cetic.br

PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Perspectivas de indivíduos, empresas e organizações públicas no Brasil

2021

PRIVACY AND PERSONAL DATA PROTECTION

Perspectives of individuals, enterprises and public organizations in Brazil

cgi.br
Comitê Gestor da Internet no Brasil

Núcleo de Informação e Coordenação do Ponto BR
Brazilian Network Information Center

PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Perspectivas de indivíduos, empresas e organizações públicas no Brasil

2021

PRIVACY AND PERSONAL DATA PROTECTION

Perspectives of individuals, enterprises and public organizations in Brazil

Comitê Gestor da Internet no Brasil
Brazilian Internet Steering Committee

https://www.cgi.br

São Paulo
2022

Núcleo de Informação e Coordenação do Ponto BR - NIC.br
Brazilian Network Information Center - NIC.br

Diretor Presidente / CEO : Demi Getschko

Diretor Administrativo / CFO : Ricardo Narchi

Diretor de Serviços e Tecnologia / CTO : Frederico Neves

Diretor de Projetos Especiais e de Desenvolvimento / Director of Special Projects and Development : Milton Kaoru Kashiwakura

Diretor de Assessoria às Atividades do CGI.br / Chief Advisory Officer to CGI.br : Hartmut Richard Glaser

Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação – Cetic.br
Regional Center for Studies on the Development of the Information Society – Cetic.br

Coordenação Executiva e Editorial / Executive and Editorial Coordination: Alexandre F. Barbosa

Consultor técnico / Technical consultant: Danilo Doneda

Coordenação de Conformidade à LGPD do NIC.br / Data Protection Officer and Compliance Coordination of NIC.br : Karen Borges

Coordenação de Projetos de Pesquisa / Survey Project Coordination: Fabio Senne (Coordenador / Coordinator), Ana Laura Martínez, Daniela Costa, Fabio Storino, Leonardo Melo Lins, Luciana Portilho, Luísa Adib Dino, Luiza Carvalho e / and Manuella Maia Ribeiro

Coordenação de Métodos Quantitativos e Estatística / Statistics and Quantitative Methods Coordination: Marcelo Pitta (Coordenador / Coordinator), Camila dos Reis Lima, Mayra Pizzott Rodrigues dos Santos, Thiago de Oliveira Meireles e / and Winston Oyadomari

Coordenação de Métodos Qualitativos e Estudos Setoriais / Sectoral Studies and Qualitative Methods Coordination: Tatiana Jereissati (Coordenadora / Coordinator), Javiera F. Medina Macaya e / and Luciana Piazzon Barbosa Lima

Coordenação de Gestão de Processos e Qualidade / Process and Quality Management Coordination: Nádilla Tsuruda (Coordenadora / Coordinator), Maísa Marques Cunha, Rodrigo Gabriades Sukarie e / and Vitor Gabriel Gonçalves Gouveia

Gestão das pesquisas em campo / Field Management: Ipec Inteligência em Pesquisa e Consultoria Ltda.: Helio Gastaldi, Rosi Rosendo, Alexandre Carvalho, Ana Cardoso, Guilherme Militão, Leticia Passos, Ligia Rubega, Regiane Sousa e / and Taís Magalhães (TIC Educação 2020, TIC Empresas 2021, TIC Governo Eletrônico 2021 e TIC Saúde 2021); Quaest Pesquisa e Consultoria : Felipe Nunes, Guilherme Russo, Jonatas Varella e / and Renata Salvo (Painel TIC)

Apoio à edição / Editing support team: Comunicação NIC.br: Carolina Carvalho e / and Renato Soares

Preparação de texto e revisão em português / Proofreading and revision in Portuguese: Tecendo Textos: Ana Carolina Nitto, Fabiana Vieira e / and Naira Gomes

Tradução para o inglês / Translation into English: Prioridade Consultoria Ltda.: Lorna Simons, Luana Guedes, Luísa Caliri e / and Maya Bellomo Johnson

Projeto gráfico / Graphic Design: Pilar Velloso (miolo / text block), Comunicação NIC.br: Klezer Kenji Uehara (capa / cover)

Editoração / Publishing: Grappa Marketing Editorial (www.grappa.com.br)

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

Privacidade e proteção de dados pessoais 2021 [livro eletrônico] : perspectivas de indivíduos, empresas e organizações públicas no Brasil = Privacy and personal data protection 2021 : 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, 2022.
PDF
Edição bilíngue : português / inglês
Vários colaboradores.
Vários tradutores.
Bibliografia.
ISBN 978-65-86949-70-4
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. II. Título: Privacy and personal data protection 2021 : perspectives of individuals, enterprises and public organizations in Brazil.

21-118282 CDD-004.6072081

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

Comitê Gestor da Internet no Brasil – CGI.br
Brazilian Internet Steering Committee – CGI.br
(em Agosto de 2022/ in August, 2022)

Coordenador / Coordinator
José Gustavo Sampaio Gontijo

Conselheiros / Counselors
Beatriz Costa Barbosa
Carlos Manuel Baigorri
Demi Getschko
Domingos Sávio Mota
Evaldo Ferreira Vilela
Fernando André Coelho Mitkiewicz
Jackline de Souza Conca
Jeferson Denis Cruz de Medeiros
José Alexandre Novaes Bicalho
Henrique Faulhaber Barbosa
Laura Conde Tresca
Marcos Dantas Loureiro
Maximiliano Salvadori Martinhão
Nivaldo Cleto
Orlando Oliveira dos Santos
Patrícia Ellen da Silva
Percival Henriques de Souza Neto
Rafael de Almeida Evangelista
Rosauro Leandro Baretta
Tanara Lauschner

Secretário executivo / Executive Secretary
Hartmut Richard Glaser

Agradecimentos

A pesquisa Privacidade e Proteção de Dados Pessoais 2021 contou com o apoio de um conjunto de especialistas, renomados por sua competência, que contribuíram de maneira significativa para a apuração dos resultados aqui apresentados. Essa colaboração é fundamental para a identificação de novos campos de pesquisa, o aperfeiçoamento dos procedimentos metodológicos e a produção de dados confiáveis. Cabe destacar que a importância das novas tecnologias para a sociedade brasileira e a relevância dos indicadores produzidos pelo Comitê Gestor da Internet no Brasil (CGI.br) para as políticas públicas e pesquisas acadêmicas serviram como motivação para que os especialistas participassem voluntariamente desse esforço coletivo. O Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br) agradece o apoio aos seguintes especialistas:

Angelini Neves Consultoria e Treinamento (ANCT)
Kelli Angelini

Associação Brasileira das Empresas de Software (ABES)
Thomaz Corte Real

Associação Brasileira das Empresas de Tecnologia da Informação e Comunicação (Brasscom)
Ana Paula Bialer

Autoridade Nacional de Proteção de Dados (ANPD)
Davi Teofilo Nunes Oliveira, Isabela Maiolino, Jeferson Barbosa, Lucas Borges, Marcelo Guedes e Miriam Wimmer

Comissão Especial de Privacidade e Proteção de Dados da OAB/SP
Analluza Bolivar Dallar

Comitê Gestor da Internet no Brasil (CGI.br)
Bia Barbosa

Data Privacy Brasil
Maria Cecilia Oliveira Gomes e Renato Leite Monteiro

EducaDigital
Priscila Gonsales

Fórum Empresarial da LGPD
Andriei Gutierrez

Fundação Getulio Vargas (FGV)
Erica Bakonyi, Luca Belli, Nicolo Zingales e Yasmin Mendonça

Hospital Israelita Albert Einstein
Rogéria Leoni Cruz

Instituto Alana
Isabella Henriques e Thais Rugolo

Instituto Brasileiro de Defesa do Consumidor (Idec)
Camila Leite Contri e Juliana Oms

Instituto Brasileiro de Direito e Ética Empresarial (IBDEE)
Adriana Esper

Instituto de Referência em Internet e Sociedade (Iris)
Gustavo Rodrigues, Lahis Kurtz e Luiza Brandão

InternetLab
Barbara Simão, Francisco Cruz e Mariana Valente

Itaú
Annete Pereira e Ticiane Rocha Santos de Andrade

KR Advogados
Karolyne Utomi

Leonardi Advogados
Marcel Leonardi e Nayara Juvenal

Núcleo de Informação e Coordenação do Ponto BR (NIC.br)
Cristine Hoepers, Isadora Peixoto, Ramon Silva Costa e Raquel Gatto

Open Knowledge Brasil
Fernanda Campagnucci

Opice Blum
Rony Vainzof

Pontifícia Universidade Católica do Rio Grande do Sul (PUC-RS)
Gabrielle Bezerra Sales Sarlet

Prado Vidigal
Luis Fernando Prado e Paulo Vidigal

Rede Nacional de Ensino e Pesquisa (RNP)
Yuri Ferreira

Sociedade Brasileira de Informática em Saúde (SBIS)
Luis Gustavo Kiatake

Universidade de Brasília (UnB)
Tel Amiel

Universidade Federal do Rio Grande do Sul (UFRGS)
Fabiano Menke

Acknowledgements

The Privacy and Personal Data Protection 2021 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 and Thais Rugolo

Albert Einstein Hospital
Rogéria Leoni Cruz

Angelini Neves Consulting and Training (ANCT)
Kelli Angelini

Brazilian Association of Information and Communication Technologies Companies (Brasscom)
Ana Paula Bialer

Brazilian Association of Software Companies (ABES)
Thomaz Corte Real

Brazilian Health Informatics Society (SBIS)
Luis Gustavo Kiatake

Brazilian Institute of Business Ethics and Law (IBDEE)
Adriana Esper

Brazilian Institute of Consumer Protection (Idec)
Camila Leite Contri and Juliana Oms

Brazilian Internet Steering Committee (CGI.br)
Bia Barbosa

Brazilian Network Information Center (NIC.br)
Cristine Hoepers, Isadora Peixoto, Ramon Silva Costa and Raquel Gatto

Data Privacy Brazil
Maria Cecilia Oliveira Gomes and Renato Leite Monteiro

EducaDigital
Priscila Gonsales

Federal University of Rio Grande do Sul (UFRGS)
Fabiano Menke

Getulio Vargas Foudation (FGV)
Erica Bakonyi, Luca Belli, Nicolo Zingales and Yasmin Mendonça

Institute for Research on Internet and Society (Iris)
Gustavo Rodrigues, Lahis Kurtz and Luiza Brandão

InternetLab
Barbara Simão, Francisco Cruz and Mariana Valente

Itaú
Annete Pereira and Ticiane Rocha Santos de Andrade

KR Law Firm
Karolyne Utomi

Leonardi Law Firm
Marcel Leonardi and Nayara Juvenal

LGPD Business Forum
Andriei Gutierrez

National Data Protection Authority (ANPD)
Davi Teofilo Nunes Oliveira, Isabela Maiolino, Jeferson Barbosa, Lucas Borges, Marcelo Guedes and Miriam Wimmer

National Education and Research Network (RNP)
Yuri Ferreira

Special Commission for Privacy and Data Protection of the OAB/SP
Analluza Bolivar Dallari

Open Knowledge Brazil
Fernanda Campagnucci

Opice Blum
Rony Vainzof

Pontifical Catholic University of Rio Grande do Sul (PUC-RS)
Gabrielle Bezerra Sales Sarlet

Prado Vidigal
Luis Fernando Prado and Paulo Vidigal

University of Brasília (UnB)
Tel Amiel

Sumário / Contents

Lista de gráficos / List of charts

Lista de tabelas / List of tables

Lista de *box* / List of boxes

Prefácio

Em agosto de 2018, o Brasil entrou para o seleto grupo de países que promulgaram uma legislação nacional relacionada à privacidade e proteção de dados. A Lei Geral de Proteção de Dados Pessoais (LGPD) instituiu regras e diretrizes para o tratamento de dados pessoais, incluindo aquele realizado por meios digitais. Já em fevereiro de 2022, o direito à proteção de dados pessoais foi incluído na Constituição Federal no rol de direitos e garantias fundamentais ao cidadão.

O novo marco regulatório e legal tem pautado agentes públicos e privados quanto ao tratamento e uso de dados pessoais. O tema é ainda mais relevante no contexto hodierno, em que há ampla adoção das tecnologias digitais na interação entre indivíduos e organizações. O processamento e a análise de uma quantidade cada vez maior de dados é a realidade.

Ao longo dos últimos anos, a promoção da privacidade e da proteção de dados pessoais, especialmente no que se refere à Internet, tem feito parte do escopo de ação do Núcleo de Informação e Coordenação do Ponto BR (NIC.br) e do Comitê Gestor da Internet no Brasil (CGI.br). Em 2009, após o CGI.br divulgar os dez princípios para a governança e uso da Internet no Brasil[1] – sendo "Liberdade, privacidade e direitos humanos" o primeiro deles –, a proteção à privacidade dos indivíduos tornou-se um dos aspectos fundamentais para balizar o uso da rede. No ano seguinte, em 2010, o CGI.br e o NIC.br passaram a realizar anualmente o Seminário de Proteção à Privacidade e aos Dados Pessoais[2], que, ao longo dos anos, colocou em pauta assuntos-chave que contribuíram para a construção da LGPD e de outros instrumentos regulatórios ligados ao tema, sendo reconhecido como um dos principais eventos da área no país. Em 2022, o seminário chega à sua 13ª edição como um espaço de debate multissetorial, com representantes dos setores governamental, privado, terceiro setor e comunidade científica e tecnológica.

[1] Para mais informações, acesse: https://principios.cgi.br/

[2] Para mais informações, acesse: https://seminarioprivacidade.cgi.br/

No âmbito da LGPD, além de notas públicas relacionadas ao tema, o CGI.br tem assento no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD), órgão consultivo da Autoridade Nacional de Proteção de Dados (ANPD). Em julho de 2021, com o propósito de fortalecer a cultura de proteção de dados no país, o NIC.br e a ANPD assinaram um acordo de cooperação. A primeira ação dessa parceria resultou no lançamento de dois fascículos da Cartilha de Segurança para Internet[3] relacionados aos temas de proteção de dados e vazamento de dados.

Em setembro de 2020, com a entrada em vigor da LGPD, tornou-se cada vez mais central compreender como organizações públicas e privadas realizam o tratamento de dados pessoais e como este tema avança nos diversos setores da sociedade. Com a intenção de contribuir na busca de evidências sobre o estado da implementação da LGPD, esta publicação reúne indicadores coletados por meio de estudos do Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), departamento do NIC.br responsável pela produção de estatísticas e estudos qualitativos relacionados ao uso de tecnologias digitais no Brasil.

O presente estudo conta com o apoio institucional da ANPD e apresenta indicadores inéditos coletados pelas pesquisas do Cetic.br|NIC.br sobre o tema da privacidade e proteção de dados pessoais em diferentes setores. O diagnóstico apresentado inclui, a partir de resultados de uma pesquisa realizada *online* com usuários de Internet, a percepção dos cidadãos sobre o tema. A publicação também aborda os principais desafios para adequação à Lei, investigando práticas implementadas para o tratamento de dados pessoais em pequenas, médias e grandes empresas. Finalmente, observa a adoção da LGPD entre as organizações públicas com base em dados coletados em escolas, estabelecimentos de saúde, órgãos públicos federais e estaduais e prefeituras.

O Cetic.br|NIC.br nos brinda, portanto, com dados relevantes e de qualidade sobre o tema, tanto para a sociedade quanto para as autoridades responsáveis por zelar pela proteção de dados no país. Assim, espera-se contribuir para a ampliação do entendimento a respeito da implementação da LGPD e de seus efeitos sobre a cultura de proteção à privacidade e aos dados pessoais no Brasil.

Boa leitura!

Demi Getschko
Núcleo de Informação e Coordenação do Ponto BR – NIC.br

[3] Para mais informações, acesse: https://cartilha.cert.br/

Apresentação

Qual é o nível de conformidade das empresas brasileiras à Lei Geral de Proteção de Dados Pessoais (LGPD)[1]? Onde estão os principais gargalos? Qual é a percepção dos cidadãos? Tais perguntas, aparentemente singelas, revestem-se de grande importância. Afinal, não são triviais os desafios associados à implementação de uma lei dotada de tamanha transversalidade, repleta de conceitos ainda pouco compreendidos, que requer de órgãos públicos e de agentes privados significativas mudanças organizacionais. Buscar tais respostas é uma empreitada de tremenda importância: afinal, o que se pretende com a nova legislação é a promoção de uma mudança cultural, e conhecer a realidade sobre a qual uma lei incide é o primeiro passo para promover a sua efetividade.

A criação da Autoridade Nacional de Proteção de Dados (ANPD), em novembro de 2020, nos termos previstos pela LGPD, reflete a importância atribuída pelo legislador ao estabelecimento de um aparato institucional dedicado à proteção dos dados pessoais dos cidadãos brasileiros, tendo em seu centro um órgão dotado de competências normativas, fiscalizadoras e sancionadoras. Por outro lado, o reconhecimento da complexidade do ambiente brasileiro tem motivado a ANPD, desde a sua criação, a buscar parcerias institucionais com órgãos e entidades com competências relacionadas à promoção da proteção de dados pessoais no Brasil.

É nesse contexto que se insere o acordo de cooperação celebrado entre a ANPD e o Núcleo de Informação e Coordenação do Ponto BR (NIC.br) em julho de 2021. Criado para implementar as decisões tomadas pelo Comitê Gestor da Internet no Brasil (CGI.br), o NIC.br é nacional e internacionalmente conhecido pelas ações em prol do desenvolvimento da Internet, com notória *expertise* no tratamento e na resposta a incidentes de segurança, assim como na produção de estudos, indicadores, estatísticas e informações estratégicas sobre a adoção das tecnologias de informação e comunicação (TIC) no país.

[1] Lei n. 13.709, de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

O acordo entre a ANPD e o NIC.br compreende ações como o intercâmbio de informações; a realização de ações de interesse comum no que diz respeito à proteção de dados pessoais e à segurança da informação; a mútua cooperação técnica científica voltada para o desenvolvimento de ações e produção de materiais de capacitação e conscientização sobre o tema; e a produção conjunta e coordenada de estudos, análises e pesquisas sobre proteção de dados pessoais, segurança da informação, privacidade nas redes e tecnologia. Dentre os resultados concretos já alcançados a partir da parceria entre ANPD e NIC.br, é possível mencionar o lançamento, em julho de 2021, de dois fascículos da Cartilha de Segurança para Internet, cuja divulgação contribui para a promoção de uma cultura de proteção de dados entre a população, ampliando o conhecimento sobre o tema para além dos especialistas na área.

A presente publicação pode também ser considerada uma das positivas ações decorrentes da parceria entre a ANPD e o NIC.br. De fato, a realização de pesquisas representativas sobre as práticas de proteção de dados pessoais e privacidade entre empresas e organizações públicas (como escolas e estabelecimentos de saúde) oferece subsídios estratégicos para a atuação da ANPD. Compreender as percepções da população brasileira sobre sua privacidade é um elemento central para desenhar iniciativas que colaborem para o maior conhecimento das normas e das políticas públicas sobre proteção de dados pessoais, bem como das medidas de segurança.

Ao estabelecer uma linha de base para compreender as percepções de indivíduos e organizações quanto ao tema da proteção de dados pessoais e privacidade, a presente publicação permite que os avanços futuros sejam monitorados. Além disso, fortalece o desenho de políticas públicas baseadas em evidências, permitindo que o país avance mais rapidamente nessa agenda.

Assim, expressando minha alegria pelo convite para apresentar esta obra, desde já convido todos a nela mergulharem e desejo uma proveitosa leitura!

Miriam Wimmer
Autoridade Nacional de Proteção de Dados

Introdução

Desde a promulgação das primeiras legislações específicas sobre proteção de dados pessoais, na década de 1970, o estabelecimento de marco legal contendo um regime regulatório sobre informações pessoais passou a ser um dos eixos primordiais em torno do qual se articulavam e eram concebidos os instrumentos responsáveis por definir o regime jurídico da informação. Desde então, em todo o mundo, tais ferramentas têm se tornado cada vez mais relevantes em diversos processos econômicos e sociais.

O arcabouço regulatório da proteção de dados é, portanto, resultado de uma evolução de mais de cinco décadas na criação de ferramentas moldadas para o desafio de regular o que parecia virtualmente incontrolável em um determinado paradigma tecnológico: o livre fluxo de dados. À medida que alguns efeitos desse fluxo passaram a proporcionar consequências consideradas nocivas, a demanda por regulação cresceu e justificou a presença hoje majoritária na comunidade internacional da opção por legislar sobre proteção de dados pessoais. De acordo com levantamentos internacionais, há mais de 140 países que atualmente contam com legislações gerais sobre proteção de dados pessoais.[1]

Percebe-se que, nas últimas décadas, a atenção dirigida à regulação da informação pessoal tem atendido a demandas cada vez mais amplas, seja no sentido geográfico, seja entre os diversos atores sociais, apresentando desdobramentos que vão além da proteção de dados pessoais. Nesse contexto, emergem intensos debates acerca da iminência da criação ou ampliação da regulação em setores como Inteligência Artificial, uso e governança de dados (não pessoais), aspectos concorrenciais da economia digital, regulação de plataformas e tantos outros. Isso permite que consideremos a proteção de dados não somente por seus aspectos intrínsecos, mas como uma porta de entrada para as questões da regulação da informação como um dos aspectos centrais do direito e das normas no nosso tempo.

A implementação de um marco regulatório de proteção de dados pessoais no Brasil vem se acelerando nos últimos anos. Isso inclui desde o envio do projeto de lei PL 5276/2016 pelo Poder Executivo ao parlamento e a sua aprovação por unanimidade nas duas casas legislativas, em 2018, até a entrada em vigor da parte mais substancial

[1] Greenleaf, G. (2021). Global Data Privacy Laws 2021: Despite COVID delays, 145 laws show GDPR dominance. *Privacy Laws & Business International Report*, *169*(1), 3-5.

da Lei Geral de Proteção de Dados Pessoais (LGPD), no ano de 2020. Os debates em torno do tema foram constantemente ganhando relevância, à medida que refletiam uma crescente demanda pela regulamentação do uso da informação, seja para a garantia e promoção de direitos, seja para a segurança na sua utilização.

O processo de formação da LGPD antecede o seu percurso legislativo. Remonta ao debate público lançado pelo Ministério da Justiça (MJ), em 30 de novembro de 2010, por meio de um texto-base a partir do qual foi elaborada e desenvolvida a proposta levada ao parlamento pelo Poder Executivo em 2016. A discussão sobre o tema também se estendeu para o âmbito do Mercado Comum do Sul (Mercosul), entre os anos de 2014 e 2020[2]. Nesse período, contudo, boa parte da discussão ocorreu sem um envolvimento mais amplo de todas as parcelas da sociedade, estando restrita a determinados setores e atores especializados – em contraste, inclusive, com um debate internacional que, há décadas, já se demonstrava bastante abrangente.

No Brasil, seguimos uma dinâmica própria, porém amplamente reconhecida como de grande relevância em relação à regulação de aplicações de tecnologia. Podemos mencionar, por exemplo, a trajetória de diplomas normativos como o Código de Defesa do Consumidor, capaz de se amoldar às dinâmicas do comércio eletrônico; a experiência pioneira do Marco Civil da Internet – que inovou quanto à modalidade de debate público e construção a partir dos *Princípios para a Governança e Uso da Internet* do Comitê Gestor da Internet no Brasil (CGI.br) –; até a própria LGPD, que, ainda que posterior a outras experiências semelhantes em diversos países, é fruto de intenso processo interno de debate e amadurecimento. Essa tradição aponta para futuras experiências potencialmente relevantes, tais como a atual instalação de Comissão de Juristas pelo Senado Federal para elaborar substitutivo de Projeto de Lei sobre Inteligência Artificial.[3]

A introdução do marco regulatório de proteção de dados pessoais vem produzindo mudanças em hábitos que, agora, começamos a poder constatar objetivamente. Desde uma demanda maior por parte dos cidadãos por respeito e transparência no uso de seus dados – ante a possibilidade de exercício dos seus direitos e na atuação de um sistema de tutela administrativa e judicial – até a verificação da implementação e efetividade de processos e práticas relacionados à proteção de dados por empresas e organizações públicas.

No setor público, particularmente, a dinâmica de incorporação efetiva da normativa de proteção de dados pessoais se dá em processos que podem ser, a princípio, menos visíveis, como na utilização de dados pessoais em políticas públicas e em ações de interesse público, o que, inclusive, encontra respaldo em lei. Não obstante, esse intenso uso de dados pessoais torna ainda maior a necessidade de respeito e transparência para com o cidadão. A confiança dos indivíduos nos órgãos públicos passa a ser, cada vez mais, definida em função do respeito que estes inspirem como controladores e protetores de dados pessoais. Nesse sentido, o espaço proporcionado pela LGPD em relação ao tratamento de dados pessoais deve ser encarado no setor público como

[2] Doneda, D. (2021). Panorama histórico da proteção de dados pessoais. In D. Doneda, I. W. Sarlet, L. S. Mendes, & O. L. Rodrigues Junior (Coords.), *Tratado de proteção de dados pessoais*. Forense.

[3] Disponível em: https://legis.senado.leg.br/comissoes/comissao?codcol=2504

um chamado para que sejam desenvolvidas ferramentas que garantam aos cidadãos transparência e controle sobre seus próprios dados. Além de atribuir maior eficácia para o serviço público, a utilização de tais ferramentas será cada vez mais elemento preponderante na relação entre o setor público e a sociedade, relação esta que somente será efetiva com a devida confiança mútua.

É fundamental também destacar que a vigência de novos marcos regulatórios não ocorre sem que haja uma mudança cultural. Nesse sentido, a investigação, a partir de métodos rigorosos e confiáveis, tanto sobre a percepção da sociedade em relação aos objetos da regulação como sobre as práticas adotadas por empresas e organizações públicas para fazer frente aos novos desafios do tratamento de dados pessoais, é elemento-chave e primordial para que se tomem decisões nos níveis gerencial e de políticas públicas.

Diante da necessidade de informações atualizadas sobre o tema da proteção de dados e do contexto de adoção da LGPD por indivíduos, empresas e organizações públicas brasileiras, o Núcleo de Informação e Coordenação do Ponto BR (NIC.br), ligado ao CGI.br, com o apoio da Autoridade Nacional de Proteção de Dados (ANPD), desenvolveu a publicação *Privacidade e proteção de dados pessoais: perspectivas de indivíduos, empresas e organizações públicas no Brasil*. A partir da coleta e do processamento de dados inéditos, produzidos pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), a publicação apresenta um levantamento atualizado dos avanços dessa discussão na sociedade brasileira. Após a apresentação dos aspectos metodológicos que orientaram o estudo, a análise dos resultados da publicação está organizada nas seguintes seções:

- **Usuários de Internet:** apresenta os resultados do Painel TIC, realizado em 2021 com usuários de Internet (com 16 anos ou mais), que investiga a percepção dos usuários sobre o tratamento e a proteção de seus dados pessoais;
- **Empresas:** identifica como as pequenas, médias e grandes empresas brasileiras tratam os dados pessoais no exercício de suas atividades, baseada na aplicação de um módulo específico durante a coleta de dados da TIC Empresas 2021;
- **Organizações públicas:** abrange resultados das pesquisas TIC Educação 2020, TIC Saúde 2021 e TIC Governo Eletrônico 2021 em relação a iniciativas de proteção de dados e da privacidade adotadas por escolas públicas de Ensino Fundamental e Médio e estabelecimentos públicos de saúde, bem como por órgãos federais e estaduais e prefeituras.

Com essa nova pesquisa, o NIC.br reafirma seu compromisso de prover o governo e a sociedade de estatísticas robustas e atualizadas sobre os avanços da sociedade da informação no país. Por meio da compilação de indicadores em diversos setores, busca oferecer insumos inéditos para políticas públicas baseadas em evidências e para a implementação de estratégias regulatórias. A partir dessa primeira medição, os dados desta pesquisa estabelecem uma linha de base para o acompanhamento futuro do ecossistema de proteção de dados pessoais no Brasil, permitindo o monitoramento e a avaliação de políticas públicas e a promoção do bem-estar da população.

RESUMO EXECUTIVO

PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Resumo Executivo
Privacidade e Proteção de Dados Pessoais 2021

A preocupação com a privacidade e com a proteção de dados pessoais tem se intensificado em diversos setores da sociedade brasileira, especialmente após 2020, quando entrou em vigor a Lei Geral de Proteção de Dados Pessoais (LGPD). Com a crescente adoção de tecnologias digitais por organizações públicas e privadas e por indivíduos – e a interação entre eles –, tendência acentuada na pandemia COVID-19, é fundamental compreender a forma como o tema é percebido e as estratégias adotadas por esses atores para garantir a privacidade e a proteção dos dados pessoais no país.

Nesse sentido, a presente publicação contribui para a discussão por meio de uma compilação de indicadores sobre o comportamento e as perspectivas de usuários de Internet, empresas e organizações públicas sobre o tema. Os resultados apontam, por exemplo, uma elevada preocupação dos usuários de Internet com riscos relacionados ao tratamento de seus dados pessoais. Por parte das empresas, indicam uma presença ainda incipiente dessa agenda. Nas organizações públicas, mesmo que haja avanço nas estratégias adotadas, há ainda desafios a ser superados para uma governança de dados que garanta a privacidade e proteção dos dados pessoais.

Usuários de Internet

PRÁTICAS ADOTADAS

A pesquisa investigou as práticas adotadas por usuários de Internet com 16 anos ou mais para gerenciar o acesso a seus dados pessoais. A verificação de segurança de página ou aplicativo (70%), como a verificação do cadeado de segurança do navegador, foi a prática reportada em maior proporção. Já a solicitação de exclusão de dados pessoais (42%) foi citada por menos da metade dos usuários de Internet (Gráfico 1).

Cerca de um quarto dos usuários de Internet (24%) buscaram por canais de atendimento para solicitações, reclamações ou denúncias sobre seus dados pessoais. Entre os que buscaram, o canal mais mencionado foi a própria empresa ou órgão público controlador do dado (80%), seguido, em menor proporção, pelos órgãos de defesa do consumidor, como os Procons (48%).

CERCA DE UM QUARTO DOS USUÁRIOS DE INTERNET (24%) BUSCARAM POR CANAIS DE ATENDIMENTO PARA SOLICITAÇÕES, RECLAMAÇÕES OU DENÚNCIAS SOBRE SEUS DADOS PESSOAIS

PREOCUPAÇÃO COM DADOS PESSOAIS

Os registros de dados que ocorrem durante o uso da Internet demonstraram ser um fator de preocupação para a maioria dos usuários em relação a seus dados pessoais, especialmente ao comprar pela Internet por páginas e aplicativos (67% preocupados ou muito preocupados) ou ao acessar páginas e aplicativos de bancos (59% preocupados ou muito preocupados). Esses resultados indicam a percepção dos usuários de maior potencial de dano relacionado a dados associados a transações financeiras. Usar aplicativos de relacionamento (34% preocupados ou muito preocupados), a despeito de ser a atividade que a menor parte dos respondentes indicou realizar, foi a terceira atividade com maior proporção de usuários preocupados ou muito preocupados entre os que a realizam (Gráfico 2).

Os usuários de Internet também apontaram preocupação com o fornecimento de dados sensíveis: 65% disseram estar preocupados ou

muito preocupados com a coleta e tratamento de dados biométricos (Gráfico 3). Outra categoria que se destaca são os dados pessoais relacionados à saúde, que expõem situações de vulnerabilidade e têm elevado potencial discriminatório: 52% declararam estar preocupados ou muito preocupados. Usuários pretos (35%) e pardos (32%) declararam estar preocupados ou muito preocupados em proporções maiores do que usuários brancos (26%) com o fornecimento de informações pessoais relativas a cor ou raça.

Motivados pela preocupação com o uso de seus dados pessoais, 77% dos usuários de Internet de 16 anos ou mais já desinstalaram algum aplicativo do celular, 69% deixaram de visitar algum *website*, 56% deixaram de utilizar algum serviço ou plataforma na Internet e 45% deixaram de comprar algum equipamento eletrônico.

Empresas

GUARDA DE DADOS PESSOAIS

Foram investigados os tipos de dados pessoais mantidos pelas empresas brasileiras e para quais fins. Destaca-se que, em 2021, apenas 37% das empresas afirmaram manter dados de funcionários terceirizados, ao passo que 67% afirmaram manter dados de parceiros e fornecedores (Gráfico 4). Em relação ao tratamento de dados pessoais, nota-se que os setores de informação e comunicação e de atividades profissionais foram aqueles que apresentaram maior presença de guarda de dados de clientes e usuários, atingindo 78% das empresas desses setores.

CAPACIDADES INTERNAS

Um aspecto central para o desenvolvimento de uma cultura de proteção de dados é a existência de ações, por parte das empresas, que busquem a capacitação e sensibilização da equipe interna. O levantamento realizado com as empresas indica que 36% delas afirmaram ter realizado reuniões específicas sobre privacidade e proteção de dados pessoais. Ainda que não sejam observadas diferenças regionais importantes, a realização de reuniões para tratar de temas relacionados à privacidade e à proteção de dados aparece de forma desigual entre os diferentes setores. Vale destacar que reuniões foram mais presentes nas grandes (73%) e médias empresas (59%), enquanto nas pequenas há uma menor proporção (32%) de empresas que buscam discutir internamente os temas de privacidade e proteção de dados pessoais.

APENAS 17% DAS EMPRESAS NOMEARAM UM ENCARREGADO DE DADOS

Também foram coletados dados sobre a presença de uma área ou de funcionários responsáveis pelo tema de proteção de dados pessoais. Observa-se que 23% das empresas afirmaram contar com tal área ou pessoal dedicado, sendo que, em sua maioria, essas empresas são de médio e grande porte. As empresas que possuem área ou pessoas dedicadas aos temas da privacidade e proteção de dados pessoais em maiores proporções também estão nas atividades que podem ter contato com maior volume de dados pessoais – como os setores de informação e comunicação e transporte, armazenamento e correio (Gráfico 5).

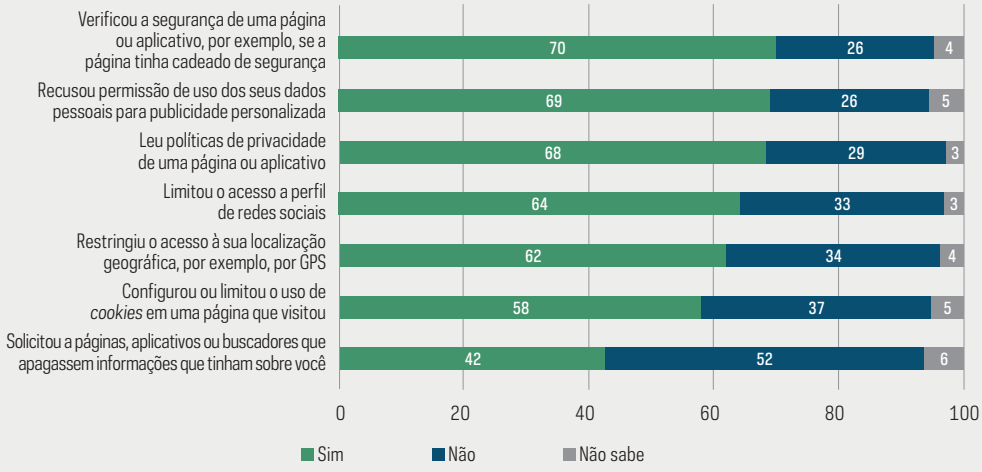
ADEQUAÇÃO À LGPD

A pesquisa também investigou aspectos críticos para a adequação à LGPD entre as empresas brasileiras, tendo como marco orientador os dispositivos da lei. Entre os aspectos mensurados, o mais citado foi o desenvolvimento de uma política de privacidade que informe como os dados pessoais são tratados pela empresa (32%). Em seguida, 30% das empresas informaram que realizaram teste de segurança contra vazamentos de dados, o que evidencia uma preocupação em ter seus processos de tratamento de dados pessoais mais explícitos, além da busca por garantir sua segurança, evitando vazamentos que possam trazer prejuízos fiscais e danos reputacionais. Apenas 17% das empresas nomearam um encarregado de dados. Já a criação de um plano

GRÁFICO 1

USUÁRIOS DE INTERNET, POR PRÁTICAS DE GERENCIAMENTO DE ACESSO A SEUS DADOS PESSOAIS (2021)

Total de usuários de Internet com 16 anos ou mais (%)



77%
dos usuários de Internet desinstalaram algum aplicativo do celular por causa de preocupações com seus dados

69%
dos usuários de Internet deixaram de visitar alguma página na Internet por causa de preocupações com seus dados

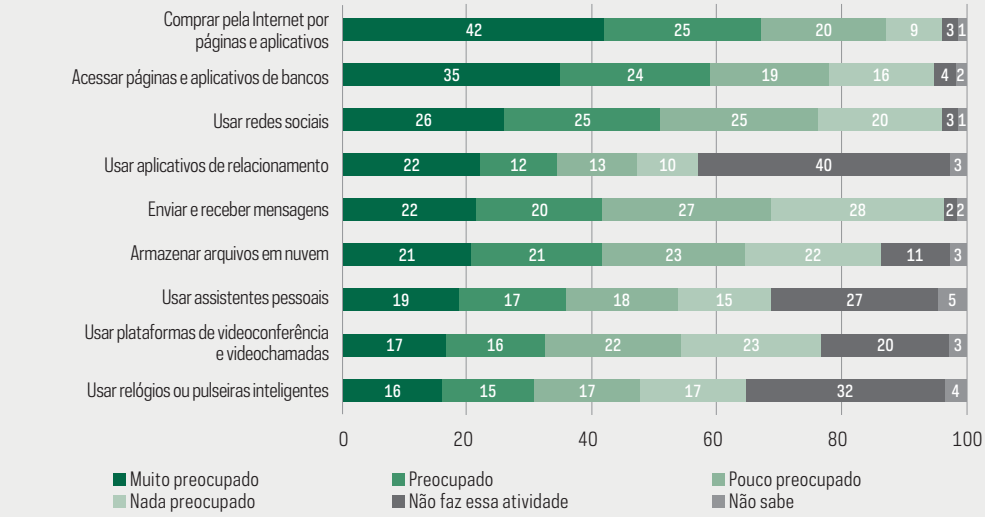
56%
dos usuários de Internet deixaram de utilizar algum serviço ou plataforma na Internet por causa de preocupações com seus dados

45%
dos usuários de Internet deixaram de comprar um aparelho eletrônico por causa de preocupações com seus dados

GRÁFICO 2

USUÁRIOS DE INTERNET, POR NÍVEL DE PREOCUPAÇÃO COM SEUS DADOS PESSOAIS, SEGUNDO ATIVIDADE REALIZADA NA INTERNET (2021)

Total de usuários de Internet com 16 anos ou mais (%)



de adequação à LGPD, que pode favorecer uma operação mais segura e em conformidade com a lei, foi citada por apenas 24% das empresas.

Metodologia da pesquisa e acesso aos dados

A pesquisa Privacidade e Proteção de Dados Pessoais 2021 reuniu dados inéditos coletados por diferentes estudos conduzidos pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br) com indivíduos, empresas e organizações públicas. A pesquisa Painel TIC entrevistou via questionário *online* 2.556 usuários de Internet com 16 anos ou mais de idade entre novembro e dezembro de 2021. A pesquisa TIC Empresas 2021 incluiu um módulo específico sobre tratamento de dados pessoais no setor privado. Foram entrevistadas 1.473 pequenas, médias e grandes empresas entre agosto de 2021 e abril de 2022. Além dos resultados inéditos, foi realizada uma análise sobre as organizações públicas no país baseada em indicadores relacionados ao tema de privacidade e proteção de dados pessoais nas pesquisas TIC Governo Eletrônico 2021, TIC Saúde 2021 e TIC Educação 2020. Os resultados das pesquisas apresentadas nessa publicação estão disponíveis no *website* do Cetic.br|NIC.br – https://www.cetic.br. O "Relatório Metodológico" pode ser consultado tanto na publicação impressa como no *website* do Centro.

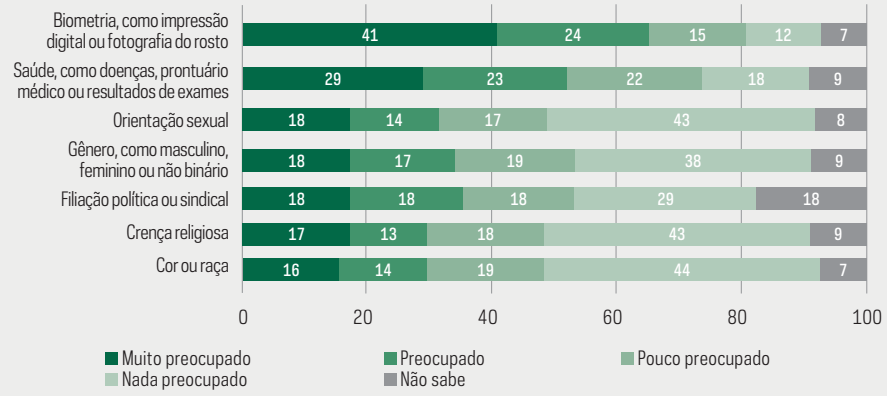
Privacidade e proteção de dados pessoais no setor público

A ampliação da transformação digital no setor público permite maior alcance das políticas públicas, mas também aumenta os riscos envolvidos no tratamento dos dados dos cidadãos. Dada a relevância do tema, esta publicação incluiu uma análise sobre a adoção de práticas relacionadas à privacidade e à proteção de dados por parte de organizações públicas, tais como órgãos federais e estaduais e prefeituras, de estabelecimentos de saúde e de escolas públicas de Educação Básica. A análise foi baseada nos indicadores coletados pelas pesquisas TIC Governo Eletrônico 2021, TIC Saúde 2021 e TIC Educação 2020, realizadas pelo Cetic.br|NIC.br. A criação de estruturas de governança de dados pessoais nas instituições públicas, a garantia de acesso aos cidadãos a informações claras e precisas sobre as formas de coleta e uso dos dados, assim como a realização de ações de conscientização sobre o tema nas instituições, foram alguns dos temas contemplados pela análise. Os resultados revelam avanços, como a existência de canais *online* para recebimento de solicitações da sociedade. No entanto, também evidenciam desigualdades de prontidão entre as diferentes instituições públicas na adequação organizacional, tecnológica e cultural às diretrizes da lei. A análise chama a atenção ainda para a crescente digitalização dos serviços públicos, especialmente a partir da pandemia COVID-19, e para a necessidade premente de ações para apoiar as organizações públicas no atendimento à privacidade e à proteção de dados da população.

GRÁFICO 3

USUÁRIOS DE INTERNET, POR NÍVEL DE PREOCUPAÇÃO COM O FORNECIMENTO DE INFORMAÇÕES PESSOAIS SENSÍVEIS (2021)

Total de usuários de Internet com 16 anos ou mais (%)



32%
das empresas desenvolveram uma política de privacidade que informa como os dados pessoais são tratados pela empresa

30%
das empresas realizaram testes de segurança contra vazamento de dados

24%
das empresas elaboraram um plano de conformidade ou adequação à proteção de dados pessoais

13%
das empresas elaboraram algum relatório de impacto à proteção de dados pessoais

GRÁFICO 4

EMPRESAS, POR TIPO DE DADO DE PESSOAL MANTIDO E PORTE (2021)

Total de empresas (%)

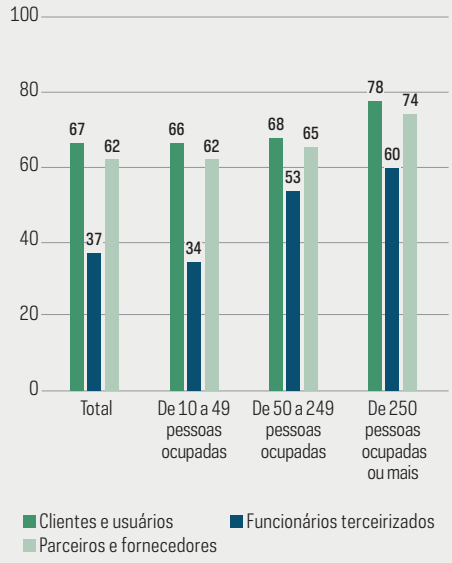
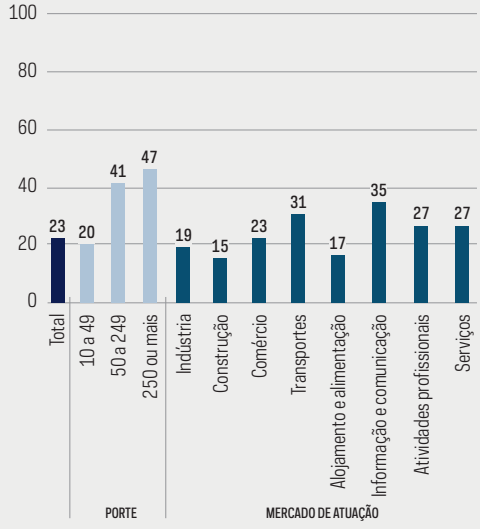


GRÁFICO 5

EMPRESAS, POR EXISTÊNCIA DE UMA ÁREA ESPECÍFICA OU FUNCIONÁRIOS RESPONSÁVEIS PELO TEMA DE PROTEÇÃO DE DADOS PESSOAIS (2021)

Total de empresas (%)



Acesse os dados completos da pesquisa

A publicação completa e os resultados da pesquisa estão disponíveis no *website* do **Cetic.br**, incluindo as tabelas de proporções, totais e margens de erro.

RELATÓRIO METODOLÓGICO

PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Relatório Metodológico
Privacidade e Proteção de Dados Pessoais 2021

O Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), departamento do Núcleo de Informação e Coordenação do Ponto BR (NIC.br), ligado ao Comitê Gestor da Internet no Brasil (CGI.br), apresenta os aspectos metodológicos da publicação *Privacidade e proteção de dados pessoais 2021: perspectivas de indivíduos, empresas e organizações públicas no Brasil.* O objetivo do projeto é apurar o cenário atual e compreender os principais desafios para a construção de um ecossistema digital que garanta o respeito à privacidade e à proteção de dados pessoais no Brasil. O levantamento se baseia na coleta e processamento de dados quantitativos da sociedade brasileira por meio de pesquisas conduzidas regularmente pelo Cetic.br|NIC.br. As informações incluem a percepção dos usuários de Internet sobre seus direitos e o tratamento de seus dados pessoais. Com relação às organizações, a publicação apresenta um levantamento de como as empresas e órgãos públicos estão se adaptando ao tema da privacidade e proteção de dados pessoais desde a vigência da Lei Geral de Proteção de Dados Pessoais (LGPD).

O projeto possui três objetivos específicos:

- Investigar a percepção da população de usuários de Internet sobre o uso e a proteção de seus dados pessoais;
- Compreender como pequenas, médias e grandes empresas tratam os dados pessoais de seus clientes/consumidores, bem como questões relevantes associadas à implementação da LGPD no Brasil;
- Traçar um panorama da proteção de dados no contexto das políticas públicas, incluindo a adoção de práticas por parte dos órgãos governamentais, estabelecimentos de saúde e escolas.

Na sequência, apresentamos os principais aspectos metodológicos das pesquisas utilizadas para a coleta dos indicadores e as referências para acesso integral ao "Relatório Metodológico" e ao "Relatório de Coleta de Dados" de cada estudo utilizado.

Painel TIC – Usuários de Internet (2021)

O Painel TIC foi criado com o objetivo de coletar informações sobre o uso da Internet durante a pandemia causada pelo novo coronavírus. Realizada por meio de questionários *online*, a pesquisa foi desenvolvida como uma alternativa à coleta de dados presencial, afetada pelas medidas de distanciamento social implementadas durante esse período. Desde então, a metodologia do Painel vem sendo adotada para o levantamento de dados sobre outros temas relevantes para o debate sobre a transformação digital.

Em 2021, um novo módulo do Painel TIC foi desenvolvido para investigar a percepção da população de usuários de Internet sobre o tratamento e a proteção de seus dados pessoais (CGI.br, 2021a). A elaboração de um questionário específico sobre privacidade entre usuários de Internet tomou como ponto de partida diversas pesquisas anteriores com objetivos convergentes. Uma das primeiras coletas de dados identificada foi a pesquisa do Eurobarômetro *Special Eurobarometer 431: Data protection*, de 2015, encomendada pela Comissão Europeia. Outra fonte relevante foi a edição de junho de 2019 da pesquisa *American Trends Panel* do Pew Research Center. Entre levantamentos oficiais produzidos por institutos nacionais de estatística, foi considerada a pesquisa *Survey of Canadians on Privacy-Related Issues*, realizada em 2020 por encomenda do Escritório do Comissariado de Privacidade do Canadá.

Também foi levada em conta a segunda edição da pesquisa *Painel TIC COVID-19* do Cetic.br|NIC.br, que incluiu um módulo de privacidade. Esse módulo fazia parte de um esforço regional liderado pelo Banco Interamericano de Desenvolvimento (BID) com o objetivo de medir atitudes e percepções em relação à proteção de dados pessoais considerando o uso das tecnologias de informação e comunicação (TIC) em medidas de contenção da pandemia (CGI.br, 2020).

A população-alvo da pesquisa é composta por indivíduos usuários de Internet com 16 anos ou mais de idade no Brasil, considerando-se tais usuários as pessoas que fizeram uso da rede nos três meses que antecederam a entrevista, segundo recomendação metodológica da União Internacional de Telecomunicações (UIT, 2020).

Para seu desenho amostral, a pesquisa utilizou como base um painel *online* de indivíduos mantido pela Quaest Consultoria e Pesquisa, com aproximadamente 167 mil painelistas. O plano amostral empregado para a obtenção da amostra de respondentes foi do tipo amostragem por cotas, considerando as variáveis: sexo, faixa etária, escolaridade, macrorregião e classe. A coleta de dados da pesquisa foi realizada entre os dias 12 de novembro e 03 de dezembro de 2021; ao todo, foram obtidas 2.556 entrevistas.

