Brazilian Ministry of Education

Mercosur – Southern Common Market

MGI – Brazilian Ministry of Management and Innovation in Public Services

MJSP – Brazilian Ministry of Justice and Public Security

MS – Brazilian Ministry of Health

NIC.br – Brazilian Network Information Center

OBIA – Brazilian Artificial Intelligence Observatory

OECD – Organisation for Economic Co-operation and Development

PAHO – Pan American Health Organization

PBIA – Brazilian Artificial Intelligence Plan

PHU – primary healthcare units

PNE – National Education Plan

Pned – National Digital Education Policy

SADT – diagnosis and therapy services

Secom – Secretariat of Social Communication of the Presidency of the Republic

SMS – Short Message Service

UN – United Nations

UN DESA – United Nations Department of Economic and Social Affairs

UNCTAD – UN Trade and Development

UNESCO – United Nations Educational, Scientific and Cultural Organization

UNODC – United Nations Office on Drugs and Crime

WHO – World Health Organization



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