Com o objetivo de minimizar os vieses de seleção encontrados em abordagens por cotas, foi construída uma estrutura de pesos para o Painel TIC, tendo como referência uma pesquisa probabilística, a TIC Domicílios 2020[1]. Na etapa inicial, os resultados dessa pesquisa foram recalibrados para a população da *Pesquisa Nacional por Amostra de Domicílios Contínua* (PNAD Contínua) (Instituto Brasileiro de Geografia e Estatística [IBGE], s.d.), referente ao último trimestre divulgado.

[1] Mais informações disponíveis no *website* da pesquisa: https://www.cetic.br/pt/pesquisa/domicilios

Na sequência, com o intuito de estimar o contingente da população representada pelos respondentes do Painel TIC, adotou-se o procedimento de estimação baseado em escores de propensão (*propensity scores*)[2]. Nessa metodologia, são calculados, inicialmente, os escores de propensão de ser usuário de Internet segundo variáveis socioeconômicas, com base na última edição disponível da pesquisa TIC Domicílios[3]. A seguir, esse mesmo modelo é utilizado para estimar os escores de propensão para os respondentes do Painel TIC.

Comparando a distribuição dos escores de propensão do Painel TIC com aquela verificada na última pesquisa TIC Domicílios, é possível determinar qual parte da população desse último levantamento (ou se toda ela) poderia ser representada pelos respondentes do Painel. Isso equivale a estimar o erro de cobertura do Painel TIC em relação à população-alvo inicialmente considerada para a pesquisa.

Na presente edição do Painel TIC, o público representado equivale a toda a população-alvo da pesquisa TIC Domicílios, o que permite a comparação direta dos resultados da edição com os indicadores equivalentes coletados. Já em relação às edições anteriores do Painel, que não representavam a totalidade da população-alvo, a comparação precisa ser feita por meio dos mesmos recortes populacionais das respectivas edições.

Os resultados completos da pesquisa, bem como as íntegras do "Relatório Metodológico" do estudo, estão disponíveis no *website* do Cetic.br|NIC.br (https://www.cetic.br).

TIC Empresas – Pequenas, médias e grandes empresas (2021)

Realizada desde 2005, a pesquisa TIC Empresas tem como objetivo principal medir a posse e o uso das TIC entre as empresas brasileiras. O levantamento apresenta indicadores que traduzem em números a realidade das empresas brasileiras em relação a diversos temas, tais como acesso às TIC; uso da Internet; governo eletrônico; comércio eletrônico; habilidades em TIC; *software*; e segurança digital e novas tecnologias.

O universo abordado na pesquisa compreende todas as empresas brasileiras ativas com 10 ou mais pessoas ocupadas[4] listadas no Cadastro Central de Empresas (Cempre) do IBGE, pertencentes aos setores da Classificação Nacional de Atividades Econômicas (CNAE) 2.0 de interesse da pesquisa TIC Empresas e à Natureza Jurídica 2 – entidades empresariais, exceto as empresas públicas (Natureza Jurídica 201-1).

[2] Diferentemente da estimativa baseada em um desenho amostral tradicional, as probabilidades de seleção no Painel são desconhecidas e indefinidas, por se tratar de um pseudodesenho amostral. A pseudoprobabilidade é a probabilidade estimada de pertencer à amostra não probabilística usada em vez de uma probabilidade conhecida. Mais informações disponíveis em 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://www.aapor.org/AAPOR_Main/media/MainSiteFiles/NPS_TF_Report_Final_7_revised_FNL_6_22_13.pdf

[3] Para esta edição do Painel TIC, foi utilizada a TIC Domicílios 2020 (CGI.br, 2021c).

[4] A pesquisa TIC Empresas considera pequenas, médias e grandes empresas aquelas com, respectivamente, 10 a 49 pessoas ocupadas, 50 a 249 pessoas ocupadas, e 250 pessoas ocupadas ou mais. As microempresas, aquelas com 1 a 9 pessoas ocupadas, não entram no escopo da pesquisa.

As empresas investigadas correspondem às seguintes seções:

C – Indústria de transformação;

F – Construção;

G – Comércio; reparação de veículos automotores e motocicletas;

H – Transporte, armazenagem e correio;

I – Alojamento e alimentação;

J – Informação e comunicação;

L – Atividades imobiliárias;

M – Atividades profissionais, científicas e técnicas;

N – Atividades administrativas e serviços complementares;

R – Artes, cultura, esporte e recreação;

S – Outras atividades de serviços.

A pesquisa TIC Empresas é desenvolvida com a preocupação de manter a comparabilidade internacional. Para isso, segue os padrões metodológicos propostos no manual da Conferência das Nações Unidas sobre Comércio e Desenvolvimento (UNCTAD, 2009), elaborado pela parceria entre a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), o Instituto de Estatísticas da Comissão Europeia (Eurostat) e a Partnership on Measuring ICT for Development – esta última, uma coalizão formada por diversas organizações internacionais, busca a harmonização de indicadores-chave em pesquisas sobre TIC.

O plano amostral é estratificado em duas etapas, e as empresas são selecionadas aleatoriamente dentro de cada estrato. A primeira etapa compreende a definição de estratos naturais por meio do cruzamento das variáveis região geográfica e mercado de atuação (CNAE 2.0). A partir de cada estrato natural, são definidos os estratos finais, que consideram a divisão dos estratos naturais por porte da empresa[5]. Em 2021, a pesquisa entrevistou um total de 4.064 empresas, sendo que 1.473 responderam às perguntas específicas do módulo sobre privacidade e proteção dos dados pessoais.

As empresas são contatadas por meio da técnica de entrevista telefônica assistida por computador (do inglês, *computer-assisted telephone interviewing* – CATI). Em todas as entidades pesquisadas, busca-se entrevistar o responsável pela área de informática, tecnologia da informação (TI), gerenciamento da rede de computadores ou área equivalente, o que corresponde a cargos como:

- Diretor da divisão de informática e tecnologia;
- Gerente de negócios (vice-presidente sênior, vice-presidente de linha de negócios, diretor);

[5] As faixas de porte consideradas são: 10 a 19 pessoas ocupadas; 20 a 49 pessoas ocupadas; 50 a 249 pessoas ocupadas; e 250 pessoas ocupadas ou mais.

- Gerente ou comprador do departamento de tecnologia;
- Influenciador tecnológico (funcionário do departamento comercial ou de operações de TI com influência sobre as decisões a respeito de questões tecnológicas);
- Coordenador de projetos e sistemas;
- Diretor de outros departamentos ou divisões (excluindo informática);
- Gerente de desenvolvimento de sistemas;
- Gerente de informática;
- Gerente de projetos;
- Dono da empresa ou sócio.

Nas empresas que declaram ter, no momento da entrevista, 250 pessoas ocupadas ou mais, a estratégia foi entrevistar um segundo profissional, preferencialmente o gestor da área contábil ou financeira. Quando não encontrado, buscou-se o responsável pela área administrativa, jurídica ou de relações com instituições governamentais, a quem cabem exclusivamente as respostas sobre comércio eletrônico, governo eletrônico e atividades realizadas na Internet.

TIC EMPRESAS 2021 – MÓDULO "PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS"

Em 2021, para atender à demanda por dados sobre como pequenas, médias e grandes empresas tratam os dados pessoais de seus clientes/consumidores, bem como questões relevantes associadas à implementação da LGPD no Brasil, foi criado um módulo a ser implementado paralelamente à realização da pesquisa TIC Empresas 2021.

Para responsabilizar-se pela resposta ao módulo específico sobre proteção de dados, foi entrevistado um respondente adicional, qualificado para responder sobre medidas relativas ao cumprimento da LGPD na empresa. Para esse módulo, era solicitado que os respondentes da pesquisa TIC Empresas indicassem a pessoa mais familiarizada com o tema na empresa, ou seja, quem poderia responder sobre procedimentos e políticas adotados para coleta, armazenamento e uso de dados pessoais, bem como sobre a adequação da empresa à LGPD. Nos casos em que o tema era liderado pelo respondente da TIC Empresas, a entrevista foi realizada com esse profissional. Não foi permitido que a organização indicasse um profissional terceirizado como respondente, buscando-se, alternativamente, identificar o funcionário interno responsável pela contratação desse serviço, de modo a garantir que as entrevistas fossem realizadas com membros da equipe interna da empresa.

Todas as empresas respondentes da pesquisa tinham a probabilidade de 50% de serem selecionadas para responder ao módulo de privacidade e proteção de dados pessoais. Com essa probabilidade de seleção, garante-se uma representatividade semelhante à esperada para a pesquisa TIC Empresas. Dado que o tamanho da amostra é menor em comparação ao obtido nesta última pesquisa, é esperado que alguns indicadores apresentem maiores erros amostrais.

A partir dessa probabilidade de seleção, o peso inicial das empresas respondentes do módulo é obtido pela Fórmula 1.

FÓRMULA 1

$$w_{ih}^{LGPD} = \frac{1}{2} \times w_{ih}^{*} = \frac{1}{2} \times w_{ih} \times \frac{N_h}{\Sigma_i w_{ih}}$$

tal que

$$w_{ih} = \frac{N_h}{n_h}$$

w_{ih}^{LGPD} é o peso básico da empresa ***i*** respondente do módulo no estrato ***h***

w_{ih}^{*} é o peso com correção de não resposta da empresa ***i*** no estrato ***h***

w_{ih} é o peso básico associado a cada empresa respondente ***i*** da pesquisa TIC Empresas no estrato ***h***

n_h é o tamanho da amostra de empresas no estrato ***h***

N_h é o total de empresas no estrato ***h***

Para corrigir os casos em que não se obtém a resposta de todos os selecionados, é realizada uma correção de não resposta, dada pela Fórmula 2.

FÓRMULA 2

$$w_{ih}^{*\,LGPD} = w_{ih}^{LGPD} \times \frac{N_h}{\Sigma_i w_{ih}^{LGPD}}$$

$w_{ih}^{*\,LGPD}$ é o peso com correção de não resposta da empresa ***i*** respondente do módulo LGPD no estrato ***h***

Por fim, esses pesos amostrais são calibrados para refletir os totais populacionais conhecidos, obtidos no Cempre do IBGE. Esse procedimento, juntamente com as correções de não resposta, tem por objetivo corrigir a variabilidade associada à não resposta da população de empresas. As variáveis consideradas para calibração são: região geográfica, mercado de atuação e porte da empresa.

A Tabela 1 traz a distribuição do número de empresas segundo região geográfica, mercado de atuação e porte, de acordo com o Cempre, além da alocação da amostra elegível para participar do módulo e a amostra realizada neste módulo. Ao todo, a taxa de resposta para o módulo foi de 74%.

TABELA 1

NÚMERO DE EMPRESAS SEGUNDO PORTE, REGIÃO GEOGRÁFICA E MERCADO DE ATUAÇÃO (2021)

	Universo	Amostra selecionada entre respondentes da TIC Empresas	Amostra realizada
Total	**509 049**	**1 982**	**1 473**
Porte			
De 10 a 19 pessoas ocupadas	310 023	696	512
De 20 a 49 pessoas ocupadas	136 438	530	391
De 50 a 249 pessoas ocupadas	51 780	326	245
Com 250 pessoas ocupadas ou mais	10 808	430	325
Região			
Norte	22 122	254	176
Nordeste	78 059	298	216
Sudeste	260 094	810	596
Sul	107 162	372	296
Centro-Oeste	41 612	248	189
Mercado de atuação (CNAE 2.0)			
Indústria de transformação	98 870	343	278
Construção	34 880	209	169
Comércio; reparação de veículos automotores e motocicletas	195 839	458	314
Transporte, armazenagem e correio	29 111	201	146
Alojamento e alimentação	56 903	192	141
Informação e comunicação	14 085	187	133
Atividades imobiliárias; atividades profissionais, científicas e técnicas; atividades administrativas e serviços complementares	66 643	208	159
Artes, cultura, esporte e recreação; outras atividades de serviços	12 718	184	133

FONTE: CGI.BR (NO PRELO).

Os resultados e as tabelas de proporções, totais e margens de erro da TIC Empresas, bem como as íntegras do "Relatório Metodológico" e do "Relatório de Coleta de Dados" do estudo, estão disponíveis no *website* do Cetic.br|NIC.br (https://www.cetic.br).

TIC Governo Eletrônico – Órgãos públicos federais e estaduais e prefeituras (2021)

Realizada a cada dois anos desde 2013, a pesquisa sobre o uso das tecnologias de informação e comunicação no setor público brasileiro – TIC Governo Eletrônico – investiga a incorporação das tecnologias digitais nos órgãos públicos e o seu uso para a oferta de serviços públicos. O estudo ainda mede a existência de iniciativas relacionadas à promoção do acesso à informação pública e participação da sociedade por meio das novas tecnologias. Em 2021, foram incluídos novos módulos relacionados a ações de uso das TIC para o combate à pandemia e adoção de novas tecnologias. A edição de 2021 também incorporou indicadores sobre privacidade e proteção de dados pessoais.

A pesquisa tem abrangência nacional e inclui duas unidades de análise: órgãos públicos federais e estaduais de todos os poderes (Executivo, Legislativo, Judiciário e Ministério Público) e prefeituras. É realizado um censo em todos os públicos de interesse, excetuando órgãos do Executivo estadual, sendo selecionada uma amostra de 400 entidades públicas. As entrevistas são realizadas por meio de questionário estruturado a partir da técnica de entrevista telefônica assistida por computador (em inglês, *computer-assisted telephone interviewing* – CATI).

Os indicadores analisados para esta publicação foram coletados entre agosto de 2021 e abril de 2022, em 580 órgãos públicos federais e estaduais e 3.543 prefeituras. Os resultados e as tabelas de proporções, totais e margens de erro da TIC Governo Eletrônico estão disponíveis no *website* do Cetic.br|NIC.br (https://www.cetic.br), bem como as íntegras do "Relatório Metodológico"[6] e do "Relatório de Coleta de Dados" do estudo.[7]

TIC Saúde – Estabelecimentos públicos de saúde (2021)

Realizada anualmente desde 2013[8], a pesquisa TIC Saúde tem o objetivo de compreender o estágio de adoção das TIC nos estabelecimentos de saúde e sua apropriação pelos profissionais da área (médicos e enfermeiros). Para isso, busca identificar a infraestrutura de TIC disponível e investigar o uso de sistemas e aplicações baseados em TIC destinados a apoiar os serviços de assistência e a gestão dos estabelecimentos de saúde. Além disso, mede as atividades realizadas por profissionais de saúde por meio das TIC, bem como as motivações e barreiras para sua adoção e uso.

[6] Disponível em: https://cetic.br/media/microdados/352/tic_egov_2021_relatorio_metodologico_v1.0.pdf

[7] Disponível em: https://cetic.br/media/microdados/353/tic_egov_2021_relatorio_coleta_de_dados_v1.0.pdf

[8] A pesquisa TIC Saúde não foi realizada no ano de 2020, devido a restrições causadas pelo acesso aos gestores e profissionais de saúde durante a pandemia COVID-19.

Em 2021, a pesquisa incluiu um indicador que investigou a adaptação dos estabelecimentos de saúde aos termos da LGPD[9]. A nova pergunta foi respondida por gestores dos estabelecimentos (CGI.br, 2021d).

A TIC Saúde tem abrangência nacional e coleta dados dos estabelecimentos de saúde nos três níveis de atenção, selecionando-os com base no Cadastro Nacional de Estabelecimentos de Saúde (CNES), mantido pelo Departamento de Informática do Sistema Único de Saúde (Datasus). As entrevistas são realizadas por meio da técnica de entrevista telefônica assistida por computador (em inglês, *computer-assisted telephone interviewing* – CATI) e há a possibilidade de autopreenchimento de questionário *web*, por meio de plataforma específica.

Os resultados da edição de 2021 foram coletados entre janeiro e agosto desse mesmo ano com 1.524 gestores, representando um universo de 112.075 estabelecimentos de saúde brasileiros. Os resultados e as tabelas de proporções, totais e margens de erro da TIC Saúde estão disponíveis no *website* do Cetic.br|NIC.br (https://www.cetic.br), bem como as íntegras do "Relatório Metodológico"[10] e do "Relatório de Coleta de Dados" do estudo.[11]

TIC Educação – Escolas públicas (2020)

Realizada desde 2010, a pesquisa TIC Educação tem abrangência nacional, sendo aplicada em escolas de Educação Básica, públicas e privadas, localizadas em áreas urbanas e rurais e que oferecem classes de Ensino Fundamental e Médio regular.

Até 2019, em áreas urbanas, a pesquisa era realizada de forma presencial nas instituições educacionais, com a aplicação de questionários estruturados a alunos, professores, coordenadores pedagógicos e diretores. Em áreas rurais, começou a ser realizada a partir de 2017, com questionários aplicados aos gestores das instituições, por telefone.

Em 2020, por conta do fechamento das escolas e da disseminação de atividades educacionais remotas como parte das medidas sanitárias implementadas por estados e municípios em todo o país no enfretamento à pandemia COVID-19, a coleta de dados da pesquisa TIC Educação foi realizada apenas com os gestores escolares e a partir de uma metodologia totalmente baseada em entrevistas telefônicas, tanto para escolas localizadas em áreas rurais quanto urbanas (CGI.br, 2021b).

Apesar das necessárias adaptações da coleta de dados às medidas sanitárias, foi possível ampliar as dimensões e os temas tratados pela pesquisa, com a inclusão de questões a respeito do uso de sistemas, plataformas e aplicações pelas instituições escolares, bem como sobre as ações implementadas por elas no que diz respeito à proteção de dados pessoais, à privacidade e à segurança digital.

[9] Na edição de 2021, não foi possível entrevistar os profissionais de saúde, dadas as restrições para atingir esse público durante a pandemia COVID-19.

[10] Disponível em: https://cetic.br/media/microdados/589/tic_saude_2021_relatorio_metodologico_v1.0.pdf

[11] Disponível em: https://cetic.br/media/microdados/588/tic_saude_2021_relatorio_coleta_dados_v1.0.pdf

Os dados analisados nesta publicação foram coletados entre setembro de 2020 e junho de 2021, em 3.678 escolas públicas e particulares, de áreas urbanas e rurais em atividade. Essas instituições ofereciam turmas de Ensino Fundamental e Médio, representando 127.171 instituições, a partir de amostra extraída da base de dados do Censo Escolar da Educação Básica, realizado pelo Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep).

Assim como para as demais pesquisas, os resultados e as tabelas de proporções, totais e margens de erro da TIC Educação estão disponíveis no *website* do Cetic.br|NIC.br (https://www.cetic.br), bem como as íntegras do "Relatório Metodológico"[12] e do "Relatório de Coleta de Dados" do estudo.[13]

Disseminação dos dados

Os resultados das pesquisas mencionadas anteriormente são apresentados de acordo com as variáveis descritas no "Relatório Metodológico" de cada estudo, no item "Domínios de interesse para análise e divulgação".

Arredondamentos fazem com que, em alguns resultados, a soma das categorias parciais difira de 100% em questões de resposta única. O somatório de frequências em questões de respostas múltiplas usualmente é diferente de 100%. Vale ressaltar que, nas tabelas de resultados, o hífen (–) é utilizado para representar a não resposta ao item. Por outro lado, como os resultados são apresentados sem casa decimal, as células com valor zero indicam que houve resposta ao item, mas ele é explicitamente maior do que zero e menor do que um.

Os resultados das pesquisas são publicados em formato *online* e disponibilizados no *website* do Cetic.br|NIC.br (https://www.cetic.br). As tabelas de proporções, totais e margens de erros calculadas para cada indicador estão disponíveis para *download* em português, inglês e espanhol. Mais informações sobre a documentação, os metadados e as bases de microdados estão disponíveis na página de microdados (https://www.cetic.br/microdados/).

[12] Disponível em: https://cetic.br/media/microdados/595/tic_educacao_2020_relatorio_metodologico_v1.0.pdf

[13] Disponível em: https://cetic.br/media/microdados/594/tic_educacao_2020_relatorio_coleta_de_dados_v1.0.pdf

Referências

Comitê Gestor da Internet no Brasil. (no prelo). *Pesquisa sobre o uso das tecnologias de informação e comunicação nas empresas brasileiras: TIC Empresas 2021*.

Comitê Gestor da Internet no Brasil. (2020). *Painel TIC COVID-19: Pesquisa sobre o uso da Internet no Brasil durante a pandemia do novo coronavírus – 2ª edição: Serviços públicos on-line, telessaúde e privacidade*. https://cetic.br/media/docs/publicacoes/1/20201001085713/painel_tic_covid19_2edicao_livro%20eletr%C3%B4nico.pdf

Comitê Gestor da Internet no Brasil. (2021a). *Painel TIC COVID-19: Pesquisa web sobre o uso da Internet no Brasil durante a pandemia do novo coronavírus*. https://cetic.br/media/docs/publicacoes/2/20210426095323/painel_tic_covid19_livro_eletronico.pdf

Comitê Gestor da Internet no Brasil. (2021b). *Pesquisa sobre o uso das tecnologias de informação e comunicação nas escolas brasileiras: TIC Educação 2020 (Edição COVID-19 — Metodologia adaptada)*. https://www.cetic.br/media/docs/publicacoes/2/20211124200326/tic_educacao_2020_livro_eletronico.pdf

Comitê Gestor da Internet no Brasil. (2021c). *Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros: TIC Domicílios 2020* (*Edição COVID-19 — Metodologia adaptada)*. https://cetic.br/media/docs/publicacoes/2/20211124201233/tic_domicilios_2020_livro_eletronico.pdf

Comitê Gestor da Internet no Brasil. (2021d). *Pesquisa sobre o uso das tecnologias de informação e comunicação nos estabelecimentos de saúde brasileiros: TIC Saúde 2021 (Edição COVID-19 — Metodologia adaptada)*. https://www.cetic.br/media/docs/publicacoes/2/20211124123911/tic_saude_2021_livro_eletronico.pdf

Conferência das Nações Unidas sobre Comércio e Desenvolvimento. (2009). *Manual for the production of statistics on the information economy 2009*. https://unctad.org/system/files/official-document/sdteecb20072rev1_en.pdf

Instituto Brasileiro de Geografia e Estatística. (s.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

União Internacional de Telecomunicações. (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

ANÁLISE DOS RESULTADOS

PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Análise dos Resultados Privacidade e Proteção de Dados Pessoais 2021
Usuários de Internet

Com o aumento da presença da Internet nos domicílios e da proporção de usuários da rede no país, também é crescente o rastro digital deixado pelos indivíduos durante as atividades realizadas no ambiente *online*. Com o avanço da transformação digital de organizações públicas e privadas, os dados pessoais dos indivíduos estão amplamente presentes em registros comerciais, financeiros, biográficos, entre outros, fazendo que essa quantidade massiva de dados receba cada vez mais atenção das áreas jurídica, econômica e social. A economia baseada em dados mobiliza uma ampla rede de atores, incluindo governos, organizações e indivíduos/consumidores (Carrière-Swallow & Haksar, 2019).

Se, por um lado, esse novo ecossistema tem o potencial de promover o bem-estar de indivíduos e sociedades, ele também traz inúmeros riscos associados ao uso indevido de dados. Diante desse cenário, muitos países têm avançado no estabelecimento de normas legais para regulamentar o uso de dados, em especial para garantir a proteção da privacidade e dos dados pessoais dos indivíduos, como é o caso do General Data Protection Regulation (GDPR), na União Europeia, e da Lei Geral de Proteção de Dados Pessoais (LGPD), no Brasil.

O aumento do interesse em torno desse tema também inspirou iniciativas de produção de estatísticas acerca da perspectiva dos indivíduos sobre sua privacidade e da percepção a respeito do uso de seus dados pessoais por atores públicos e privados. Para ampliar o entendimento sobre o tema, o Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br) realizou, em 2021, uma nova edição da pesquisa Painel TIC, dedicada ao tema da privacidade e proteção de dados pessoais, cuja análise é apresentada aqui. Os resultados do levantamento estão organizados nas dimensões descritas a seguir:

- **Conceito:** dimensão que busca identificar como os respondentes entendem e elaboram o significado do termo privacidade.
- **Práticas:** reúne indicadores sobre a gestão, pelos indivíduos, dos acessos a seus dados pessoais, bem como a busca por canais de atendimento para solicitações, reclamações ou denúncias.

- **Riscos:** inclui uma análise dos níveis de preocupação em relação a diversos temas, como registros de dados, atividades realizadas na Internet, guarda de dados por empresas e governos, dados considerados sensíveis e riscos em relação ao uso dos dados pessoais.
- **Controle:** dimensão que aborda motivos para o fornecimento de dados pessoais por indivíduos, percepção de controle sobre o acesso por terceiros a seus dados e atitudes em relação às políticas de privacidade.
- **Modelo de negócio:** mede indicadores que tratam do conhecimento sobre a prática de perfilamento, reconhecimento de publicidade direcionada e percepção sobre riscos associados a ela.

A relação entre a percepção de riscos à privacidade e as práticas dos usuários que efetivamente aumentam sua exposição a esses riscos ou ajudam a mitigá-los é complexa, e a discrepância observada entre elas é conhecida como "paradoxo da privacidade" (Barth & de Jong, 2017). Com base nos resultados da pesquisa, a presente análise tem como objetivo ampliar a compreensão sobre como os indivíduos entendem o tema da privacidade em um contexto de crescente digitalização e engajamento das pessoas no ambiente *online*, lançando luz sobre a relação entre as percepções e as práticas efetivamente adotadas pelos usuários de Internet.

Conceito

A primeira dimensão investigada pela pesquisa explora o entendimento do conceito de privacidade entre os usuários de Internet. Para melhor compreender opiniões e práticas relacionadas à privacidade, uma questão aberta foi incluída na pesquisa. As respostas foram analisadas e codificadas em categorias amplas, permitindo compreender a quais domínios as pessoas se referem quando pensam em "privacidade".[1]

O exercício de categorização das respostas abertas, cuja metodologia é descrita no *Box* 1 mais adiante, gerou seis categorias:

- **Liberdade:** garantia da liberdade em aspectos privados da vida ("liberdade" — própria e de outros —, "direito").
- **Individualidade:** a busca pela individualidade, seja em espaços ou em situações ("individualidade", "intimidade", "espaço", "particular", "privado").
- **Proteção de dados:** desejo de proteção contra acesso a seus dados por terceiros ("proteção de dados contra terceiros", "vazamentos").
- **Controle:** desejo de possuir controle sobre seus próprios dados ("controle sobre acesso a dados", "escolha sobre o que é público", "consentimento").
- **Segurança:** menções mais genéricas a segurança ("segurança", "proteção", "sigilo", "monitoramento").

[1] A pergunta feita aos respondentes foi: "Usando as suas próprias palavras e pensando no seu cotidiano, o que significa 'privacidade' para você?".

- **Outras:** respostas válidas não enquadradas nas demais categorias (“paz”, “tranquilidade”, “sossego”, “importante”, “essencial”, “tudo” [não elaborado], “não existe”).

Os resultados indicam que a maior parte dos usuários de Internet define “privacidade” partindo de domínios associados à liberdade e à individualidade (Gráfico 1) — entendidos como aspectos cruciais da vida cotidiana — e, em alguns casos, equiparada a um direito fundamental.

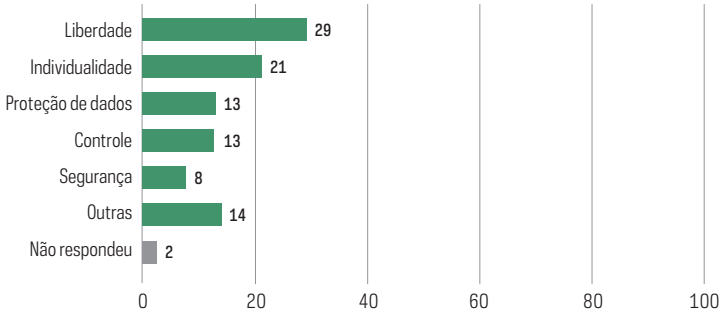
Em menor proporção estão aqueles que definem a privacidade a partir de um repertório associado ao uso da Internet, de plataformas *online* e de redes sociais. Nesses casos, a proteção de dados é descrita como uma barreira ao acesso desautorizado, o controle sobre quem pode ter acesso a eles (como em redes sociais) e a segurança contra roubos e vazamentos de dados no ambiente digital.

A alta incidência de respostas classificadas como “Outros” reforça, ainda, o caráter multifacetado do tema entre os respondentes.

GRÁFICO 1

CATEGORIZAÇÃO DA DEFINIÇÃO DO CONCEITO DE PRIVACIDADE (2021)

Total de usuários de Internet com 16 anos ou mais (%)



A categoria “Proteção de dados” apresentou variações por classe social (17% entre os usuários das classes AB e 8% entre os das classes DE) e grau de instrução (6% entre aqueles com até o Ensino Fundamental e 17% entre os com Ensino Superior). Entre as faixas etárias, destaca-se a proporção dos mais jovens que foram categorizados em “Individualidade” (32% dos que têm de 16 a 24 anos e 27% daqueles entre 25 e 34 anos) e a proporção dos mais velhos que foram categorizados em “Liberdade” (43% dos que têm 60 anos ou mais).

Esses resultados indicam que uma parcela relevante dos respondentes descreve a privacidade sob uma perspectiva abstrata, ligada a um direito fundamental, como a liberdade, assim como dimensões associadas à intimidade e à vida privada. Outra parcela dos respondentes descreveu a privacidade sob uma perspectiva objetiva e diretamente vinculada aos dados pessoais, sua proteção contra usos indevidos, acessos indesejados e estratégias de controle e segurança, dentro e fora do ambiente de Internet, redes sociais e plataformas.

BOX 1

METODOLOGIA USADA PARA A ANÁLISE DAS RESPOSTAS DA QUESTÃO ABERTA

Para a análise das respostas abertas, foi utilizado um método de aprendizado de máquina supervisionado para classificação dos textos em categorias de análise. Em um primeiro momento, uma amostra de 500 respostas foi selecionada aleatoriamente e categorizada manualmente por um grupo de pesquisadores. O exercício de classificação teve como referência uma iniciativa semelhante nos Estados Unidos coordenada pelo *Pew Research Center* (Auxier *et al.*, 2019). A classificação foi adaptada ao contexto brasileiro, o que gerou um conjunto inicial de 11 categorias.

Dado que algumas das categorias possuíam um número muito baixo de observações, na sequência buscou-se reduzir seu número pela utilização de modelagem de tópico (Chen & Yang, 2016). A melhor diferenciação foi obtida usando seis tópicos, que correspondem a uma aproximação das classificações utilizadas e a agregação em "Outros" do que não se encaixava nas demais categorias.

Para iniciar a análise estatística, foram removidas as palavras mais comuns na língua portuguesa (*stop words*), acentos e caracteres especiais, e mantidos apenas os radicais das palavras remanescentes (*stemming*). Com base nos novos textos, foram realizadas análises descritivas para identificar possíveis termos comuns a diversas categorias que não possuíam significado substantivo, que também foram removidos.

Como a amostra contava com um número reduzido de respostas, a análise demandou mais cuidado para que o modelo não fosse sobreajustado – ou seja, que aprendesse muito somente sobre as respostas classificadas manualmente e não generalizasse para as demais respostas. Para isso, foi aplicado um modelo que identifica o parâmetro com melhor desempenho na classificação a partir de um processo de validação cruzada[2]. Assim, em um processo que aumentava a confiabilidade do modelo nos dados de treinamento, as 500 respostas da amostra foram divididas em cinco grupos de forma aleatória, com quatro grupos sendo utilizados como dados de treinamento e um como teste. O processo ainda foi repetido por dez vezes, sendo que em cada repetição a distribuição aleatória dos grupos era diferente.

A partir do modelo ajustado, a técnica foi aplicada para classificação de todas as respostas obtidas na pesquisa. Em uma primeira etapa, calculou-se a estimativa pontual para as proporções de cada categoria, ajustando seus respectivos pesos dentro do conjunto de respostas. Na sequência, para estimar os intervalos de confiança, foram utilizadas 200 diferentes subamostras em um processo de *bootstrap*, um método de *reamostragem*, com os pesos atualizados para cada uma delas (Efron, 1979).

O exercício de categorização das respostas abertas gerou seis categorias: "Liberdade", "Individualidade", "Proteção de dados", "Controle", "Segurança" e "Outras".[3]

[2] Modelos Lasso hiperparametrizados. Ver Bertrand *et al*. (2020) e Šehić *et al*. (2021).

[3] As categorias "Não respondeu", "Segurança", "Controle" e "Proteção de dados" não tiveram grande variação no *bootstrap*, gerando menores intervalos de confiança e estimativas pontuais próximas à mediana. Já as categorias "Outras", "Individualidade" e "Liberdade" tiveram variabilidade maior no processo, com intervalos de confiança bastante amplos. No entanto, as estimativas pontuais das duas primeiras ficaram próximas à mediana, diferentemente de "Liberdade", que ficou bem superior à mediana de sua distribuição. Essa maior variação pode ter duas explicações distintas. Na primeira, a categoria "Outras" é bastante heterogênea, contando com respostas que não constituíam agrupamentos relevantes para desagregação. Já a segunda está relacionada às categorias "Individualidade" e "Liberdade", que, em muitos momentos, possuíam distinções bastante sutis mesmo para a classificação manual.

Práticas

A segunda dimensão investigada busca entender o que os usuários de Internet fazem para proteger seus dados pessoais, quais cuidados tomam no uso cotidiano da rede e das plataformas e como procedem caso tenham algum problema relacionado a esse tema. O conjunto de atividades investigadas compõe diversas decisões que os usuários têm de tomar quando estão *online*, como dar consentimento ao tratamento de dados para publicidade ou configurar as permissões de *cookies* ao visitar um *website*.

Entre as atividades realizadas para gerenciar o acesso a seus dados pessoais (Gráfico 2), a que foi reportada pelos usuários de Internet com 16 anos ou mais em maior proporção foi a verificação de segurança de página ou aplicativo (70%), como a verificação do cadeado de segurança do navegador[4]. A proporção foi menor entre aqueles que acessaram a Internet exclusivamente pelo telefone celular (59%). Isso seria de certa forma esperado, visto que se trata de um elemento muitas vezes suprimido ou com menor visibilidade para o usuário na interface dos aplicativos de dispositivos móveis.[5]

Entre as práticas mais realizadas também estavam a recusa de permissão de uso de seus dados para publicidade personalizada (69%) e a leitura de políticas de privacidade de páginas ou aplicativos (68%).

Entre as atividades menos mencionadas, constaram configurar ou limitar o uso de *cookies* (58%) e solicitar exclusão de dados junto a agentes de tratamento de dados, como páginas (*websites*), aplicativos ou buscadores (42%). Cabe lembrar que a solicitação de exclusão de dados é também a prática que requer uma ação mais proativa por parte dos indivíduos, uma vez que o usuário deve contatar diretamente o controlador das informações. Por ser também um direito previsto na LGPD (art. 18, inciso VI) ainda pouco difundido no país, é possível que grande parte dos usuários desconheça essa possibilidade.

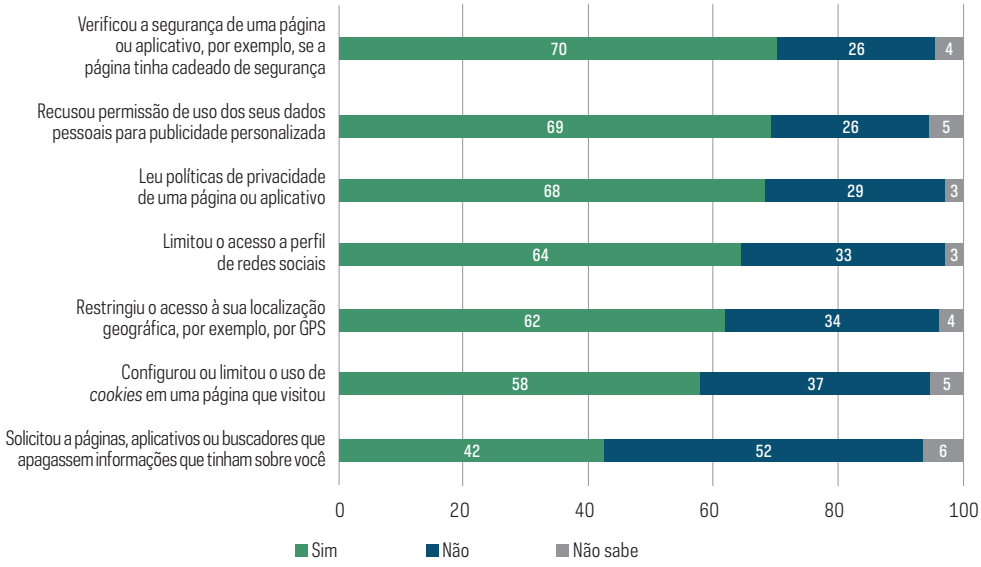
[4] Tal aspecto surge com frequência em entrevistas cognitivas realizadas para testes de questionário das pesquisas TIC Domicílios e TIC Kids Online Brasil como indicativo da segurança de um *website*, relevante na percepção do usuário de que seus dados estão protegidos contra invasão ou roubo por terceiros.

[5] Devido ao tamanho mais limitado de tela em dispositivos móveis, *apps* de navegação, como Chrome ou Firefox, ocultam a barra de endereço (onde aparecem os elementos visuais relacionados ao certificado de segurança) quando a tela é rolada. Quando o acesso à Web acontece por outras categorias de aplicativos, como de comércio eletrônico, muitas vezes esse tipo de informação não chega a ser disponibilizada ao usuário.

GRÁFICO 2

PRÁTICAS DE GERENCIAMENTO DE ACESSO A DADOS PESSOAIS (2021)

Total de usuários de Internet com 16 anos ou mais (%)



A busca por canais de atendimento para solicitações, reclamações ou denúncias foi realizada por 24% dos usuários de Internet com 16 anos ou mais (Gráfico 3). Entre os que buscaram, o canal mais mencionado foi a própria empresa ou órgão público controlador do dado (80%). A maioria dos usuários busca resolver sua demanda diretamente com a organização controladora dos dados — como a empresa, plataforma ou aplicativo que registra e detém os dados referentes à solicitação. Isso reforça para organizações controladoras de dados a importância de estabelecerem procedimentos efetivos para receber e solucionar esse tipo de demanda.

Em menores proporções são mencionados órgãos de defesa do consumidor, como o Procon (48%), ou a Justiça, como Juizado Especial Cível (28%). A Autoridade Nacional de Proteção de Dados (ANPD)[6] aparece em um patamar inferior (27%).[7]

[6] A ANPD mantém um canal em seu *website* para denúncias de descumprimento da LGPD: https://www.gov.br/anpd/pt-br/canais_atendimento/cidadao-titular-de-dados/denuncia-de-descumprimento-da-lgpd

[7] A busca por canais de atendimento para solicitações, reclamações ou denúncias pode ser entendida por respondentes como um conjunto amplo de ações, desde a busca por informações a respeito de direitos e procedimentos até a realização de serviços interativos, como o registro de reclamações ou a abertura de processos administrativos ou judiciais. Essa percepção é corroborada pela experiência do Cetic.br com a coleta de indicadores sobre serviços de governo eletrônico nas pesquisas TIC Domicílios e TIC Governo Eletrônico, cujos resultados mostram que uma parcela relevante dos usuários de serviços de governo eletrônico apenas consulta informações oficiais (diretamente nos *websites* governamentais ou via mecanismos de busca).

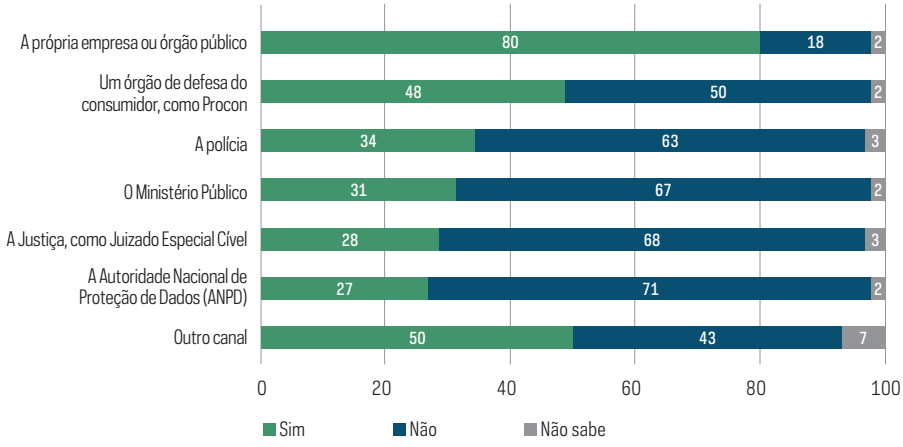
Já entre os que não buscaram canais de atendimento para solicitações, reclamações ou denúncias, os canais mais mencionados em caso de necessidade futura seriam o Procon (79%), seguido da empresa ou órgão público controlador do dado (74%), a polícia (65%) e a ANPD (62%).

Os dados indicam, assim, que os órgãos de defesa do consumidor, fortalecidos pelo Código de Defesa do Consumidor desde a década de 1990, estão mais presentes no repertório dos usuários. Portanto, os titulares vinculam, em maiores proporções, suas reclamações ou solicitações a uma relação de consumo, ou até mesmo a um crime, denunciando junto às autoridades policiais.

GRÁFICO 3

CANAL DE ATENDIMENTO QUE BUSCARAM SOBRE SEUS DADOS PESSOAIS (2021)

Total de usuários de Internet com 16 anos ou mais que buscaram algum canal de atendimento sobre seus dados pessoais (%)



Riscos

Os resultados da pesquisa apontam que os níveis de preocupação com dados pessoais dos usuários de Internet são maiores em relação a prejuízos financeiros, fraudes bancárias e golpes do que em relação a outros tipos de riscos, como aqueles relacionados à reputação ou discriminação. Isso revela maior familiaridade com a existência de ameaças e prejuízos financeiros no ambiente digital, além de apontar para o elevado potencial de dano que esse tipo de risco representa aos usuários.[8]

[8] Tendência observada anteriormente na 2ª edição da pesquisa Painel TIC (CGI.br, 2020b).

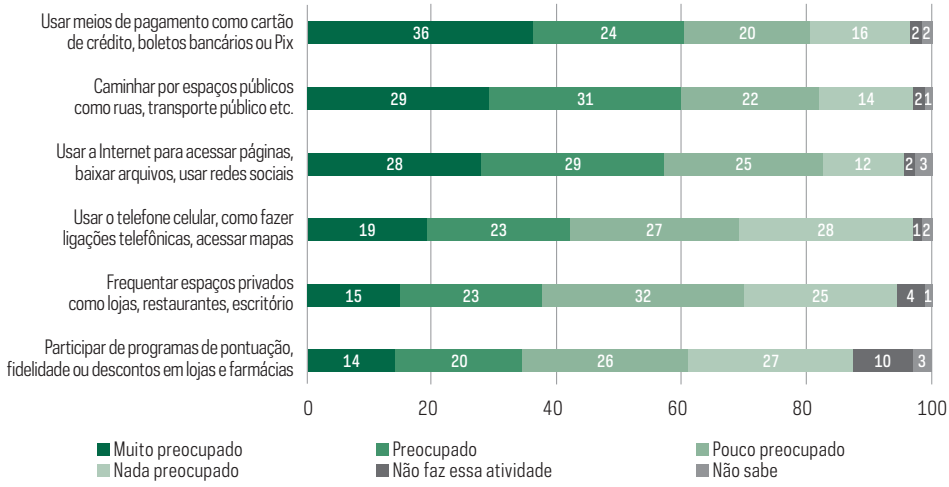
Entre os níveis de preocupação com o registro de dados de atividades, incluindo daquelas que ocorrem fora do ambiente *online*[9], 36% dos usuários de Internet de 16 anos ou mais afirmaram estar muito preocupados e 24% preocupados quando usam meios de pagamento como cartão de crédito, boletos bancários ou Pix (Gráfico 4). Outras atividades investigadas que apresentaram maior patamar de preocupação com seu registro foram: caminhar por espaços públicos ou usar transporte público (29% muito preocupados e 31% preocupados) e usar a Internet para acessar páginas, baixar arquivos ou usar redes sociais (28% muito preocupados e 29% preocupados).

O indicador revela que a preocupação com o registro de dados estende-se para além das atividades realizadas pelos usuários na Internet, uma vez que as categorias mais mencionadas estão relacionadas a registros de pagamentos (dados bancários, CPF, endereço, entre outros) e no espaço público (registros de câmeras de segurança, uso de transporte público, entre outros).

GRÁFICO 4

NÍVEL DE PREOCUPAÇÃO COM REGISTROS DE ATIVIDADES SEGUNDO TIPO DE REGISTRO (2021)

Total de usuários de Internet com 16 anos ou mais (%)



Os registros de dados que ocorrem durante o uso da Internet também geram preocupação na maioria dos usuários de Internet. Especificamente em relação às atividades realizadas *online* (Gráfico 5), o nível de preocupação mais elevado foi identificado no momento de comprar pela Internet por páginas e aplicativos (42% muito preocupados e 25% preocupados), seguido de acessar páginas e aplicativos de bancos (35% muito preocupados e 24% preocupados). Cabe ressaltar também que usar aplicativos de relacionamento, a despeito de ser a atividade com a maior proporção

[9] Texto apresentado aos respondentes antes da pergunta sobre preocupação com registros de dados: "Hoje em dia, muitas das nossas atividades são registradas de diversas formas, tanto na Internet, como histórico de páginas acessadas ou *posts* em redes sociais, quanto fora dela, como quando pagamos com cartão ou somos filmados por câmeras de vigilância".

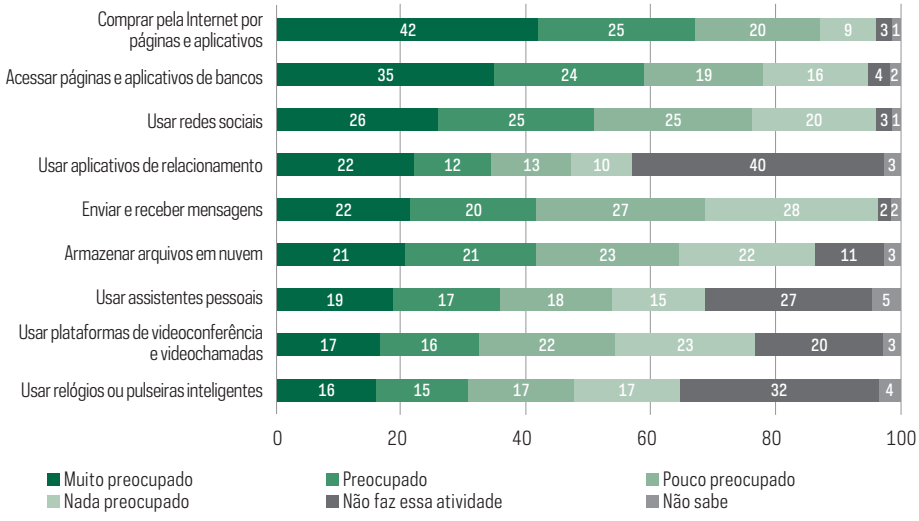
de respondentes que indicaram não realizar[10], foi a terceira com maior proporção de usuários preocupados (12%) ou muito preocupados (22%), considerando apenas os que realizam as atividades investigadas.

Esses resultados reforçam, mais uma vez, a avaliação dos usuários de que o risco relacionado a dados de transações e pagamentos tem maior potencial de dano. Também revela a preocupação dos usuários com o tratamento de seus dados em outras atividades, como uso de aplicativos de relacionamento, até então pouco explorado em outros estudos. Importante destacar que mais da metade dos usuários está muito preocupada (26%) ou preocupada (25%) com o uso de redes sociais.[11]

GRÁFICO 5

NÍVEL DE PREOCUPAÇÃO COM DADOS PESSOAIS SEGUNDO ATIVIDADE REALIZADA NA INTERNET (2021)

Total de usuários de Internet com 16 anos ou mais (%)



Os governos armazenam e tratam grande quantidade de dados pessoais dos cidadãos no desempenho de suas atividades regulares, como segurança, identificação, tributação e prestação de serviços públicos. Nesse contexto, 40% dos usuários de Internet declaram estar muito preocupados e 29% preocupados com o uso que o poder público faz de seus dados. O nível de preocupação varia um pouco quando comparado a outro

[10] É relevante mencionar que a medida de percepção subjetiva reflete a visão do respondente e a forma como se posiciona em relação a um conceito ou tema e não representa o volume de pessoas que adotam determinada prática ou realizam determinada atividade. Por exemplo, não se imagina que as pessoas que afirmam seu nível de preocupação ou sua percepção de controle sobre cada atividade sejam efetivamente pessoas que realizam essas atividades.

[11] Segundo a pesquisa TIC Domicílios 2021 (CGI.br, no prelo), as redes sociais são um dos tipos de plataforma em que os usuários de Internet brasileiros estão mais presentes e conta com maiores proporções de uso nas mais variadas faixas etárias e classes (81% dos usuários de Internet usaram redes sociais).

indicador sobre o uso feito por empresas: 47% declararam estar muito preocupados e 28% preocupados.

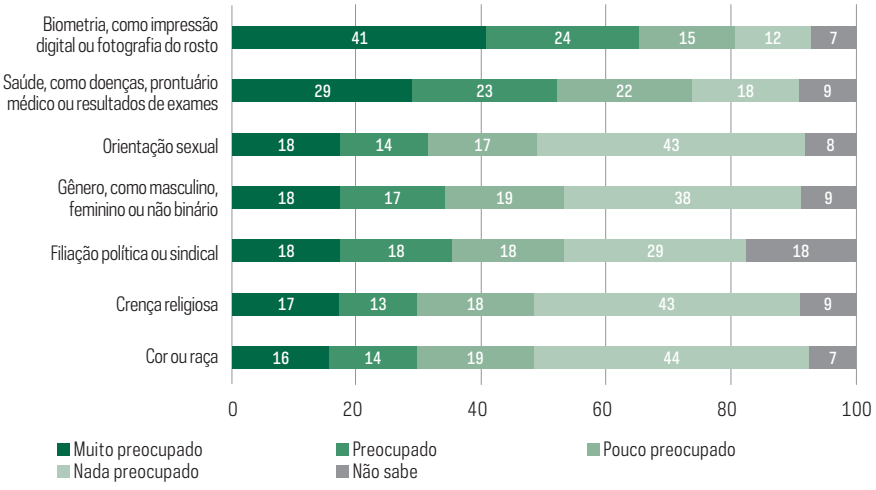
É possível observar uma diferença no nível de preocupação sobre o uso de dados pessoais feito pelas empresas pelo recorte de cor ou raça do respondente. Pretos (52%) e pardos (49%) declararam estar muito preocupados em uma proporção maior do que brancos (43%), o que sugere uma percepção de uso discriminatório desses dados. Quando esse uso é feito por governos, há maior preocupação entre os pretos (47% declaram estar muito preocupados), enquanto esse percentual é inferior entre pardos (41%) e brancos (37%).

Quanto aos dados sensíveis, os usuários de Internet declararam maior nível de preocupação com o fornecimento de dados biométricos, superando o que ocorre com os demais tipos de dados pessoais investigados: 41% disseram estar muito preocupados e 24% preocupados (Gráfico 6). O avanço da biometria em diversos contextos da vida cotidiana, aliado à natureza íntima, tangível e material desse dado e seu elevado potencial de dano em caso de comprometimento ajudam a explicar esses resultados. Cabe lembrar que o uso de dados biométricos em eleições foi testado inicialmente no pleito de 2008, contava com cerca de 120 milhões de biometrias cadastradas em 2020 e pretende alcançar a totalidade dos eleitores até 2026[12]. Também já se pode observar o uso da biometria pelo setor privado em bancos, farmácias, academias de ginástica e condomínios fechados.[13]

GRÁFICO 6

NÍVEL DE PREOCUPAÇÃO COM FORNECIMENTO DE INFORMAÇÕES PESSOAIS SENSÍVEIS (2021)

Total de usuários de Internet com 16 anos ou mais (%)



[12] Para informações sobre a implantação da biometria pelo TSE, ver https://www.tse.jus.br/eleitor/biometria/biometria

[13] Ver questionamento sobre coleta de dados biométricos pelo Instituto Brasileiro de Defesa do Consumidor (Idec) (https://idec.org.br/release/idec-questiona-coleta-de-impressao-digital-em-farmacias) e campanha contra o uso de reconhecimento facial (https://tiremeurostodasuamira.org.br/).

Outra categoria que se destaca é a dos dados de saúde: 29% dos respondentes declararam estar muito preocupados e 23% preocupados. Segundo a LGPD, os dados pessoais relacionados à condição de saúde, além dos que revelam orientação sexual, convicção religiosa, opinião política, raça e dados genéticos ou biométricos, entre outros, são caracterizados como dados pessoais sensíveis, visto que sua utilização inadequada pode permitir identificação e causar situações de discriminação (Botelho & Camargo, 2021). Isso ressalta a importância de se levar em conta o contexto de vulnerabilidade dos titulares e os potenciais efeitos e riscos no tratamento desse tipo de dado (Costa, 2022).

A natureza sensível desses dados está no fato de que sua utilização inadequada pode ocasionar prejuízos a direitos fundamentais das pessoas, especialmente os relacionados a privacidade, intimidade, igualdade e dignidade da pessoa humana (Bioni, 2019). Portanto, essa maior preocupação com dados de saúde pode estar relacionada ao fato de eles possuírem um potencial invasivo na esfera da privacidade e da intimidade muito maior do que um dado pessoal comum. Nesse sentido, os efeitos discriminatórios não estão no dado em si, mas nos usos que são feitos dele (Doneda, 2019).

Os riscos no uso de dados pessoais percebidos pelos usuários de Internet com 16 anos ou mais estão mais associados a prejuízos financeiros, fraudes bancárias e vazamento ou roubo de dados (87%)[14]. Outros riscos, como de reputação (74%), discriminação (65%) ou recebimento de propaganda indesejada (60%), são bastante mencionados, porém em um patamar inferior. Interessante observar que, entre os que se declaram pretos, a percepção de risco de discriminação foi superior à média (72%).

Controle

Apesar de terem manifestado preocupação quanto aos riscos relacionados ao uso de seus dados pessoais, os usuários de Internet com 16 anos ou mais também relataram ter muito controle sobre o acesso de terceiros e o uso que as organizações controladoras fazem de seus dados.

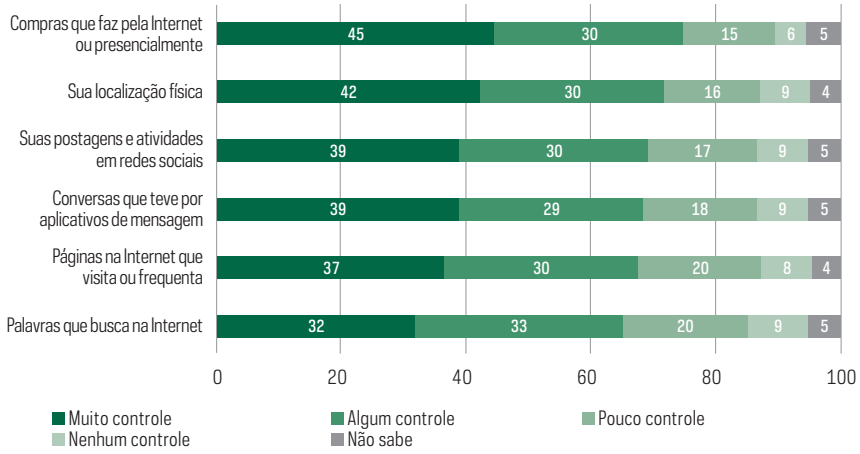
Dos usuários de Internet com 16 anos ou mais, 45% afirmam possuir muito controle sobre quem pode acessar dados pessoais de compras feitas pela Internet ou presenciais e 42% afirmaram possuir muito controle sobre dados relacionados à localização física (Gráfico 7). Entre os tipos de informações pesquisados, o que alcançou menor percepção de controle foram as palavras buscadas na Internet: 32% acreditavam ter muito controle e 29% acreditavam ter pouco ou nenhum controle.

[14] A ANPD e o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), departamento do Núcleo de Informação e Coordenação do Ponto BR (NIC.br), produziram um fascículo sobre vazamento de dados contendo ações de prevenção e informações sobre como proceder em caso de ocorrências (ANPD & NIC.br, 2021a).

GRÁFICO 7

NÍVEL DE CONTROLE PERCEBIDO SOBRE QUEM PODE ACESSAR DADOS, SEGUNDO TIPO DE INFORMAÇÃO (2021)

Total de usuários de Internet com 16 anos ou mais (%)



A maioria dos usuários afirmou ter muito ou algum controle sobre todos os itens pesquisados. Essa sensação de controle pode estar relacionada com a possibilidade de fazer escolhas nas configurações de privacidade de plataformas e redes sociais. Também pode ser entendida como um desconhecimento a respeito de práticas de compartilhamento dos registros e dados pessoais entre empresas, conforme explicitado nas suas políticas de privacidade. Essa última hipótese é corroborada pela baixa proporção dos que realizam leitura integral das políticas de privacidade, como será detalhado a seguir.

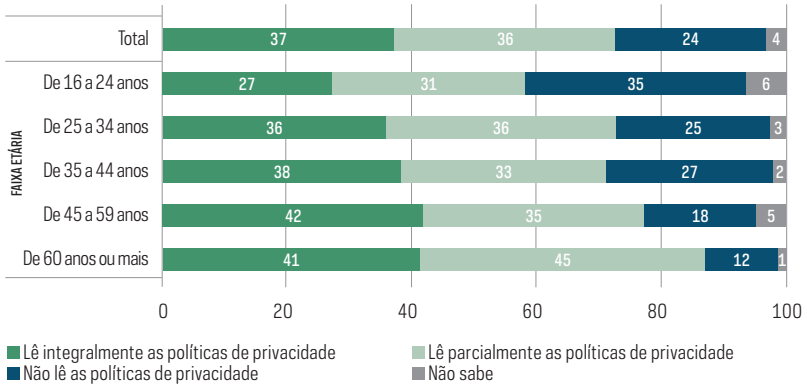
Diante dos avanços na legislação acerca da coleta, tratamento e uso dos dados pessoais dos visitantes e usuários, os *websites* e as plataformas passaram a solicitar o aceite de políticas de privacidade, bem como a configuração de *cookies*. Na maior parte dos casos, é necessário consentir com as políticas para poder acessar o conteúdo ou serviço. No entanto, muitos usuários afirmaram que não realizam a leitura integral desses documentos: 37% dos usuários de Internet com 16 anos ou mais afirmaram ler os termos de políticas de privacidade integralmente, enquanto 36% afirmaram ler parcialmente e 24% afirmaram não realizar a leitura (Gráfico 8).[15]

[15] Apesar da exigência do consentimento explícito do usuário, em alguns casos só sendo possível prosseguir após a rolagem até o final do texto do documento, dados de *Web analytics* e experimentos curiosos — incluindo cláusulas obrigando o usuário a "ceder seu primogênito à empresa por toda a eternidade" ou oferecendo prêmios em dinheiro — mostram que esse número pode ser ainda menor na prática. Ver Kon (s.d.) e Obar e Oeldorf-Hirsch (2018).

GRÁFICO 8

LEITURA DE POLÍTICAS DE PRIVACIDADE DE PÁGINAS OU APLICATIVOS (2021)

Total de usuários de Internet com 16 anos ou mais (%)



Esse indicador apresenta uma variação relevante no comportamento por faixa etária. Os usuários entre 16 e 24 anos relataram ler integralmente as políticas de privacidade (27%) em proporção abaixo da média, além de afirmarem não as ler em proporção acima da média (35%).

Entre os usuários de Internet de 16 anos ou mais que não leem ou que leem parcialmente as políticas de privacidade, os motivos mais mencionados para não ler integralmente foram por serem muito longas (81%) e difíceis de entender (69%).

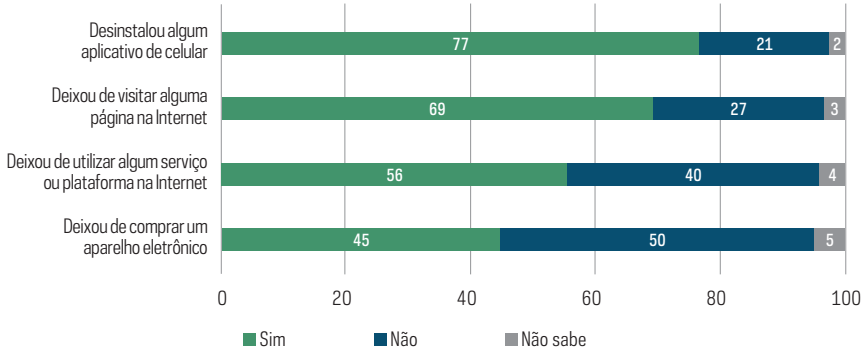
Motivados pela preocupação com o uso de seus dados pessoais, 77% dos usuários de Internet de 16 anos ou mais já desinstalaram aplicativos, 69% deixaram de visitar algum *website*, 56% deixaram de utilizar algum serviço na Internet e 45% deixaram de comprar algum equipamento eletrônico (Gráfico 9). A escolha por adotar alguma restrição no uso reforça a percepção de riscos apresentada anteriormente. Ainda que a pesquisa não tenha investigado a frequência ou a intensidade desse comportamento autorrestritivo, é possível afirmar que a preocupação com o tratamento de dados pessoais orienta as decisões da maior parte dos usuários em algum momento.[16]

[16] A ANPD e o CERT.br, departamento do NIC.br, produziram um documento contendo ações para fortalecer a proteção de dados pessoais, reduzindo os riscos de vazamentos e roubos. Entre as ações propostas estão a realização regular de *backups*, a criação de pastas criptografadas, o uso de senhas fortes, a instalação de aplicativos somente de origem conhecida e a atualização de sistemas (ANPD & NIC.br, 2021b).

GRÁFICO 9

ATIVIDADES QUE DEIXOU DE REALIZAR POR PREOCUPAÇÕES COM DADOS PESSOAIS (2021)

Total de usuários de Internet com 16 anos ou mais (%)



Modelo de negócio

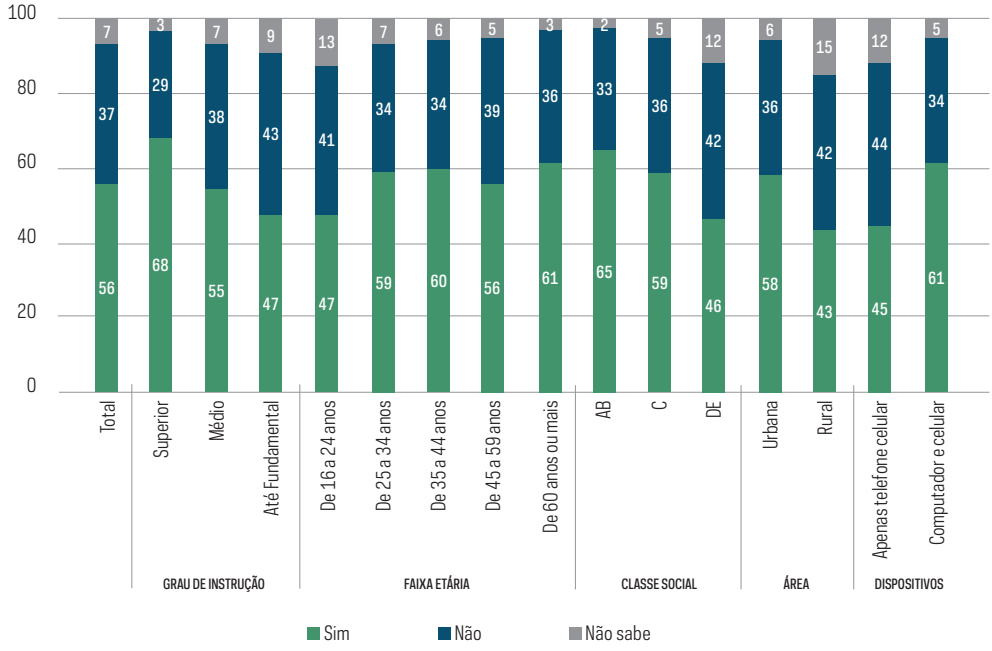
Após serem apresentados a uma explicação sobre a prática de perfilamento (*profiling*)[17], 56% dos usuários de Internet afirmaram já ter ouvido falar a respeito dessa prática. Esse indicador apresenta variações relevantes por diversas variáveis de cruzamento (Gráfico 10). Entre os indivíduos com grau de instrução até o Ensino Fundamental, 47% afirmaram conhecer o conceito. Já entre os com Ensino Superior, 68% responderam afirmativamente. Uma menor proporção dos indivíduos de 16 a 24 anos declararam conhecer o conceito (47%). O conhecimento sobre tais práticas também é menor nas classes DE (46%), entre os usuários da área rural (43%) e entre indivíduos que acessam a rede exclusivamente pelo telefone celular (45%).

[17] Texto apresentado aos respondentes antes das perguntas sobre perfilamento: "Hoje em dia é possível combinar dados das pessoas a partir de diversas fontes, como dados de compras e pagamentos, hábitos de busca e navegação na Internet, páginas curtidas em redes sociais, entre outras. Essa combinação cria perfis detalhados dos hábitos, interesses e características das pessoas. Empresas podem usar esses perfis para oferecer publicidade personalizada e direcionada ou para avaliar riscos de ter esses perfis como clientes".

GRÁFICO 10

CONHECIMENTO SOBRE PERFILAMENTO E PUBLICIDADE PERSONALIZADA (2021)

Total de usuários de Internet com 16 anos ou mais (%)



Entre os que conhecem o conceito, 46% afirmaram visualizar publicidade personalizada muitas vezes, 21% afirmaram ver algumas vezes, 7% poucas vezes e 23% disseram não ter visto. Além das variáveis que foram relevantes para o indicador de conhecimento do conceito, também é interessante a diferença observada por sexo: entre os homens, 51% viram publicidade personalizada muitas vezes e 17% não viram. Já entre as mulheres, 43% viram muitas vezes e 27% não viram.[18]

O perfilamento dos usuários é parte importante dos modelos de negócios de Internet de muitas empresas, tanto de tecnologia quanto de outros setores, e está no centro de muitos debates e esforços regulatórios sobre privacidade. O desconhecimento dessa prática por 37% dos usuários de Internet indica que ela não informa o processo de tomada de decisão nas atividades *online* de parcela considerável dos usuários, seja no sentido de evitar condutas que aumentem a exposição a riscos ou de adotar medidas que ajudem a mitigá-los, independentemente da preocupação manifestada com o tema ou das habilidades digitais necessárias para fazê-lo.

[18] A pesquisa TIC Empresas 2019 mostrou que 36% das empresas brasileiras pagaram por anúncios na Internet. Ainda que não haja diferenças entre os portes das empresas, a pesquisa indica que os anúncios são mais presentes nas empresas dos setores de alojamento e alimentação (50%) e informação e comunicação (46%) (CGI.br, 2020a).

Considerações finais: agenda para políticas públicas

Essa pesquisa representou é um esforço inédito de investigação sobre o tema da privacidade e proteção de dados pessoais entre usuários de Internet. Os resultados revelam práticas e percepções por parte dos usuários acerca do tema em um momento oportuno, dada a recente entrada em vigor da LGPD e a também recente criação da ANPD.

A pesquisa aponta a prevalência de uma percepção sobre o conceito de privacidade associada à liberdade e à individualidade, com menor presença das visões que relacionam o tema diretamente à proteção de dados e ao controle sobre quem pode acessá-los. Os resultados da pesquisa também apontam uma maior percepção de riscos associada a prejuízos financeiros, como é o caso das fraudes bancárias ou do uso de identidade para aplicar golpes. Isso sugere a necessidade de se reforçar a confiança no ambiente virtual como um todo, especialmente no que tange às transações financeiras e ao comércio eletrônico.

Também é relevante a preocupação com roubos e compartilhamento de informações com terceiros sem a devida autorização. Além de estabelecer políticas de privacidade e mecanismos de proteção de dados que assegurem aos titulares uma gestão de dados transparente e responsável, também é fundamental que as organizações controladoras de dados implementem práticas e procedimentos de proteção efetiva dos dados dos seus usuários.

Além disso, do modo como são apresentadas atualmente, as políticas de privacidade ainda não são apropriadas pela maior parte dos usuários, embora, com frequência, aceitá-las seja uma condição para acesso ao serviço, aplicativo ou conteúdo. Isso fica evidenciado pela declaração dos usuários que não leem as políticas de que elas são muito longas e difíceis de entender. Nesse sentido, são relevantes as estratégias que envolvem a simplificação da apresentação das políticas aos usuários, usando linguagem clara e concisa, destacando no início os principais pontos e evitando jargões técnicos, para que os usuários possam tomar decisões informadas.

Não menos importante são outras questões apontadas nos resultados, como a preocupação com o uso de dados biométricos, dados de saúde e os riscos de discriminação e de reputação. Apesar de mencionados em patamares inferiores às questões financeiras, são temas que já fazem parte da rotina dos usuários.

Os dados biométricos foram os mais mencionados entre as categorias pesquisadas como tipo de informação que preocupa os usuários de Internet, o que também demanda uma reflexão por parte de organizações públicas e privadas sobre a sua coleta. Também é importante ressaltar a diferença nos resultados em relação aos temas de discriminação entre os que se autodeclararam pretos ou pardos, o que reflete a demanda por estratégias específicas de enfrentamento de práticas discriminatórias que levem em conta marcadores sociais como cor ou raça.

Em suma, os resultados representam uma linha de base para o acompanhamento do tema no país e ajudam a reforçar a importância de aprofundar o debate público em prol de uma cultura de proteção de dados.

Referências

Autoridade Nacional de Proteção de Dados & Núcleo de Informação e Coordenação do Ponto BR. (2021a). *Cartilha de segurança para Internet: fascículo vazamento de dados*. https://cartilha.cert.br/fasciculos/vazamento-de-dados/fasciculo-vazamento-de-dados.pdf

Autoridade Nacional de Proteção de Dados & Núcleo de Informação e Coordenação do Ponto BR. (2021b). *Cartilha de segurança para Internet: fascículo proteção de dados*. https://cartilha.cert.br/fasciculos/protecao-de-dados/fasciculo-protecao-de-dados.pdf

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

Barth, S. & de Jong, M. D. T. (2017). The privacy paradox: Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics, 34*(7), 1038-1058. https://doi.org/10.1016/j.tele.2017.04.013

Bertrand, Q., Klopfenstein, Q., Blondel, M., Vaiter, S., Gramfort, A., & Salmon, J. (2020). Implicit differentiation of Lasso-type models for hyperparameter optimization. *Proceedings of Machine Learning Research, 119*, 810-821.

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

Botelho, M. C., & Camargo, E. P. do A. (2021). A aplicação da Lei Geral de Proteção de Dados na saúde. *Revista de Direito Sanitário, 21*(e0021). https://doi.org/10.11606/issn.2316-9044.rdisan.2021.168023

Carrière-Swallow, Y., & Haksar, V. (2019). *The Economics and Implications of Data: An Integrated Perspective* (IMF Departmental Paper Series No. 19/16). https://doi.org/10.5089/9781513511436.087

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

Cisco. (2021). *Cisco 2021 Consumer Privacy Survey: Building Consumer Confidence Through Transparency and Control*. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-cybersecurity-series-2021-cps.pdf

Comitê Gestor da Internet no Brasil. (no prelo). *Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros: TIC Domicílios 2021*.

Comitê Gestor da Internet no Brasil. (2020a). *Pesquisa sobre o uso das tecnologias de informação e comunicação nas empresas brasileiras: TIC Empresas 2019*. https://cetic.br/pt/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-nas-empresas-brasileiras-tic-empresas-2019/

Comitê Gestor da Internet no Brasil. (2020b). *Painel TIC COVID-19: Pesquisa sobre o uso da Internet no Brasil durante a pandemia do novo coronavírus — 2ª edição: Serviços públicos online, telessaúde e privacidade*. https://www.cetic.br/pt/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/

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

Costa, R. (2022). Personalidade Hackeada: considerações sobre proteção de dados pessoais sensíveis, vigilância digital e discriminação. In C. Teffé & S. Branco (Coords.), *Proteção de dados e tecnologia: estudos da pós-graduação em Direito Digital* (pp. 52-78). Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS); Obliq.

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

Efron, B. (1979). Bootstrap Methods: Another Look at the Jackknife. *The Annals of Statistics, 7*(1), 1-26. https://doi.org/10.1214/aos/1176344552

Kon, G. (s.d.). *Does anyone read privacy notices? The facts.* https://www.linklaters.com/en/insights/blogs/digilinks/does-anyone-read-privacy-notices-the-facts

Obar, J. A., & Oeldorf-Hirsc, A. (2018). The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services. *Information, Communication & Society*. https://ssrn.com/abstract=2757465

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

Šehić, K., Gramfort, A., Salmon, J., & Nardi, L. (2021). *LassoBench: A high-dimensional hyperparameter optimization benchmark suite for lasso*. ArXiv. https://doi.org/10.48550/arXiv.2111.02790

Análise dos Resultados
Privacidade e Proteção de Dados Pessoais 2021
Empresas

Atualmente, os dados são um recurso indispensável para a melhoria do desempenho de organizações do setor privado. A capacidade de coleta, armazenamento e análise de dados confere às empresas a possibilidade de planejamento e avaliação de suas atividades, uma vez que permite o uso de informações detalhadas sobre o comportamento e as demandas dos usuários ou clientes dos mais diversos serviços. Inúmeros organismos internacionais reconhecem os dados como um dos mais valiosos insumos da economia atual, destacando seu impacto econômico nas diversas transações (Conferência das Nações Unidas sobre Comércio e Desenvolvimento [UNCTAD], 2021). Há, entretanto, crescentes preocupações quanto à necessidade de colaboração multissetorial para a promoção da regulação e do uso responsável das informações pessoais (Internet & Jurisdiction Policy Network, 2021).

Em 2021, 145 países dispunham de leis sobre privacidade e proteção de dados pessoais, evidenciando uma preocupação global quanto à regulação do tema (Greenleaf, 2021). A aprovação de leis que impõem um crescente controle ao tratamento de dados pessoais vem colocando desafios às empresas de todo o mundo, na medida em que rotinas estabelecidas devem ser alteradas e o fortalecimento de uma cultura de proteção de dados precisa ser fomentada, ao mesmo tempo que investimentos devem ser direcionados à melhoria da segurança digital.[1]

No contexto brasileiro, iniciou-se uma ampla discussão no setor empresarial sobre a adequação à Lei Geral de Proteção de Dados Pessoais (LGPD) e seus impactos desde que entrou em vigor, em setembro de 2020. Posto que as empresas realizam o tratamento de dados pessoais, seja de clientes, funcionários ou mesmo de terceiros, a vigência da lei trouxe inúmeros desafios e oportunidades para o setor produtivo.

[1] Dificuldades semelhantes foram relatadas para que as empresas europeias buscassem se adequar ao Regulamento Geral sobre a Proteção de Dados (*General Data Protection Regulation* [GDPR]). Em um momento inicial, diversas empresas fizeram uso de medidas paliativas para adequação, sendo que muitos desafios ainda são persistentes, tais como relatórios de impacto e auditorias, que são pouco presentes (Mikkelsen *et al.*, 2019).

Com o objetivo de compreender como pequenas, médias e grandes empresas tratam os dados pessoais de seus clientes, funcionários, fornecedores e parceiros, bem como mapear as questões relevantes associadas à implementação da LGPD no Brasil, o Cetic.br|NIC.br criou, ao longo de 2021, um módulo específico para a produção de indicadores sobre o tema. Implementado como parte do esforço de campo da pesquisa TIC Empresas 2021, os indicadores trazem um panorama amplo de práticas e mudanças organizacionais impulsionadas por esse momento inicial de aplicação da LGPD pela autoridade competente[2] e sua adequação entre as empresas brasileiras.

O novo módulo, desenvolvido com a contribuição de diversos especialistas no tema, destaca as principais práticas que as empresas estão realizando para que os dados pessoais sejam tratados de forma segura e em conformidade com a lei — embora muitos dos aspectos sobre a devida adequação à LGPD e entendimentos sobre o seu escopo ainda sejam alvo de intenso debate, alguns inclusive carecendo de regulamentação para que produzam a integralidade de seus efeitos.[3]

No presente relatório, os dados do módulo de privacidade e proteção de dados pessoais serão apresentados em quatro dimensões:

- **Guarda de dados pessoais e finalidade de uso:** indicadores sobre os tipos de dados pessoais que as empresas mantêm e para qual objetivo são utilizados;
- **Desenvolvimento de capacidades internas:** indicadores sobre ações para a sensibilização da equipe interna das empresas sobre o tema de privacidade e proteção de dados pessoais;
- **Adequação à LGPD:** indicadores sobre ações que visam à conformidade com a lei, bem como atitudes que buscam fortalecer boas práticas de tratamento de dados pessoais na empresa;
- **Barreiras e oportunidades:** indicadores sobre as percepções de dificuldades para adequação à LGPD e opiniões sobre possibilidades para a atuação da empresa.

[2] No marco da LGPD, foi criada a Autoridade Nacional de Proteção de Dados (ANPD), responsável pela implementação e aplicação da lei, como órgão da administração pública federal vinculado à Presidência da República. A natureza da Autoridade foi alterada para "autarquia de natureza especial, dotada de autonomia técnica e decisória, com patrimônio próprio e com sede e foro no Distrito Federal", pela Medida Provisória n. 1.124, de 2022.

[3] Um dos exemplos desse momento de definições sobre a aplicação da LGPD é o entendimento sobre as assimetrias regulatórias a micro e pequenas empresas. A ANPD definiu regras especiais para a adequação da lei em agentes de pequeno porte na resolução CD/ANPD n. 2, de 27 de janeiro de 2022, compreendendo empresas com faturamento de até R$ 4.800.000,00, *start-ups* e microempreendedores individuais com renda anual de até R$ 360.000,00. Disponível em https://in.gov.br/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019

Guarda de dados pessoais e finalidade de uso

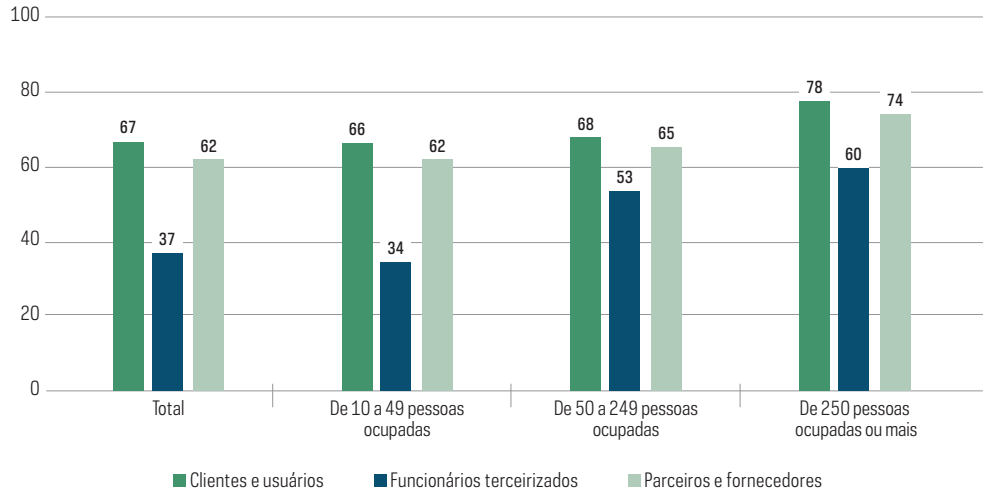
O objetivo desta seção é averiguar os tipos de dados pessoais que as empresas mantêm e para qual finalidade são utilizados. De acordo com o Artigo 5º da LGPD, um dado pessoal é "uma informação relacionada a pessoa natural identificada ou identificável". Portanto, a lei versa sobre o tratamento[4] dentro das organizações, de qualquer dado que possa remeter a uma pessoa natural, entendida como a titular dos dados, isto é, "a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento" (inciso V).

Segundo os dados da pesquisa, em 2021, apenas 37% das empresas mantinham dados de funcionários terceirizados, ao passo que 62% mantinham os de parceiros e fornecedores (Gráfico 1). Não há grandes diferenças na manutenção de dados por porte e setor, mas vale a menção de que os setores de informação e comunicação e de atividades profissionais foram aqueles que apresentaram uma maior presença de guarda de dados de clientes e usuários, atingindo 78% das empresas desses setores.

GRÁFICO 1

EMPRESAS, POR TIPO DE DADO PESSOAL MANTIDO E PORTE (2021)

Total de empresas (%)



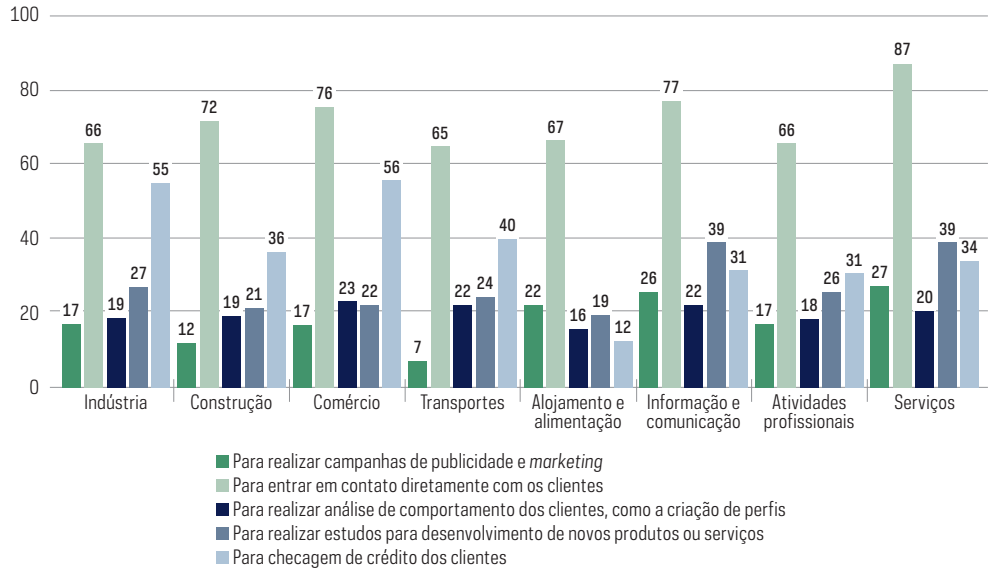
[4] De acordo com a LGPD (Artigo 5º, inciso X), tratamento é: "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".

Quanto ao uso dos dados pessoais mantidos, a maior parte das empresas declara manter os dados pessoais para entrar em contato direto com os clientes (71%) e para checagem de crédito dos clientes (45%)[5]. Não há grandes diferenças quanto às finalidades do uso dos dados pessoais por setor, à exceção de uma utilização mais acentuada da checagem de crédito no comércio e na indústria. Outro ponto de destaque é o uso de dados pessoais de clientes e usuários para realizar estudos para desenvolvimento de novos produtos ou serviços, reportado por 39% das empresas do setor de informação e comunicação e das empresas do setor de serviços.

GRÁFICO 2

EMPRESAS, POR TIPO DE FINALIDADE DE USO DOS DADOS PESSOAIS E SETOR (2021)

Total de empresas que mantêm dados pessoais de clientes e usuários (%)



Um aspecto crítico para o tratamento de dados pessoais nas empresas são os dados sensíveis. De acordo com a LGPD, um dado pessoal sensível diz respeito a "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à orientação sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (Artigo 5º, inciso II). O objetivo da lei é evitar tratamento de dados sensíveis que possam levar a ações discriminatórias, tendo em vista que a própria natureza destes dados exarceba esses riscos. Em seu Artigo 11, a LGPD deixa claro que o uso de dados pessoais sensíveis é permitido apenas em situações muito específicas, tais

[5] Para o adequado uso desses tipos de dados pessoais, a empresa deve possuir o consentimento dos titulares dos dados no primeiro caso, e, no segundo, há amparo legal para o tratamento. De acordo com o Artigo 7º da LGPD, dialogando diretamente com os usos mais relatados na pesquisa: "O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular; [...] X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente".

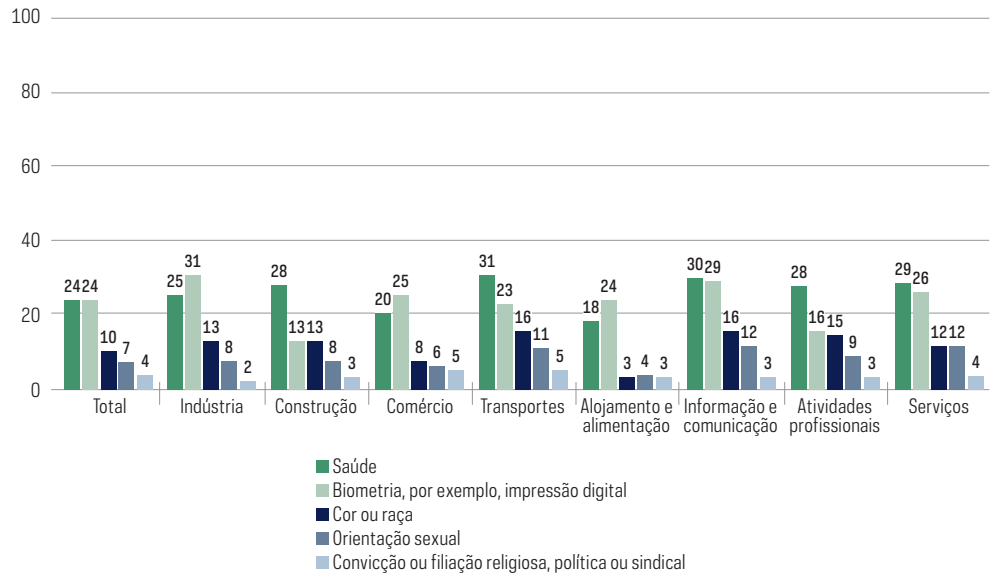
como em circunstâncias de proteção da vida do titular ou de terceiros, ainda que com diversas restrições com relação à comunicação e ao compartilhamento dessas informações. Portanto, o tratamento de dados pessoais sensíveis deve ser avaliado por todas as empresas, buscando sempre justificar seu uso com base na lei ou até mesmo minimizar ou evitar seu uso sempre que não seja necessário para o modelo de negócio.[6]

A pesquisa realizada com pequenas, médias e grandes empresas indica que a maior parte dos dados pessoais sensíveis mantidos por elas são de biometria e saúde (24%) — o que pode ter relação com o tratamento de dados pessoais de funcionários. Dados pessoais sensíveis relacionados a questões raciais, sexuais ou ideológicas são mantidos em menor frequência. Ainda que apenas um número reduzido de empresas tenham reportado o tratamento de dados pessoais sensíveis, é importante que todas as organizações realizem um inventário de dados para averiguar os tipos de dados mantidos e as medidas cabíveis para o correto tratamento.[7]

GRÁFICO 3

EMPRESAS, POR TIPO DE DADO PESSOAL SENSÍVEL MANTIDO (2021)

Total de empresas (%)



[6] Um ponto para as empresas levarem em conta ao lidarem com o tratamento de dados pessoais é a atenção aos princípios da LGPD, conforme descritos em seu Artigo 6º. Se os usos previstos ferem alguns dos princípios da referida lei, é preciso reavaliar se o uso de dados pessoais é de fato imprescindível.

[7] Uma referência é o *Guia de elaboração de inventário de dados pessoais* (Ministério da Economia, 2021), que oferece um *template* para que órgãos públicos busquem detalhar seus processos de tratamento de dados pessoais. Apesar de direcionado para o setor público, o Guia pode ser aplicado em organizações privadas, na medida em que a metodologia de mapeamento pode ser adaptada. Outro ponto importante é que o inventário sugerido pelo guia busca alinhamento com o Artigo 37 da LGPD, qual seja: "o controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse".

Desenvolvimento de capacidades internas

Outro aspecto central para o desenvolvimento de uma cultura de proteção de dados é a existência de ações, por parte das empresas, que promovam a capacitação e a sensibilização da equipe. Assim, é fundamental averiguar a presença de atividades que incluam o conjunto dos membros da organização, em seus mais diversos níveis hierárquicos.[8]

O levantamento indica que 36% das empresas realizaram reuniões específicas para tratar do tema privacidade e proteção de dados pessoais. Ainda que não sejam observadas diferenças regionais significativas, a realização de reuniões para tratar temas relacionados à privacidade e à proteção de dados aparece de forma desigual entre os diferentes setores, sendo que os de informação e comunicação foram os que apresentaram maior frequência, e o setor de construção, a menor incidência. Ademais, vale destacar que reuniões foram mais presentes nas grandes (73%) e médias empresas (59%), enquanto nas pequenas houve uma menor proporção que buscou discutir internamente os temas de privacidade e proteção de dados pessoais.[9]

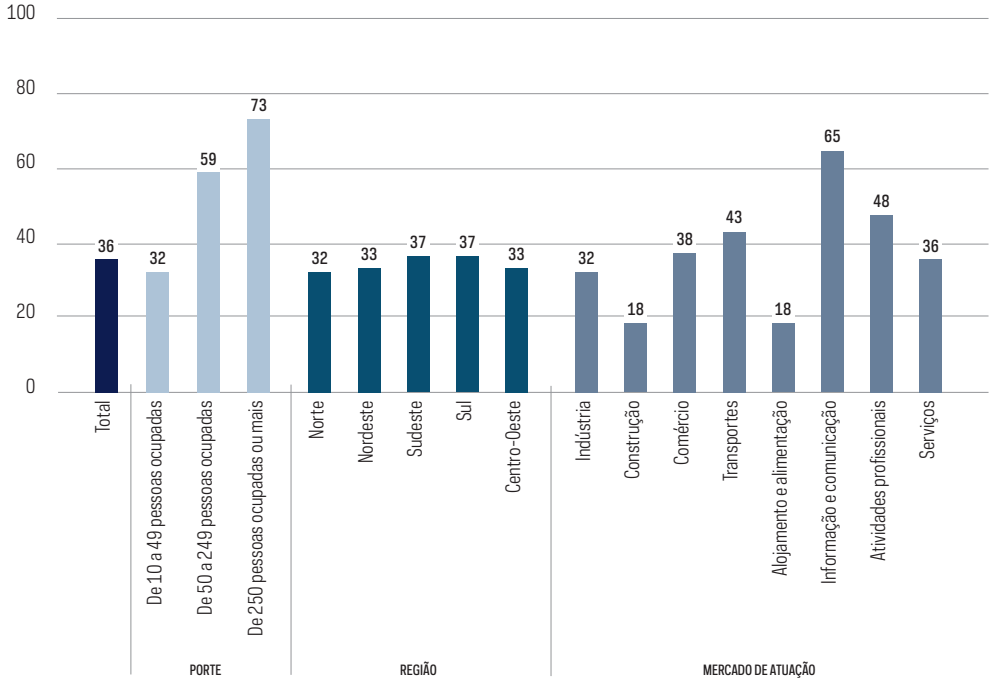
[8] A publicação *Segurança digital: uma análise da gestão de risco em empresas brasileiras* (NIC.br, 2021) traz estudos de caso que evidenciam a necessidade de uniformização dos conhecimentos sobre cuidados básicos de segurança digital, na medida em que as organizações estão expostas a diversos riscos que podem levar a vazamentos de dados pessoais, causando danos financeiros e reputacionais que podem ser irreversíveis. Entre os aspectos tratados pela LGPD está a mitigação de riscos, como a redução dos incidentes de segurança com dados pessoais, tal como disposto no Artigo 50: "os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais".

[9] A ANPD elaborou um guia para implementação de práticas de segurança da informação visando fornecer subsídios para o fortalecimento da proteção de dados em agentes de pequeno porte, especificamente micro e pequenas empresas e *start-ups* (ANPD, 2021).

GRÁFICO 4

EMPRESAS, POR REALIZAÇÃO DE REUNIÕES INTERNAS PARA TRATAR DO TEMA DE PROTEÇÃO DE DADOS (2021)

Total de empresas (%)

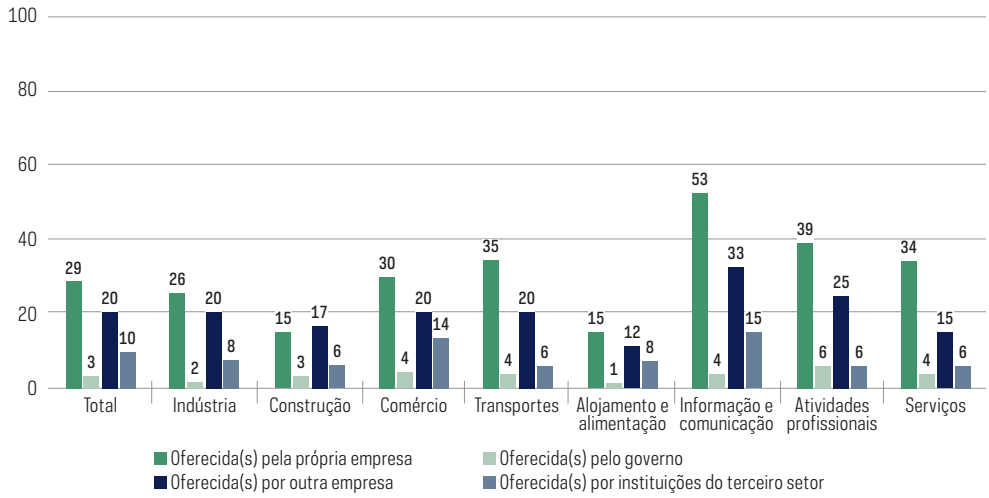


Em termos de ações mais efetivas para alcançar a conformidade com as novas regras de proteção de dados, observa-se que uma proporção reduzida das empresas adotaram medidas para elevar suas capacidades em torno do tema da privacidade e proteção de dados pessoais. Entre os treinamentos, o modelo mais citado foi o fornecimento da capacitação pela própria empresa (29%), evidenciando a prevalência de esforços da própria organização. Nos setores que mais apresentam ações de capacitação ou treinamento — como é o caso de informação e comunicação ou atividades profissionais — estão mais presentes iniciativas internas e de outras empresas, evidenciado uma preocupação em buscar uma qualificação mais completa. A busca por capacitação ainda pode ter relação com setores em que o tratamento dos dados pessoais assume papel mais estratégico para o desempenho das empresas ou fornecimento de serviços.

GRÁFICO 5

EMPRESAS, POR TIPO DE AÇÕES DE TREINAMENTO E CAPACITAÇÃO SOBRE PROTEÇÃO DE DADOS PESSOAIS (2021)

Total de empresas (%)



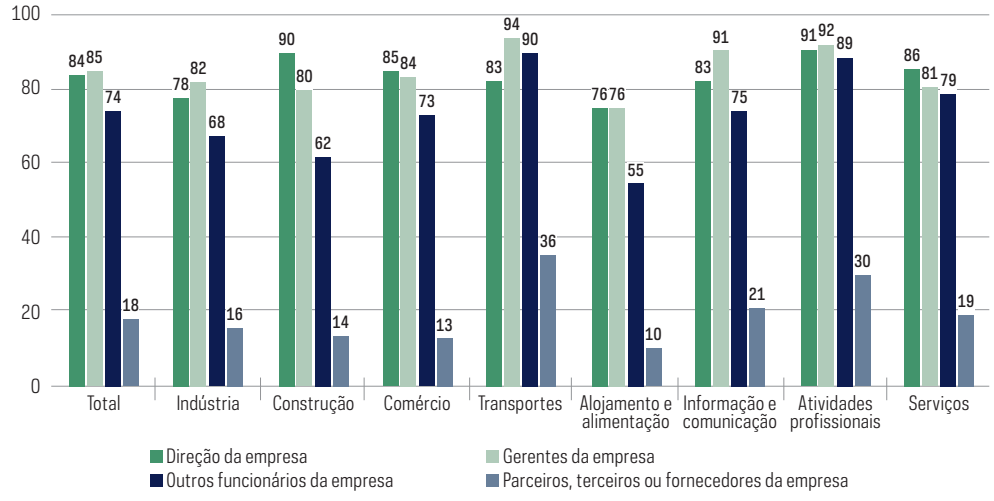
A pesquisa também traz dados sobre o público-alvo das ações de treinamento e capacitação sobre privacidade e proteção de dados pessoais ocorridos nas empresas. Em 84% das empresas que realizaram ações de treinamento, houve participação da diretoria e 85% contaram com a participação da gerência. Por sua vez, em 74% das empresas que ofereceram treinamento sobre proteção de dados houve participação de funcionários. Em menor medida, o treinamento foi oferecido aos parceiros e funcionários terceirizados, sendo destinado para os colaboradores da empresa em todos os escalões.

Portanto, ainda que poucas empresas ofereçam capacitações internas, destaca-se a preocupação em distribuir os conhecimentos por toda a organização, na medida em que é necessária a sensibilização de todos os membros sobre os cuidados no tratamento de dados pessoais, reduzindo os riscos relacionados à proteção de dados e a possíveis infrações da lei. Observa-se, ainda, que o setor de construção foi o que menos direcionou esses treinamentos para funcionários, comparados aos treinamentos direcionados aos gestores das empresas.

GRÁFICO 6

EMPRESAS, POR PÚBLICO PARTICIPANTE DAS AÇÕES DE TREINAMENTO OU CAPACITAÇÃO SOBRE PROTEÇÃO DE DADOS PESSOAIS (2021)

Total de empresas que realizaram ações de treinamento ou capacitação sobre proteção de dados pessoais (%)

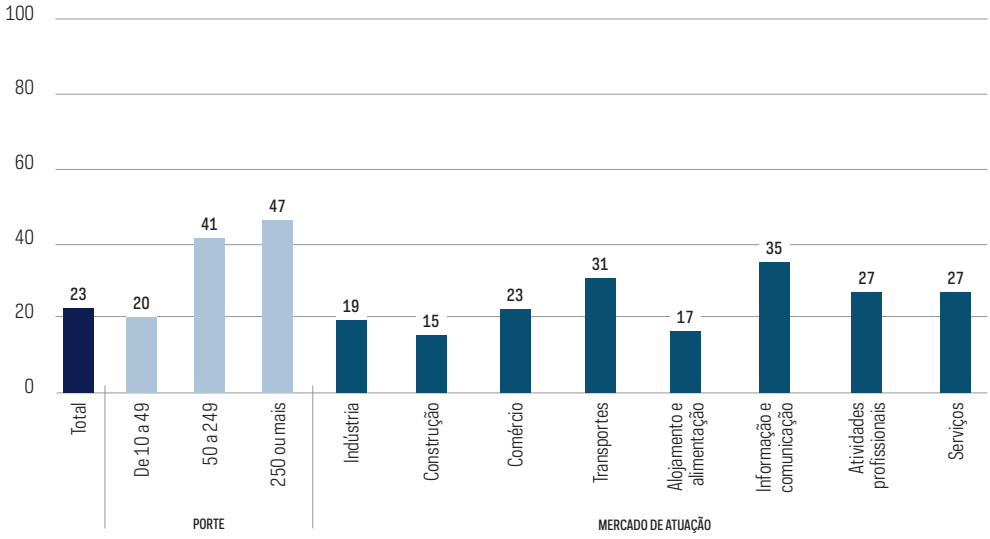


A pesquisa também mediu a presença de uma área ou de funcionários responsáveis pelo tema de proteção de dados pessoais. Observa-se que em 23% das empresas há uma área ou pessoas responsáveis pelos assuntos relacionados à LGPD, sendo que em sua maioria essas empresas são de médio e grande porte. As empresas que possuem área ou pessoas dedicadas aos temas da privacidade e proteção de dados pessoais em maiores proporções também estão nas atividades que podem ter contato com maior volume de dados pessoais — como os setores de informação e comunicação e transporte, armazenamento e correio.

GRÁFICO 7

EMPRESAS, POR EXISTÊNCIA DE UMA ÁREA ESPECÍFICA OU FUNCIONÁRIOS RESPONSÁVEIS PELO TEMA DE PROTEÇÃO DE DADOS PESSOAIS (2021)

Total de empresas (%)



Entre as empresas que possuem responsáveis ou área de proteção de dados pessoais, há maior presença de pessoas contratadas para outras funções e que foram deslocadas ou acumularam as funções relacionadas à LGPD (88%), fator que apresenta pouca variação segundo porte, região e setor. A escolha de uma pessoa da própria empresa para lidar com os temas de proteção e privacidade de dados pode ter relação com a necessidade de conhecimentos sobre o fluxo de dados específicos da organização, sendo importante certo nível de apropriação dos processos para avaliar os diversos riscos dispersos em diferentes setores da organização.

TABELA 1

EMPRESAS, POR FUNCIONÁRIOS RESPONSÁVEIS PELO TEMA DE PROTEÇÃO DE DADOS PESSOAIS (2021)

Percentual (%)		Foram contratados especificamente para atuar com proteção de dados	Foram contratados para outras funções e passaram a lidar também com as questões de proteção de dados
Total		**22**	**88**
Porte	De 10 a 49 pessoas ocupadas	24	87
	De 50 a 249 pessoas ocupadas	16	94
	De 250 pessoas ocupadas ou mais	12	95

CONTINUA ▸

▸ CONCLUSÃO

Percentual (%)		Foram contratados especificamente para atuar com proteção de dados	Foram contratados para outras funções e passaram a lidar também com as questões de proteção de dados
Região	Norte	24	83
	Nordeste	14	97
	Sudeste	22	88
	Sul	21	86
	Centro-Oeste	38	78
Mercado de atuação	Indústria	13	96
	Construção	22	80
	Comércio	30	91
	Transportes	28	88
	Alojamento e alimentação	6	80
	Informação e comunicação	16	83
	Atividades profissionais	16	81
	Serviços	21	95

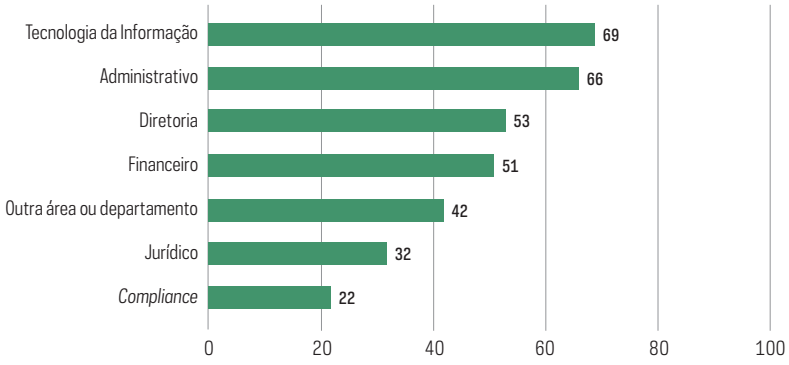
Considerando a grande presença de colaboradores deslocados ou que acumularam funções relacionadas ao tema da proteção de dados pessoais, convém averiguar a origem desses profissionais dentro da organização. Diversos documentos que discutem as melhores práticas para a adequação das empresas à LGPD salientam a necessidade da manutenção de equipes interdepartamentais para lidar com o tema da proteção de dados pessoais, bem como a necessidade de distribuição de informações por todos os departamentos, tendo em vista que se trata de assunto que afeta a organização como um todo (Sombra & Castellano, 2021; Instituto Brasileiro de Defesa do Consumidor [Idec], 2021).

Em sua maioria, as pessoas responsáveis pela adequação à LGPD, em empresas que possuem área ou pessoa específica, são provenientes do setor de tecnologia da informação (69%), seguido por membros do administrativo (66%) e da diretoria (53%). Essa maior presença de pessoas provenientes da área de TI é observada nas empresas de médio e grande porte, mostrando ser uma tendência nas organizações com processos mais complexos.

GRÁFICO 8

EMPRESAS, POR ÁREA OU DEPARTAMENTO A QUE PERTENCE OS FUNCIONÁRIOS RESPONSÁVEIS PELO TEMA DA PROTEÇÃO DE DADOS PESSOAIS (2021)

Total de empresas com área específica ou funcionários responsáveis pelo tema de proteção de dados pessoais (%)

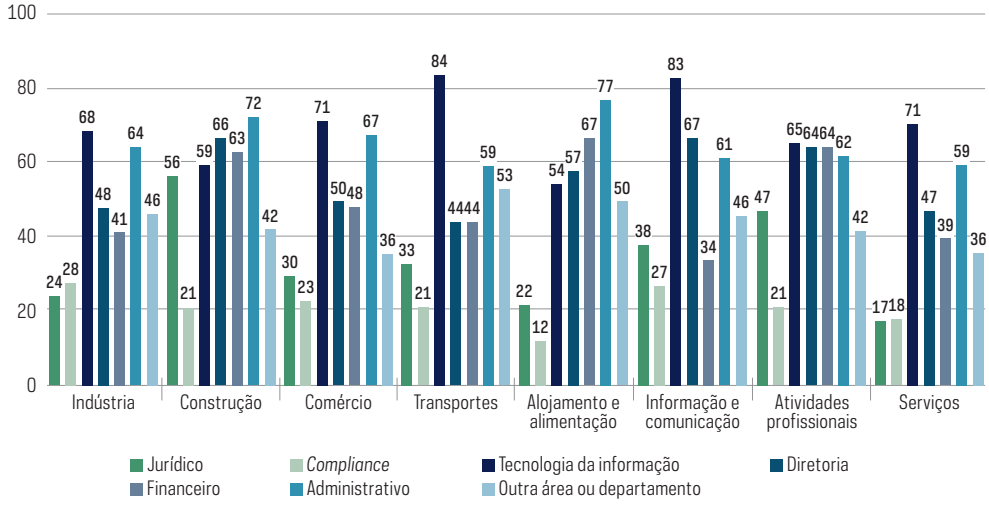


Ainda que a maioria dos responsáveis pela proteção de dados nas empresas seja originariamente do setor de tecnologia da informação ou do administrativo, há diferenças importantes entre os setores de atividade econômica em termos de composição das equipes responsáveis pela conformidade à LGPD.

GRÁFICO 9

EMPRESAS, POR ÁREA OU DEPARTAMENTO A QUE PERTENCEM OS FUNCIONÁRIOS RESPONSÁVEIS PELO TEMA DA PROTEÇÃO DE DADOS PESSOAIS, POR SETOR DE ATIVIDADE ECONÔMICA (2021)

Total de empresas com área específica ou funcionários responsáveis pelo tema de proteção de dados pessoais (%)



Adequação à LGPD

A pesquisa também investigou aspectos críticos para a adequação à LGPD entre as empresas brasileiras, tendo como marco orientador os dispositivos da lei. Sabe-se que os percursos de implementação podem variar entre as empresas, a depender do porte e dos dados pessoais em sua guarda. No entanto, algumas boas práticas podem ser destacadas, uma vez que refletem o entendimento do fluxo de dados na empresa, buscando garantir a integridade das operações que envolvem o tratamento de dados pessoais, a redução riscos de vazamento e o aumento da transparência diante os titulares (ANPD, 2021; Idec, 2021).

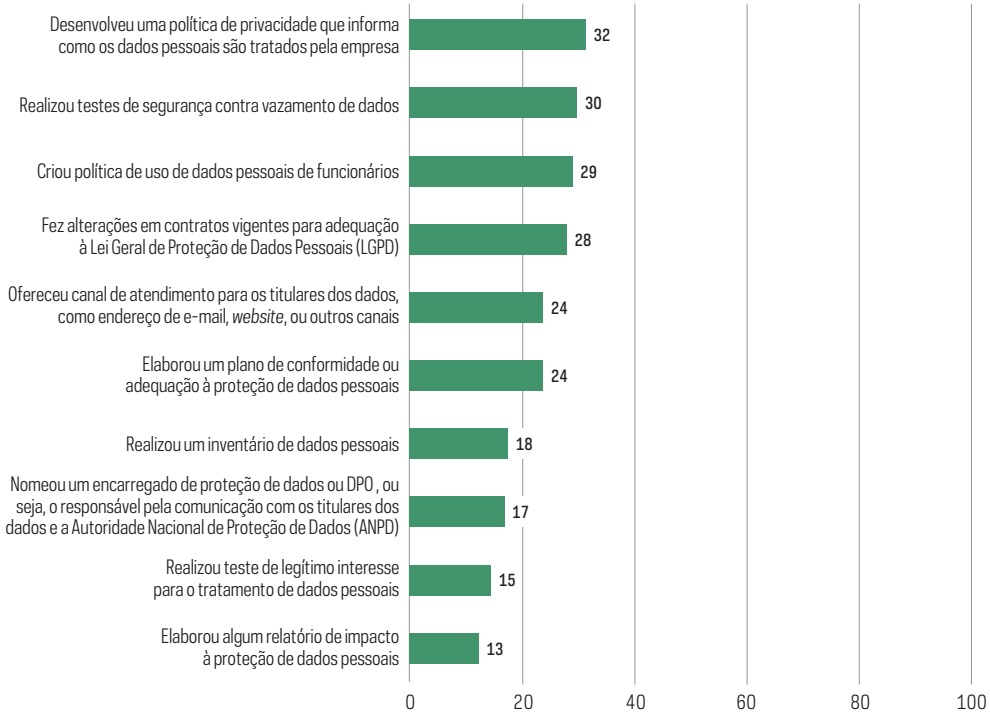
Entre os aspectos mensurados, o mais citado foi o desenvolvimento de uma política de privacidade que informa como os dados pessoais são tratados pela empresa (32%). Em seguida, 30% das empresas informaram que realizaram teste de segurança contra vazamentos de dados, o que evidencia uma preocupação em terem seus processos de tratamento de dados pessoais mais explícitos, ao mesmo tempo em que buscam garantir sua segurança, evitando assim vazamentos que possam trazer prejuízos fiscais e danos reputacionais. Vale mencionar que a produção de relatório de impacto à proteção de dados pessoais — previsto na LGPD em seu Artigo 5º — foi o aspecto menos citado pelas empresas[10]. A criação de um plano de adequação à LGPD, que pode favorecer uma operação mais segura e em conformidade com a lei, foi citada em apenas 24% das empresas (Gráfico 10).

[10] O relatório de impacto à proteção de dados pessoais é definido no Artigo 5º como: "documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco". Em outra menção na lei, o relatório de impacto à proteção de dados pessoais é colocado como passível de exigência pela ANPD, conforme disposto no Artigo 38: "A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial". Necessário ressaltar que a LGPD não menciona a sua obrigatoriedade em nenhum caso específico, sendo sua realização compulsória somente quando solicitada pela ANPD.

GRÁFICO 10

EMPRESAS, POR TIPO DE AÇÃO DE ADEQUAÇÃO À LGPD (2021)

Total de empresas que mantêm dados de pessoas físicas (%)



Entre algumas das atividades mais realizadas para adequação à LGPD, observa-se que as empresas dos setores de informação e comunicação e de atividades profissionais são aquelas que apresentaram mais diversificação de ações. Como mostra a Tabela 2 a seguir, poucos setores apresentaram ações que buscam capacitar a empresa no aprimoramento da gestão interna de dados pessoais, bem como no fortalecimento da segurança digital.

TABELA 2
AÇÕES PARA ADEQUAÇÃO À LGPD POR SETOR (2021)

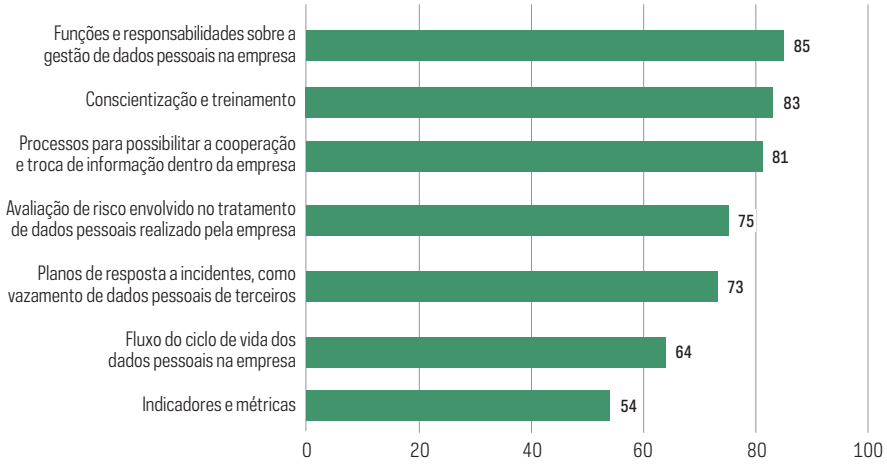
	Indústria	Construção	Comércio	Transportes	Alojamento e alimentação	Informação e comunicação	Atividades profissionais	Serviços
Elaborou um plano de conformidade ou adequação à proteção de dados pessoais	26	19	21	33	14	41	32	24
Criou política de uso de dados pessoais de funcionários	26	21	31	33	13	45	35	22
Realizou um inventário de dados pessoais	20	13	17	21	8	24	22	17
Elaborou algum relatório de impacto à proteção de dados pessoais	14	10	9	23	12	25	17	15
Desenvolveu política de privacidade que informa como os dados pessoais são tratados pela empresa	29	27	30	37	30	41	43	29
Nomeou um encarregado de proteção de dados ou DPO	16	14	18	21	7	22	22	11
Fez alterações em contratos vigentes para adequação à LGPD	30	22	22	38	23	57	38	26
Realizou testes de segurança contra vazamento de dados	28	20	31	36	22	46	36	24
Ofereceu canal de atendimento para os titulares dos dados, como endereço de *e-mail*, *website*, ou outros canais	24	23	17	27	21	45	39	34
Realizou teste de legítimo interesse para o tratamento de dados pessoais	15	13	15	25	5	25	19	16

Entre as empresas que possuem um plano de conformidade ou adequação à LGPD, a maioria das iniciativas determina as funções e responsabilidade sobre a gestão de dados pessoais na empresa (85%). Na sequência são citadas ações de conscientização e treinamento e processos para possibilitar a cooperação e troca de informação dentro da empresa (81%) — o que pode ter relações com as estratégias de capacitação discutidas acima. Portanto, as ações previstas nos planos de conformidade ou adequação à LGPD versam sobre a definição de atribuições em torno das exigências da lei, ao mesmo tempo em que há diretivas sobre capacitações internas, tanto do ponto de vista de fornecimento de conhecimentos quanto de melhoria da comunicação entre departamentos.

GRÁFICO 11

EMPRESAS, POR ABRANGÊNCIA DO PLANO DE CONFORMIDADE OU ADEQUAÇÃO À PROTEÇÃO DE DADOS PESSOAIS (2021)

Total de empresas que possuem um plano de conformidade ou adequação à LGPD (%)



Uma das ações para adequação à LGPD é a nomeação do encarregado de dados da organização, ou DPO (do inglês, *Data Protection Officer*), responsável pela comunicação com os titulares dos dados e com a ANPD, prevista no Artigo 41 da lei[11]. Além disso, o encarregado também se responsabiliza por observar a adequação à LGPD, tendo papel central na conformidade dos processos de tratamento de dados pessoais, instituindo uma governança de dados efetiva na organização (CIPL & Cedis-IDP, 2021). Apesar de a lei se referir ao encarregado como uma pessoa, não há restrições à criação de equipes de proteção de dados formada de modo interdepartamental, ou até mesmo com um agente externo contratado, sendo a única restrição a impossibilidade da atuação como encarregado em mais de uma organização (ANPD, 2022a). A pesquisa revela que 17% das empresas nomearam um encarregado de proteção de dados, sendo que esta proporção compreende 41% das empresas de grande porte, 29% de médio porte e 15% das empresas de pequeno porte[12]. A pesquisa TIC Empresas investiga ainda a origem do encarregado de dados. Na maioria dos casos (77%), o encarregado da proteção de dados é uma pessoa ou comitê da própria empresa, sendo esta origem preponderante em todas as estratificações da pesquisa.

[11] De acordo com a LGPD, as atribuições do encarregado de dados pessoais são: "I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; II - receber comunicações da autoridade nacional e adotar providências; III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares".

[12] A Resolução CD/ANPD n. 2, de 27 de janeiro de 2022, em seu Artigo 11, dispensa as organizações de pequeno porte de nomear um encarregado de proteção de dados pessoais (ANPD, 2022b). No entanto, é importante salientar que a ANPD toma como conceito de porte o faturamento da organização. Na pesquisa TIC Empresas, o porte é concebido a partir do número de pessoas ocupadas, sendo a pequena empresa entendida como aquela com até 49 pessoas ocupadas.

TABELA 3

EMPRESAS, POR ORIGEM DO ENCARREGADO DE PROTEÇÃO DE DADOS PESSOAIS, PORTE, REGIÃO E SETOR (2021)

Total de empresas que possuem um encarregado de proteção de dados pessoais (%)

Percentual (%)		É uma pessoa ou comitê da própria empresa	É um terceiro contratado	Não sabe	Não respondeu
Total		**77**	**22**	**1**	**0**
Porte	De 10 a 49 pessoas ocupadas	75	24	1	0
	De 50 a 249 pessoas ocupadas	85	15	0	0
	De 250 pessoas ocupadas ou mais	80	17	3	0
Região	Norte	57	31	0	12
	Nordeste	90	10	0	0
	Sudeste	70	28	2	0
	Sul	89	10	1	0
	Centro-Oeste	58	42	0	0
Mercado de atuação	Indústria	82	10	6	2
	Construção	58	42	0	0
	Comércio	78	22	0	0
	Transportes	63	37	0	0
	Alojamento e alimentação	100	0	0	0
	Informação e comunicação	64	36	0	0
	Atividades profissionais	80	20	0	0
	Serviços	88	12	0	0

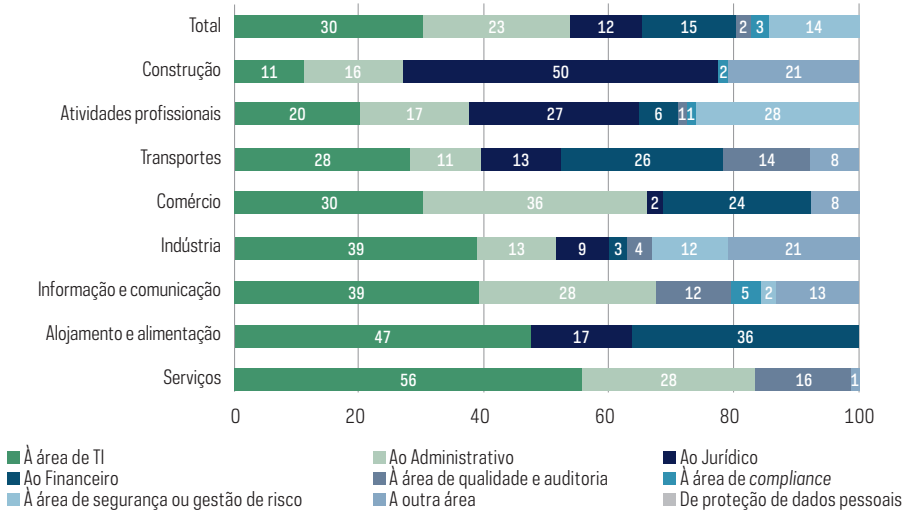
Tal qual a origem das pessoas destacadas para tratar da proteção de dados pessoais, os encarregados de dados pessoais são em sua maioria oriundos da área de TI da empresa (30%), seguido pelo setor administrativo (23%).[13]

[13] Para os órgãos públicos do governo federal, a nomeação de um encarregado de proteção de dados oriundo do setor de tecnologia da informação foi vetada pela Instrução Normativa SGD/ME n. 117, de 19 de novembro de 2020. O objetivo é evitar que o responsável pelo tratamento dos dados acumule a função de reportar sobre eles ao público externo. No entanto, para as demais organizações não há restrições quanto à origem do encarregado de proteção de dados.

GRÁFICO 12

EMPRESA, POR ÁREA DE ORIGEM DO ENCARREGADO DE PROTEÇÃO DE DADOS PESSOAIS, POR SETOR DE ATIVIDADE ECONÔMICA (2021)

Total de empresas que possuem um encarregado de proteção de dados pessoais vindo da própria empresa (%)



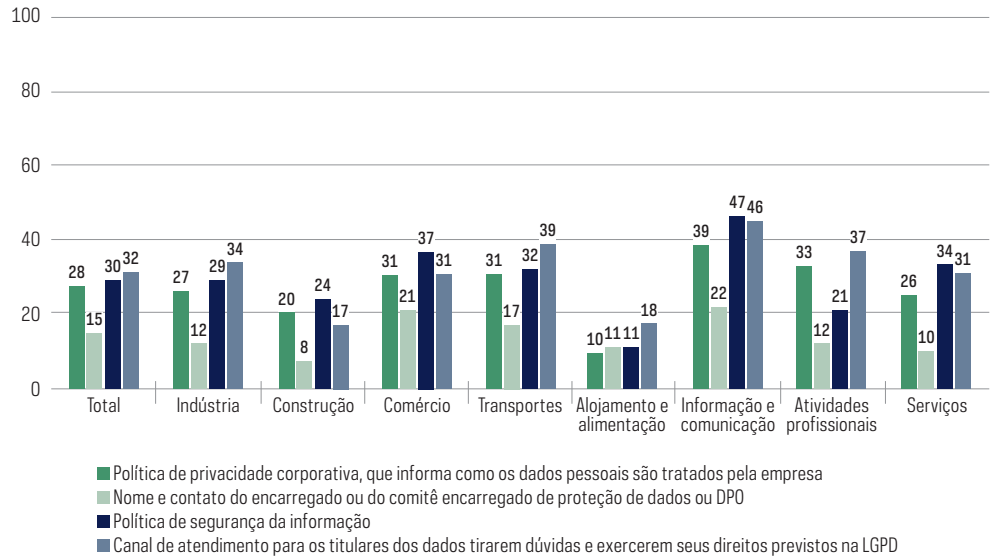
Outra ação fundamental para a empresa entrar em conformidade com a LGPD é o fornecimento de informações em seu *website*. Ainda que não seja uma exigência explícita da lei, a disposição de informações sobre a política de proteção de dados da empresa fortalece uma cultura de transparência sobre as operações que as empresas realizam com os dados pessoais dos titulares. Na LGPD, as menções sobre funcionalidades dos *websites* estão nas especificações do tratamento de dados pessoais no setor público (Artigo 23) e, para toda as organizações, na exigência de fornecimento de nome e contato do encarregado de dados (Artigo 41, parágrafo 1º)[14]. Apenas 15% das empresas informaram o contato do encarregado da proteção de dados no *website* da empresa, sendo que a informação mais fornecida foi a política de segurança da informação, explicitada por 30% das empresas, seguida pelo fornecimento da política de privacidade corporativa, que informa como os dados pessoais são tratados pela empresa (28%). Segundo a pesquisa TIC Empresas 2019 (CGI.br, 2020), observa-se que no setor de informação e comunicação há maior presença de alguns recursos nos *websites* do que em setores como construção ou alojamento e alimentação.

[14] Segundo a TIC Empresas 2019 (Comitê Gestor da Internet no Brasil [CGI.br], 2020), 54% das empresas possuem *website*, sendo que em sua maioria essas páginas estão concentradas nas grandes e médias empresas. As pequenas empresas se restringem ao uso de redes sociais, que não permitem a customização de suas utilidades de modo a ter um espaço para o fornecimento do nome e o contato do encarregado de dados pessoais.

GRÁFICO 13

EMPRESAS, POR RECURSOS OFERECIDOS NO *WEBSITE* (2021)

Total de empresas que possuem website (%)



Barreiras e oportunidades

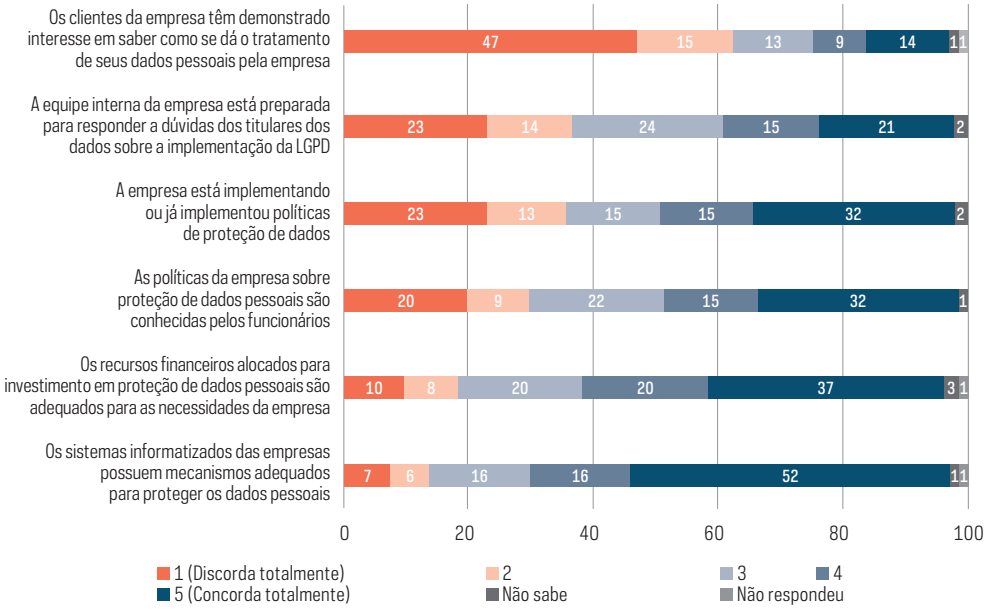
A pesquisa também investigou as percepções das empresas sobre barreiras e oportunidades criadas pela LGPD. O objetivo desta seção é discutir as dificuldades que as empresas estão enfrentando para buscar a conformidade com a lei, bem como a visão delas sobre uma série de ações que envolvem a proteção de dados pessoais.

Em relação ao público atendido, 47% das empresas discordam da afirmação de que os clientes têm demonstrado interesse em saber como se dá o tratamento de seus dados pessoais. Do ponto de vista da preparação da empresa, 52% delas concordam totalmente com a afirmação de que seus sistemas informatizados possuem mecanismos adequados para proteger os dados pessoais. Portanto, os dados indicam menor percepção das empresas quanto à preocupação dos clientes sobre como seus dados pessoais são manejados, ao mesmo tempo em que existem ações para garantir a correta e segura manutenção de dados pessoais.

GRÁFICO 14

EMPRESAS, POR GRAU DE PERCEPÇÃO SOBRE BARREIRAS[15] (2021)

Total de empresas (%)



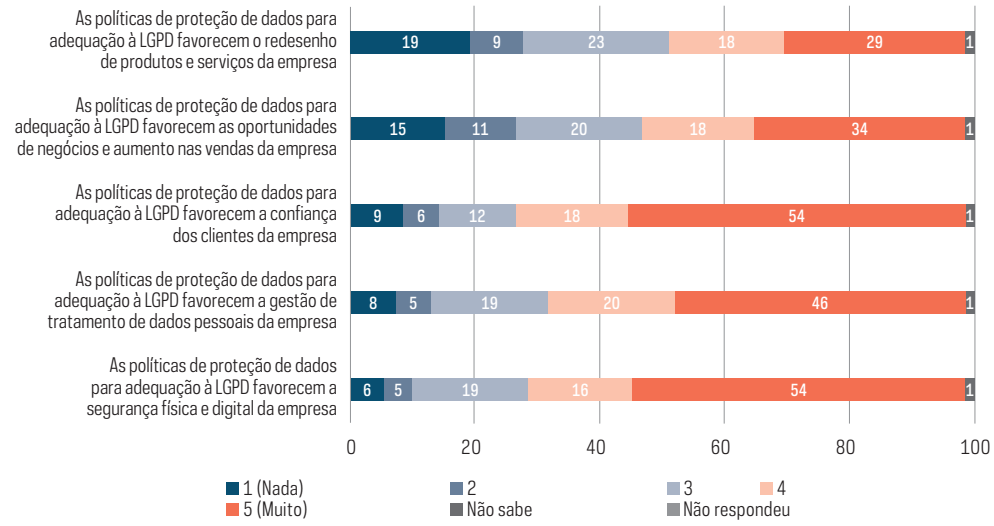
No que diz respeito às oportunidades criadas pela LGPD, a maioria das empresas concorda que a lei traz possibilidades diversas que podem favorecer sua atuação, tanto na melhoria de processos internos quanto em sua reputação com clientes. Como exemplo, 54% das empresas afirmaram que as políticas de proteção de dados para adequação à LGPD favorecem sua segurança física e digital. No sentido de oportunidades para a relação da empresa com seu público, 54% afirmaram que as políticas de proteção de dados para adequação à LGPD favorecem a confiança dos clientes. Portanto, a maioria das empresas afirma que a busca pela adequação à lei pode trazer benefícios para sua atuação, uma vez que a proteção de dados pessoais demanda melhoria de processos para garantir a integridade do tratamento dos dados dos clientes, garantindo assim uma relação positiva com o público atendido.

[15] A pergunta utilizada para criar o indicador foi: "Considerando uma escala de 1 a 5, onde 5 significa "Concordo totalmente" e 1 significa "Discordo totalmente", o quanto o(a) senhor(a) concorda ou discorda que [ITEM DE RESPOSTA]?

GRÁFICO 15

EMPRESAS, POR GRAU DE PERCEPÇÃO SOBRE OPORTUNIDADES[16] (2021)

Total de empresas (%)



Considerações finais: agenda para políticas públicas

Os resultados do módulo de privacidade e proteção de dados pessoais, coletados de forma inédita na pesquisa TIC Empresas 2021, indicam a presença ainda incipiente nas empresas brasileiras de ações para a adequação à LGPD. Ainda que grande parte das empresas esteja realizando atividades de treinamento e conscientização de seus membros sobre o escopo da lei e criando atribuições de responsabilidades sobre os cuidados no tratamento de dados pessoais, as organizações ainda reportam um conjunto reduzido de ações para uma adequação efetiva ao novo cenário. Os resultados da pesquisa denotam, portanto, desafios substantivos para que as empresas desenvolvam uma cultura de proteção de dados pessoais em suas rotinas.

Dispositivos previstos na LGPD, tais como a nomeação de um encarregado de dados pessoais ou a elaboração de um relatório de impacto à proteção de dados pessoais, estão refletidos em menos da metade das empresas brasileiras. Tal resultado revela limites significativos para as capacidades financeira e de qualificação para que as organizações de todos os portes e segmentos de atividade econômica atinjam um nível alto de maturidade na proteção de dados pessoais.

Tendo em vista a ampla disseminação da presença de dados pessoais no conjunto das empresas, bem como as diversas formas pelas quais os fluxos de dados se constituem nas rotinas das organizações, também é central um esforço para que o mapeamento da entrada e saída de dados seja feito com detalhes e com a participação de todos os

[16] A pergunta utilizada para criar o indicador foi: "Considerando uma escala de 1 a 5, onde 5 significa "Muito" e 1 significa "Nada", o quanto o(a) senhor(a) considera que as políticas de proteção de dados pessoais para adequação à LGPD favorecem [ITEM DE RESPOSTA]?

setores. Além disso, a forma como as empresas lidam com a privacidade e proteção de dados pessoais tende a ser cada vez mais decisiva para a manutenção de uma boa reputação, levando à confiança dos clientes para fornecimento de informações que são cruciais para o desempenho da organização na economia atual.

Outro aspecto a se destacar é a presença de guias e normativas que podem servir de referência para as empresas que contam com poucos recursos[17]. Nesse contexto, é fundamental a atuação da ANPD para a orientação das empresas sobre como se adequarem à lei.[18]

Os resultados da pesquisa indicam que há espaço para melhorar a sensibilização quanto ao tema entre empresas de todos os portes e segmentos de mercado. Ações mais complexas que garantem a transparência e a integridade dos processos de tratamento de dados pessoais possuem presença incipiente entre as empresas, sendo importante monitorar o quanto a proteção de dados pessoais assume centralidade nas estratégias empresariais. Ainda que a lei seja recente e haja incertezas quanto à sua correta adequação, as empresas precisam tornar a proteção de dados pessoais uma constante em suas rotinas, uma vez que garantir o bom uso dos dados é cada vez mais central para a reputação da organização, para a promoção de uma boa relação com os clientes, bem como para evitar punições que possam trazer danos irreversíveis.

A introdução do módulo sobre privacidade e proteção de dados pessoais na pesquisa TIC Empresas proporciona indicativos relevantes sobre como tem se dado o processo de implementação da LGPD nas empresas e se há avanços em termos de construção de uma cultura de proteção de dados no país. Vale lembrar que a LGPD estipula o desenvolvimento econômico, tecnológico e a inovação entre seus fundamentos, bem como os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. Dessa forma, dados e análises sobre como as empresas brasileiras estão se adequando à LGPD são essenciais para uma devida efetivação da lei e para o desenvolvimento de diálogos importantes na consolidação de atividades econômicas alinhadas a direitos fundamentais, como a privacidade e a proteção de dados pessoais.

Portanto, o que os resultados da pesquisa TIC Empresas 2021 indicam é que há espaço para ações de capacitações entre as empresas brasileiras sobre a importância de ter a proteção de dados pessoais como parte da estratégia da organização, independentemente do seu porte e mercado de atuação, sendo a entrada em vigor da LGPD o início de uma nova forma de atuar no país.

[17] Diversas ações do Governo Federal indicam processos que podem ser adaptados no setor privado: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados

[18] Diversos guias orientativos estão disponíveis no *website* da instituição: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes. São interessantes também as discussões abertas promovidas pela ANPD em seu canal no YouTube: https://www.youtube.com/c/anpdgov

Referências

Autoridade Nacional de Proteção de Dados. (2021). *Guia orientativo – Segurança de informação para agentes de tratamento de pequeno porte*. https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf

Autoridade Nacional de Proteção de Dados. (2022a). *Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado*. https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf

Autoridade Nacional de Proteção de Dados. (2022b). *Resolução CD/ANPD n. 2, de 27 de janeiro de 2022*. https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019

Centre for Information Policy Leadership, & Centro de Direito, Internet e Sociedade do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa. (2021). *O papel do/a encarregado/a conforme a Lei Geral de Proteção de Dados Pessoais (LGPD)*. https://www.idp.edu.br/o-papel-do-a-encarregado-a-conforme-a-lei-geral-de-protecao-de-dados-pessoais-lgpd/

Comitê Gestor da Internet no Brasil. (2020). *Pesquisa sobre o uso das tecnologias de informação e comunicação nas empresas brasileiras: TIC Empresas 2019*. https://cetic.br/media/docs/publicacoes/2/20200707094721/tic_empresas_2019_livro_eletronico.pdf

Conferência das Nações Unidas sobre Comércio e Desenvolvimento. (2021). *Digital Economy Report 2021: Cross-border data flows and development: for whom the data flow.* https://unctad.org/webflyer/digital-economy-report-2021

Greenleaf, G. (2021). Global data privacy laws 2021: Despite COVID delays, 145 laws show GDPR dominance. *Privacy Laws & Business International Report, 169*(1), 3-5. http://doi.org/10.2139/ssrn.3836348

Internet & Jurisdiction Policy Network. (2021). *We need to talk about data: Framing the debate around free flow of data and data sovereignty*. https://www.internetjurisdiction.net/news/aboutdata-report

Instituto Brasileiro de Defesa do Consumidor. (2021). *Manual prático de adequação à Lei Geral de Proteção de Dados para micro e pequenas empresas*. https://idec.org.br/manual-lgpd-micro-pequenas-empresas

Instrução Normativa SGD/ME n. 117, de 19 de novembro de 2020. (2020). Dispõe sobre a indicação do Encarregado pelo Tratamento dos Dados Pessoais no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional. https://www.in.gov.br/en/web/dou/-/instrucao-normativa-sgd/me-n-117-de-19-de-novembro-de-2020-289515596

Lei Geral de Proteção de Dados Pessoais – LGPD. Lei n. 13.709, de 14 de agosto de 2018. (2018). Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Medida Provisória n. 1.124, de 13 de junho de 2022. (2022). Altera a Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), pois transforma a Autoridade Nacional de Proteção de Dados em autarquia de natureza especial e transforma cargos em comissão. http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Mpv/mpv1124.htm

Mikkelsen, D., Soller, H., Jansson, M., & Whalers, M. (2019). *GDPR compliance since May 2018: A continuing challenge*. McKinsey & Company. https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/gdpr-compliance-after-may-2018-a-continuing-challenge

Ministério da Economia. (2021). *Guia de elaboração de inventário de dados pessoais – LGPD*. https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_inventario_dados_pessoais.pdf/view

Núcleo de Informação e Coordenação do Ponto BR. (2021). *Segurança digital: uma análise de gestão de risco em empresas brasileiras*. https://www.nic.br/publicacao/seguranca-digital-uma-analise-de-gestao-de-risco-em-empresas-brasileiras/

Sombra, T., & Castellano, A. (Orgs.). (2021). *Proteção de dados e experiências setoriais: a visão do setor privado na implementação da LGPD*. Jota. https://conteudo.jota.info/setor-privado-lgpd

Análise dos Resultados
Privacidade e Proteção de Dados Pessoais 2021
Organizações públicas

A ampliação de iniciativas de transformação digital no setor público — que incluem a prestação de serviços por meios digitais e a adoção de novas tecnologias que facilitam a análise de dados e a tomada de decisão — está associada à melhoria da provisão de políticas públicas para a sociedade (Departamento de Assuntos Econômicos e Sociais das Nações Unidas [*United Nations Department of Economic and Social Affairs* – UN DESA], 2020). Constata-se que a digitalização do setor também intensificou a coleta, o armazenamento e a análise de dados dos cidadãos por parte das entidades públicas no exercício de suas funções. Nesse contexto, é fundamental compreender os possíveis riscos que o acesso e o uso desse grande volume de dados acarretam à proteção da privacidade e dos dados pessoais (Bleeker, 2020).

Tais preocupações se tornaram ainda mais evidentes com a pandemia COVID-19, quando a adoção de ferramentas digitais foi fundamental para manter a prestação dos serviços públicos durante as medidas de distanciamento social. As tecnologias digitais tiveram papel central nas estratégias dedicadas a informar a população sobre o novo vírus, monitorar o avanço da doença e auxiliar na tomada de decisões em relação à crise sanitária (UN DESA, 2020).

A disseminação de aplicações como *contact tracing*[1], que geralmente possibilitam o acesso a dados de geolocalização e de condições de saúde de seus usuários, estimularam a divulgação de uma série de recomendações por organizações nacionais e internacionais sobre a necessidade de que as entidades públicas encontrassem um equilíbrio entre o tratamento de dados dos cidadãos para o combate à pandemia e a garantia do direito à privacidade e proteção dos dados pessoais (Organização para a Cooperação e Desenvolvimento Econômico [OCDE], 2020b; Comitê Gestor da Internet no Brasil [CGI.br], 2020; European Data Protection Board [EDPB], 2020). Nesse sentido, o Programa das Nações Unidas para o Desenvolvimento (PNUD)

[1] Tecnologia que permite o rastreamento de contatos para localizar indivíduos infectados com a COVID-19 e seus contactantes e mensurar a disseminação da doença (Gomes, 2022).

ressaltou a importância de que os governos adotassem normas gerais ou marcos referenciais regionais ou internacionais para a proteção de dados sensíveis, garantindo privacidade e confidencialidade aos cidadãos (PNUD, 2020).

No Brasil, em 2018, foi promulgada a primeira norma geral sobre o tema. A Lei Geral de Proteção de Dados Pessoais (LGPD) regulou as diretrizes para o tratamento de dados nos meios físicos e digitais por indivíduos e organizações, incluindo o poder público. Além das exigências gerais, foi inserido um capítulo próprio na lei com disposições específicas para as organizações públicas.

Ao mesmo tempo que a nova legislação definiu princípios e limites, ela também possibilitou maior segurança para o uso de dados pessoais em prol da melhoria de serviços, ao incluir a execução de políticas públicas como um dos usos previstos para o tratamento de dados. Com a promulgação da LGPD, a ampliação das ações relacionadas à privacidade e à proteção de dados torna-se um dos principais desafios para a administração pública. Esse aspecto é ainda mais relevante no âmbito da implementação de programas governamentais, uma vez que se deve buscar o equilíbrio entre o tratamento de dados pessoais para melhorar a atuação do setor público e minimizar potenciais riscos aos cidadãos, como incidentes de segurança envolvendo dados pessoais, ações discriminatórias ou estigmatizantes resultantes da implementação de sistemas automatizados, vigilância indevida, entre outros.

Em alguns setores, a proteção de dados pessoais recebe ainda uma tutela jurídica especial por causa dos riscos aos titulares desses dados caso suas informações sejam indevidamente utilizadas. Entre eles, cabe destacar a coleta e o processamento de dados pessoais de crianças e adolescentes e de dados sensíveis ligados à saúde dos cidadãos. Isso gera a necessidade de maior cautela em termos de tratamento dos dados, especialmente em políticas públicas que costumam utilizar tais informações, como aquelas relacionadas à saúde e à educação. Ressalta-se ainda a necessidade de que os profissionais que atuam na coleta e análise desses dados estejam cientes e em conformidade com os requisitos de segurança e privacidade dos mesmos, como preconiza a LGPD.

Desta forma, levando-se em consideração o contexto apresentado anteriormente, o objetivo desta análise é traçar um panorama da proteção de dados no contexto das políticas públicas no país, incluindo a adoção de práticas por parte das organizações públicas, estabelecimentos de saúde e escolas. Inicialmente, analisa a forma como os órgãos públicos federais, estaduais e prefeituras estão adotando medidas para a proteção de dados dos cidadãos. Em seguida, concentra-se no setor da saúde, focando na adequação dos estabelecimentos públicos às exigências da LGPD. Por fim, são apresentados resultados sobre privacidade e proteção de dados pessoais no setor da educação, com foco nas instituições educacionais públicas de Educação Básica. As análises são baseadas nos resultados das pesquisas TIC Governo Eletrônico 2021, TIC Saúde 2021 e TIC Educação 2020, realizadas pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), departamento ligado ao Núcleo de Informação e Coordenação do Ponto BR (NIC.br).

Órgãos públicos federais e estaduais e prefeituras

Com a crescente preocupação em torno da privacidade e da proteção de dados pessoais e a entrada em vigor da LGPD no segundo semestre de 2020, a pesquisa TIC Governo Eletrônico 2021 (CGI.br, 2022) incluiu um novo módulo que buscou compreender como as organizações públicas brasileiras estão se estruturando para se adequarem à nova legislação. Foram adicionadas questões tanto para órgãos públicos federais e estaduais quanto prefeituras, que buscavam medir a presença de ações voltadas para a implementação das diretrizes e exigências previstas na lei.

Apesar de a LGPD não detalhar a necessidade de se criar estruturas ou áreas específicas, as organizações públicas e privadas foram instadas a realizar uma série de ações de adequação à lei. Um exemplo é o estímulo à criação de programas de governança de dados pessoais para dar suporte às atividades relacionadas à proteção de dados (Crespo, 2021). Para atender a essa disposição, há, no âmbito do Ministério da Economia (2020), uma recomendação de que os órgãos federais estabeleçam uma estrutura organizacional específica para governança e gestão da proteção de dados pessoais nas entidades da administração pública federal.

Segundo os resultados da pesquisa TIC Governo Eletrônico 2021, observa-se uma presença maior de pessoa ou área responsável pela implementação da LGPD nas organizações públicas federais (89%) do que nas estaduais (55%). Entre os poderes, destacam-se os órgãos públicos do Judiciário (94%) e do Ministério Público (73%). Por outro lado, apenas pouco mais da metade dos órgãos do Poder Executivo (56%) e 68% do Legislativo mencionaram a presença de pessoa ou área responsável pela implementação da legislação. Cabe salientar que na administração pública federal[2] e nos órgãos do Judiciário, por meio do Conselho Nacional de Justiça[3], já existe uma série de normativas e recomendações a respeito da aplicação da LGPD, o que pode explicar a maior institucionalização do tema nesses órgãos públicos.

Já entre as prefeituras brasileiras, apenas 28% declararam possuir pessoa ou área responsável pela efetivação da LGPD, sendo mais frequente entre as capitais (66%) e naqueles municípios com mais de 500 mil habitantes (62%), conforme o Gráfico 1.

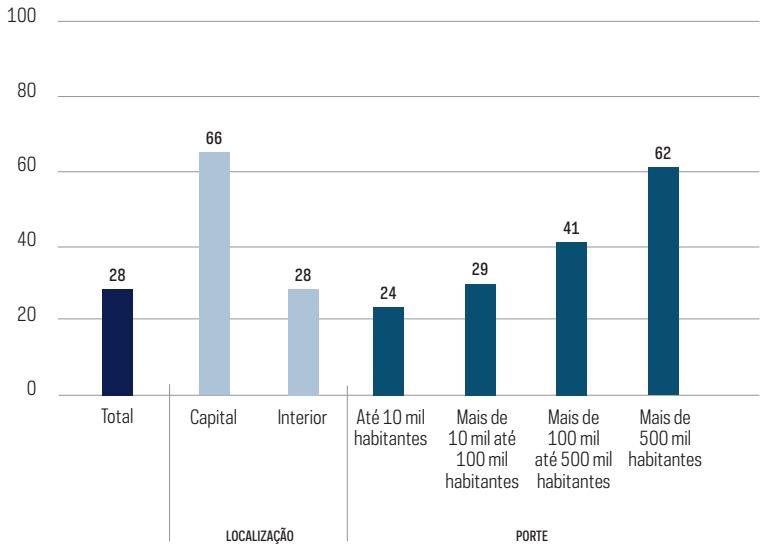
[2] Para mais informações, acesse https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados

[3] Para mais informações, acesse https://atos.cnj.jus.br/atos/detalhar/3668 e https://atos.cnj.jus.br/atos/detalhar/3432

GRÁFICO 1

PREFEITURAS, POR EXISTÊNCIA DE ÁREA OU PESSOA RESPONSÁVEL POR PROCEDIMENTOS E POLÍTICAS PARA A COLETA, O ARMAZENAMENTO OU O USO DE DADOS PESSOAIS OU PELA IMPLEMENTAÇÃO DA LGPD (2021)

Total de prefeituras (%)

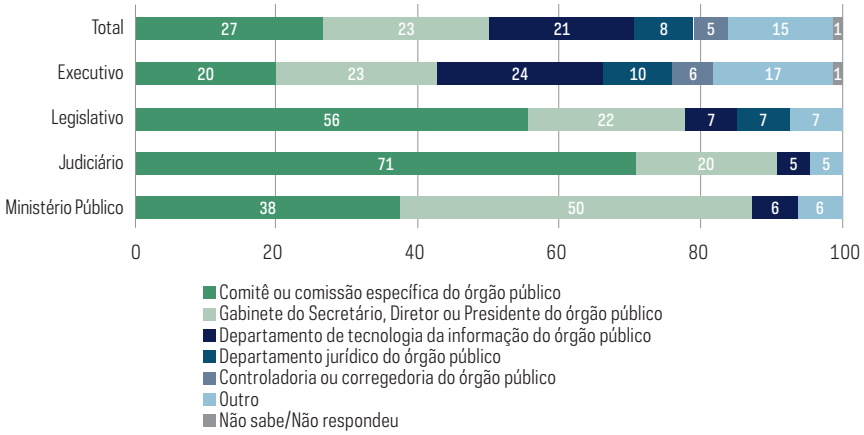


A pesquisa TIC Governo Eletrônico 2021 também identificou em que setor dos órgãos públicos esse tema estava sendo tratado. Verificou-se uma diversidade de setores responsáveis pela implementação da lei entre os poderes. Enquanto no Executivo não existia a predominância de um setor (Gráfico 2), nos órgãos públicos do Judiciário e do Legislativo, a implementação da lei geralmente era de responsabilidade de um comitê ou comissão específica. Nos órgãos do Executivo, a implementação da LGPD se divide principalmente entre o departamento de tecnologia da informação (TI) (24%), o gabinete do Secretário, Diretor ou Presidente (23%) e algum comitê ou comissão específica (20%). Já no Ministério Público, o setor mais mencionado — por metade dos órgãos públicos desse poder — foi o gabinete do Secretário, Diretor ou Presidente (50%), sendo a presença de comitê ou comissão específica o segundo setor mais declarado (38%).

GRÁFICO 2

ÓRGÃOS PÚBLICOS FEDERAIS E ESTADUAIS, POR SETOR DA PESSOA OU ÁREA RESPONSÁVEL PELO PROJETO DE IMPLEMENTAÇÃO DA LGPD (2021)

Total de órgãos públicos federais e estaduais com pessoa ou área responsável pela LGPD (%)



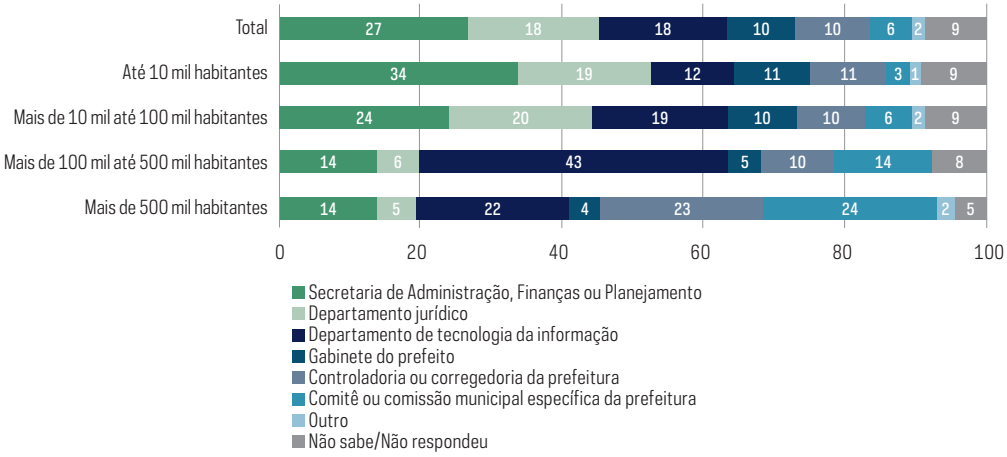
No caso das prefeituras, também foram identificados múltiplos setores responsáveis pela conformidade à LGPD. Entre os municípios com até 100 mil habitantes, as áreas mais citadas foram as secretarias de Administração, Finanças ou Planejamento; o departamento jurídico; e o departamento de TI (Gráfico 3). Nos municípios com população acima de 100 mil até 500 mil habitantes, quase metade das prefeituras mencionaram que a responsabilidade pela implementação da LGPD estava no departamento de TI. Entre as prefeituras com população superior a meio milhão de habitantes, não foi observado um padrão entre os setores responsáveis. Aproximadamente um quarto dessas prefeituras citaram um comitê ou comissão específica, 23% apontaram a controladoria ou corregedoria municipal; e 22% mencionaram que a área responsável era o departamento de TI.

Vale destacar que as estruturas dos governos municipais também diferem quanto à presença de certos departamentos ou setores e às suas capacidades organizacionais, o que poderia explicar a maior incidência de certas áreas como responsáveis pela conformidade à LGPD nas prefeituras. Cabe mencionar que pouco menos da metade das prefeituras brasileiras possui área ou departamento de TI, situação diferente das capitais e municípios com mais de 100 mil habitantes, em que quase a totalidade das prefeituras conta com esse setor em sua estrutura organizacional (CGI.br, 2022).

GRÁFICO 3

PREFEITURAS, POR SETOR DA PESSOA OU ÁREA RESPONSÁVEL PELO PROJETO DE IMPLEMENTAÇÃO DA LGPD (2021)

Total de prefeituras com pessoa ou área responsável pela LGPD (%)



A TIC Governo Eletrônico 2021 também investigou a nomeação do encarregado pelo tratamento de dados pessoais ou *Data Protection Officer* (DPO)[4]. A designação do encarregado ocorreu com maior frequência entre os órgãos federais (81%) do que nos estaduais (33%). Entre os poderes, foi mais citada pelos órgãos do Judiciário (81%) e do Ministério Público (73%). Menos da metade dos órgãos do Legislativo (40%) e do Executivo (34%) havia definido o encarregado pelo tratamento de dados pessoais no momento da pesquisa.

Nas prefeituras, entre as ações medidas pela pesquisa, essa foi a menos mencionada (Gráfico 4), sendo que somente 14% tinham nomeado esse profissional. Mesmo entre as prefeituras com maior porte populacional, menos da metade daquelas com mais de 500 mil habitantes tinha constituído algum encarregado. As proporções são ainda menores nos municípios com população de mais de 100 mil até 500 mil habitantes, nos quais apenas duas a cada dez prefeituras tinham um encarregado de dados.

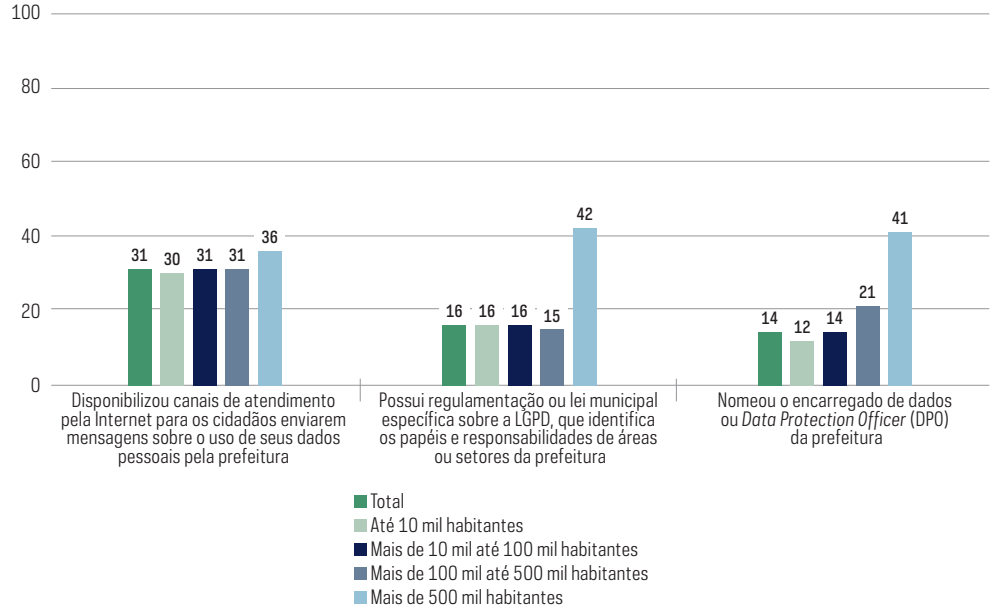
Portanto, apesar de o Artigo 23, inciso III, da LGPD, apontar a obrigatoriedade de o poder público indicar um encarregado ao realizar tratamento de dados pessoais, ainda é bastante incipiente a sua nomeação entre as organizações públicas investigadas pela TIC Governo Eletrônico 2021. Cabe destacar, além disso, que no futuro a Autoridade Nacional de Proteção de Dados (ANPD) pode eventualmente apresentar diretrizes e especificações para a definição do encarregado pelo tratamento de dados pessoais de acordo com as diferentes características das instituições públicas, a exemplo da desobrigação de indicá-lo entre os agentes de pequeno porte (ANPD, 2022c).

[4] Pessoa indicada para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD (Artigo 5º, inciso VIII). É responsável por garantir a conformidade da organização à LGPD (ANPD, 2022a).

GRÁFICO 4

PREFEITURAS, POR AÇÕES RELACIONADAS À LGPD, TOTAL E PORTE (2021)

Total de prefeituras (%)



Um dos princípios da LGPD é o da transparência quanto ao tratamento de dados pessoais, garantindo aos titulares o acesso a informações claras, precisas e facilmente acessíveis sobre esse tratamento[5] e imputando ao poder público a responsabilidade pela disponibilização dessas informações em meios de fácil acesso, preferencialmente pela Internet (ANPD, 2022b). Entre outras ações, isso inclui fornecer canais para os indivíduos entrarem em contato com as organizações públicas para obter informações e esclarecimentos sobre o tratamento de seus dados pessoais por essas entidades. A Lei n. 14.129/2021 reforça esse ponto, indicando que as plataformas de governo digital devem permitir que o cidadão efetue requisições às entidades públicas controladoras dos seus dados.

No entanto, ainda é pouco presente a disponibilidade de canais de atendimento pela Internet para que os titulares dos dados enviem solicitações a respeito do tratamento de seus dados pessoais e exerçam os direitos previstos na LGPD. Enquanto 65% dos órgãos federais tinham esse tipo de canal pela Internet, ele estava presente em apenas um terço dos órgãos estaduais. Entre os poderes destaca-se mais uma vez os órgãos do Judiciário, em que três a cada quatro possuíam atendimento *online* para esse fim.

[5] Artigo 6º, inciso VI.

Menos de um terço das prefeituras dispunha de canais de atendimento pela Internet para os cidadãos encaminharem solicitações sobre o uso de seus dados pessoais. Mesmo entre as prefeituras com mais de 500 mil habitantes, apenas 36% disponibilizavam esse tipo de atendimento, destacando a necessidade de canais digitais que estejam preparados para receber esse tipo de demanda.

Por outro lado, dados da TIC Governo Eletrônico 2021 apontam que os canais *online*, inclusive de recebimentos de solicitações da sociedade, já estão presentes em grande parte das organizações públicas no país. Mais de 80% dos órgãos federais e estaduais e 71% das prefeituras tinham ouvidoria *online* em 2021 (CGI.br, 2022). Também é bastante frequente a disponibilização de formas de contato para os cidadãos pelo *website* das organizações públicas, como endereço de *e-mail*, canais de denúncia e serviço de solicitação de acesso à informação. Assim, experiências de atendimento *online* em outras áreas poderiam ser utilizadas para auxiliar na ampliação de canais de contato para os titulares de dados sobre questões relativas à LGPD.

Por fim, uma das dimensões associadas à implantação de uma cultura de respeito à privacidade e proteção de dados pessoais nas organizações é a presença de ações de conscientização para seus funcionários em torno do tema e dos regulamentos existentes. O Artigo 50, da LGPD, dispõe que um programa de governança em privacidade pode incluir ações educativas como uma de suas atividades. Ressaltando a importância desse tema, o *Guia de Elaboração de Programa de Governança em Privacidade*, do governo federal, assinala a necessidade de programas educativos voltados aos colaboradores que os informem sobre políticas e práticas de proteção à privacidade (Ministério da Economia, 2021).

A TIC Governo Eletrônico 2021 investigou se as organizações públicas ofertaram alguma capacitação, curso ou treinamento sobre a LGPD para pelo menos um funcionário da área ou departamento de TI. Entre os órgãos federais e estaduais que tinham departamento de TI (87%), esse tipo de ação foi mais frequente nas organizações do Judiciário (91%) e do Ministério Público (82%) — justamente aquelas que já possuíam pessoa ou área responsável pela implementação da conformidade à LGPD em maiores proporções. Cerca de metade dos órgãos públicos do Executivo e Legislativo realizou esse tipo de formação entre funcionários do departamento de TI.

No nível local, as prefeituras de capitais (63%) ofertaram mais frequentemente capacitação, curso ou treinamento sobre a LGPD no setor de tecnologia do que aquelas localizadas no interior (24%). Entre as prefeituras com população superior a 500 mil habitantes, três a cada quatro ofereceram alguma formação sobre a lei ao departamento de TI.

Os indicadores coletados junto a órgãos públicos demonstraram disparidades na institucionalização da legislação, principalmente entre órgãos estaduais e prefeituras e nos órgãos públicos do Executivo e Legislativo quando comparado aos demais poderes. Apesar de a LGPD só ter entrado em vigência dois anos após a sua promulgação e de as suas sanções só passarem a valer a partir de agosto de 2021, as organizações públicas no país parecem estar ainda em uma fase inicial de adequação à legislação.

Além de lidarem com os impactos da pandemia COVID-19, o que direcionou os esforços das entidades públicas desde 2020, cabe ressaltar que a adaptação à lei envolve ações em diversos aspectos e setores de uma organização, incluindo mudanças organizacionais, tecnológicas e culturais em prol de uma atuação voltada para a proteção de dados (Crespo, 2021). Nesse sentido, ampliar o entendimento sobre as diferentes estruturas e capacidades das organizações públicas se torna fundamental para compreender os desafios relacionados à implementação da LGPD. Isso é especialmente relevante para as entidades responsáveis pelo cumprimento da lei, como a ANPD, orientarem suas ações às dimensões mais desafiadoras para o poder público garantir a privacidade e proteção de dados pessoais dos cidadãos.

Estabelecimentos públicos de saúde

Nos últimos anos, a assistência e a gestão em saúde têm passado por uma ampla transformação. Esse processo pode ser observado com o avanço da saúde digital, que inclui a expansão da infraestrutura de tecnologias de informação e comunicação (TIC) nos estabelecimentos, o desenvolvimento de aplicações digitais pelos setores público e privado e a sua apropriação pelos profissionais da área.

Essa transformação tem gerado um rápido crescimento na variedade e no volume de informações dos pacientes disponíveis em formato eletrônico. Além disso, cada vez mais, tais informações são coletadas nos prontuários eletrônicos dos pacientes e nas atividades de telessaúde e são trocadas entre estabelecimentos de saúde e instituições da área. Assim, é fundamental a padronização e a regulamentação que garanta um tratamento seguro dos dados gerados digitalmente.

Nesse sentido, a Organização Pan-Americana da Saúde (OPAS), ao estabelecer oito princípios norteadores para a transformação digital na área, dedica um deles à instituição de mecanismos de confiança e segurança da informação para o ambiente digital da saúde pública. Entre as ações sugeridas estão a adoção de instrumentos regulatórios sobre o tratamento e o acesso aos dados de saúde. Isso inclui privacidade, sigilo e segurança da informação; definição de perfis de acesso a partir de ações que o usuário deve realizar e treinamento de todos os atores envolvidos no fluxo de informações de saúde sobre diretrizes de segurança e riscos associados. Além disso, refere-se a adoção de mecanismos de monitoramento que permitam a detecção de incidentes de segurança nos sistemas de informação em saúde; instrumentos de consentimento informado para acesso, registro e proteção das informações confidenciais, entre outros (OPAS, 2021).

As diretrizes recomendadas internacionalmente são convergentes com o que normatiza a LGPD no Brasil. No caso do setor da saúde, a lei exige uma profunda adequação dos estabelecimentos dessa área, das empresas do ramo farmacêutico, dos centros de pesquisa clínica e dos órgãos de pesquisa públicos e privados que controlam dados pessoais sensíveis referentes à saúde (Dallari & Monaco, 2021).

Para fins de regulação das atividades de tratamento de dados, a lei categoriza uma diferenciação entre dados pessoais e os dados pessoais sensíveis. O dado pessoal é composto de informações relacionadas a pessoa natural identificada ou identificável

(Artigo 5º, inciso I). Já os dados sensíveis são exemplificados como aqueles que se referem à "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (Artigo 5º, inciso II) (Mulholland, 2018).

Assim, os dados das condições de saúde de pacientes, como histórico médico, doenças, tratamentos realizados, uso de medicamentos, entre outros, são tutelados como dados sensíveis. São classificados dessa maneira por apresentarem maior potencial de risco para seus titulares no caso de tratamento abusivo ou ilícito, justamente por se referir a características do titular que possam, com maior probabilidade, acarretar preconceito, discriminação ou outras formas de abuso. Esses dados podem revelar certa situação de vulnerabilidade, e sua utilização indevida pode ocasionar prejuízos a direitos fundamentais das pessoas, especialmente ligados a privacidade, igualdade, intimidade e dignidade da pessoa humana (Botelho & Camargo, 2021).

Contudo, um dado pessoal pode se transformar em um dado sensível em razão de ferramentas existentes para o seu tratamento, permitindo a correlação de um dado com um objetivo e identificando o seu titular (Bioni, 2018). Desse modo, é possível uma extensão interpretativa daqueles dados que mesmo inicialmente não entendidos como sensíveis demonstrem sensibilidade a depender de seu contexto de tratamento, como previsto no Artigo 11, parágrafo 1º da LGPD. Essa extensão interpretativa exige uma análise contextual sobre o tratamento de dados pessoais, devendo ser observados fatores como ilicitude, discriminação, vulnerabilidade do titular e potenciais danos (Costa, 2022).

Consequentemente, a LGPD determinou uma proteção mais cautelosa para o tratamento de dados pessoais sensíveis e que possam causar dano ao titular (paciente). Para sua utilização, é necessário que haja consentimento do titular, com exceção de casos que envolvam proteção à vida dele ou de terceiros ou tutela de saúde, execução de políticas públicas previstas em leis ou regulamentos e realização de estudos por órgãos de pesquisas, entre outras hipóteses. O tratamento dos dados deve prever a garantia, sempre que possível, da anonimização destes.

Para uma efetiva proteção de dados pessoais, a LGPD define alguns conceitos e estipula algumas medidas que devem ser adotadas pelas instituições detentoras das informações. Para o caso do setor da saúde, o titular dos dados é o paciente, o controlador é o estabelecimento de saúde, os operadores são aqueles que tratam os dados em nome do controlador, como organizações contratadas para serviços terceirizados, devendo ser observado que os funcionários de um estabelecimento não se enquadram como operadores, pois tratam os dados em virtude do trabalho subordinado, não podendo ser responsabilizados pelas decisões do controlador. Já o encarregado de dados é o responsável indicado pelo estabelecimento de saúde como canal de comunicação entre estabelecimento, titular-paciente e a ANPD, órgão que fiscaliza o cumprimento dessa lei (Hawryliszyn *et al.*, 2021). Devido ao viés voltado ao interesse público, a LGPD veda a comunicação ou uso compartilhado entre controladores de dados pessoais sensíveis relativos à saúde com objetivo de vantagem econômica, com exceção dos casos envolvendo prestação de serviço de saúde, assistência farmacêutica e de assistência à saúde (Botelho & Camargo, 2021).

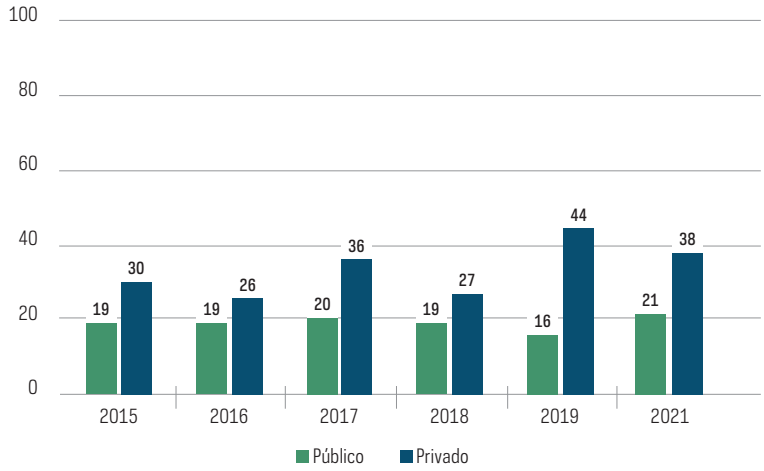
Nesse contexto, a pesquisa TIC Saúde já investigava, antes da promulgação da lei, ações voltadas à proteção de dados realizadas pelos estabelecimentos de saúde como instituição de política de segurança da informação e treinamento de profissionais sobre o tema, além da adoção de ferramentas de segurança da informação. Segundo os resultados da pesquisa, em 2021, apenas 21% dos estabelecimentos de saúde públicos e 38% dos privados tinham um documento que definia uma política de segurança da informação (Gráfico 5). Esse resultado apresenta pouca variação entre os estabelecimentos públicos ao longo da série histórica, visto que, em 2015, o percentual era de 19%, mostrando que a vigência da lei ainda não impactou significativamente a presença de uma política de segurança da informação nos sistemas públicos de saúde (CGI.br, 2021b).

Também é investigada a existência de treinamento de funcionários dos estabelecimentos de saúde em relação à segurança da informação. Em 2021, 69% das instituições que tinham uma política de segurança da informação realizaram algum tipo de treinamento sobre esse tema, sendo que a atividade foi mais comum nos estabelecimentos privados (72%) do que nos públicos (62%).

GRÁFICO 5

ESTABELECIMENTOS DE SAÚDE, POR EXISTÊNCIA DE DOCUMENTO QUE DEFINE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (2021)

Total de estabelecimentos de saúde que utilizaram a Internet nos últimos 12 meses (%)



Portanto, os resultados mostram um percentual reduzido de estabelecimentos de saúde que possuem institucionalizadas as políticas de segurança e privacidade das informações sensíveis dos pacientes. No entanto, nos estabelecimentos em que essa política foi instituída, a maioria dos gestores informou que são oferecidos treinamentos para os seus profissionais. Uma política de segurança da informação abrangente deve considerar além de ferramentas de segurança e responsáveis pelos dados, o treinamento dos funcionários, para melhor uso das ferramentas e aplicações em saúde.

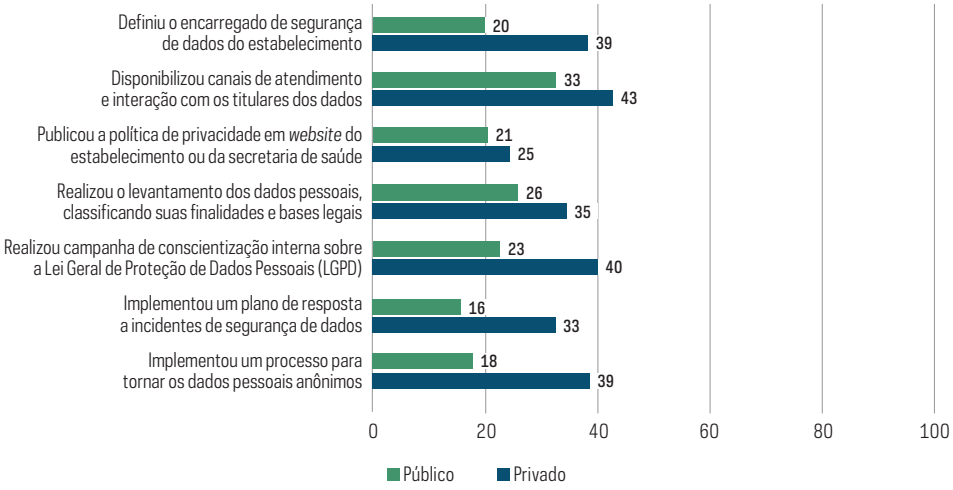
Dada a relevância da LGPD para o setor, a pesquisa TIC Saúde incluiu, em sua edição de 2021, um novo indicador, que investigou a adequação dos estabelecimentos de saúde aos termos estabelecidos pela lei. Com entrevistas realizadas no primeiro semestre de 2021, os resultados permitem monitorar as medidas implementadas pelos estabelecimentos no contexto da entrada em vigência da lei.

Assim, a pesquisa TIC Saúde passou a medir a constituição da figura do encarregado de dados pessoais nos estabelecimentos de saúde, cujas atividades consistem em ser um canal de comunicação com os pacientes, aceitando reclamações, prestando esclarecimentos e adotando providências cabíveis, receber comunicações da ANPD e dar providências, além de orientar os funcionários e contratados da entidade sobre as práticas a serem adotadas (Artigo 41). Em relação a essa exigência da lei, verificou-se que apenas 20% dos estabelecimentos públicos e 39% dos privados haviam se adequado a essa medida (Gráfico 6).

GRÁFICO 6

ESTABELECIMENTOS DE SAÚDE, POR MEDIDAS ADOTADAS EM RELAÇÃO À LGPD (2021)

Total de estabelecimentos de saúde que utilizaram a Internet nos últimos 12 meses (%)



A LGPD também determina que o tratamento dos dados pessoais deve ser realizado com base em uma finalidade com propósitos legítimos, específicos, explícitos e informados aos titulares, conforme o Artigo 6º, inciso I. No caso dos estabelecimentos públicos, apenas 26% deles realizaram um levantamento dos dados pessoais, classificando suas finalidades e bases legais. No setor privado, esse levantamento foi realizado por 35% dos estabelecimentos.

Outro ponto que, além de seguir a determinação da lei, impacta também a transparência da utilização dos dados dos titulares é a necessidade de disponibilização de canais de atendimento e interação com os mesmos, de forma a garantir maior transparência das operações (Artigo 6º, incisos IV e VI). Essa foi a medida que

apresentou maior percentual de estabelecimentos de saúde tanto públicos (33%) quanto privados (43%) que informaram ter disponibilizado canais com essa finalidade.

A lei também recomenda a elaboração de um plano com regras de boas práticas e de governança em privacidade que leve em consideração, em relação ao tratamento dos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes do tratamento de dados, conforme o Artigo 50. Esse plano deve contemplar processos e políticas internas que assegurem o cumprimento de normas e boas práticas relativas à proteção de dados pessoais, estabelecendo uma relação transparente e garantindo mecanismos de participação do titular, contando com planos de resposta a incidentes e remediação, entre outros recursos necessários para assegurar e garantir à proteção destes dados. O plano deve, ainda, ser publicado e atualizado periodicamente.

Quanto a essas recomendações, uma grande parcela dos estabelecimentos públicos de saúde ainda não está adequada às referidas medidas. Apenas 21% publicaram uma política de privacidade no *website* do estabelecimento ou da secretaria de saúde. Nesse item, os estabelecimentos privados (25%) apresentam resultado muito próximo ao dos públicos. Em relação a outras medidas verificadas, um maior percentual de estabelecimentos de saúde privados se adequou às necessidades exigidas pela lei em comparação aos públicos. Apenas 18% dos públicos implementaram um processo para tornar os dados pessoais anônimos e 16% implementaram um plano de resposta a incidentes de segurança de dados, enquanto os privados apresentaram taxa de 39% e 33%, respectivamente.

Para que os processos adotados e as políticas internas assegurem a adequação, de forma abrangente, das normas e boas práticas relativas à proteção de dados pessoais, é necessário o conhecimento destas e a conscientização de sua importância por parte dos atores envolvidos em todos os níveis da atenção e gestão do estabelecimento. Apesar da relevância da realização de campanhas para conscientização interna sobre a LGPD, esse tipo de medida foi realizado por 23% dos estabelecimentos públicos e 40% dos privados. É imprescindível que essas medidas sejam ampliadas de modo que todos os funcionários e profissionais de saúde de um estabelecimento de saúde estejam engajados e reconheçam a importância do cumprimento da LGPD, visto que desde a entrada do paciente na recepção até sua alta, dados sensíveis estão sendo trabalhados, tornando o setor um dos mais direta e amplamente impactados pela nova legislação.

É inequívoco que os resultados apresentados indicam um grande desafio para a adaptação dos estabelecimentos de saúde às exigências da lei. O surgimento da pandemia COVID-19 demandou dos estabelecimentos medidas emergenciais em outros âmbitos de atendimento e gestão, o que pode ter comprometido o avanço da tomada de medidas em relação à LGPD. No entanto, é imperativo que os estabelecimentos de saúde se adequem à lei e garantam a segurança das informações e o direito à privacidade dos titulares.

Escolas públicas de Educação Básica

No início de 2021, a Organização das Nações Unidas (ONU) realizou o lançamento global do *Comentário Geral nº 25 sobre os direitos da criança em relação ao ambiente digital* (ONU, 2021), documento que amplia o escopo de aplicação da Convenção sobre os Direitos da Criança também para os espaços digitais. A privacidade é compreendida no documento como um dos aspectos pertinentes aos direitos digitais de crianças e adolescentes, que deve ser preservado a partir dos meios cabíveis em prol de seu melhor interesse.

Desde 2000, a discussão sobre privacidade, segurança e proteção de dados de crianças e adolescentes, especialmente nos ambientes digitais, está presente na Children's Online Privacy Protection Act (COPPA) (U.S. Congress, 1998), legislação aplicada pelos Estados Unidos que tem como objetivo principal evitar a exposição desse público aos riscos *online*, principalmente à pornografia. O General Data Protection Regulation (GDPR) (European Union, 2018), implementado pela União Europeia a partir de 2018, também dedica atenção especial ao tema da proteção de dados de crianças e adolescentes. Desde então, os países do bloco europeu têm realizado esforços para o desenvolvimento de diretrizes específicas, principalmente no que diz respeito à oferta de serviços *online* para esse público, como em aplicações, jogos, *websites* e redes sociais. No Brasil, a LGPD, em sua seção III, do capítulo II, também dedica um espaço específico às diretrizes sobre o tratamento de dados de crianças e adolescentes, atribuindo a pais e responsáveis legais a incumbência de controlar os processos de tratamento de dados por meio de consentimento apropriado.

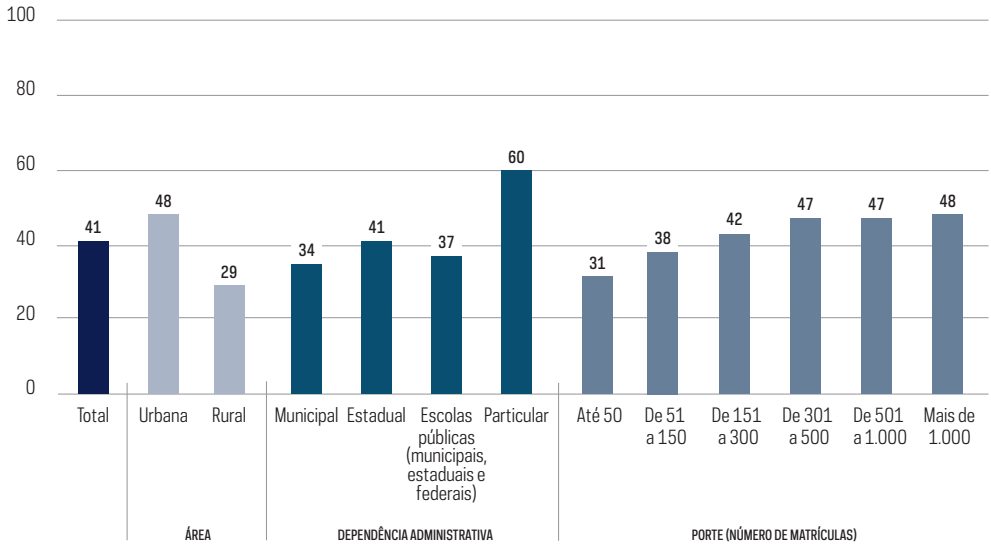
Embora as discussões em torno da privacidade de crianças e adolescentes tenham ganhado relevância, especialmente nas últimas duas décadas, a aplicação prática de tais princípios ainda é bastante complexa. Um dos desafios está na diversidade de formas de coleta de dados pessoais de crianças e adolescentes, uma vez que não se trata apenas das informações compartilhadas conscientemente por eles ou por seus cuidadores (pais, responsáveis legais, instituições educacionais, professores, entre outros), mas também das informações derivadas de suas práticas *online*. Esse desafio fica bastante evidente quando se analisa o contexto educacional, especialmente o contexto das escolas públicas de Educação Básica, cuja responsabilidade pela coleta e pela proteção dos dados dos estudantes têm de ser compartilhada com órgãos da administração pública, como secretarias e diretorias de ensino.

Segundo dados da pesquisa TIC Educação 2020 (CGI.br, 2021a), 41% das escolas de Educação Básica no Brasil possuíam um documento que definia a política de proteção de dados e de segurança da informação na instituição, percentual que era de 60% entre as escolas particulares e de 37% entre as públicas (municipais, estaduais e federais) (Gráfico 7). No entanto, o ecossistema de uso de tecnologias no âmbito educacional se torna cada vez mais amplo e diverso, dificultando que as instituições educacionais consigam prever todos os tipos e as formas de dados pessoais tratados, direta ou indiretamente, a partir das atividades realizadas pela comunidade escolar.

GRÁFICO 7

ESCOLAS QUE POSSUEM DOCUMENTO QUE DEFINE A POLÍTICA DE PROTEÇÃO DE DADOS E DE SEGURANÇA DA INFORMAÇÃO NA INSTITUIÇÃO (2020)

Total de escolas (%)



Os dados pessoais de crianças e adolescentes podem ser categorizados em três tipos (van der Hof, 2016; Livingstone *et al.*, 2019; OCDE, 2020a):

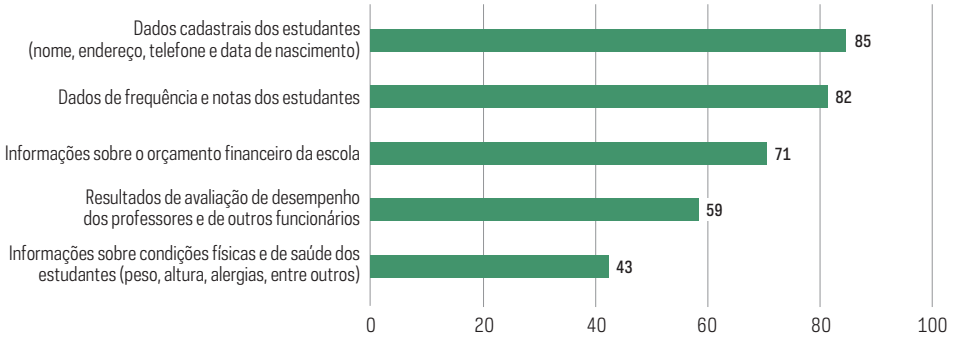
- **Dados fornecidos**, ou seja, informações que são fornecidas por crianças e adolescentes ou por seus pais, responsáveis e instituições educacionais;
- **Dados rastreados**, resultado das atividades realizadas por eles de forma *online*, como *cookies*, impressão digital, dados de geolocalização, buscas em navegadores e *websites*, entre outros;
- **Dados inferidos**, que são aqueles derivados de análises realizadas a partir das informações fornecidas e dos rastros deixados durante o uso de aplicações.

No que diz respeito aos dados fornecidos, 82% das escolas públicas com turmas de Ensino Fundamental e Médio registravam ou consultavam em formato eletrônico dados de frequência e notas e 85% registravam ou consultavam dados cadastrais dos estudantes, como nome, endereço, telefone e data de nascimento. Além da coleta e do armazenamento desses dados, 43% das escolas públicas registravam ou consultavam em formato eletrônico informações sobre condições físicas dos estudantes, por exemplo, peso, altura, alergias, entre outros (Gráfico 8).

GRÁFICO 8

ESCOLAS PÚBLICAS QUE REGISTRAM OU CONSULTAM DADOS DOS ESTUDANTES E DA ESCOLA EM FORMATO ELETRÔNICO (2020)

Total de escolas (%)



Para além dos dados armazenados nos sistemas de gestão das instituições, as escolas fazem uso também de outros sistemas que podem coletar informações sensíveis dos estudantes. De acordo com a edição 2020 da pesquisa TIC Educação, uma porcentagem pequena de escolas públicas contava com sistemas de identificação dos estudantes pela digital ou palma da mão (2%), mas o uso de dados biométricos tem se intensificado entre as redes de ensino[6]. Por outro lado, 30% das escolas públicas possuíam sistema interno de câmeras de vídeo, percentual que chegava a 59% entre as escolas estaduais e a 71% entre as escolas públicas com mais de mil matrículas.

Um quarto das escolas públicas contava com um aplicativo da própria instituição para telefone celular ou *tablet* e, em 6% delas, o aplicativo permitia o monitoramento das atividades dos estudantes por meio de acesso às câmeras de vídeo da escola. Em 12% das escolas públicas, o aplicativo permitia também o registro de acompanhamento das atividades diárias dos estudantes, como alimentação, comportamento, humor e participação.

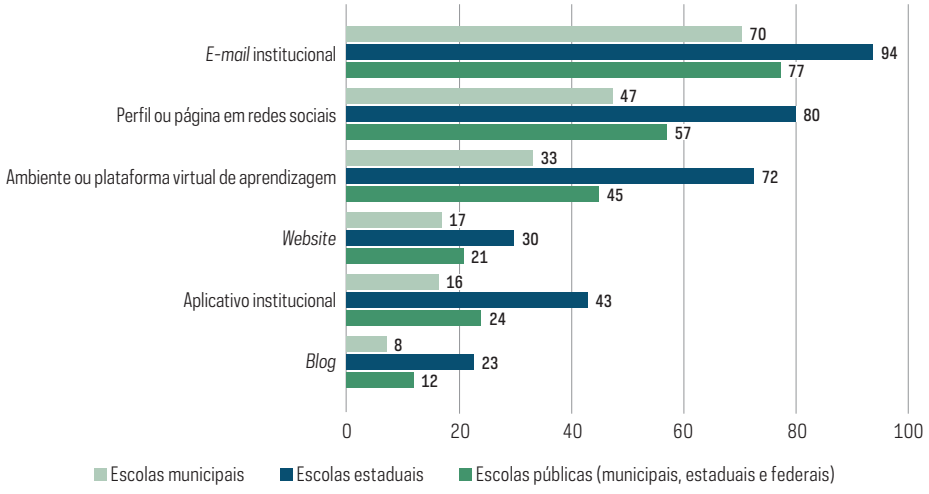
As escolas coletam e armazenam ainda uma grande quantidade de dados de rastreamento e que podem ser também fontes de informações para dados inferidos. No geral, o grande fluxo de informações sobre os estudantes ocorre por meio de plataformas e ambientes virtuais de aprendizagem e por aplicações e plataformas de redes sociais. Segundo a pesquisa TIC Educação, em 2020, 45% das escolas públicas de Educação Básica utilizavam ambientes ou plataformas virtuais de aprendizagem, percentual que apresentava variações de acordo com o nível de conectividade das escolas, estando mais presentes em instituições localizadas em áreas urbanas (61%), em capitais (71%), em escolas com mais de mil matrículas (79%) e entre as escolas estaduais (72%), onde também era possível observar maior presença e uso de sistemas, plataformas e redes sociais (Gráfico 9).

[6] Escolas públicas de município baiano usam reconhecimento facial para controlar frequência dos alunos (9/2/2022). https://g1.globo.com/jornal-nacional/noticia/2022/02/09/escolas-publicas-de-municipio-baiano-usam-reconhecimento-facial-para-controlar-frequencia-dos-alunos.ghtml

GRÁFICO 9

ESCOLAS PÚBLICAS, PRESENÇA E USO DE SISTEMAS, PLATAFORMAS E REDES SOCIAIS DIGITAIS, POR DEPENDÊNCIA ADMINISTRATIVA (2020)

Total de escolas públicas (%)



As medidas sanitárias de enfrentamento à pandemia COVID-19, como o distanciamento social e o consequente fechamento das escolas, com a implementação de atividades educacionais remotas, impulsionaram ainda mais o uso de plataformas, ambientes, aplicações e redes digitais na Educação Básica, com uma crescente participação da iniciativa privada na oferta de tais recursos. De acordo com a pesquisa TIC Educação 2020, a realização de aulas a distância por meio de plataformas de videoconferência, por exemplo, foi citada por 59% dos gestores de escolas públicas como uma medida adotada para a continuidade da realização de atividades pedagógicas durante a pandemia, e o uso de redes sociais e aplicativos de mensagem instantânea com essa finalidade chegou a 90%.

Em grande parte dos casos, as plataformas ou os ambientes virtuais de aprendizagem são utilizados pelos professores de escolas públicas para aplicar provas e exercícios para os estudantes (42%), para que estes possam enviar atividades aos professores (41%), ou ainda, para que possam tirar dúvidas com os docentes por meio de videoconferência (38%). No entanto, a disponibilização de ferramentas baseadas em técnicas de Inteligência Artificial pode oferecer outras opções de uso dos dados dos estudantes coletados a partir de tais recursos, como a possibilidade de que eles realizem testes de desempenho e possam criar um plano de estudo individualizado (29%) ou ainda de que os professores e gestores escolares tenham acesso a relatórios de desempenho dos estudantes (39%).

A analítica de aprendizagem (*Learning Analytics*, no inglês) é outra área que tem sido aprimorada com o uso de plataformas e ambientes virtuais de aprendizagem. Para 41% dos gestores de escolas públicas, as plataformas educacionais utilizadas permitem que os educadores analisem a forma como os estudantes aprendem, 39%

dizem que é possível avaliar o progresso da aprendizagem e 29% que é possível realizar análises sobre as características emocionais dos estudantes, como ansiedade, tristeza ou entusiasmo.

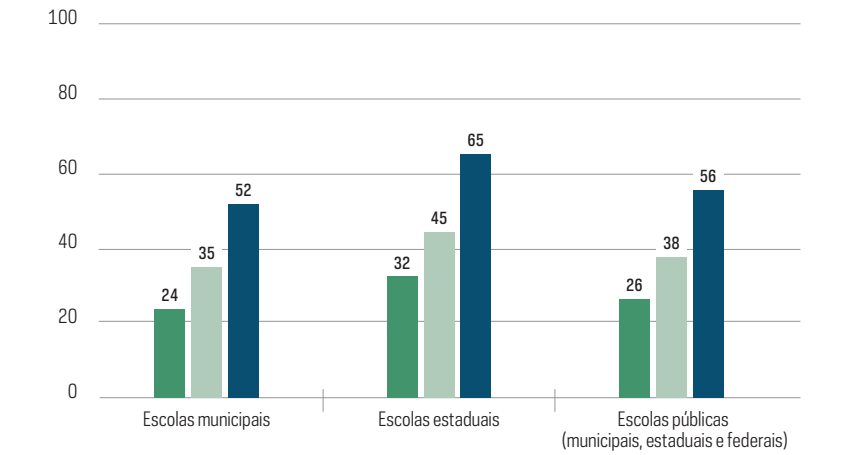
Grande parte dos rastros deixados por estudantes e professores nos ambientes virtuais pode se tornar fonte de dados inferidos, ou seja, base para análises sobre as características pessoais dos usuários. Além de as escolas, os estudantes e os professores não terem controle sobre os dados coletados nesses ambientes, um dos riscos associados ao uso de tais plataformas, aplicações e redes é o compartilhamento dos dados dos usuários por parte das empresas de tecnologia com serviços de *marketing* digital, a exibição de anúncios baseados em análises comportamentais e contextuais e a criação de perfis segmentados para recomendação de conteúdo personalizado (Organização das Nações Unidas para a Educação, a Ciência e a Cultura [UNESCO], 2022; Human Rights Watch, 2022).

Como ações de enfrentamento em relação a tais riscos, documentos e análises sobre a privacidade e a proteção de dados no âmbito educacional (Henriques & Hartung, 2021; Laterça *et al.*, 2021; UNESCO, 2022) chamam a atenção para a importância da garantia legal dos direitos dos estudantes e do incentivo para que haja um maior envolvimento das empresas de tecnologias no desenvolvimento de aplicações que respeitem tais direitos *by design*, ou seja, que contenham em seus modelos computacionais princípios de ética em relação ao bem-estar de crianças e adolescentes.

GRÁFICO 10

ESCOLAS PÚBLICAS, ATIVIDADES DE FORMAÇÃO REALIZADAS PELA INSTITUIÇÃO (2020)

Total de escolas públicas (%)



Para além de tais ações, instituições envolvidas na defesa dos direitos digitais de crianças e adolescentes enfatizam também a importância do envolvimento dos próprios atores educacionais na promoção de espaços digitais mais adequados. Em 2020, 26% das escolas públicas haviam citado a realização de debates ou palestras promovidos pela escola sobre privacidade e proteção de dados pessoais nos 12 meses anteriores à realização da pesquisa (Gráfico 10). É importante que tais iniciativas sejam disseminadas para um maior número de escolas. O desenvolvimento de habilidades digitais e de criticidade entre estudantes, educadores e pais e responsáveis é considerado de extrema relevância para a conscientização sobre as diversas formas de coleta e uso de dados pessoais, além de medidas que podem atribuir maior segurança e proteção durante o uso dos recursos digitais.

Considerações finais: agenda para políticas públicas

Ao mesmo tempo em que o desenvolvimento tecnológico possibilitou a incorporação das TIC nas mais diversas atividades nas organizações públicas, incluindo o uso de dados dos cidadãos para os mais diferentes propósitos, também trouxe à tona a importância de garantir a segurança da privacidade e da proteção de dados pessoais. Além disso, a crescente digitalização do setor público tornou mais evidentes as desigualdades entre as instituições e os órgãos públicos no que diz respeito à prontidão para lidar com esse tipo de dado, sobretudo em situações de emergência como a da pandemia COVID-19. Com a ampla atenção de organizações nacionais e internacionais em relação ao tema e a promulgação da LGPD no Brasil, as instituições públicas passaram a ter uma série de atribuições para realizarem o tratamento de dados pessoais. Nesse sentido, a análise reuniu uma visão geral sobre a privacidade e a proteção de dados nas organizações públicas no país a partir de indicadores de pesquisas do Cetic.br|NIC.br.

Os dados apresentados indicam que, em geral, a presença de estruturas voltadas para a implementação da LGPD ainda é incipiente nas organizações públicas brasileiras, sugerindo que estão na fase inicial de adequação à legislação. Destacam-se os órgãos públicos do Judiciário, em que grande parte das estruturas e ações relacionadas à LGPD medidas pela pesquisa já estava em andamento. Além disso, os órgãos federais também possuíam, em maiores proporções, iniciativas sobre o tema, especialmente quando comparadas a órgãos estaduais e prefeituras. Uma das possíveis explicações para a considerável presença das ações investigadas no nível federal e nos órgãos do Judiciário é a maior institucionalização de recomendações e normativas a respeito do assunto nessas instituições. Entre as recomendações existentes estão uma série de guias operacionais para adequação à LGPD elaboradas pelo Ministério da Economia, por meio da Secretaria de Governo Digital, além de questionários para o diagnóstico da maturidade de privacidade e segurança na administração pública federal[7]. Também foram criadas normas voltadas para a implementação da lei nesse nível de governo, a exemplo da Instrução Normativa SGD/ME n. 117, que trata das diretrizes para

[7] Para mais informações, acesse https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados

a indicação do encarregado de dados. Já o Conselho Nacional de Justiça, entre outras iniciativas, estabeleceu medidas para a adequação à LGPD pelos tribunais (Resolução n. 363/2021).

Portanto, os resultados evidenciam disparidades na implementação da LGPD nos órgãos públicos federais e estaduais e prefeituras, indicando a necessidade de ações para compreender em profundidade os principais desafios enfrentados por essas organizações para atender às exigências previstas na lei. O maior entendimento sobre quais são as principais barreiras para a adequação pode auxiliar as entidades responsáveis pelo cumprimento da legislação, como a ANPD, a direcionarem seus esforços para garantir a privacidade e a proteção de dados pessoais na atuação do poder público.

Os resultados apresentados sobre o setor da saúde demonstram um grande desafio que se impõe para que os estabelecimentos públicos de saúde se adequem às exigências estabelecidas pela LGPD. Para obter avanços nessa área, é necessária uma coordenação entre os entes federativos para que as medidas e os processos sejam estabelecidos e adotados pelos atores do setor da saúde, como gestores, funcionários e profissionais. Tal preceito é requisito para que não ocorra utilização inapropriada de dados sensíveis dos pacientes e que estes se sintam cada vez mais confiantes e seguros quanto ao uso de suas informações, estando plenamente informados e cientes do uso destes dados. Entre as penalidades aplicáveis às instituições que não estiverem em conformidade com a LGPD estão tanto as que se referem ao aspecto financeiro, como multas, quanto a suspensão do direito de coletar qualquer tipo de dado dos titulares, causando a interrupção das atividades e do funcionamento do estabelecimento de saúde.

O Ministério da Saúde tem realizado estudos para avançar na discussão e elaborar um normativo elencando dois temas fundamentais: a definição dos perfis da LGPD e a definição sobre o consentimento na Rede Nacional de Dados em Saúde (RNDS) (Ministério da Saúde, 2021). No entanto, ainda permanecem lacunas sobre como deve ser realizada a troca de dados, a interoperabilidade em saúde e a definição de procedimentos para os serviços em saúde e os profissionais da área, com conhecimento para atuar em saúde digital, na coleta e uso de dados para o registro em prontuários clínicos. Muitos desafios devem ser superados para garantir a segurança jurídica que sustentará o avanço da saúde digital no país e a transparência sobre o uso das informações dos titulares.

Na área da educação, os resultados apontaram que as escolas públicas de Educação Básica possuem grande quantidade de informações dos estudantes, não apenas dados pessoais registrados na própria escola, mas também aqueles gerados por meio de aplicativos de monitoramento de atividades, inclusive por meio de imagens de crianças e adolescentes. No entanto, menos da metade delas possuía um documento que definisse uma política de proteção de dados e de segurança da informação na instituição.

O Ministério da Educação tem realizado ações para mapear e diagnosticar o uso de dados pessoais internamente, como o desenvolvimento do Programa Institucional de Proteção de Dados Pessoais e Privacidade, institucionalização do Subcomitê de Segurança da Informação e Proteção de Dados Pessoais e do Núcleo de Estudos

para Implantação da Lei Geral de Proteção de Dados Pessoais, além da realização de levantamento das atividades de tratamento de dados pessoais. Do lado das escolas públicas, é necessária a elaboração de processos e a adoção de medidas, por parte das secretarias de educação, que auxiliem essas escolas a adotarem soluções que protejam as informações dos estudantes e garantam sua privacidade.

Diante desse cenário, verificam-se ainda um conjunto de desafios para a adequação das instituições públicas às exigências da LGPD. Evidencia-se a necessidade de o setor público elaborar planos com regras de boas práticas e de governança em privacidade que mapeiem os dados pessoais sensíveis utilizados por suas diversas instituições e determinem como devem ser realizados os tratamentos desses dados. É necessária ainda a elaboração de protocolos claros e objetivos, além de uma ampla conscientização sobre a relevância dessas ações por todos os atores envolvidos.

Referências

Autoridade Nacional de Proteção de Dados. (2022a). *Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado*. https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf

Autoridade Nacional de Proteção de Dados. (2022b). G*uia orientativo: tratamento de dados pessoais pelo poder público*. https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf

Autoridade Nacional de Proteção de Dados. (2022c). *Resolução CD/ANPD n. 2, de 27 de janeiro de 2022*. https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019

Botelho, M. C., & Camargo, E. P. A. (2021). A aplicação da Lei Geral de Proteção de Dados na saúde. *Revista De Direito Sanitário*, *21*, e0021. https://doi.org/10.11606/issn.2316-9044.rdisan.2021.168023

Bioni, B. R. (2018). *Proteção de dados pessoais: a função e os limites do consentimento*. Forense.

Bleeker, A. (2020). Creating an enabling environment for e-government and the protection of privacy rights in the Caribbean: a review of data protection legislation for alignment with the General Data Protection Regulation. *Studies and Perspectives – ECLAC Subregional Headquarters for the Caribbean*, (94).

Comitê Gestor da Internet no Brasil. (2020). *Nota pública sobre tratamento de dados pessoais e vigilância no período de isolamento social pela pandemia da Covid-19*. https://cgi.br/esclarecimentos/ver/nota-publica-sobre-tratamento-de-dados-pessoais-e-vigilancia-no-periodo-de-isolamento-social-pela-pandemia-da-covid-19.pdf

Comitê Gestor da Internet no Brasil. (2021a). *Pesquisa sobre o uso das tecnologias de informação e comunicação nas escolas brasileiras: TIC Educação 2020 (Edição COVID-19 — Metodologia adaptada)*. https://www.cetic.br/media/docs/publicacoes/2/20211124200326/tic_educacao_2020_livro_eletronico.pdf

Comitê Gestor da Internet no Brasil. (2021b). *Pesquisa sobre o uso das tecnologias de informação e comunicação nos estabelecimentos de saúde brasileiros: TIC Saúde 2021 (Edição COVID-19 — Metodologia adaptada)*. https://cetic.br/media/docs/publicacoes/2/20211124123911/tic_saude_2021_livro_eletronico.pdf

Comitê Gestor da Internet no Brasil. (2022). *Pesquisa sobre o uso das tecnologias de informação e comunicação no setor público brasileiro: TIC Governo Eletrônico 2021*. https://cetic.br/media/docs/publicacoes/2/20220725170710/tic_governo_eletronico_2021_livro_eletronico.pdf

Costa, R. (2022). Personalidade Hackeada: considerações sobre proteção de dados pessoais sensíveis, vigilância digital e discriminação. In C. Teffé, & S. Branco (Coords.), *Proteção de dados e tecnologia: estudos da pós-graduação em Direito Digital* (pp. 52-78). Instituto de Tecnologia e Sociedade do Rio de Janeiro; ITS/Obliq.

Crespo, M. (2021). Proteção de dados pessoais e o poder público: noções essenciais. In C. D. Cravo, D. Z. G. Cunda, & R. Ramos (Orgs.), *Lei Geral de Proteção de Dados e o poder público* (pp. 16-28). Escola Superior de Gestão e Controle Francisco Juruena; Centro de Estudos de Direito Municipal.

Dallari, A. B., & Monaco, G. F. C. (Orgs.). (2021). *LGPD na saúde*. Thomson Reuters, Revista dos Tribunais.

Departamento de Assuntos Econômicos e Sociais das Nações Unidas. (2020). *E-Government Survey 2020: Digital government in the decade of action for sustainable development: With addendum on COVID-19 Response*. https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf

European Data Protection Board. (2020). *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

European Union. (2018). *General Data Protection Regulation*. https://gdpr.eu/

Gomes, M. C. O. (2022). Políticas públicas e o relatório de impacto à proteção de dados: análise do caso do aplicativo NHS COVID-19. In Comitê Gestor da Internet no Brasil. *Pesquisa sobre o uso das tecnologias de informação e comunicação no setor público brasileiro: TIC Governo Eletrônico 2021* (pp. 139-152). https://cetic.br/media/docs/publicacoes/2/20220725170710/tic_governo_eletronico_2021_livro_eletronico.pdf

Hawryliszyn, L. O., Coelho, N. G. S. C., & Barja, P. R. (2021). Lei Geral de Proteção de Dados (LGPD): o desafio de sua implantação para a saúde. *Revista Univap, 27*(54).

Henriques, I., & Hartung, P. (2021). Children's rights by design in AI development for education. *The International Review of Information Ethics, 29*.

Human Rights Watch. (2022). *"How Dare They Peep into My Private Life?": Children's rights violations by governments that endorsed online learning during the covid-19 pandemic*. https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments

Laterça, P., Fernandes, E., Teffé, C., & Branco, S. (2021). *Privacidade e Proteção de Dados de Crianças e Adolescentes*. Instituto de Tecnologia e Sociedade do Rio de Janeiro; Obliq.

Lei Geral de Proteção de Dados Pessoais – LGPD. Lei n. 13.709, de 14 de agosto de 2018. (2018). Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

Lei n. 14.129, de 29 de março de 2021. (2021). Dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública e altera a Lei nº 7.116, de 29 de agosto de 1983, a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), a Lei nº 12.682, de 9 de julho de 2012, e a Lei nº 13.460, de 26 de junho de 2017. https://www.in.gov.br/en/web/dou/-/lei-n-14.129-de-29-de-marco-de-2021-311282132

Livingstone, S., Stoilova, M., & Nandagiri, R. (2019). *Talking to children about data and privacy online: research methodology*. London School of Economics and Political Science.

Ministério da Economia. (2020). *Lei Geral de Proteção de Dados (LGPD): guia de boas práticas para implementação na administração pública federal*. https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf

Ministério da Economia. (2021). *Guia de elaboração de programa de governança em privacidade*. https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_governanca_privacidade.pdf/view

Ministério da Saúde. (2021). *1º Relatório de Monitoramento e Avaliação da Estratégia de Saúde Digital para o Brasil 2020-2028*. https://bvsms.saude.gov.br/bvs/publicacoes/relatorio_monitoramento_estrategia_saude_digital.pdf

Mulholland, C. (2018). Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/18). *Revista de Direitos e Garantias Fundamentais, 19*(3), 159-180. https://www.sumarios.org/Artigo/dados-pessoais-sens%C3%ADveis-e-tutela-de-direitos-fundamentais-uma-an%C3%A1lise-%C3%A0-luz-da-lei-geral-de

Organização das Nações Unidas. (2021). *Comentário geral n. 25 sobre os direitos das crianças em relação ao ambiente digital*. Comitê dos Direitos da Criança da Organização das Nações Unidas. https://criancaeconsumo.org.br/biblioteca/comentario-geral-n-25/

Organização das Nações Unidas para a Educação, a Ciência e a Cultura. (2022). *Minding the data: Protecting learners' privacy and security*. https://unesdoc.unesco.org/ark:/48223/pf0000381494

Organização Pan-Americana da Saúde. (2021). *Oito princípios orientadores para transformação digital do setor da saúde: um apelo à ação pan-americana*. https://iris.paho.org/handle/10665.2/54669

Organização para a Cooperação e Desenvolvimento Econômico. (2020a). *Growing up online: Addressing the needs of children in the digital environmen*t. https://www.oecd.org/sti/ieconomy/growing-up-online.pdf

Organização para a Cooperação e Desenvolvimento Econômico. (2020b). *Tracking and tracing COVID: Protecting privacy and data while using apps and biometrics*. http://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protectingprivacy-and-data-while-using-apps-and-biometrics-8f394636/

Programa das Nações Unidas para o Desenvolvimento. (2020). *Guidance to UNDP Country Offices on the privacy, data protection and broader human rights dimensions of using digital technologies to combat Covid-19*. https://www.sdg16hub.org/content/covid-19-guidance-undp-country-offices-privacy-data-protection-and-digital-technologies

Resolução n. 363, de 12 de janeiro de 2021. (2021). Estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos tribunais. https://atos.cnj.jus.br/atos/detalhar/3668

U.S. Congress. (1998). *Children's online privacy protection act*. https://www.congress.gov/bill/105th-congress/senate-bill/2326/text

van der Hof, S. (2016). I agree… or do I? A rights-based analysis of the law on children's consent in the digital world. *Wisconsin International Law Journal, 34*(2), 409-445.

ENGLISH

Foreword

In August 2018, Brazil joined the select group of countries that have enacted national legislation related to privacy and data protection. The Brazilian General Data Protection Law (LGPD) established rules and guidelines for the processing of personal data, including in digital form. In February 2022, the right to the protection of personal data was included in the Federal Constitution under the list of fundamental civil rights and guarantees.

The new regulatory and legal framework provides guidelines for public and private agents on how to process and use personal data. The topic is even more relevant in today's context, in which there is widespread adoption of digital technologies in the interactions between individuals and organizations. The processing and analysis of an ever-increasing amount of data is the current reality.

Over the past few years, the promotion of privacy and the protection of personal data, especially on the Internet, has been part of the scope of actions of the Brazilian Network Information Center (NIC.br) and the Brazilian Internet Steering Committee (CGI.br). In 2009, after CGI.br disseminated ten principles for the governance and use of the Internet[1] in Brazil — the first of which is "Freedom, privacy and human rights" —, the protection of personal privacy has become one of the essential aspects guiding Internet use. The following year, in 2010, CGI.br and NIC.br began holding the annual Seminar on Privacy and Personal Data Protection[2], which over the years has placed key issues on the agenda that contributed to the creation of the LGPD and other related regulatory instruments, gaining recognition as one of the main events in the area in Brazil. In 2022, the seminar will be held for the 13th time, and will provide a space for multisectoral discussions among representatives from the government, the private sector, the third sector, and the scientific and technological community.

Within the scope of the LGPD, in addition to public notices related to the topic, CGI.br is represented on the National Council for the Protection of Personal Data and Privacy (CNPD), an advisory body of the National Data Protection Authority (ANPD). In July 2021, with the purpose of strengthening the country's data protection culture, NIC.br and ANPD entered into a cooperation agreement. The first action

[1] More information available at: https://principios.cgi.br/

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

carried out by this partnership was the launch of two issues of the Internet Security Primer (*Cartilha de Segurança para Internet*, in Portuguese)[3], on the topics of data protection and data leakage.

In September 2020, when the LGPD came into force, it became increasingly crucial to understand how public and private organizations processed personal data and how this topic was advancing in the various sectors of society. To contribute to the search for evidence on the state of the implementation of the LGPD in the country, the present publication gathers indicators collected by surveys conducted by the Regional Center for Studies on the Development of the Information Society (Cetic.br), the department of NIC.br responsible for producing statistics and qualitative studies on the use of digital technologies in Brazil.

This survey has received the institutional support of ANPD and presents new indicators collected by the Cetic.br|NIC.br surveys regarding privacy and personal data protection in different sectors. Based on the results of an online survey with Internet users, the diagnosis includes the perception of citizens on the topic. The publication also addresses the main challenges to compliance with the law, investigating practices implemented for processing personal data in small, medium, and large enterprises. Finally, it provides an overview of the adoption of the LGPD among public organizations, based on data collected in schools, healthcare facilities, and federal and state government organizations and local governments.

Cetic.br|NIC.br offers relevant and quality data on the subject, for both society and the authorities responsible for ensuring data protection in the country. We hope to contribute to an increased understanding of the implementation of the LGPD and its effects on the culture of privacy and personal data protection in Brazil.

Enjoy your reading!

Demi Getschko
Brazilian Network Information Center – NIC.br

[3] More information available at: https://cartilha.cert.br/

Presentation

What is the level of compliance of Brazilian enterprises with the Brazilian General Data Protection Law (LGPD)[1]? Where are the main bottlenecks? What are the perceptions of citizens? These questions, which appear to be simple, are of great importance. The challenges associated with the implementation of a law endowed with such cross-sectionality, full of concepts still poorly understood, are not trivial. Addressing these challenges requires significant organizational changes by public agencies and private agents. Seeking answers to these questions is an undertaking of tremendous importance, as the new legislation intends to foster cultural change, and the first step toward promoting its effectiveness is knowing about the reality on which the law focuses.

The creation of the National Data Protection Authority (ANPD), in November 2020, under the terms set forth in the LGPD, reflects the importance attributed by legislators to the establishment of an institutional instrument dedicated to protecting the personal data of Brazilian citizens, placing at the center of this endeavor an organization endowed with normative, supervisory and sanctioning powers. Furthermore, the recognition of the complexity of the Brazilian environment has motivated ANPD, ever since its creation, to seek institutional partnerships with organizations and entities with competencies related to the promotion of personal data protection in Brazil.

It is in this context that a cooperation agreement was signed between ANPD and the Brazilian Network Information Center (NIC.br) in July 2021. Created to implement the decisions made by the Brazilian Internet Steering Committee (CGI.br), NIC.br is nationally and internationally known for actions that foster the development of the Internet, with broad expertise in handling and responding to security incidents, and in producing studies, indicators, statistics, and strategic information on the adoption of information and communication technologies (ICT) in the country.

The agreement between ANPD and NIC.br includes activities such as information exchange; carrying out actions of common interest regarding the protection of personal data and information security; mutual scientific and technical cooperation

[1] Law No. 13.709, of August 14, 2018. Available at: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

to develop actions, produce training materials, and raise awareness on the subject; and joint and coordinated production of studies, analyses, and research on personal data protection, information security, online privacy, and technology. Among the concrete results already derived from the partnership between ANPD and NIC.br, special mention goes to the launch, in July 2021, of two issues of the Internet Security Primer (*Cartilha de Segurança para Internet*, in Portuguese), whose dissemination contributes to promoting a culture of data protection among the population, expanding knowledge on the topic to a wider circle rather than just among experts in the field.

The present publication can also be considered one of the positive results of the partnership between ANPD and NIC.br. In fact, carrying out representative research on personal data protection and privacy practices among enterprises and government organizations (such as schools and healthcare facilities) offers strategic support for ANPD's performance. Understanding the perceptions of the Brazilian population about their privacy is a central factor in designing initiatives that contribute to having greater knowledge of personal data protection rules and public policies, as well as security measures.

By establishing a baseline to understand the perceptions of individuals and organizations about personal data protection and privacy, this publication allows for future progress in the area to be monitored. In addition, it strengthens the design of evidence-based public policies, allowing the country to advance this agenda faster.

It was a pleasure to be invited to present this publication, and I encourage everyone to dive in and enjoy your reading!

Miriam Wimmer
National Data Protection Authority

Introduction

Since the enactment of the first specific legislation on the protection of personal data in the 1970s, the establishment of a legal framework containing a regulatory system for personal information has become one of the main axes for helping coordinate and create the instruments responsible for defining the legal system for information. Subsequently, all over the world, these tools have become increasingly important in various economic and social processes.

The regulatory framework for data protection is therefore the result of an evolution of more than five decades in the creation of tools shaped toward addressing the challenge of regulating what seemed virtually uncontrollable in a given technological paradigm: the free flow of data. As some effects of this flow began to result in consequences that were considered harmful, the demand for regulation grew and led to the current situation in which a majority of nations in the international community has opted to legislate the protection of personal data. According to international surveys, more than 140 countries currently have general legislation on the protection of personal data.[1]

It should be noted that, in recent decades, the attention directed toward the regulation of personal information has met increasingly broad demands, both in geographical aspects and among the various social actors, presenting developments that go beyond the protection of personal data. In this context, intense discussions have emerged about the imminence of the creation or expansion of regulation in sectors such as Artificial Intelligence and the governance of (non-personal) data, competitive aspects of the digital economy, regulation of platforms, and many others. This allows us to consider data protection, not only in terms of its intrinsic aspects, but as a gateway to the issues of information regulation as one of the aspects of law and norms in our time.

The implementation of a regulatory framework for the protection of personal data in Brazil has been accelerating in recent years. It started with the executive branch sending Bill PL No. 5276/2016 to the National Congress. In 2018, it was approved

[1] Greenleaf, G. (2021). Global Data Privacy Laws 2021: Despite COVID delays, 145 laws show GDPR dominance. *Privacy Laws & Business International Report, 169*(1), 3-5.

unanimously in both legislative houses, and culminated with the entry into force of the most substantial part of the Brazilian General Data Protection Law (LGPD), in 2020. Discussions about the topic were constantly gaining importance, as they reflected a growing demand for the regulation of the use of information, either to guarantee and promote rights or to ensure its safe use.

The process of creating the LGPD preceded its legislative path. It dates back to a public debate launched by the Ministry of Justice on November 30, 2010, through a base text from which the proposal presented by the executive branch to Congress in 2016 was created and developed. The discussion on the topic also extended to the scope of the Southern Common Market (Mercosur) between 2014 and 2020[2]. In this period, however, much of the discussion took place without the broader involvement of all segments of society, being restricted to certain sectors and specialized actors — in contrast, even, with the international debate that, for decades, had already been quite comprehensive.

Brazil has had its own dynamics, but is widely recognized as having great importance in terms of the regulation of technology applications. Examples include the trajectory of normative actions such as the Consumer Protection Code, capable of adapting to the dynamics of electronic commerce; the pioneering experience of the Brazilian Civil Rights Framework for the Internet, which innovated in terms of the modality of public debate and construction based on the *Principles for the Governance and Use of the Internet* set forth by the Brazilian Internet Steering Committee (CGI.br); and even the LGPD itself, although subsequent to other similar experiences in several countries, it is the result of an intense internal process of debate and maturation. This tradition points to future potentially relevant experiments, such as the current establishment of a Committee of Jurists by the Federal Senate to draft a bill on Artificial Intelligence.[3]

The introduction of the regulatory framework for the protection of personal data has produced changes in habits that can now begin to be objectively verified. This ranges from greater demand on the part of citizens for respect and transparency in the use of their data — considering the possibility of exercising their rights and in the presence of a system of administrative and judicial protection — to the verification of the implementation and effectiveness of processes and practices related to data protection by enterprises and public organizations.

In the public sector, the dynamics of effective incorporation of personal data protection regulations occur in processes that may be, at first glance, less visible, such as in the use of personal data in public policies and in actions of public interest, which is supported by law. Nevertheless, this intense use of personal data makes the need to provide citizens with respect and transparency even greater. The trust of individuals in public organizations is increasingly defined by the respect they inspire as controllers and protectors of personal data. In this regard, the space provided by the LGPD in relation to the processing of personal data should be seen in the public sector

[2] Doneda, D. (2021). Panorama histórico da proteção de dados pessoais. In D. Doneda, I. W. Sarlet, L. S. Mendes, & O. L. Rodrigues Junior (Coords.), *Tratado de proteção de dados pessoais*. Forense.

[3] Available at: https://legis.senado.leg.br/comissoes/comissao?codcol=2504

as a call for the development of tools that guarantee citizens transparency and control over their own data. In addition to attributing greater effectiveness to government services, the use of such tools will be an increasingly preponderant element in the relationship between the public sector and society, a relationship that will only be effective with the mutual trust.

It is also essential to highlight that new regulatory frameworks are not fully implemented without cultural change. Using rigorous and reliable methods, investigating both the perceptions of society in relation to the objects of regulation and the practices adopted by enterprises and public organizations to address the new challenges of data processing, is a central and essential element for decisions to be made at the managerial and public policy levels.

Faced with the need for updated information about data protection and the context of the adoption of the LGPD by Brazilian individuals, enterprises, and public organizations, the Brazilian Network Information Center (NIC.br), linked to the CGI.br, and with the support of the National Data Protection Authority (ANPD), developed the publication *Privacy and personal data protection 2021: Perspectives of individuals, enterprises and public organizations in Brazil.* Based on the collection and processing of unpublished data produced by the Regional Center for Studies on the Development of the Information Society (Cetic.br), this publication presents an updated study of the advances in this area in Brazilian society. After presenting the methodological aspects that guided the survey, the analysis of the results of the publication is organized in the following sections:

- **Internet users:** Presents the results of the ICT Panel survey, carried out in 2021 with Internet users (16 years old and older), which investigates users' perceptions of the processing and protection of their personal data;
- **Enterprises:** Identifies how small, medium, and large Brazilian enterprises process personal data in their operations, based on the application of a specific module during the data collection process for the ICT Enterprises 2021 survey;
- **Public organizations:** Covers the results of the ICT in Education 2020, ICT in Health 2021, and ICT Electronic Government 2021 surveys in relation to data protection and privacy initiatives adopted by public Primary and Secondary schools and public healthcare facilities, in addition to federal and state government organizations and local governments.

With this new survey, NIC.br reaffirms its commitment to providing the government and society with robust and up-to-date statistics on the advances of the information society in Brazil. Through the compilation of indicators in various sectors, the goal is to offer unprecedented inputs to underpin evidence-based public policies and the implementation of regulatory strategies. Based on this first measurement, the data of this survey establishes a baseline for the future monitoring of the personal data protection ecosystem in Brazil, allowing the monitoring and evaluation of public policies and the promotion of the well-being of the population.

EXECUTIVE SUMMARY

PRIVACY AND PERSONAL DATA PROTECTION

Executive Summary
Privacy and Personal Data Protection 2021

Concerns about privacy and personal data protection have intensified in various sectors of Brazilian society, especially since 2020, when the Brazilian General Data Protection Law (LGPD) came into force. With the growing adoption of digital technologies by public and private organizations and by individuals — and the interaction between them — a marked trend in the COVID-19 pandemic, it is essential to understand how the topic is perceived by these actors and identify the strategies they adopt to ensure privacy and personal data protection in the country.

In this regard, this publication contributes to the discussion through a compilation of indicators on the behaviors and perspectives of Internet users, enterprises, and government organizations on the matter. The results indicate the high concern of Internet users with risks related to the processing of their personal data. On the part of enterprises, they point to the incipient presence of this agenda. In government organizations, even if there is progress in the adopted strategies, there are still challenges that need to be overcome to ensure data governance with greater privacy and personal data protection.

ABOUT ONE-QUARTER OF INTERNET USERS (24%) SOUGHT OUT CUSTOMER SERVICE CHANNELS TO MAKE REQUESTS, COMPLAINTS, OR FILE REPORTS ABOUT THEIR PERSONAL DATA

Internet users

PRACTICES ADOPTED

The survey investigated the practices adopted by Internet users 16 years old and older to manage access to their personal data. Checking the security of web pages or apps (70%), for instance, by verifying whether a web page had a security padlock, was the practice reported with the highest proportion. Requesting that personal data be deleted (42%) was mentioned by less than half of Internet users (Chart 1).

About one-quarter of Internet users (24%) sought out customer service channels to make requests, complaints, or file reports about their personal data. Among those who sought out these channels, they mostly mentioned channels of the enterprise or government organization itself (80%), followed by consumer protection agencies (48%).

CONCERNS WITH PERSONAL DATA

Data records generated while using the Internet are a factor of concern for most users regarding their personal data, especially when making purchases online via web pages and apps (67% were concerned or very concerned) or when accessing online banking via web pages or apps (59% were concerned or very concerned). These results indicate users' perceptions of the high potential for harm related to financial transaction data. Although dating apps were cited the least often by Internet users, among those who did use them, it was the activity with the third highest proportion of concerned or very concerned users (34%) (Chart 2).

Internet users also showed concern about the provision of sensitive data: 65% said they were concerned or very concerned with the collection and processing of biometric data

(Chart 3). Another category that stands out is health-related personal data, which can expose individuals' situations of vulnerability and have high discriminatory potential: 52% of respondents said they were concerned or very concerned. Black (35%) and Brown (32%) users reported being concerned or very concerned in greater proportions than White (26%) users about providing personal information related to color or race.

Motivated by concerns about the use of their personal data, 77% of Internet users 16 years old or older uninstalled apps, 69% refrained from visiting a web page, 56% refrained from using an online service or platform, and 45% refrained from buying an electronic device.

ONLY 17% OF ENTERPRISES APPOINTED DATA PROTECTION OFFICERS

Enterprises

STORAGE OF PERSONAL DATA

The survey investigated the types of personal data stored by Brazilian enterprises and the purposes for which they store it. It should be noted that, in 2021, only 37% of enterprises said they kept data from outsourced personnel, while 67% said they kept data from partners and suppliers (Chart 4). Regarding the processing of personal data, the information and communication segment and professional activities presented a greater presence of data storage of customers and users, reaching 78% of the enterprises in these sectors.

INTERNAL CAPACITIES

Another central aspect for the development of a data protection culture is actions carried out by enterprises that promote staff training and awareness. The results of the survey carried out among enterprises showed that 36% held specific meetings related to privacy and personal data protection. Although no major regional differences were observed, holding meetings to address issues related to privacy and data protection presented disparities among different sectors. It is worth noting that meetings were held more in large (73%) and medium (59%) enterprises, while the proportion of small enterprises that sought to discuss privacy and personal data protection issues internally was lower (32%).

Data were also collected on whether there were areas or persons responsible for personal data protection. It was observed that 23% of enterprises said they had such areas or persons, and most of these enterprises were medium and large. The type of enterprises that presented a higher proportion of areas or persons in charge of the topics of privacy and personal data protection were those whose activities put them in contact with a greater volume of personal data — such as those in the information and communication and transportation and storage segments (Chart 5).

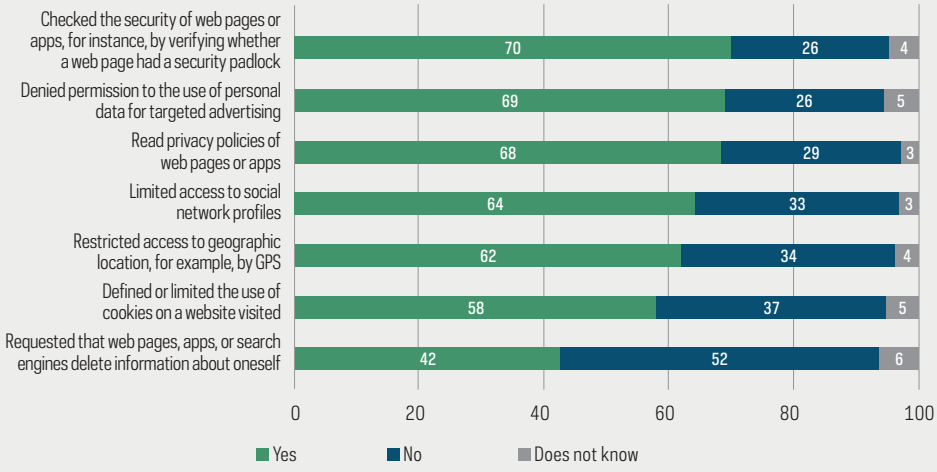
COMPLIANCE WITH THE LGPD

The survey also investigated aspects critical to compliance with the LGPD by Brazilian enterprises, which are guided by the framework set forth by the provisions of the law. Among the measured aspects, the most cited was the formulation of privacy policies that outline how personal data is processed by the enterprises (32%). This was followed by 30% of enterprises that conducted data leakage security tests, which shows concern with making their personal data processing more explicit, while also trying to ensure their own security, thus preventing leaks that can cause fiscal harm and tarnish their reputation. Only 17% of enterprises appointed data protection officers. Creating personal data protection compliance plans, which can promote safer and more law-compliant operations, was mentioned by only 24% of enterprises.

CHART 1

INTERNET USERS BY PERSONAL DATA ACCESS MANAGEMENT PRACTICES (2021)

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



77%
of Internet users uninstalled apps because of concerns about their data

69%
of Internet users refrained from visiting a website because of concerns about their data

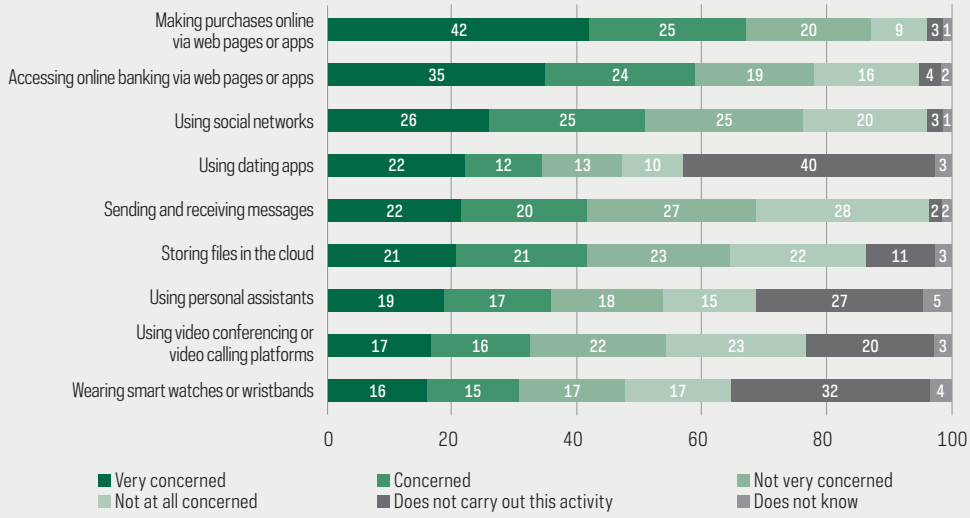
56%
of Internet users refrained from using an online service or platform because of concerns about their data

45%
of Internet users refrained from buying an electronic device because of concerns about their data

CHART 2

INTERNET USERS BY LEVEL OF CONCERN ABOUT THEIR PERSONAL DATA AND INTERNET ACTIVITY (2021)

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



Survey methodology and access to data

The Privacy and Personal Data Protection 2021 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 interviewed, via an online questionnaire, 2,556 Internet users 16 years or older between November and December 2021. The ICT Enterprises 2021 survey included a specific module on the processing of personal data in the private sector. Interviews were conducted with 1,473 small, medium and large enterprises between August 2021 and April 2022. In addition to the unprecedented results, an analysis of Brazilian public organizations was carried out based on indicators related to the topic of privacy and personal data protection in the ICT Electronic Government 2021, ICT in Health 2021 and ICT in Education 2020 surveys. The results of the surveys presented in this publication are available on the Cetic.br|NIC.br's website (https://www.cetic.br/en/). The "Methodological Report" can be accessed in both the printed publication and the website.

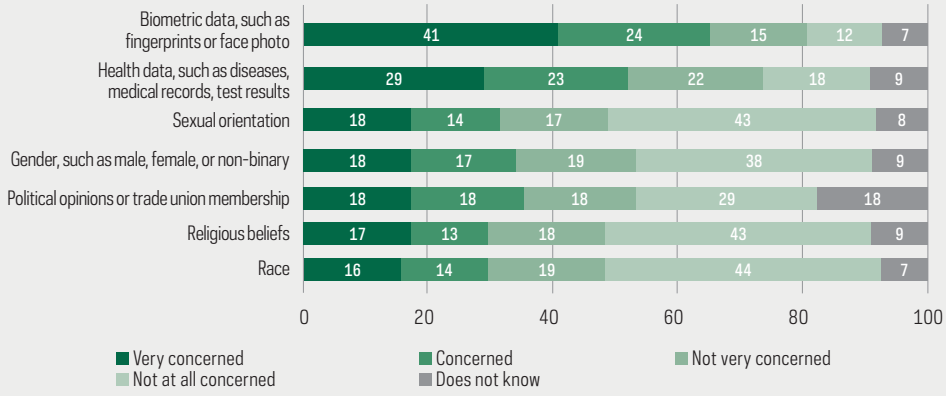
Privacy and personal data protection in the public sector

The expansion of digital transformation in the public sector allows greater reach of public policies, but also increases the risks involved in the processing of citizens' data. Given the relevance of the topic, this publication included an analysis of the adoption of practices related to privacy and data protection by government organizations, such as federal and state organizations and local governments, healthcare facilities, and public Basic Education schools. The analysis was based on the indicators collected by the ICT Electronic Government 2021, ICT in Health 2021, and ICT in Education 2020 surveys, conducted by Cetic.br|NIC.br. The creation of personal data governance structures in public institutions, ensuring citizens' access to clear and accurate information about how data is collected and used, in addition to carrying out awareness-raising actions on the topic in institutions, were some of the topics covered by the analysis. The results showed advances, such as the presence of online channels to receive requests from society. However, they also showed inequalities in readiness among different public institutions in organizational, technological and cultural adaptation to the guidelines of the law. The analysis also drew attention to the growing digitization of public services, especially since the COVID-19 pandemic, and to the urgent need for actions that support government organizations in meeting the privacy and data protection needs of the population.

CHART 3

INTERNET USERS BY LEVEL OF CONCERN ABOUT PROVISION OF SENSITIVE PERSONAL INFORMATION (2021)

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



32% of enterprises formulated privacy policies that outline how personal data is processed by the enterprises

30% of enterprises conducted data leakage security tests

24% of enterprises created personal data protection compliance plans

13% of enterprises prepared personal data protection impact assessments

CHART 4

ENTERPRISES BY TYPE OF PERSONAL DATA STORED AND SIZE (2021)

Total number of enterprises (%)

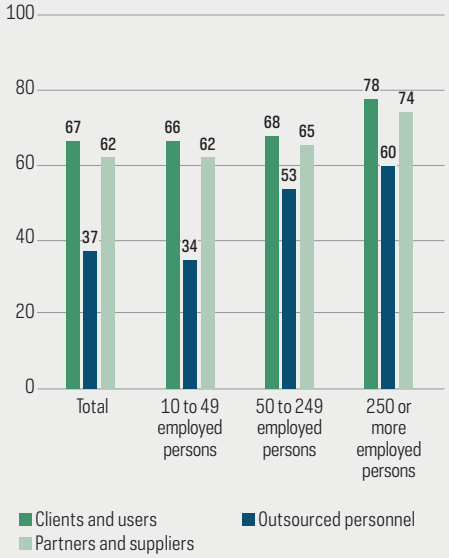
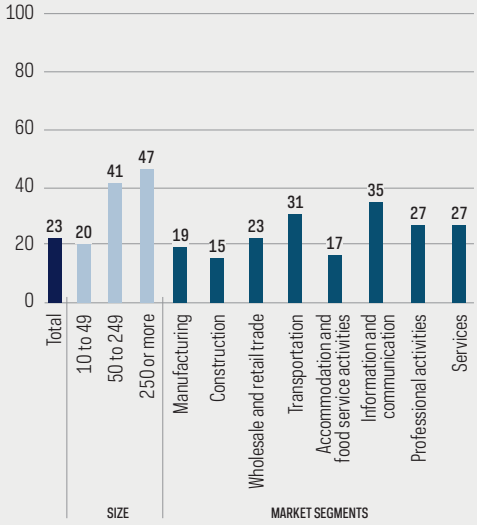


CHART 5

ENTERPRISES BY PRESENCE OF SPECIFIC AREAS OR EMPLOYEES RESPONSIBLE FOR PERSONAL DATA PROTECTION (2021)

Total number of enterprises (%)



Access complete data from the survey

The full publication and survey results are available on the **Cetic.br** website, including the tables of proportions, totals and margins of error.

ACCESS
WWW.CETIC.BR

METHODOLOGICAL REPORT

PRIVACY AND PERSONAL DATA PROTECTION

Methodological Report
Privacy and Personal Data Protection 2021

The Regional Center for Studies on the Development of the Information Society (Cetic.br), a department of the Brazilian Network Information Center (NIC.br), and affiliated with the Brazilian Internet Steering Committee (CGI.br), presents the methodological aspects of the publication *Privacy and personal data protection 2021: Perspectives of individuals, enterprises and public organizations in Brazil*. The objective of the project was to determine the current scenario and understand the main challenges to the construction of a digital ecosystem that guarantees respect for privacy and protection of personal data in Brazil. The survey was based on the collection and processing of quantitative data from Brazilian society through surveys conducted regularly by Cetic.br|NIC.br. The information includes the perceptions of Internet users about their rights and the processing of their personal data. With regard to organizations, the publication presents a survey on how enterprises and government organizations are adapting to the topic of privacy and protection of personal data since the enactment of the Brazilian General Data Protection Law (LGPD).

The project had 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 customers/consumers, as well as relevant issues associated with the implementation of the LGPD in Brazil;
- To establish an overview of data protection in the context of public policies, including the adoption of practices by government organizations, healthcare facilities, and schools.

In the next sections, we present the main methodological aspects of the surveys used to collect the indicators and provide the references for full access to the "Methodological Report" and the "Data Collection Report" of each survey used.

ICT Panel – Internet users (2021)

The ICT Panel was created with the goal of collecting information on Internet use during the pandemic caused by the novel coronavirus. Carried out via web questionnaires, the survey was developed as an alternative to in-person data collection, which was affected by the social distancing measures implemented during this period. Since then, the panel's methodology has been adopted to collect data on other topics relevant to the discussion about the 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, 2021a). The creation of a specific questionnaire on privacy to be administered to Internet users was based on various previous studies with converging objectives. One of the first data collections used was Eurobarometer Special Survey No. 431 on personal data protection, carried out in 2015 and commissioned by the European Commission. Another relevant source was the June 2019 issue of the *American Trends Panel* by the Pew Research Center. Among official surveys produced by national statistical institutes, we included the *Survey of Canadians on Privacy-Related Issues*, carried out in 2020 by order of the Office of the Privacy Commissioner of Canada.

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

The target population of the survey was composed of Internet users 16 years old or older in Brazil, who were defined as individuals who had used the Internet in the three months prior to the interview, according to the methodological recommendation of the International Telecommunication Union (ITU, 2020).

The survey's sampling design was an online panel of individuals maintained by Quaest Consultoria e Pesquisa, with approximately 167,000 panelists. Quota sampling was used to obtain the sample of respondents, considering the following variables: sex, age group, level of education, macro-region, and social class. The survey data collection was carried out between November 12 and December 3, 2021; in all, 2,556 interviews were conducted.

To minimize the selection biases found in quota approaches, a weighting structure was created for the ICT Panel, based on the ICT Households 2020 survey[1], a probabilistic survey. In the initial stage, the results of this survey were recalibrated for the population of the *Continuous National Household Sample Survey* (Continuous Pnad) (Brazilian Institute of Geography and Statistics [IBGE], n.d.), considering the last quarter released.

[1] More information available at the survey's website: https://www.cetic.br/en/pesquisa/domicilios/

Subsequently, the number of the population represented by the respondents of the ICT Panel was estimated based on propensity scores[2]. According to this methodology, first, the propensity scores of being an Internet user were calculated according to socioeconomic variables, based on the last edition available of the ICT Households survey[3]. Next, this same model was used to estimate the propensity scores for respondents of the ICT Panel.

On comparing the distribution of propensity scores of the ICT Panel with that verified in the last ICT Household survey, it was possible to determine which part of the population of the latter (or if all of it) could be represented by the respondents of the Panel. This meant estimating the coverage error of the ICT Panel in relation to the target population initially considered in the survey.

In this edition of the ICT Panel, the audience represented was equivalent to the entire target population of the ICT Households survey, which allowed direct comparison of the results of the edition with the equivalent indicators collected. In relation to the previous editions of the Panel, which did not represent the entire target population, this comparison needed to be made using the same population cutouts of the respective editions.

The full results of the survey are available at Cetic.br|NIC.br's website (http://www.cetic.br/en/), in addition to the survey's full "Methodological Report".

ICT Enterprises – Small, medium, and large enterprises (2021)

Conducted since 2005, the ICT Enterprises survey aims to measure the ownership and use of ICT among Brazilian companies. The survey presents indicators that translate into numbers for the reality of Brazilian companies in relation to various topics, such as ICT access; Internet use; e-government; e-commerce; ICT skills; software; digitalsecurity and new technologies.

The universe covered in the survey includes all active Brazilian enterprises with 10 or more employed persons[4] registered in the Central Register of Enterprises (Cempre) of IBGE, belonging to the sectors of the National Classification of Economic Activities (CNAE) 2.0 of interest to ICT companies, and meeting the definition of Legal Nature Type 2 — business entities — except for public enterprises (Legal Nature. 201-1).

[2] Unlike estimates based on a traditional sample design, the selection probabilities in the Panel are unknown and undefined, because of its pseudo-sample design. Pseudoprobability is the estimated probability of belonging to the non-probability sample used instead of a known probability. More information in 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://www.aapor.org/AAPOR_Main/media/MainSiteFiles/NPS_TF_Report_Final_7_revised_FNL_6_22_13.pdf

[3] For the this edition of the ICT Panel, the ICT Households 2020 survey was used (CGI.br, 2021c).

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

The surveyed enterprises operated in the following segments:

C – Manufacturing;

F – Construction;

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

H – Transportation and storage;

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 was developed to maintain international comparability. It uses the methodological standards proposed in the Manual for the Production of Statistics on the Information Economy (UNCTAD, 2009), prepared in partnership with the Organisation for Economic Co-operation and Development (OECD), the Statistical Office of the European Communities (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 is stratified in two steps, and the enterprises are selected randomly within each stratum. The first step covers the definition of natural strata by correlating the variables geographic region and market segment (CNAE 2.0). The final strata are defined from each natural stratum, which considers the division of natural strata by enterprise size[5]. In 2021, the survey interviewed a total of 4,064 enterprises and 1,473 answered specific questions about privacy and personal data protection, Enterprises were contacted for interviews using the computer-assisted telephone interviewing (CATI) technique. In all enterprises, the survey sought to interview the persons in charge of information technology, 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;

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

- 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;
- Project managers;
- Enterprise owners or partners.

In enterprises with 250 or more employed persons at the time of the interview, the strategy employed was to interview a second professional, preferably the accounting or finance manager. If this professional was not found, the person responsible for the administrative, legal or relations with government institutions was sought, who exclusively answered questions about electronic commerce, electronic government, and activities carried out on the Internet.

ICT ENTERPRISES 2021 – "PRIVACY AND PERSONAL DATA PROTECTION" MODULE

In 2021, to meet the demand for data on how small, medium, and large enterprises process the personal data of their customers/consumers, in addition to relevant issues associated with the implementation of the LGPD in Brazil, a module was created to be implemented in parallel with the ICT Enterprises 2021 survey.

An additional person considered qualified to respond about measures relative to LGPD compliance in the enterprise was chosen to be interviewed for the specific data protection module. The respondents of the ICT Enterprises survey were asked to recommend the person that most knew about the topic in the enterprise, i.e., someone who could provide information about the procedures and policies adopted in the collection, storage, and use of personal data, in addition to the enterprise's compliance with the LGPD. In cases where the topic was handled by the same respondent of ICT Enterprises, the interview was conducted with this professional. The enterprise could not appoint a third-party professional as a respondent. Instead, they had to identify the in-house employee responsible for hiring this service, ensuring that interviews were conducted with members of the enterprise's internal team.

All enterprisesresponding to the survey had a 50% probability of being selected to respond to the privacy and personal data protection module. This selection probability guaranteed representativeness like that expected for the ICT Enterprises survey. Given that the sample size was smaller compared to that obtained in this last survey, some indicators were expected to present higher sampling errors.

Based on this probability of selection, the initial weight of the enterprises that responded to the data protection and privacy module was obtained by Formula 1.

FORMULA 1

$$w_{ih}^{LGPD} = \frac{1}{2} \times w_{ih}^{*} = \frac{1}{2} \times w_{ih} \times \frac{N_h}{\Sigma_i w_{ih}}$$

w_{ih}^{LGPD} is the basic weight of enterprise i respondent in stratum h

w_{ih}^{*} is the weight with nonresponse adjustment for enterprise i in stratum h

where

$$w_{ih} = \frac{N_h}{n_h}$$

w_{ih} is the basic weight associated with each enterprise i responding to the ICT Enterprises survey in the stratum h

n_h is the enterprise sample size in stratum h

N_h is the total number of enterprises in stratum h

To adjust for cases when not all the selected enterprises answered the questionnaire, an adjustment for nonresponse was given by Formula 2.

FORMULA 2

$$w_{ih}^{*LGPD} = w_{ih}^{LGPD} \times \frac{N_h}{\Sigma_i w_{ih}^{LGPD}}$$

w_{ih}^{*LGPD} isthe weight with nonresponse adjustment for enterprise i respondent in stratum h

Finally, these sampling weights were calibrated to reflect the known population totals, obtained in the IBGE Cempre. This procedure, together with the non-response adjustments, aimed to correct the variability associated with non-response among the enterprise population. The variables considered for calibration were geographic region, market segment, and enterprise size.

Table 1 shows the distribution of the number of enterprises by geographic region, market segment, and size, according to Cempre, in addition to the allocation of the sample eligible to participate in the module and the sample that responded to this module. The response rate for the module was 74%.

TABLE 1

NUMBER OF ENTERPRISES BY SIZE, GEOGRAPHIC REGION, AND MARKET SEGMENT (2021)

	Universe	Sample selected among respondents from ICT Enterprises	Respondent sample
Total	**509 049**	**1 982**	**1 473**
Size			
10 to 49 employed persons	310 023	696	512
20 to 49 employed persons	136 438	530	391
50 to 249 employed persons	51 780	326	245
250 or more employed persons	10 808	430	325
Region			
North	22 122	254	176
Northeast	78 059	298	216
Southeast	260 094	810	596
South	107 162	372	296
Center-West	41 612	248	189
Market segment (CNAE 2.0)			
Manufacturing	98 870	343	278
Construction	34 880	209	169
Wholesale and retail trade; repair of motor vehicles	195 839	458	314
Transportation and storage	29 111	201	146
Accommodation and food service activities	56 903	192	141
Information and communication	14 085	187	133
Real estate activities; professional, scientific, and technical activities; administrative and support service activities	66 643	208	159
Arts, culture, sports, and recreation; other service activities	12 718	184	133

SOURCE: CGI.BR (IN PRESS).

The results and tables of proportions, estimates and margins of error for ICT Enterprises are available for download on Cetic.br|NIC.br's website (https://www.cetic.br/en/), in addition to the full version of the survey's Methodological Report and Data Collection Report.

ICT Electronic Government – Federal and state government organizations and local governments (2021)

Carried out every two years since 2013, the Survey about the use of information and communication technology in the Brazilian public sector — ICT Electronic Government — investigates the incorporation of digital technology in government organizations and its use in the provision of public services. This survey also measures the presence of initiatives related to promoting access to ICT and societal participation via the new technologies. In 2021, new modules were included related to the use of ICT in the fight against the pandemic and the adoption of new technologies. The 2021 edition also incorporated indicators on privacy and protection of personal data.

The survey was carried out nationwide and included two units of analysis: federal and state government organizations of all branches (executive, legislative, judiciary, and the Public Prosecutor's office) and local governments. A census was carried out in all the audiences of interest, except for state executive organizations, in which a sample of 400 government entities was selected. All interviews were carried out using a structured questionnaire using the computer-assisted telephone interviewing (CATI) technique.

The indicators analyzed for this publication were collected between August 2021 and April 2022, in 580 federal and state government organizations and 3,543 local governments. The results and tables of proportions, estimates and margins of error for ICT Electronic Government are available for download on Cetic.br|NIC.br's website (http://www.cetic.br/en/), in addition to the full version of the survey's Methodological Report and Data Collection Report.[6]

ICT in Health – Public healthcare facilities (2021)

Carried out annually since 2013[7], the ICT in Health survey has the objective of understanding the stage of ICT adoption in healthcare facilities and its appropriation by professionals in the area (physicians and nurses). To this end, it seeks to identify the available ICT infrastructure and investigate the use of ICT-based systems and applications directed at supporting the care delivery and management services of healthcare facilities. Furthermore, it measures the activities carried out by healthcare professionals via ICT, in addition to motivations for and barriers to its adoption and use.

[6] Available at: https://cetic.br/media/docs/publicacoes/2/20220725170710/tic_governo_eletronico_2021_livro_eletronico.pdf

[7] The ICT in Health survey was not carried out in 2020, due to the restrictions imposed on access to healthcare managers and professionals during the COVID-19 pandemic.

In 2021, the survey included one indicator that investigated the healthcare facility's compliance with the terms of the LGPD[8]. This new question was answered by healthcare facility managers (CGI.br, 2021d).

The ICT in Health survey is carried out nationwide and collects data from healthcare facilities at the three levels of care, selected based on the National Registry of Healthcare Facilities (CNES) maintained by the SUS Informatics Department (Datasus). Interviews were conducted using the using the computer-assisted telephone interviewing (CATI) technique, and for those who could not answer it online, there was a self-administered web version of the questionnaire that could be accessed via a specific platform.

The results of the 2021 edition were collected between January and August of the same year with 1,524 managers, representing a universe of 112,075 Brazilian healthcare facilities. The results and tables of proportions, estimates and margins of error for ICT in Health are available for download on Cetic.br|NIC.br's website (https://www.cetic.br/en/), in addition to the full version of the survey's Methodological Report and Data Collection Report.[9]

ICT in Education – Public schools (2020)

Carried out nationwide since 2010, the ICT in Education survey is administered in Basic Education schools, both public and private, that are located in urban and rural areas and provide regular Elementary and Secondary Education.

Up to 2019, in urban areas, the survey was carried out in person at the educational facilities, administering structured questionnaires to students, teachers, directors of studies, and principals. In rural areas, it began to be carried out in 2017, with questionnaires applied to the managers of the institutions by phone.

In 2020, because of school closures and the dissemination of remote educational activities as part of the health measures implemented by states and municipalities across the country to fight against the COVID-19 pandemic, data collection for the ICT in Education survey was carried out only with school managers and based on completely telephone-based interviews, for schools located in both rural and urban areas (CGI.br, 2021b).

Despite the necessary adjustments of data collection to comply with health measures, it was possible to expand the dimensions and themes addressed by the survey, with the inclusion of questions about the use of systems, platforms, and applications by schools, in addition to actions implemented by them regarding personal data protection, privacy, and digital security.

[8] In the 2021 edition, it was not possible to interview healthcare professionals given the restriction to accessing this audience during the COVID-19 pandemic.

[9] Available at: https://cetic.br/media/docs/publicacoes/2/20211130124545/tic_saude_2021_livroeletronico.pdf

The data analyzed in this publication was collected between September 2020 and June 2021, in 3,678 functioning public and private schools in urban and rural areas. These institutions offered Elementary and Secondary Education, representing 127,171 schools, based on a sample extracted from the database of the Basic Education School Census carried out by the National Institute for Educational Studies and Research "Anísio Teixeira" (Inep).

Like the other surveys, the results, and tables of proportions, estimates and margins of error for ICT in Education are available for download on Cetic.br|NIC.br's website (http://www.cetic.br/en/), in addition to the full version of the survey's Methodological Report and Data Collection Report.[10]

Data dissemination

The results of the surveys mentioned above are presented according to the variables described in each survey's Methodological Report, under the item "Domains of interest for Analysis and Dissemination."

Rounding made it so that for 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 the results are presented without decimal places, a cell's content is zero whenever an answer was given to that item, but the result for this cell is greater than zero and smaller than one.

The survey results are published on the Cetic.br|NIC.br website (http://www.cetic.br/en/). The tables of proportions, estimates 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 bases are available on the Cetic.br|NIC.br microdata page (https://cetic.br/en/microdados/).

[10] Available at: https://cetic.br/media/docs/publicacoes/2/20211124200326/tic_educacao_2020_livro_eletronico.pdf

References

Brazilian Institute of Geography and Statistics (n.d.). *Continuous National Household Sample Survey (Continuous Pnad)*. https://www.ibge.gov.br/estatisticas/sociais/trabalho/9173-pesquisa-nacional-por-amostra-de-domicilios-continua-trimestral.html

Brazilian Internet Steering Committee. (in press). *Survey on the use of information and communication technologies in Brazilian enterprises: ICT Enterprises 2021.*

Brazilian Internet Steering Committee. (2020). *Painel TIC COVID-19: Pesquisa sobre o uso da Internet no Brasil durante a pandemia do novo coronavírus - 2ª edição: Serviços públicos on-line, telessaúde e privacidade.* https://cetic.br/media/docs/publicacoes/1/20201001085713/painel_tic_covid19_2edicao_livro%20eletr%C3%B4nico.pdf

Brazilian Internet Steering Committee. (2021a). *Web survey on the use of Internet in Brazil during the new coronavirus pandemic: ICT Panel COVID-19.* https://cetic.br/media/docs/publicacoes/2/20210426095323/painel_tic_covid19_livro_eletronico.pdf

Brazilian Internet Steering Committee. (2021b). *Survey on the use of information and communication technologies in Brazilian schools: ICT in Education 2020 (COVID-19 edition — Adapted methodology).* https://www.cetic.br/media/docs/publicacoes/2/20211124200326/tic_educacao_2020_livro_eletronico.pdf

Brazilian Internet Steering Committee. (2021c). *Survey on the use of information and communication technologies in Brazilian households: ICT Households 2020 (COVID-19 edition — Adapted methodology).* https://cetic.br/media/docs/publicacoes/2/20211124201233/tic_domicilios_2020_livro_eletronico.pdf

Brazilian Internet Steering Committee. (2021d). *Survey on the use of information and communication technologies in Brazilian healthcare facilities: ICT in Health 2021 (COVID-19 edition — Adapted methodology).* https://www.cetic.br/media/docs/publicacoes/2/20211124123911/tic_saude_2021_livro_eletronico.pdf

International Telecommunications 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

United Nations Conference on Trade and Development. (2009). *Manual for the production of statistics on the information economy 2009.* http://www.unctad.org/en/docs/sdteecb20072rev1_en.pdf

ANALYSIS OF RESULTS

PRIVACY AND PERSONAL DATA PROTECTION

Analysis of Results
Privacy and Personal Data Protection 2021
Internet users

Given the increased presence of the Internet in households and the proportion of Internet users in Brazil, the digital trail left by individuals during activities carried out online is also growing. With the advancement of the digital transformation of public and private organizations, the personal data of individuals is widely present in commercial, financial, and biographical records, among others, lending increasing attention to this massive amount of data in the legal, economic, and social spheres. This data-driven economy mobilizes a broad network of actors, including governments, private and civil society organizations, and individuals/consumers (Carrière-Swallow & Haksar, 2019).

While this new ecosystem has the potential to promote the well-being of individuals and societies, there are also risks associated with the misuse of this data. Many countries have advanced legal norms regulating this data ecosystem, particularly focusing on the protection of privacy and personal data of individuals, as is the case with the General Data Protection Regulation (GDPR) in the European Union, and the Brazilian General Data Protection Law (LGPD).

The growing interest in this topic has also mobilized the production of statistical data on how individuals perceive their privacy and the use of their personal data by public and private actors. To broaden the understanding of this topic, in 2021, the Regional Center for Studies on the Development of the Information Society (Cetic.br|NIC.br) carried out a new wave of the ICT Panel survey on the topic of privacy and protection of personal data, the analysis of which is presented here. The survey results are organized into the following dimensions:

- **Concept:** Seeks to identify how respondents understand and define the meaning of the term "privacy."
- **Practices:** Gathers indicators on how individuals manage third-party access to their personal data, in addition to whether they seek out customer service channels to make requests or complaints or to report the misuse of their data.

- **Risks:** Includes an analysis of the levels of concern about varied topics, such as data records, activities carried out online, data storage by enterprises and governments, data considered sensitive, and risks in relation to the use of personal data.
- **Control:** Addresses the reasons for the provision of personal data by individuals, perception of control over third-party access to their data, and attitudes toward privacy policies.
- **Business models:** Measures indicators that address individuals' knowledge about the practice of profiling, awareness about targeted advertising, and perception of associated risks.

The relationship between users' perception of privacy risks and behaviors that effectively increase their exposure to such risks or help mitigate them is complex, and the inconsistency observed between them is known as the "privacy paradox" (Barth & de Jong, 2017). Based on the results of the ICT Panel survey, the present analysis broadens the understanding of how individuals perceive the topic of privacy in a context of increasing digitization and engagement in the online environment, shedding light on the relationship between perceptions and practices effectively adopted by Internet users.

Concept

The first dimension investigated by the survey explores how Internet users understand the concept of privacy. To better investigate opinions and practices related to privacy, an open-ended question was included in the survey. The answers were analyzed and coded into broad categories, allowing the researchers to understand which domains people were referring to when they thought of "privacy."[1]

The methodology employed to categorize the open responses, described in Box 1 below, produced six categories:

- **Freedom:** Guarantee of freedom in private aspects of life ("freedom" — one's own and that of others —, "a right").
- **Individuality:** The search for individuality, whether in places or situations ("individuality," "intimacy," "space," "private").
- **Data protection:** A desire to protect one's own data against third parties ("data protection against third parties," "leaks").
- **Control:** A desire to have control over one's own data ("control over data access," "choice over what is 'public'," "consent").
- **Security:** More generic mentions of security ("security," "protection," "confidentiality," "monitoring").

[1] Respondents were asked the following question: "In your own words and considering your day-to-day life, what does 'privacy' mean to you?"

- **Other:** Valid answers that did not fall into any of the previous categories ("peace," "tranquility," "quiet," "important," "essential," "everything" [no further explanation], "does not exist").

The results indicate that most Internet users defined "privacy" based on domains associated with freedom and individuality (Chart 1), understood as crucial aspects of everyday life and even equated with a fundamental right.

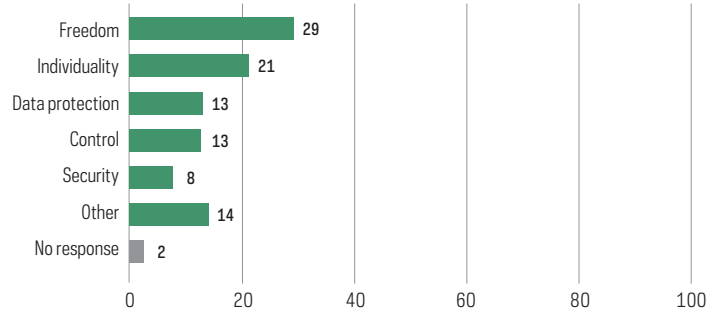
A lower proportion of respondents defined privacy with expressions associated with the use of the Internet, online platforms, and social networks. In those cases, privacy was put in terms of protection of data against unauthorized access, control regarding those who can have access to data (such as on social networks), and security against data theft and leaks in the digital environment.

The high incidence of responses classified as "Other" also reinforces the multifaceted nature of the topic among respondents.

CHART 1

CATEGORIES OF THE DEFINITION OF THE CONCEPT OF PRIVACY (2021)

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



The category "Data protection" presented variations by social class (17% among users in classes AB and 8% among those in classes DE) and level of education (6% among those with up to Elementary Education and 17% among those with Secondary Education). Between age groups, it is worth noting the proportion of the youngest respondents in the category "Individuality" (32% of those 16 to 24 years old and 27% of those 25 to 34 years old) and the proportion of the oldest respondents in the category "Freedom" (43% of those 60 years old or older).

These results indicate that a considerable portion of respondents described privacy in more abstract terms, tied to a fundamental right, such as freedom, in addition to dimensions associated with intimacy and the private realm. Another portion of respondents described privacy from a more objective perspective and direct link to personal data, to protection against their misuse and unwanted access, and to control and security strategies, both on and off the Internet, the social networks, and other online platforms.

BOX 1

METHODOLOGY USED TO ANALYZE THE ANSWERS TO THE OPEN-ENDED QUESTION

To analyze the responses to the open-ended question, a supervised machine learning method was used to classify the texts into analytical categories. At first, a sample of 500 responses was randomly selected and manually categorized by a group of researchers. The classification exercise was based on a similar initiative coordinated by the Pew Research Center in the United States (Auxier et al., 2019). The classification was adapted to the Brazilian context, which generated an initial set of 11 categories.

Given the low number of observations in some of the categories, the next step was to limit the categories through topic modeling (Chen & Yang, 2016). The best differentiation was found with six topics, which correspond to an approximation of the classifications used and the grouping of those that did not fit into the main categories in "Other."

Before performing the statistical analysis, the most common words in the Portuguese language were removed (stop words), as were diacritical marks and special characters, retaining only the radicals of the remaining words (stemming). Based on the new texts, descriptive analyses were performed to identify possible terms common to several categories that did not have substantive meaning, which were then also removed.

Because the sample had a smaller number of responses, the analysis required great attention not to overadjust the model, i.e., so it did not learn too much only about the manually classified answers and generalize it to the other responses. To this end, a model was applied that identified the parameter with the best performance in the classification based on a cross-validation process[2]. In a process that increased the reliability of the model in the training data, the 500 sample responses were randomly divided into five groups, with four groups being used as training data and one as test data. The process was then repeated ten times, randomizing the distribution of the groups in each repetition.

Based on the adjusted model, this technique was employed to classify all the answers obtained in the survey. First, point estimates for the proportions of each category were calculated, adjusting their respective weights within the set of responses. Next, to estimate the confidence intervals, 200 different subsamples were used in bootstrap, a resampling method, with updated weights for each (Efron, 1979).

The exercise of categorizing the open responses yielded six categories: "Freedom," "Individuality," "Data Protection," "(Data) Control," "Security," and "Other."[3]

[2] Hyperparameter tuning in Lasso models. See Bertrand et al. (2020) and Šehić et al. (2021).

[3] The categories "No response," "Security," "Control," and "Data Protection" did not present great variation in the bootstrap, generating lower confidence intervals and point estimates close to the median. On the other hand, the categories "Other," "Individuality," and "Freedom" presented greater variability, with fairly high confidence intervals. However, the point estimates of the first two were close to the median, unlike "Freedom," which was well above the median of its distribution. There are two possible explanations for this greater variation. The first is that the category "Other" was very heterogeneous, with answers that did not constitute relevant groups for disaggregation. The second relates to the categories "Individuality" and "Freedom" which, at times, had quite subtle distinctions even in the manual classification process.

Practices

The second dimension sought to understand what Internet users do to protect their personal data, the precautions they take in their daily use of the Internet and online platforms, and how they proceed when they have a problem related to this topic. The set of activities investigated consisted of routine decisions that users are presented with when they are online, such as providing consent for the processing of one's own data for advertising or defining cookie permissions when visiting websites.

Among the activities carried out to manage access to one's own personal data (Chart 2), Internet users 16 years old or older reported at a higher proportion the verification of the security of web pages or apps (70%), for instance, by checking whether a web page had a security padlock[4]. The proportion was lower among those who accessed the Internet exclusively via mobile phones (59%). This is to be expected, since this element is often suppressed or made less visible to users in mobile apps.[5] Another common practice was denying permission to the use of personal data for targeted advertising (69%) and reading privacy policies of web pages or apps (68%).

Among the least mentioned activities were defining or limiting the use of cookies (58%) and requesting that data processing agents, such as web pages, apps, or search engines, delete information about oneself (42%). It is worth highlighting that requesting the deletion of personal data requires greater proactivity on the part of individuals, since the user must directly contact the data controller. Since this is a lesser-known provision of the LGPD (Article 18, Item -VI), it is possible that most users are unaware of this possibility.

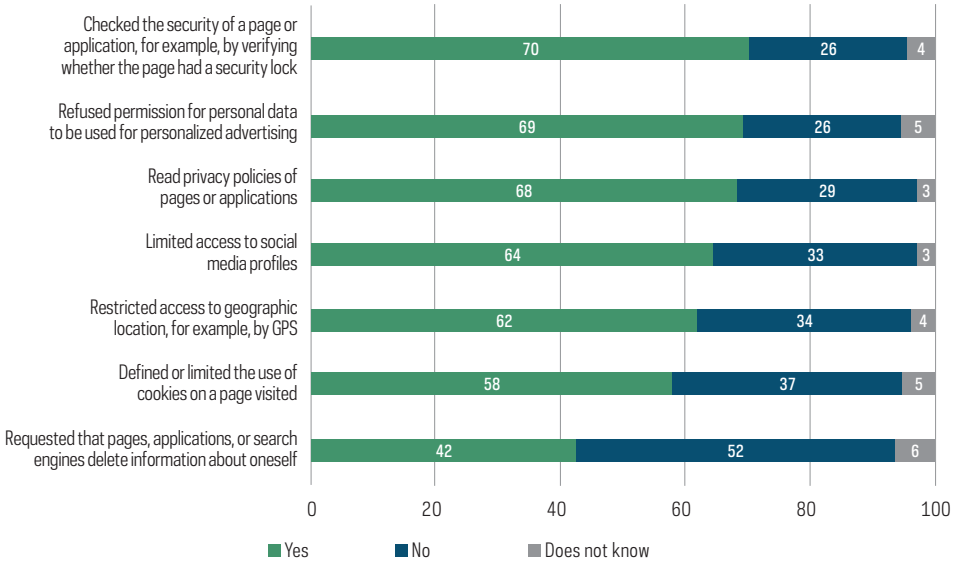
[4] This aspect frequently appeared in the cognitive interviews conducted for the questionnaire tests of the ICT Households and ICT Kids Online surveys as indicative of a website's safety, relevant to the users' perception that their data is protected from intrusion or theft by third parties.

[5] Because of the reduced screen size of mobile devices, Internet browsers such as Chrome or Firefox hide the address bar (where the usual elements related to security certification appear) when scrolling down the screen. When access to the Internet happens via other categories of applications, such as e-commerce, this type of information is not made available to users.

CHART 2

PERSONAL DATA ACCESS MANAGEMENT PRACTICES (2021)

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



Seeking out customer service channels to file requests, complaints, or reports was an activity carried out by 24% of Internet users 16 years old and older (Chart 3). Among those who performed this activity, the most mentioned channel was the data-controlling enterprise or government organization (80%). Most users attempt to resolve their requests directly with data controllers — such as enterprises, online platforms, or apps that collect or store the personal data in question. This reinforces the importance of data controllers establishing effective procedures to receive and process this type of demand.

Consumer protection agencies (e.g., Procon) (48%), or the justice system (e.g., Special Civil Courts) (28%), were mentioned in smaller proportions. The National Data Protection Authority (ANPD)[6] was mentioned by 27% of the users.[7] Among those who did not seek out customer service channels to file requests, complaints, or reports, the most mentioned channels they would seek out in such an event would be consumer protection agencies (79%), followed by the data-controlling enterprise or government organization (74%), the police (65%), and the ANPD (62%).

[6] The National Data Protection Authority website offers data subjects the possibility to register complaints online: https://www.gov.br/anpd/pt-br/canais_atendimento/cidadao-titular-de-dados/denuncia-de-descumprimento-da-lgpd

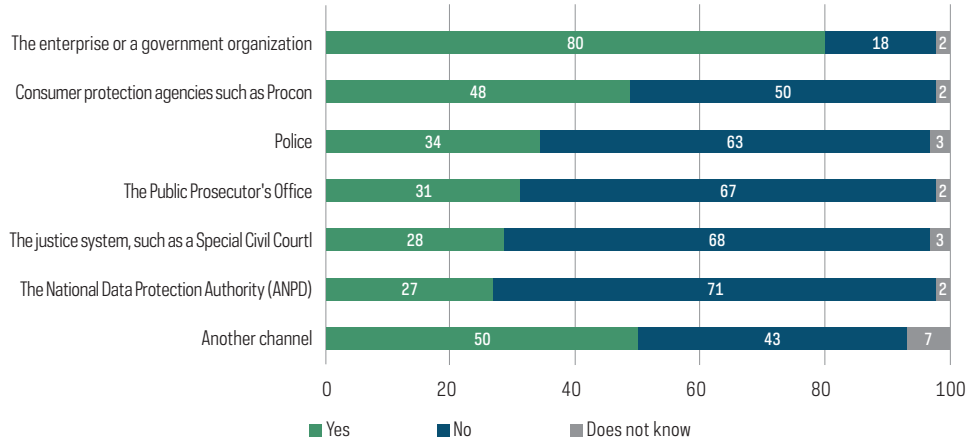
[7] Seeking out customer service channels for filing requests, complaints, or reports can be understood by respondents as a broad set of actions, from searching for information about legal rights and the appropriate course of action to carrying out interactive services such as filing complaints or legal claims. This perception is corroborated by the experience of Cetic.br|NIC.br with the collection of data about e-government services in the ICT Households and ICT Electronic Government surveys, which show that a considerable portion of users of e-government services only search for official information (either directly on government websites or through search engines).

The data indicate that consumer protection agencies, strengthened by the Consumer Protection Code in the 1990s, are more present in the repertoire of users. Therefore, data subjects associated in greater proportions filing complaints or requests regarding personal data to a consumer issue, or even to a crime, by reporting it to police authorities.

CHART 3

CUSTOMER SERVICE CHANNELS SOUGHT OUT ABOUT PERSONAL DATA (2021)

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



Risks

The results of the survey show that Internet users' levels of concern about personal data are most often related to financial losses, such as banking fraud or other types of Internet fraud involving identity theft, rather than to risks associated with reputation or discrimination. This reveals that users are more familiar with the existence of financial threats and losses in the digital environment, in addition to the high potential for damage that this type of risk represents to users.[8]

In terms of concerns about data records, including of offline activities[9], 36% of Internet users 16 years old and older said they were very concerned and 24% said they were concerned about data records when using means of payment such as credit cards, bank payment slips, or Pix, the Brazilian instant payment system (Chart 4). Users also expressed high levels of concern about data records when circulating in public spaces or using public transit (29% very concerned and 31% concerned) and

[8] A trend previously observed in the 2nd edition of the ICT Panel survey (CGI.br, 2020b).

[9] Text presented to respondents before the question on concern about data records: "Today, many of our activities are recorded in various ways, both online, such as the history of pages we have accessed or our posts on social networks, and offline, such as when we pay with a credit card or when we are filmed by surveillance cameras."

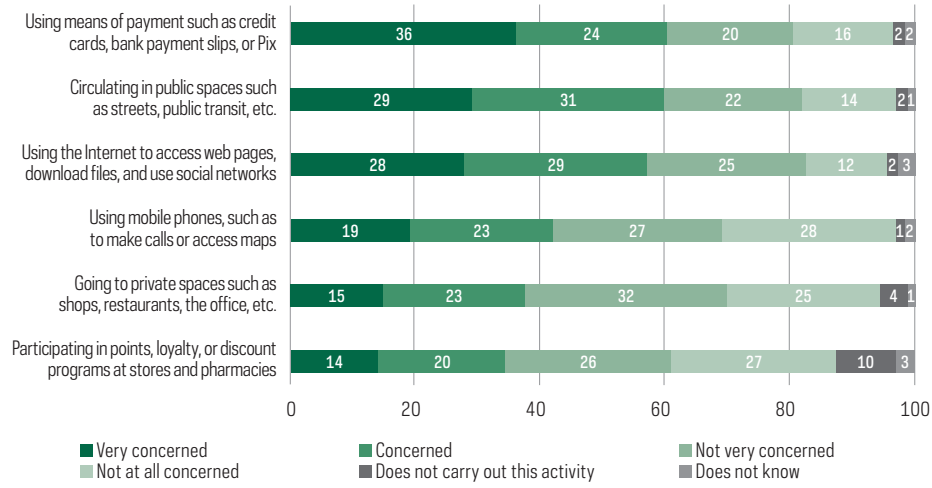
using the Internet to access web pages, download files, or use social networks (28% very concerned and 29% concerned).

The indicator reveals that concerns with data records span beyond online activities, since the most mentioned categories were related to payment records (bank information, individual taxpayer identification number [CPF], physical address, among others) and public spaces (such as records from security cameras and from using public transit).

CHART 4

LEVEL OF CONCERN ABOUT RECORDS OF ACTIVITIES BY TYPE OF RECORD (2021)

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



Data records that are generated when using the Internet were also a source of concern among most Internet users. Among online activities (Chart 5), users reported higher levels of concern when making purchases online via web pages or apps (42% very concerned and 25% concerned), followed by accessing online banking via web pages or apps (35% very concerned and 24% concerned). It is also worth mentioning that using dating apps, despite being the least carried out activity by the respondents[10], presented the third highest proportion of concerned users (22% very concerned and 12% concerned), considering only those who carried out the investigated activities.

These results underpin the users' assessment of the higher potential for harm of data related to financial transactions and e-commerce. They also reveal the concern of users about the processing of their data in other activities, such as the use of dating

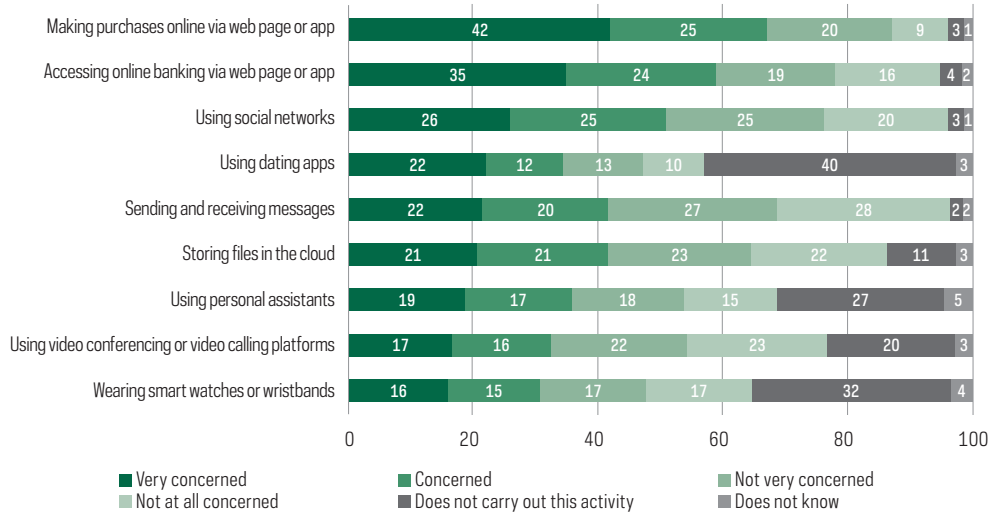
[10] It is important to mention that subjective perceptions reflect the views of the respondents and their positions on a topic, and do not necessarily embody all who adopt a given practice. For example, those who reported their level of concern or perception of control over each activity do not necessarily carry out these activities.

apps, which had been little explored in previous studies. It is important to highlight that more than half of users were very concerned (26%) or concerned (25%) about the use of social networks.[11]

CHART 5

LEVEL OF CONCERN ABOUT PERSONAL DATA BY INTERNET ACTIVITY (2021)

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



Governments store and process large amounts of citizens' personal data when performing their regular activities, such as security, identification, taxation, and delivery of public services. In this context, 40% of Internet users said they were very concerned, and 29% concerned, about how public authorities used their data. The level of concern varied somewhat when compared to another indicator on data use by enterprises: 47% said they were very concerned and 28% were concerned.

There were differences in levels of concern about the use of personal data by enterprises according to the color or race of the respondents. Black (52%) and Brown (49%) users said they were very concerned at higher proportions than White (43%) respondents, which suggests a perception of discriminatory use of this data. When used by governments, there was greater concern among Black users (47% were very concerned), with lower proportions among Brown (41%) and White (37%) ones.

Regarding sensitive personal information, Internet users reported a higher level of concern about the provision of biometric data (41% very concerned and 24% concerned), surpassing that of the other types of personal data investigated (Chart 6). The advancement of biometrics in various contexts of everyday life, combined with

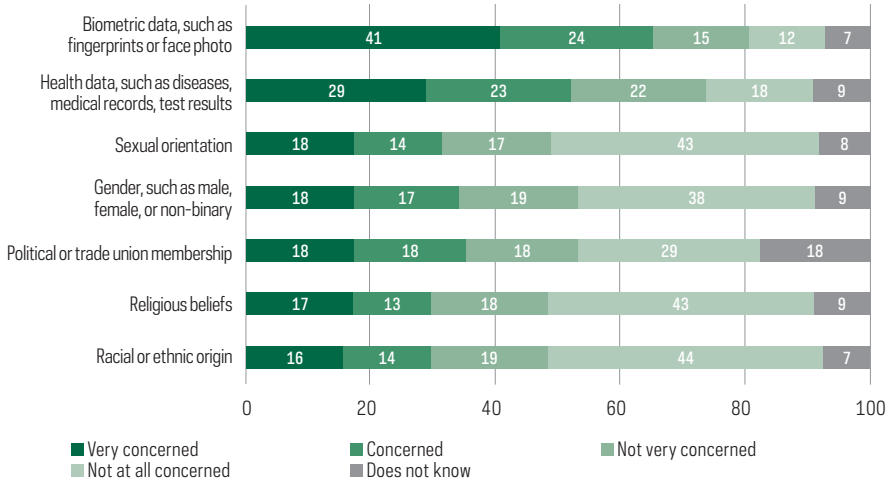
[11] According to the ICT Households 2021 survey (CGI.br, in press), social networks are one of the most common types of platforms used by Internet users in Brazil, with higher usage rates in all age groups and social classes (81% of Internet users used social networks).

the intimate, tangible, and material nature of this type of data and its high potential for damage once compromised, help explain these results. It is worth highlighting that the use of biometric data in elections was introduced in the 2008 election and there were 120 million voters registered with biometric data in 2020, with the goal of reaching all voters by 2026[12]. It is also possible to observe the use of biometrics by the private sector in banks, pharmacies, gyms, and gated communities.[13]

CHART 6

LEVEL OF CONCERN ABOUT PROVISION OF SENSITIVE PERSONAL INFORMATION (2021)

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



Another category that stood out was health data: 29% of respondents said they were very concerned and 23% concerned with providing them. According to the LGPD, personal health data, in addition to data about sexual orientation, religious beliefs, political opinions, race, and genetic or biometric data, among others, are categorized as sensitive personal data, since their improper use can allow for the identification of individuals and cause situations of discrimination (Botelho & Camargo, 2021). This highlights the importance of considering the context of vulnerability of data subjects and the potential effects and risks in the processing of this type of data (Costa, 2022).

The sensitive nature of this type of data lies in the fact that its inappropriate use can cause damage to people's fundamental rights, especially those related to a person's privacy, intimacy, equality, and dignity (Bioni, 2019). Therefore, this greater concern about health data may be related to its potential to invade the sphere of privacy and

[12] More information about the implementation of biometrics by the Superior Electoral Court (TSE) at https://www.tse.jus.br/eleitor/biometria/biometria

[13] See inquiries about biometric data collection made by the Brazilian Institute of Consumer Protection (Idec) (https://idec.org.br/release/idec-questiona-coleta-de-impressao-digital-em-farmacias) and the campaign against the use of facial recognition (https://tiremeurostodasuamira.org.br/).

intimacy to a much greater extent than ordinary personal data. In this sense, the discriminatory effects are not in the data itself, but in how it is used (Doneda, 2019).

The risks on the use of personal data perceived by Internet users 16 years old or older were mostly associated with financial losses, banking fraud, and data leaks or theft (87%)[14]. Other risks, such as reputation (74%), discrimination (65%) or receiving unwanted advertising (60%) were often mentioned, but at a lower level. It is interesting to note that, among those self-identified as Black, the perception of risk of discrimination was higher than average (72%).

Control

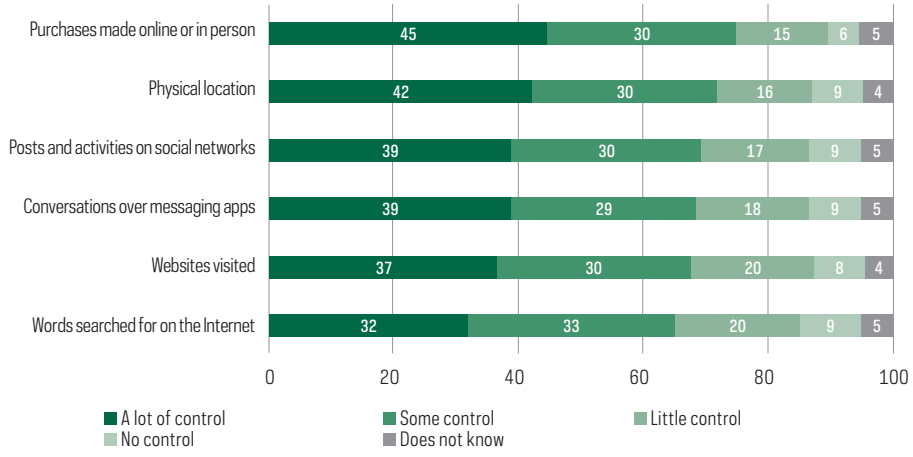
Although they reported concern about the risks related to the use of their personal data, Internet users 16 years old or older also reported having a lot of control over the access of third parties and the use that data-controlling organizations make of their data.

Of Internet users 16 years old and older, 45% said they have a lot of control over who can access personal data from purchases made online or in person, and 42% said they have a lot of control over data related to their physical location (Chart 7). Among the types of information investigated, those that presented the lowest perception of control were the words searched for on the Internet: 32% believed they had a lot of control and 29% believed they had little or no control.

CHART 7

PERCEIVED LEVEL OF CONTROL OVER WHO CAN ACCESS DATA BY TYPE OF INFORMATION (2021)

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



[14] The ANPD and the Brazilian National Computer Emergency Response Team (CERT.br), a department of the Brazilian Network Information Center (NIC.br), produced a booklet on data leaks that includes prevention actions and information on how to proceed in case of incidents (ANPD & NIC.br, 2021a).

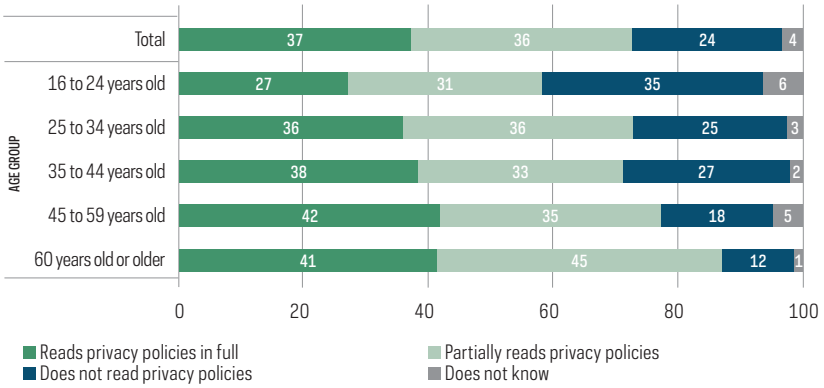
Most users claimed to have a lot or some control over all the types of information investigated. This sense of control may be related to the possibility of making choices in the privacy settings of social networks and other online platforms. It can also be understood as a lack of knowledge about how enterprises share personal data, as explained in their privacy policies. This is supported by the low proportion of those who said they read privacy policies in full, as shown below.

Advances in legislation regarding the collection, processing, and use of personal data of visitors and users led websites and online platforms to begin requesting the acceptance of privacy policies and cookie settings. In most cases, users must consent to the policies to access the content or service. However, many users stated they do not read these documents in full: 37% of Internet users 16 years old or older said they read privacy policies in full, while 36% said they partially read them, and 24% said they did not read the policies at all (Chart 8).[15]

CHART 8

READING PRIVACY POLICIES OF WEB PAGES OR APPS (2021)

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



This indicator presented a considerable variation in behavior according to age group. Users 16 to 24 years old said they read privacy policies in full (27%) at a proportion lower than average, but also said that they did not read privacy policies (35%) at a proportion higher than average. Among Internet users 16 years old or older who did not read or partially read privacy policies, the most mentioned reasons for not reading them in full were because they were too long (81%) and difficult to understand (69%).

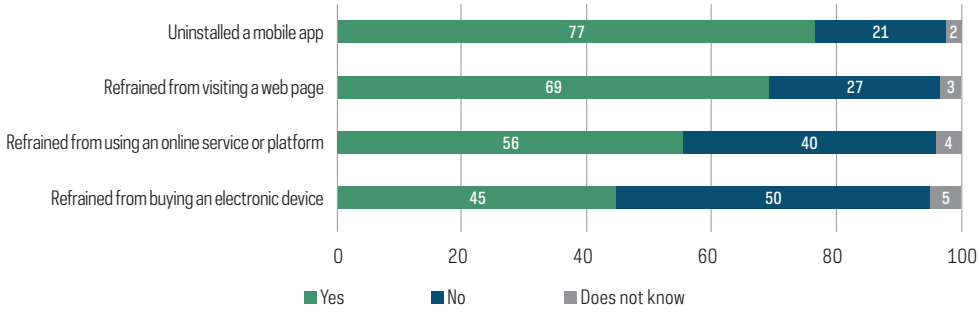
[15] Despite the requirement for explicit consent to be obtained from users, and in some cases, it is only possible to proceed after scrolling to the end of the text of the document, data obtained from Web analytics and curious experiments — including clauses that oblige users to "hand over their firstborn to the enterprise for all eternity" or that offer cash prizes — show that this percentage could be even lower in practice. See Kon (n.d.) and Obar and Oeldorf-Hirsch (2018).

Motivated by concerns about the use of their personal data, 77% of Internet users 16 years old or older uninstalled apps, 69% refrained from visiting a web page, 56% refrained from using an online service or platform, and 45% refrained from buying an electronic device (Chart 9). The choice to adopt some form of self-restraint online reinforces the perception of high risks presented previously. Although the survey did not investigate the frequency or intensity of this self-restrictive behavior, it can be said that concerns about the processing of personal data shape the decisions of most users are at some point.[16]

CHART 9

MEASURES TAKEN DUE TO CONCERNS ABOUT PERSONAL DATA (2021)

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



Business model

After being presented with an explanation of what profiling is[17], 56% of Internet users said they had heard of this practice before. This indicator showed significant differences by some variables (Chart 10). Among individuals with up to Elementary Education, 47% said they were familiar with the concept. This was true of 68% of those with Tertiary Education. A smaller proportion of individuals 16 to 24 years old (47%) said they were familiar with the concept. Knowledge about such practices was also lower in classes DE (46%), among those in rural areas (43%), and among individuals who accessed the Internet exclusively via mobile phones (45%).

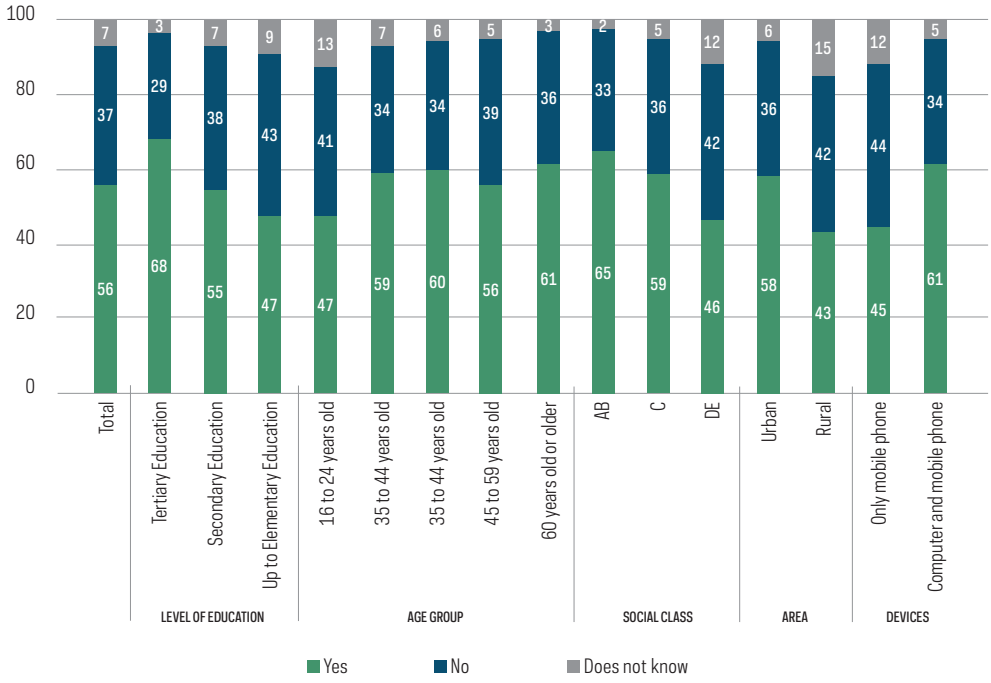
[16] The ANPD and the CERT.br|NIC.br produced a document containing actions to strengthen the protection of personal data, reducing the risks of leaks and theft. Among the proposed actions are the regular implementation of backups, the creation of encrypted folders, the use of strong passwords, the installation of applications only of known origin and the updating of systems (ANPD & NIC.br, 2021b).

[17] Text presented to respondents before questions about profiling: "Today it is possible to combine people's data from various sources, such as shopping and payment data, search and browsing habits on the Internet, and liked pages on social networks. This combination creates detailed profiles of people's habits, interests, and characteristics. Enterprises can use these profiles to offer personalized and targeted advertising or to assess risks of having these profiles as customers."

CHART 10

KNOWLEDGE ABOUT PROFILING AND TARGETED ADVERTISING (2021)

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



Among those familiar with the concept, 46% said they saw targeted ads often, 21% said they saw it sometimes, 7% rarely, and 23% said they had never seen it. In addition to the variables that were relevant to the indicator on knowledge of the concept, variations by sex are also worth noting: among men, 51% said they saw targeted ads often and 17% had never seen it. Among women, 43% saw it often and 27% had never seen it.[18]

User profiling is an important part of the Internet business models of many enterprises in technology and other industries and is at the center of many debates and regulatory efforts regarding privacy. The lack of awareness of this practice by 37% of Internet users indicates that it does not inform the decision-making process of a considerable portion of Internet users regarding online activities, whether to avoid behaviors that increase exposure to perceived risks or to adopt measures that help mitigate them, regardless of their level of concern about the topic or the digital skills necessary to do so.

[18] The ICT Enterprises 2019 survey showed that 36% of Brazilian enterprises paid for online advertising. Although there were no differences between the sizes of the enterprises, the survey results indicate that advertising was more present in enterprises in the accommodation and food service activities (50%) and information and communication (46%) segments (CGI.br, 2020a).

Final considerations: Agenda for public policies

This survey represented an unprecedented effort to investigate the topic of privacy and data protection among Internet users in Brazil. The results shed light on the practices and perceptions of Brazilians users about the topic at an opportune moment, given the recent coming into force of the LGPD and creation of the ANPD.

The survey points out that the concept of privacy was mostly associated with freedom and individuality, with fewer users connecting it more directly to data protection and control over who can access data. The results also indicate a higher perception of risks associated with financial losses, such as banking frauds or other types of Internet fraud involving identity theft. This suggests the need to strengthen trust in the digital environment, especially regarding financial transactions and e-commerce.

It is also worth noting the respondents' concern about information theft and unauthorized sharing with third parties. In addition to establishing privacy policies and data protection mechanisms that ensure to data subjects a transparent and responsible stewardship of their personal data, it is essential that data controllers implement practices and procedures to effectively protect their users' data.

Additionally, as currently presented, privacy policies remain elusive to most users, even though accepting them is often a requirement to access the service, application, or content. This is shown by the perception of users who did not read the policies that they are too long and difficult to understand. In this sense, it is important to develop strategies to simplify the presentation of such policies to users, such as using clear language, highlighting the main points up-front, and avoiding technical jargon, assisting users in making informed decisions.

No less important are other issues pointed out in the results, such as concerns about the use of biometric and health data, and the discrimination and reputation risks. Although mentioned at lower levels than financial issues, they are themes that are already part of the routine of users.

Biometric data was the most mentioned among the categories investigated as a type of information that concerns Internet users, which also requires public and private organizations to reflect on its collection. It is also important to highlight the difference in the results related to the topic of discrimination among Black and Brown users, which reflects the demand for specific strategies to confront discriminatory practices that take into account social markers such as color or race.

In short, the results represent a baseline for monitoring the topic in Brazil and help underpin the importance of deepening the public debate in favor of a culture of personal data protection.

References

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

Barth, S., & de Jong, M. D. T. (2017). The privacy paradox: Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics, 34*(7), 1038–1058. https://doi.org/10.1016/j.tele.2017.04.013

Bertrand, Q., Klopfenstein, Q., Blondel, M., Vaiter, S., Gramfort, A., & Salmon, J. (2020). Implicit differentiation of Lasso-type models for hyperparameter optimization. *Proceedings of Machine Learning Research, 119*, 810–821.

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

Botelho, M. C., & Camargo, E. P. do A. (2021). A aplicação da Lei Geral de Proteção de Dados na saúde. *Revista de Direito Sanitário, 21*(e0021). https://doi.org/10.11606/issn.2316-9044.rdisan.2021.168023

Brazilian Internet Steering Committee. (in press). *Survey on the use of information and communication technologies in Brazilian households: ICT Households 2020*.

Brazilian Internet Steering Committee. (2020a). *Survey on the use of information and communication technologies in Brazilian enterprises: ICT Enterprises 2019*. https://cetic.br/pt/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-nas-empresas-brasileiras-tic-empresas-2019/

Brazilian Internet Steering Committee. (2020b). *Painel TIC COVID-19: Pesquisa sobre o uso da Internet no Brasil durante a pandemia do novo coronavírus – 2ª edição: serviços públicos online, telessaúde e privacidade*. https://www.cetic.br/pt/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/

Carrière-Swallow, Y., & Haksar, V. (2019). *The economics and implications of data: An integrated perspective* (IMF Departmental Paper Series No. 19/16). https://doi.org/10.5089/9781513511436.087

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

Cisco. (2021). *Cisco 2021 consumer privacy survey: Building consumer confidence through transparency and control*. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-cybersecurity-series-2021-cps.pdf

Costa, R. (2022). Personalidade hackeada: Considerações sobre proteção de dados pessoais sensíveis, vigilância digital e discriminação. In C. S. Teffé & S. Branco (Eds.), *Proteção de dados e tecnologia: Estudos da pós-graduação em Direito Digital* (pp. 52–78). Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS); Obliq.

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

Efron, B. (1979). Bootstrap methods: Another look at the jackknife. *The Annals of Statistics, 7*(1), 1–26. http://www.jstor.org/stable/2958830

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

Kon, G. (n.d.). *Does anyone read privacy notices? The facts.* https://www.linklaters.com/en/insights/blogs/digilinks/does-anyone-read-privacy-notices-the-facts

National Data Protection Authority, & Brazilian Network Information Center. (2021a). *Cartilha de segurança para Internet: Fascículo vazamento de dados.* https://cartilha.cert.br/fasciculos/vazamento-de-dados/fasciculo-vazamento-de-dados.pdf

National Data Protection Authority, & Brazilian Network Information Center. (2021b). *Cartilha de segurança para Internet: Fascículo proteção de dados.* https://cartilha.cert.br/fasciculos/protecao-de-dados/fasciculo-protecao-de-dados.pdf

Obar, J. A., & Oeldorf-Hirsc, A. (2018). The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services. *Information, Communication & Society.* https://ssrn.com/abstract=2757465

Office of the Privacy Commissioner of Canada. (2021). *2020 Survey of Canadians on privacy-related issues: Final report.* https://publications.gc.ca/collections/collection_2021/cpvp-opc/IP54-109-2021-eng.pdf

Šehić, K., Gramfort, A., Salmon, J., & Nardi, L. (2021). *LassoBench: A high-dimensional hyperparameter optimization benchmark suite for lasso.* ArXiv. https://doi.org/10.48550/arXiv.2111.02790

Analysis of Results
Privacy and Personal Data Protection 2021
Enterprises

Data is currently an indispensable resource for improving the performance of private sector organizations. The ability to collect, store and analyze data enables enterprises to plan and evaluate their activities, since it allows the use of detailed information about the behavior and demands of users and clients of the most diverse services. Numerous international organizations recognize data as one of the most valuable inputs in today's economy, highlighting its economic impact on various transactions (United Nations Conferenceon Trade and Development [UNCTAD], 2021). There are, however, growing concerns about the need for multisectoral collaboration to promote responsible use and regulation of personal information (Internet & Jurisdiction Policy Network, 2021).

In 2021, 145 countries had privacy and personal data protection laws, showing a global concern about the regulation of the subject (Greenleaf, 2021). The approval of laws that impose increasing control over the processing of personal data has posed challenges to enterprises around the world, as established routines must be changed and the strengthening of a data protection culture must be fostered, while investments must be directed to improving digital security.[1]

In the Brazilian context, a broad discussion has begun in the business sector about compliance with the Brazilian General Data Protection Law (LGPD) and its impacts since it took effect in September 2020. Since enterprises process personal data, whether of clients, employees, or even third parties, the coming into force of the law has brought numerous challenges and opportunities for the productive sector.

Aiming to understand how small, medium and large enterprises process personal data of their clients, employees, suppliers and partners, as well as map relevant issues associated with the implementation of the LGPD in Brazil, Cetic.br|NIC.br created,

[1] Similar difficulties have been reported for European enterprises in complying with the General Data Protection Regulation (GDPR). Initially, several enterprises made use of palliative measures to be compliant, but many challenges remain, such as impact assessments and audits, which are not often carried out (Mikkelsen et al., 2019).

throughout 2021, a specific module for the production of indicators on the topic. Implemented as part of the ICT Enterprises 2021 survey fieldwork, the indicators provide a broad overview of organizational changes and practices driven by this initial period of LGPD implementation by the competent authority[2] and its compliance among Brazilian enterprises.

The new module, developed with the contribution of several experts on the subject, highlights the main practices that enterprises are adopting so that personal data is processed securely and in compliance with the law – even though many aspects regarding proper compliance with the LGPD and understanding about its scope are still subject to intense debate, some of which even lack regulations for the law to produce its full effect.[3]

In this analysis, the data from the privacy and personal data protection module will be presented in four dimensions:

- **Personal data storage and purposes for use:** Indicators on the types of personal data enterprises keep and the purposes for which they use them;
- **Development of internal capacity:** Indicators on actions to raise awareness of the internal staff of enterprises on the subject of privacy and personal data protection;
- **Compliance with the LGPD:** Indicators on actions aimed at compliance with the law, as well as attitudes that seek to strengthen good personal data processing practices in the enterprises;
- **Barriers and opportunities:** Indicators on perceptions of difficulties in complying with the LGPD and opinions on possibilities for enterprises' operations.

Personal data storage and purposes for use

The purpose of this section is to verify the types of personal data that enterprises keep and the purposes for which they use them. According to Article 5 of the LGPD, personal data refers to "information regarding an identified or identifiable natural person." Therefore, the law addresses the processing[4] of any data, within organizations,

[2] The LGPD included the creation of the National Data Protection Authority (ANPD), responsible for the implementation and enforcement of the law, as a federal government organization linked to the Presidency of the Republic. The nature of the Authority was changed to "an autarchy of a special nature, with technical and decision-making autonomy, in addition to its own assets and head office and jurisdiction in the Federal District," by Provisional Measure 1124, of 2022.

[3] One of the examples of this moment of definitions about the application of the LGPD is the understanding about the regulatory asymmetries in relation to micro and small enterprises. The ANPD has defined special rules for compliance with the law in the case of small data processing agents in Resolution CD/ANPD No. 2, of January 27, 2022, comprising enterprises with revenues up to BRL 4,800,000, start-ups and individual microentrepreneurs with annual income up to BRL 360,000. Available at: https://in.gov.br/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019

[4] According to the LGPD (Article 5, item X), processing is defined as "any operation carried out with personal data, such as collection, production, receipt, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, deletion, evaluation or control of the information, modification, communication, transfer, dissemination or extraction".

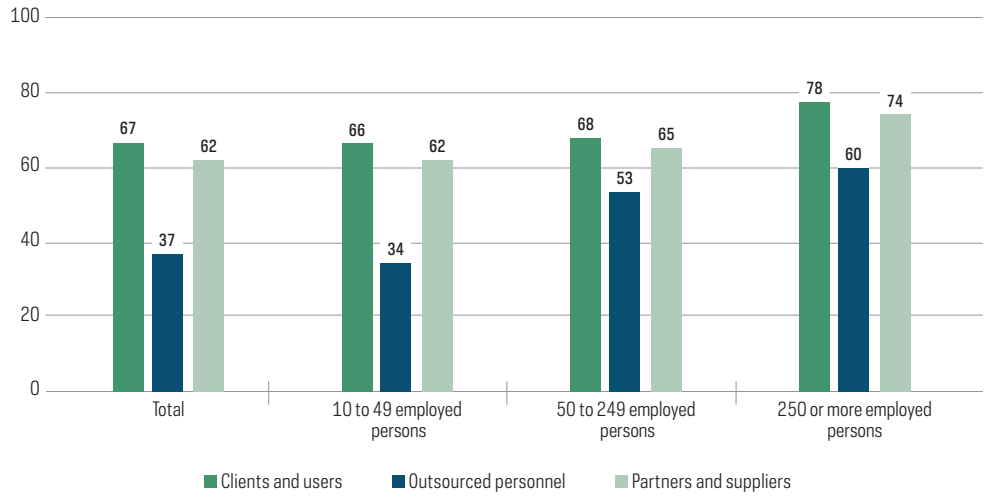
that can refer to a natural person, understood as the data subject, that is, "a natural person to whom the personal data that are the object of processing refer" (item V).

According to the survey data, in 2021, only 37% of enterprises stored outsourced personnel data, whereas 62% kept the data of partners and suppliers (Chart 1). There were no major differences in data maintenance by size and market segment, but it is worth mentioning that the segments of information and communication and professional activities showed the highest levels of client and user data storage, reaching 78% of the enterprises in these segments.

CHART 1

ENTERPRISES BY TYPE OF PERSONAL DATA STORED AND SIZE (2021)

Total number of enterprises (%)



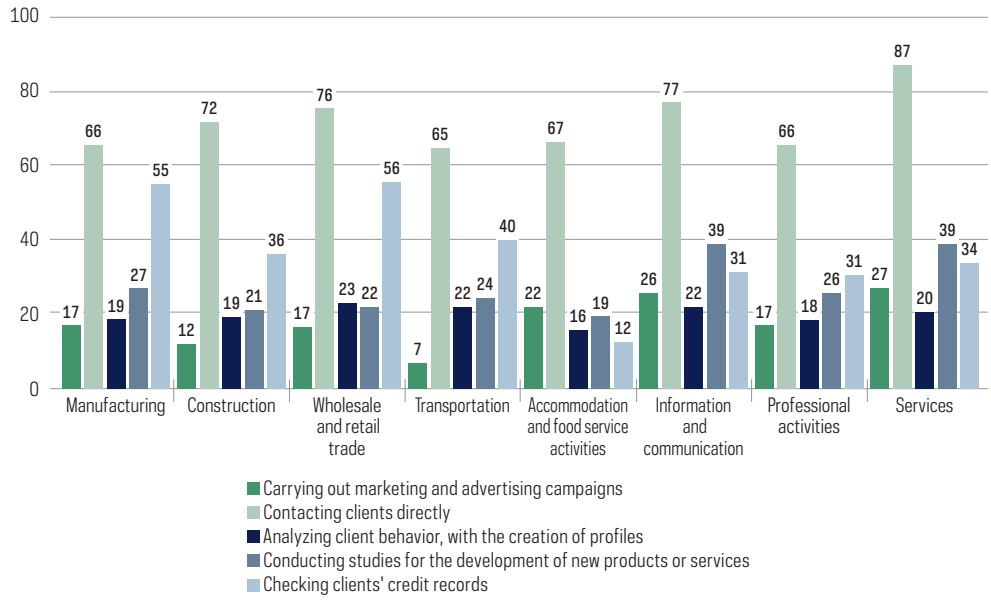
Regarding the use of stored personal data, most enterprises reported holding personal data in order to contact clients (71%) directly and to check their credit records (45%)[5]. There were no major differences in the purposes for which personal data was used by sector, with the exception of a more pronounced use of credit record verification in manufacturing and wholesale and retail trade enterprises. Another highlight was the use of personal data of clients and users to conduct studies for the development of new products or services, reported by 39% of the enterprises in the segments of information and communication and services.

[5] For the proper use of these types of personal data, enterprises must have the consent of data subjects in the first case, and, in the second case, there is legal support for data processing. According to Article 7 of the LGPD, directly in line with the types of use most commonly reported in the survey: "Processing of personal data shall only be carried out under the following circumstances: I – with the consent of the data subject; [...] X – for the protection of credit, including as provided in the pertinent legislation."

CHART 2

ENTERPRISES BY PURPOSES FOR THE USE OF PERSONAL DATA AND SECTOR (2021)

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



Sensitive data is a critical aspect for processing personal data in enterprises. According to the LGPD, sensitive personal data refers to "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" (Article 5, item II). The objective of the law is to prevent processing of sensitive data that could lead to discriminatory actions, given that the very nature of this data exacerbates these risks. Article 11 of the LGPD makes it clear that the use of sensitive personal data is only allowed in very specific situations, such as in the circumstance of protecting the life of the data subject or that of third parties, albeit with various restrictions regarding communication and sharing of this information. Therefore, the processing of sensitive personal data must be evaluated by all enterprises, always seeking to justify its use based on the law or even minimize or avoid using it whenever it is not necessary for the business model.[6]

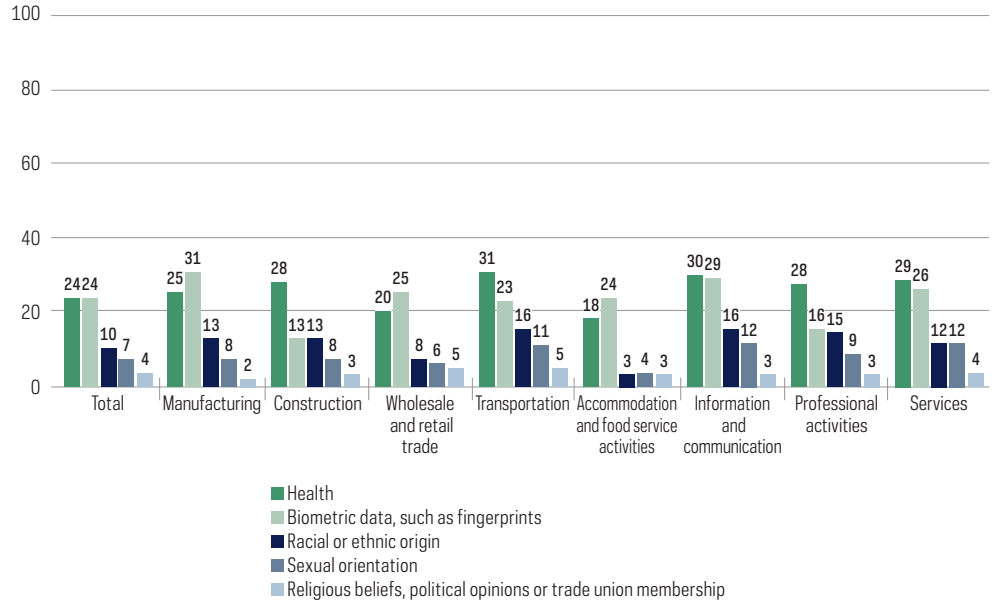
[6] One point for companies to take into account when dealing with the processing of personal data is to pay attention to the principles of the LGPD, as described in its Article 6. If the intended uses contravene any of the law's principles, it is necessary to reassess whether the use of personal data is in fact indispensable.

The survey conducted with small, medium and large enterprises indicated that most of the sensitive personal data kept by companies involved biometric and health data (24%) – which may be related to the processing of employees' personal data. Sensitive personal data relating to racial, sexual, or ideological issues were less frequently stored. Even though only a small number of enterprises reported processing sensitive personal data, it is important that all organizations make a data inventory to ascertain the types of data stored and the necessary measures for proper processing.[7]

CHART 3

ENTERPRISES BY TYPE OF SENSITIVE PERSONAL DATA STORED (2021)

Total number of enterprises (%)



[7] One reference is the *Guide to creating an inventory of personal data* (in Portuguese, *Guia de elaboração de inventário de dados pessoais*) (Ministry of Economy, 2021), which offers a template for government organizations to detail their personal data processing operations. Although it is aimed at the public sector, the guide can be applied to private organizations, considering that the mapping methodology can be adapted. Another important point is that the inventory suggested by the guide seeks alignment with Article 37 of the LGPD: "The controller and the processor shall keep records of personal data processing operations carried out by them, especially when based on legitimate interest."

Development of internal capacity

Another central aspect for the development of a data protection culture is actions carried out by enterprises that promote staff training and awareness. It is essential to verify the presence of activities that include all members of organizations, at their various hierarchical levels.[8]

The survey showed that 36% of enterprises carried out internal meetings to specifically address privacy and personal data protection. Although there were no significant regional differences, these meetings were carried out unevenly among the different market segments: information and communication had the highest frequency, and construction, the lowest. Additionally, it is worth noting that meetings were held more in large (73%) and medium (59%) enterprises, while the proportion of small enterprises that sought to discuss privacy and personal data protection issues internally was lower.[9]

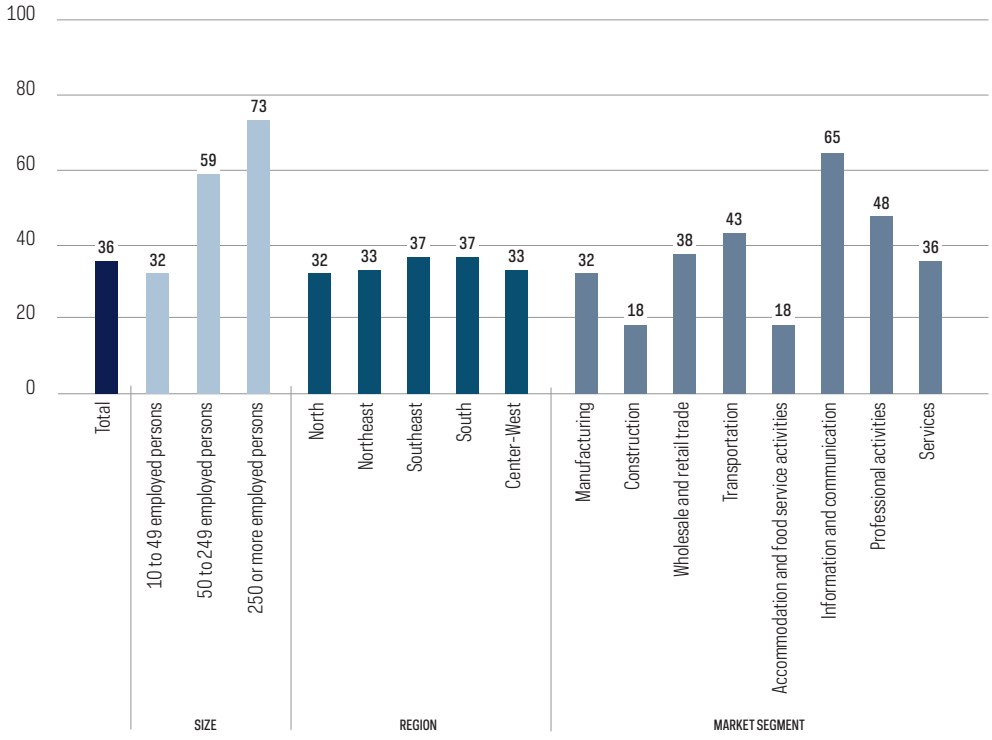
[8] The publication *Digital security: An analysis of risk management in Brazilian enterprises* (NIC.br, 2021) presents case studies that highlight the need to standardize knowledge about basic digital security, because organizations are exposed to various risks that can lead to personal data leaks, causing financial and reputational damage that may be irreversible. One of the aspects addressed by the LGPD is risk mitigation, such as the reduction of personal data security incidents, as set forth in Article 50: "Controllers and processors, within the scope of their controllers and processors, within the scope of their functions, concerning the processing of personal data, individually or by associations, may formulate rules for good practices and governance that set forth conditions of organization, a regime of operation, the procedures, including those for complaints and petitions from data subjects, security norms, technical standards, specific obligations for the various parties involved in the processing, educational activities, internal mechanisms of supervision and risk mitigation and other aspects related to the processing of personal data."

[9] The ANPD prepared a guide for the implementation of information security practices to underpin the strengthening of data protection among small agents, specifically micro and small enterprises and start-ups (ANPD, 2021).

CHART 4

ENTERPRISES BY INTERNAL MEETINGS CARRIED OUT TO ADDRESS DATA PROTECTION (2021)

Total number of enterprises (%)

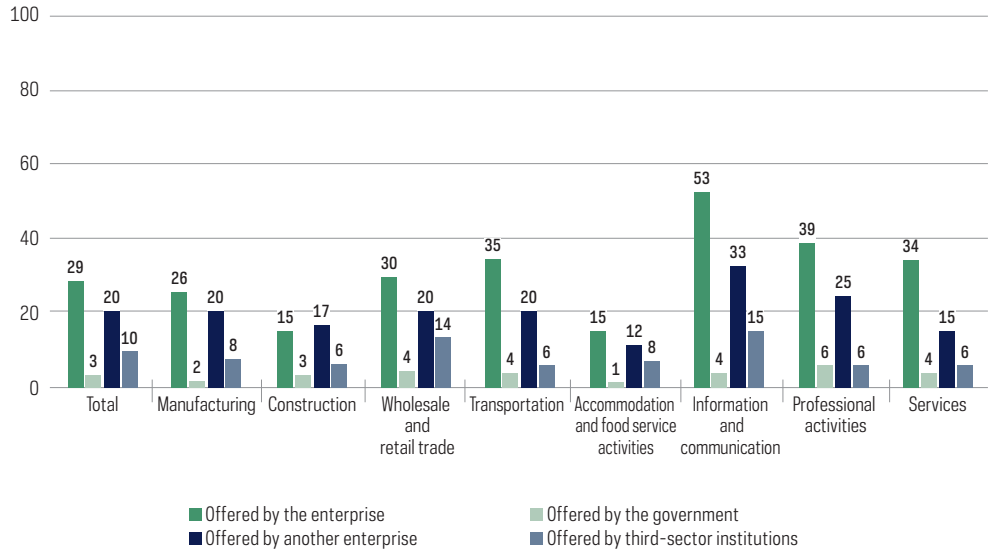


Regarding the most effective actions to achieve compliance with the new data protection rules, few enterprises carried out measures to increase their capacities relative to the topic of privacy and personal data protection. Among the different types of training, the most mentioned model was that offered by the enterprises (29%), showing the prevalence of the organizations' own efforts. In the segments that most carried out capacity building or training actions – as in the case of information and communication or professional activities – the most prevalent were internal initiatives and those of other enterprises, indicating a concern about seeking more comprehensive training. The search for training may also be related to segments in which the processing of personal data takes on a more strategic role for the performance of enterprises or in service delivery.

CHART 5

ENTERPRISES BY TYPES OF TRAINING PROGRAMS ON PERSONAL DATA PROTECTION (2021)

Total number of enterprises (%)



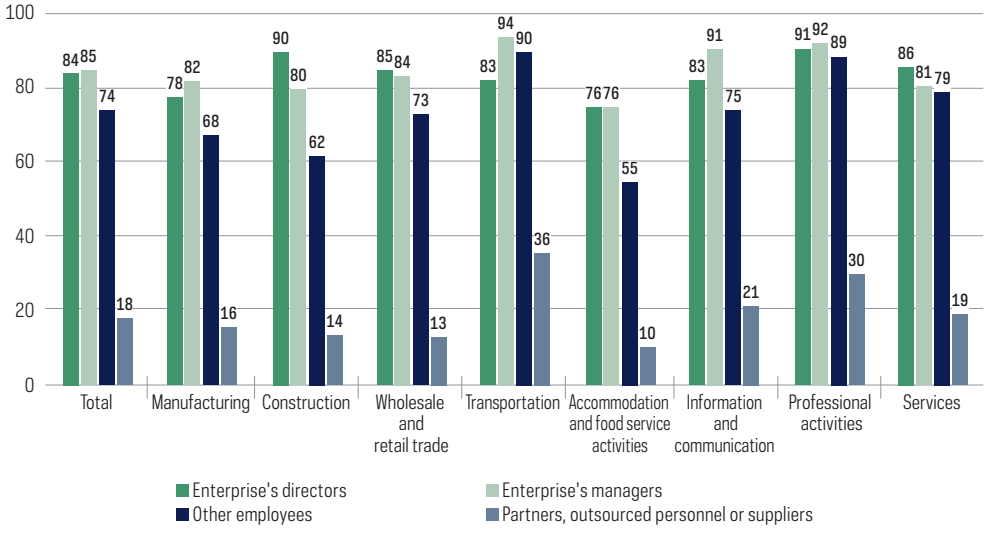
The survey also provided data on the target audience of training and capacity-building actions on privacy and personal data protection that take place in enterprises. Of the enterprises that carried out training actions, directors participated 84% of the time, and managers, 85%. In turn, there was employee participation in 74% of the enterprises that offered training on data protection. To a lesser extent, training was offered to partners and outsourced personnel, and was intended for enterprise employees at all positions.

Therefore, even though few companies offered internal training, there was concern in terms of distributing knowledge throughout the organization, because it is necessary to raise awareness of all members about the necessary precautions when processing personal data, reducing the risks related to data protection and possible violations of the law. The construction sector presented the lowest level of training aimed at employees, compared to training directed at the managers of the enterprises.

CHART 6

ENTERPRISES BY AUDIENCE PARTICIPATING IN TRAINING PROGRAMS ON PERSONAL DATA PROTECTION (2021)

Total number of enterprises that carried out training programs on personal data protection (%)

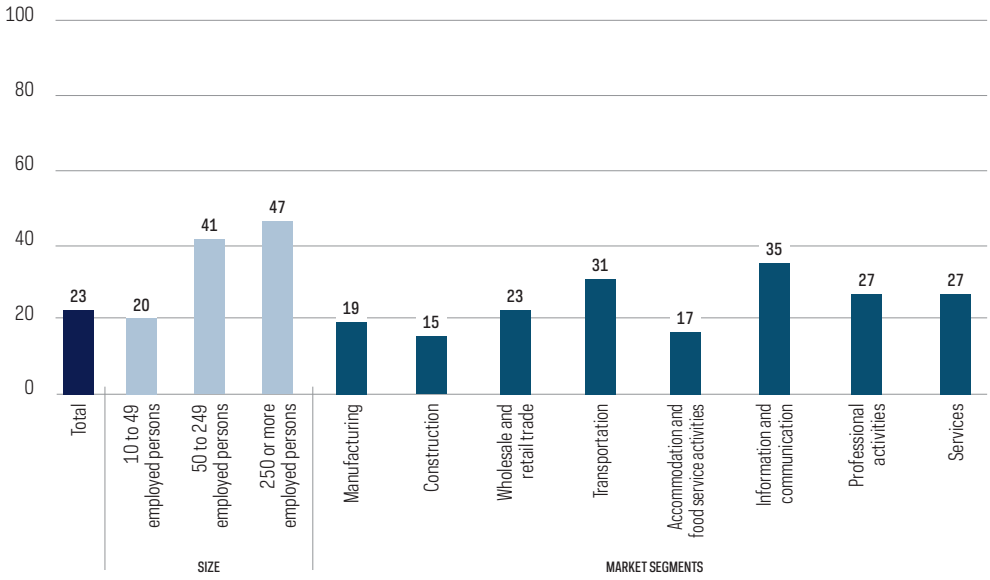


The survey also measured the presence of areas or persons in charge of the topic of personal data protection. In 23% of the enterprises, there were areas or persons responsible for matters related to the LGPD, and most of these enterprises were medium and large. The enterprises that presented higher proportions of areas or persons in charge of the topic of privacy and personal data protection were those whose activities put them in contact with a greater volume of personal data – such as those in the information and communication and transportation and storage segments.

CHART 7

ENTERPRISES BY WHETHER THERE WERE AREAS OR PERSONS RESPONSIBLE FOR PERSONAL DATA PROTECTION (2021)

Total number of enterprises (%)



Among enterprises that had persons or areas responsible for personal data protection, there was a greater presence of people hired for other functions and who were displaced or given additional functions relative to the LGPD (88%), a factor that presented little variation according to size, region, and sector. The selection of enterprise employees to handle data protection and privacy may be related to the need for knowledge about the specific data flow of the organizations and a certain level of appropriation of the processes in order to assess the different levels of risks spread around different sectors of the organizations.

TABLE 1

ENTERPRISES BY EMPLOYEES IN CHARGE OF PERSONAL DATA PROTECTION (2021)

Percentage (%)		Specifically to handle data protection	For other purposes, but started handling data protection issues as well
Total		**22**	**88**
Size	10 to 49 employed persons	24	87
	50 to 249 employed persons	16	94
	250 or more employed persons	12	95

CONTINUES ▸

Percentage (%)		Specifically to handle data protection	For other purposes, but started handling data protection issues as well
Region	North	24	83
	Northeast	14	97
	Southeast	22	88
	Southeast	21	86
	Center-West	38	78
Market segments	Manufacturing	13	96
	Construction	22	80
	Wholesale and retail trade	30	91
	Transportation	28	88
	Accommodation and food service activities	6	80
	Information and communication	16	83
	Professional activities	16	81
	Services	21	95

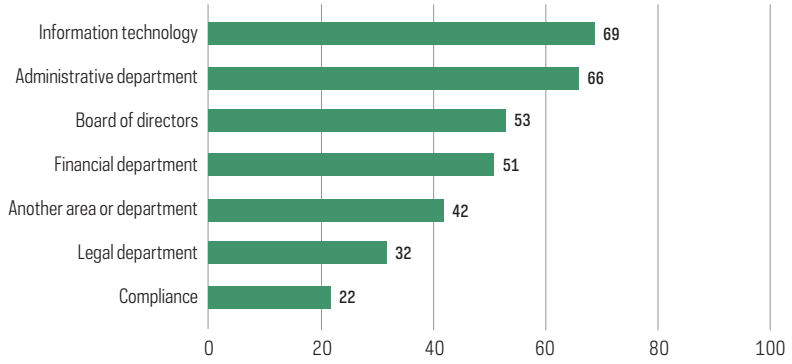
Considering the large presence of employees who had been displaced or who had additional functions relative to the subject of personal data protection, it is worth investigating the origin of these professionals within the organizations. Several documents that discuss best practices for enterprises to comply with the LGPD highlight the need to maintain interdepartmental teams to handle the issue of personal data protection, in addition to the need to distribute information across all departments, as this is a subject that affects organizations as a whole (Sombra & Castellano, 2021; Brazilian Institute of Consumer Protection [Idec], 2021).

Most of the people responsible for compliance with the LGPD came from information technology departments (69%), followed by administrative departments (66%), and boards of directors (53%). The higher presence of people from IT areas was observed in medium and large enterprises, proving to be a trend in organizations with more complex processes.

CHART 8

ENTERPRISES BY AREAS OR DEPARTMENTS OF THE PERSONS RESPONSIBLE FOR PERSONAL DATA PROTECTION (2021)

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

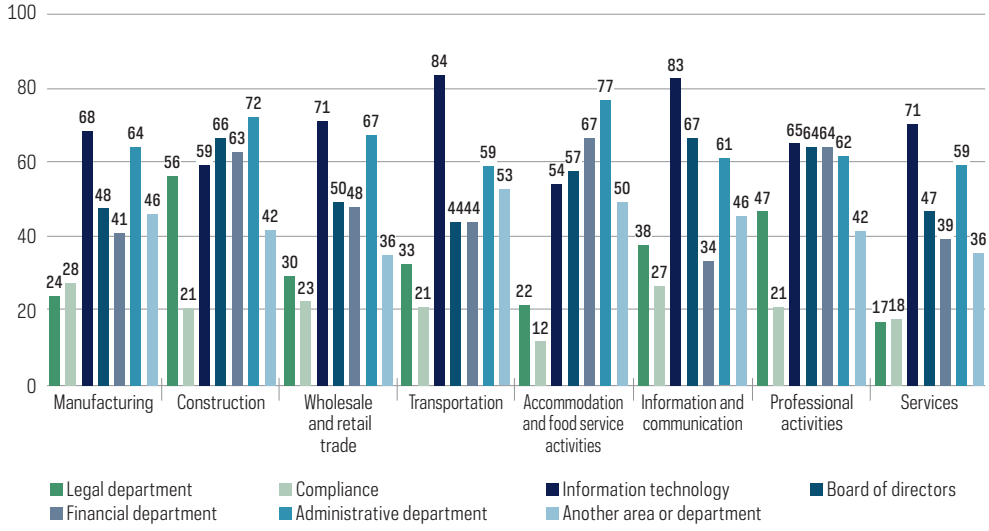


Even though most of those responsible for personal data protection in enterprises were originally from information technology or administrative departments, it is worth noting the important differences among the market segments in terms of the composition of the teams responsible for compliance with the LGPD.

CHART 9

ENTERPRISES BY AREAS OR DEPARTMENTS OF THE PERSONS RESPONSIBLE FOR PERSONAL DATA PROTECTION AND MARKET SEGMENT (2021)

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



Compliance with the LGPD

The survey also investigated critical aspects for adaptation to the LGPD by Brazilian enterprises, which are guided by the framework set forth by the provisions of the law. The paths towards implementation can differ among enterprises, depending on their size and the type of personal data in their custody. However, some best practices can be highlighted, because they reflect the understanding of data flow in the enterprises, seeking to guarantee the integrity of operations that involve the processing of personal data, reducing risks of data leaks and increasing transparency for data subjects (ANPD, 2021; Idec, 2021).

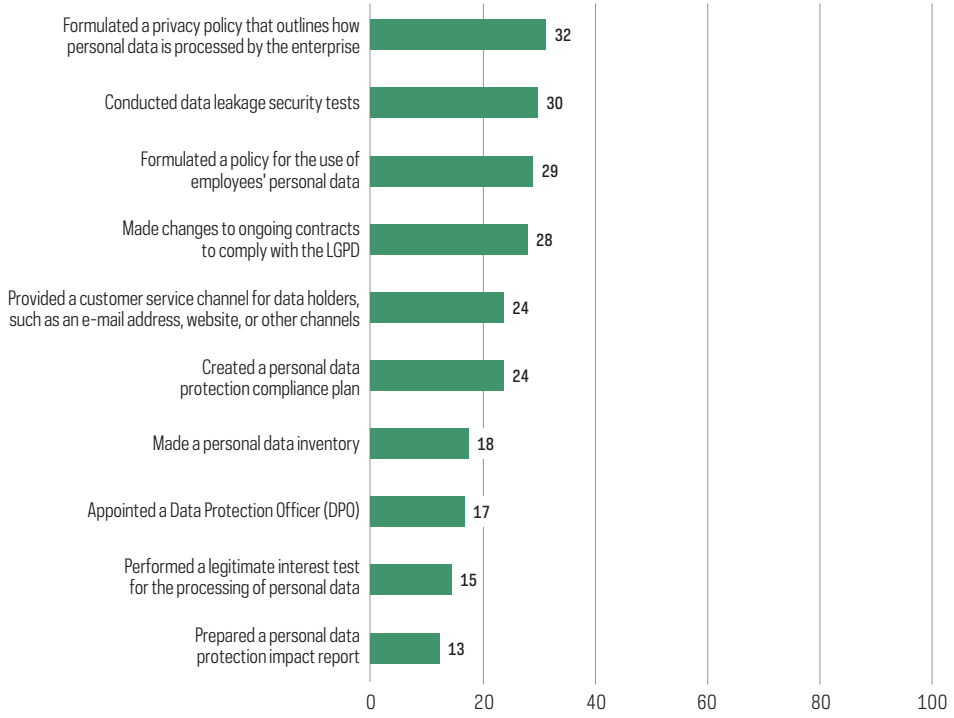
Among the measured aspects, the most cited was the formulation of privacy policies that inform how personal data is processed by the enterprises (32%). This was followed by 30% of enterprises that conducted data leakage security tests, showing their concern about making their personal data processing more explicit, while also trying to ensure their own security, preventing leaks that can cause fiscal damage and tarnish their reputation. It is worth mentioning that the production of personal data protection impact assessments – provided for in Article 5 of the LGPD – was the activity least mentioned by the enterprises[10]. Creating personal data protection compliance plans, which can promote safer and more law-compliant operations, was mentioned by only 24% of the enterprises (Chart 10).

[10] A personal data protection impact assessment is defined in Article 5 as "documentation from the controller that contains the description concerning the proceedings of the personal data processing that could pose risks to civil liberties and fundamental rights, as well as measures, safeguards and mechanisms to mitigate said risk." In Article 38 of the same law, a personal data protection impact assessment is posited as a requirement that can be demanded by the ANPD: "The national authority may determine that the controller must prepare a data protection impact assessment, which shall include personal data or sensitive data, and refer to its data processing operations, pursuant to regulations, subject to commercial and industrial secrecy." It is necessary to emphasize that the LGPD does not mention its obligation in any specific case, only when requested by the ANPD.

CHART 10

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

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



Among some of the most performed activities to adapt to the LGPD, enterprises in the information and communication and the professional activities segments presented the greatest variety of actions. As shown in Table 2, only a few segments presented actions to enable enterprises to improve the internal management of personal data and strengthen digital security.

TABLE 2

ACTIONS TO COMPLY WITH THE LGPD BY SECTOR (2021)

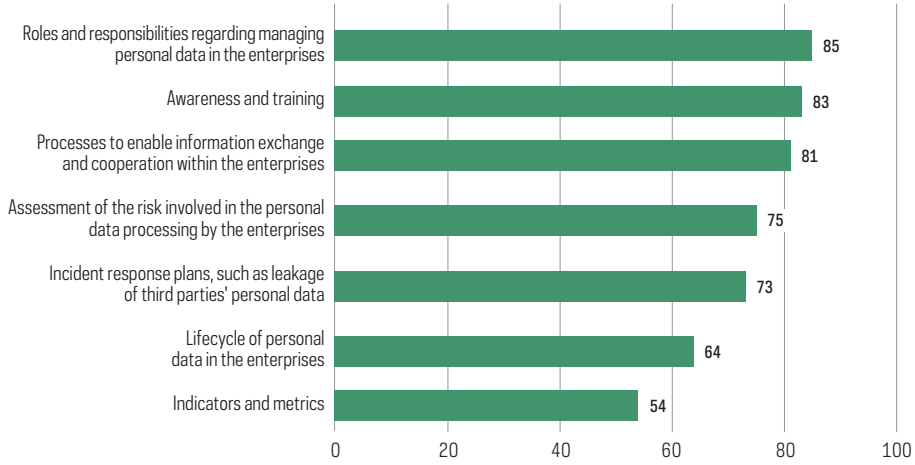
	Manufacturing	Construction	Wholesale and retail trade	Transportation	Accommodation and food service activities	Information and communication	Professional activities	Services
Created a personal data protection compliance plan	26	19	21	33	14	41	32	24
Formulated a policy for the use of employees' personal data	26	21	31	33	13	45	35	22
Made a personal data inventory	20	13	17	21	8	24	22	17
Prepared a personal data protection impact assessment	14	10	9	23	12	25	17	15
Formulated privacy policies that inform how personal data is processed by the enterprises	29	27	30	37	30	41	43	29
Appointed a data protection officer (DPO)	16	14	18	21	7	22	22	11
Made changes to ongoing contracts to comply with the LGPD	30	22	22	38	23	57	38	26
Conducted data leakage security tests	28	20	31	36	22	46	36	24
Provided a customer service channel for data holders, such as an e-mail address, website, or other channels	24	23	17	27	21	45	39	34
Performed a legitimate interest test for the processing of personal data	15	13	15	25	5	25	19	16

Among enterprises with LGPD compliance plans, most of the initiatives determined the roles and responsibilities regarding managing personal data in the enterprises (85%). Next came awareness and training actions and processes to enable information exchange and cooperation within the enterprises (81%) – which may be related to the training strategies discussed above. Therefore, the actions foreseen in LGPD compliance plans establish the roles regarding the requirements of the law, while also setting forth directives on internal training, from the point of view of both providing knowledge and improving communication between departments.

CHART 11

ENTERPRISES BY COVERAGE OF PERSONAL DATA PROTECTION COMPLIANCE PLANS (2021)

Total number of enterprises with LGPD compliance plans (%)



One of the actions for LGPD compliance is the appointment of the organizations' data protection officers, or DPOs, who are responsible for communication with data subjects and with the ANPD, as provided for in Article 41 of the law[11]. In addition, the DPOs are also responsible for observing compliance with the LGPD, playing a central role in the compliance of personal data processing operations, and establishing effective data governance in the organization (CIPL & Cedis-IDP, 2021). Although the law refers to the DPO as a person, there are no restrictions on the creation of interdepartmental data protection teams, or even of using hired third-party agents – the only restriction is that one person cannot act as the DPO of more than one enterprise (ANPD, 2022a). The survey revealed that 17% of enterprises appointed a DPO: 41% of large enterprises, 29% of medium enterprises, and 15% of small

[11] According to the LGPD, the duties of the DPO are: "I – accepting complaints and communications from data subjects, providing explanations and adopting measures; II – receiving communications from the national authority and adopting measures; III – orienting entity's employees and contractors regarding practices to be taken in relation to personal data protection; and IV – carrying out other duties as determined by the controller or set forth in complementary rules."

enterprises[12]. The ICT Enterprises survey also investigated the origin of the DPO. In most cases (77%), they were persons or committees within the enterprises, which was the case in most enterprises in all strata of the survey.

TABLE 3

ENTERPRISES BY ORIGIN OF DPOS, SIZE, REGION AND MARKET SEGMENT (2021)

Total number of enterprises with DPOs (%)

Percentage (%)		Persons or committees of the enterprise	Outsourced professionals	Does not know	Did not answer
Total		**77**	**22**	**1**	**0**
Size	10 to 49 employed persons	75	24	1	0
	50 to 249 employed persons	85	15	0	0
	250 or more employed persons	80	17	3	0
Region	North	57	31	0	12
	Northeast	90	10	0	0
	Southeast	70	28	2	0
	Southeast	89	10	1	0
	Center-West	58	42	0	0
Market segments	Manufacturing	82	10	6	2
	Construction	58	42	0	0
	Wholesale and retail trade	78	22	0	0
	Transportation	63	37	0	0
	Accommodation and food service activities	100	0	0	0
	Information and communication	64	36	0	0
	Professional activities	80	20	0	0
	Services	88	12	0	0

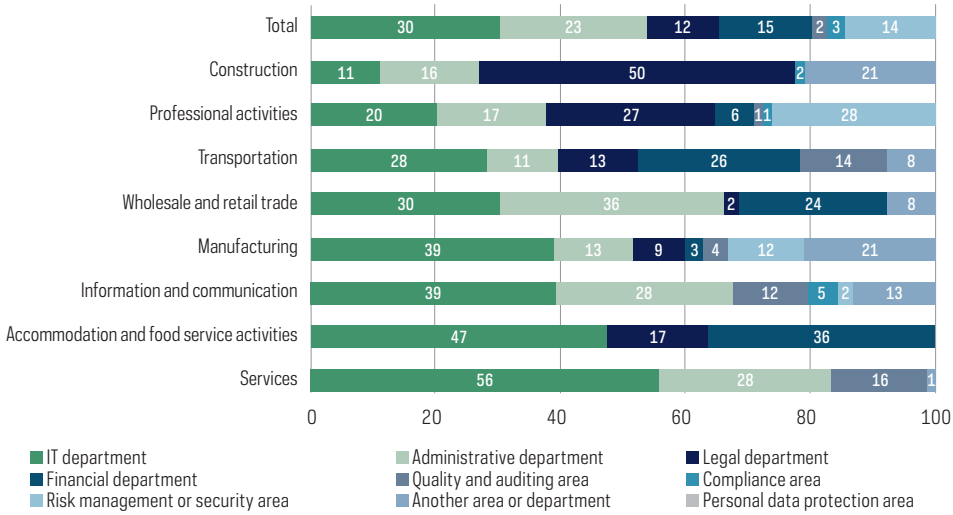
[12] Article 11 of Resolution CD/ANPD No. 2 of January 27, 2022, exempts small enterprises from having to appoint DPO (ANPD, 2022b). However, it is important to note that the ANPD defines an enterprise's size based on their revenue. In the ICT Enterprises survey, size is based on the number of persons employed: A small enterprise is understood as having up to 49 employed persons.

As well as the origin of the persons assigned to deal with the protection of personal data, the DPO are mostly from the IT area of the enterprises (30%), followed by the administrative sector (23%).[13]

CHART 12

ENTERPRISES BY AREAS OR DEPARTMENTS OF THE DPOS AND MARKET SEGMENT (2021)

Total number of enterprises with DPOs at the enterprises (%)



Another essential action for enterprises to comply with the LGPD is making information available on their websites. Although it is not an explicit requirement of the law, providing information on enterprise data protection policies strengthens a culture of transparency about the operations carried out by enterprises with the personal data of subjects. The LGPD mentions resources provided on websites when specifying the processing of personal data in the public sector (Article 23) and, for all organizations, in the requirement to provide name and contact information of DPOs (Article 41, paragraph 1)[14]. Only 15% of enterprises provided name and contact information of DPOs on their websites, and the most commonly offered information was information security policies, disclosed by 30% of the enterprises, followed by corporate privacy policies, which provide information about how personal data is processed by the enterprises (28%). According to the ICT Enterprises 2019 survey

[13] Among federal government organizations, the appointment of DPOs from the information technology sector was vetoed by Normative Instruction SGD/ME No. 117 of November 19, 2020. The purpose is to prevent the DPOs from taking on the function of reporting on data to the external public. However, for other organizations there are no restrictions on the types of the DPOs.

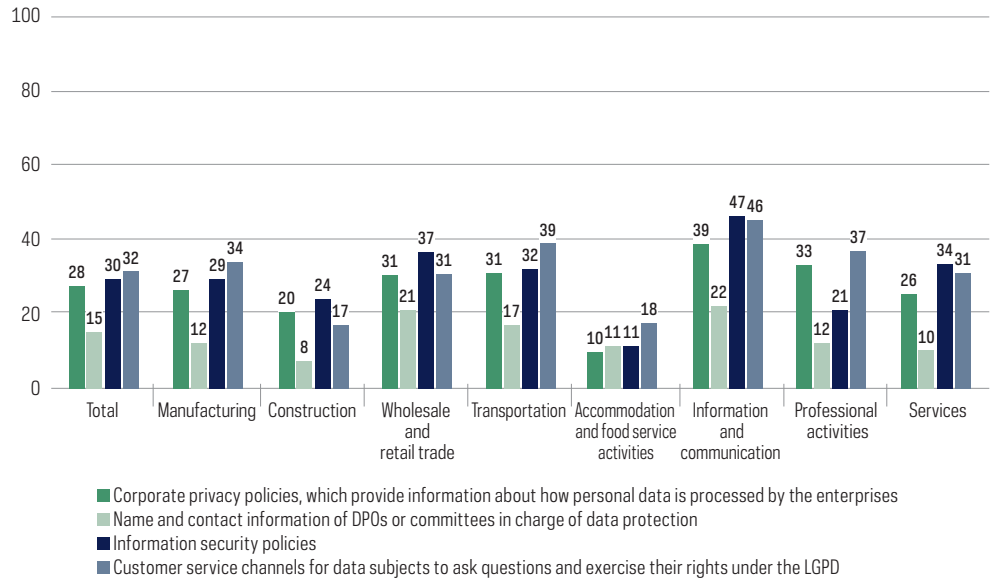
[14] According to the ICT Enterprises 2019 (Brazilian Internet Steering Committee [CGI.br], 2020), 54% of enterprises had websites, with a higher concentration among large and medium enterprises. Small enterprises are restricted to the use of social networks, which do not allow the customization of their resources in order to create a space to disclose names and contact information of DPOs.

(CGI.br, 2020), there was a greater presence of some resources on websites in the information and communication segment than in segments such as construction or accommodation and food service activities.

CHART 13

ENTERPRISES BY RESOURCES AVAILABLE ON THEIR WEBSITES (2021)

Total number of enterprises with websites (%)



Barriers and opportunities

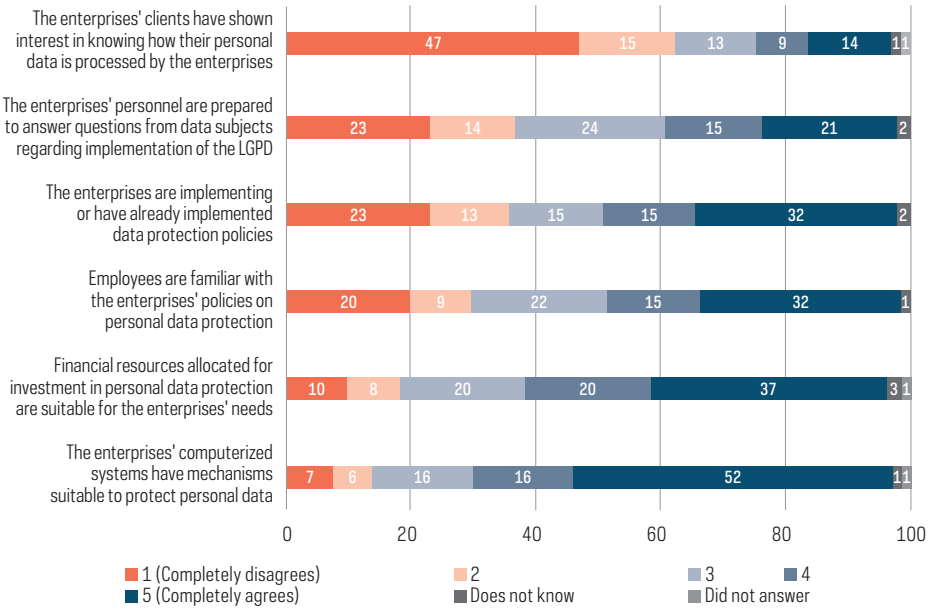
The survey also investigated the perceptions of enterprises of the barriers and opportunities created by the LGPD. The purpose of this section is to discuss the difficulties they faced when seeking to comply with the law, in addition to their view on various actions involving the protection of personal data.

In relation to the public served, 47% of enterprises disagreed with the statement that their clients have shown interest in knowing how their personal data is processed. From the point of view of enterprise readiness, 52% completely agreed that the enterprises' computerized systems had mechanisms suitable to protect personal data. Therefore, the data suggests little understanding by enterprises of their clients' concerns about how their personal data is managed, while enterprises have taken many actions to ensure the correct and safe maintenance of personal data.

CHART 14

ENTERPRISES BY LEVEL PERCEPTION OF BARRIERS (2022)[15]

Total number of enterprises (%)



Regarding the opportunities created by the LGPD, most enterprises agreed that the law presents many possibilities that can favor their operations, both in terms of improving internal processes and in terms of their reputation with clients. As an example, 54% of the enterprises stated that data protection policies for compliance with the LGPD favor the enterprises' physical and digital security. Regarding the opportunities for the enterprises in relation to their clients, 54% stated that data protection policies for compliance with the LGPD favored their trust in the enterprises. Therefore, most enterprises stated that seeking to comply with the law can benefit their operations, because personal data protection demands the improvement of processes to ensure the integrity of client data processing, thus ensuring a positive relationship with their clients.

[15] The question used to create the indicator was: "Considering a scale from 1 to 5, where 5 means "I totally agree" and 1 means "I totally disagree", how much do you agree or disagree that".

CHART 15

ENTERPRISES BY PERCEPTIONS OF OPPORTUNITIES[16] (2021)

Total number of enterprises (%)

Final considerations: Agenda for public policies

The results of the module on privacy and personal data protection, collected for the first time in the ICT Enterprises 2021 survey, point to the still incipient presence of actions for compliance with the LGPD in Brazilian enterprises. Although most enterprises carried out awareness and training activities for their personnel about the scope of the law and assigned responsibilities for the processing of personal data, enterprises still reported a reduced set of actions to effectively adapt to the new scenario. The survey results, therefore, demonstrate substantive challenges for enterprises to develop a culture of personal data protection in their routines.

Provisions set forth in the LGPD, such as the appointment of DPOs and the preparation of personal data protection impact assessments, were followed in less than half of Brazilian enterprises. This result points to significant limits on the financial and qualification capacities of organizations of all sizes and segments of economic activity to achieve a high level of personal data protection maturity.

In view of the widespread presence of personal data in all enterprises, in addition to the many different ways data flows during the enterprises' routine operations, it is also key to make an effort to create detailed maps of data input and output, with the participation of all sectors. Furthermore, the way enterprises handle privacy and personal data protection tends to be increasingly decisive for maintaining a good reputation, leading to clients' trust in providing information that is crucial to the performance of the enterprises in today's economy.

[16] The question used to create the indicator was: "Considering a scale from 1 to 5, where 5 means "Very much" and 1 means "Not at all", how much do you consider that personal data protection policies for compliance with the LGPD support".

Another aspect worth highlighting is the presence of guidelines and regulations that can serve as a framework for enterprises with few resources[17]. In this context, the action of the ANPD is essential to guide enterprises on how to comply with the law.[18]

The results of the survey indicate that there is room to improve awareness of the issue among enterprises of all sizes and market segments. More complex actions that ensure the transparency and integrity of personal data processing operations have an incipient presence among enterprises, and it is important to monitor to what extent the protection of personal data will take on a central role in business strategies. Although the law is recent and there are uncertainties about how to correctly comply with it, enterprises need to make personal data protection a constant in their routines, because ensuring the proper use of data is increasingly central to the reputation of the organizations, promoting good relationships with clients, and avoiding penalties that can bring about irreversible damage.

The inclusion of the privacy and personal data protection module in the ICT Enterprises 2021 survey provided relevant indications on how the enterprises have been implementing the LGPD and whether there is progress in the construction of a data protection culture in the country. It is worth remembering that the LGPD stipulates economic and technological development and innovation among its foundations, in addition to human rights, the free development of personality, dignity, and the exercise of citizenship by natural persons. Data and analyses on how Brazilian enterprises are adapting to the LGPD are essential for the proper enforcement of the law and the development of important conversations about the consolidation of economic activities aligned with fundamental rights, such as privacy and personal data protection.

Therefore, the results of the ICT Enterprises 2021 survey indicate that there is room for training actions among Brazilian enterprises on the importance of including personal data protection as part of the organizations' strategy, regardless of their size and market segment, and that the coming into force of the LGPD has established a new way of operating in the country.

[17] Several of the federal government's actions indicate processes that can be adapted in the private sector: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados

[18] Several guides are available on the institution's website: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes. The open discussions promoted by the ANPD on its YouTube channel are also interesting: https://www.youtube.com/c/anpdgov

References

Brazilian General Data Protection Law – LGPD. Law No. 13.709 of August 14, 2018. (2018). Provides for the processing of personal data, including in digital media, by a natural person or by a legal person governed by public or private law, with the aim of protecting the fundamental rights of freedom and privacy and the free development of the personality of the natural person. http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Brazilian Institute of Consumer Protection. (2021). *Manual prático de adequação à Lei Geral de Proteção de Dados para micro e pequenas empresas.* https://idec.org.br/manual-lgpd-micro-pequenas-empresas

Brazilian Internet Steering Committee. (2020). *Survey on the use of information and communication technologies in Brazilian enterprises: ICT Enterprises 2019.* https://cetic.br/media/docs/publicacoes/2/20200707094721/tic_empresas_2019_livro_eletronico.pdf /

Brazilian Ministry of the Economy. (2021). *Guia de elaboração de inventário de dados pessoais – LGPD.* https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_inventario_dados_pessoais.pdf/view

Brazilian Network Information Center. (2021). *Segurança digital: uma análise de gestão de risco em empresas brasileiras.* https://www.nic.br/publicacao/seguranca-digital-uma-analise-de-gestao-de-risco-em-empresas-brasileiras/

Centre for Information Policy Leadership, & Centro de Direito, Internet e Sociedade do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa. (2021). *The role of the Data Protection Officer ("Encarregado") under the Brazilian General Data Protection Law (LGPD).* https://wpcdn.idp.edu.br/idpsiteportal/2021/10/Artigo-Encarregado-LGPD-Efetiva.ing_.pdf

Greenleaf, G. (2021). Global data privacy laws 2021: Despite COVID delays, 145 laws show GDPR dominance. *Privacy Laws & Business International Report, 169*(1), 3-5.http://doi.org/10.2139/ssrn.3836348

Internet & Jurisdiction Policy Network. (2021). *We need to talk about data: Framing the debate around free flow of data and data sovereignty.* https://www.internetjurisdiction.net/news/aboutdata-report

Mikkelsen, D., Soller, H., Jansson, M., & Whalers, M. (2019). *GDPR compliance since May 2018: A continuing challenge.* McKinsey & Company. https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/gdpr-compliance-after-may-2018-a-continuing-challenge

National Data Protection Authority. (2021). *Guia orientativo – Segurança de informação para agentes de tratamento de pequeno porte.* https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf

National Data Protection Authority. (2022a). *Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado.* https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf

National Data Protection Authority. (2022b). *Resolução CD/ANPD n. 2, de 27 de janeiro de 2022.* https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019

Normative Instruction SGD/ME No. 117, of 19 November 2020. (2020). Provides for the appointment of the person in charge of the processing of personal data within the framework of the bodies and entities of the direct, local and foundational federal public administration. https://www.in.gov.br/en/web/dou/-/instrucao-normativa-sgd/me-n-117-de-19-de-novembro-de-2020-289515596

Provisional Measure No. 1.124, of June 13, 2022. (2022). Amends Law No. 13709, of August 14, 2018, on the Brazilian General Data Protection Law (LGPD), as it transforms the National Data Protection Authority into a special autarchy and positions into commissioning. http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Mpv/mpv1124.htm

Sombra, T., & Castellano, A. (Orgs.). (2021). *Proteção de dados e experiências setoriais: a visão do setor privado na implementação da LGPD.* Jota. https://conteudo.jota.info/setor-privado-lgpd

United Nations Conference on Trade and Development. (2021). *Digital economy report 2021: Cross-border data flows and development: For whom the data flow.* https://unctad.org/webflyer/digital-economy-report-2021

Analysis of Results
Privacy and Personal Data Protection 2021
Public organizations

The expansion of digital transformation initiatives in the public sector – which include the provision of services through digital means and the adoption of new technologies that facilitate data analysis and decision making – is associated with improving the provision of public policies to society (United Nations Department of Economic and Social Affairs [UN DESA], 2020). The digitization of the sector has also intensified the collection, storage, and analysis of citizens' data by government organizations in the exercise of their functions. In this context, it is essential to understand the possible risks entailed by the access to and use of this large volume of data to the protection of privacy and personal data (Bleeker, 2020).

These concerns have become even more evident with the COVID-19 pandemic, when the adoption of digital tools was essential to maintain the provision of public services while social distancing measures were in force. Digital technologies have played a central role in strategies dedicated to informing the population about the new virus, monitoring the progress of the disease, and assisting in decision making in relation to the health crisis (UN DESA, 2020).

The adoption of contact tracing applications[1], which generally allow access to geolocation data and the health conditions of their users, have encouraged the dissemination of a series of recommendations by national and international organizations on the need for government organizations to find a balance between processing citizens' data to combat the pandemic and guaranteeing the right to privacy and protection of personal data (Organisation for Economic Co-operation and Development [OECD], 2020b; Brazilian Internet Steering Committee [CGI.br], 2020; European Data Protection Board [EDPB], 2020). In this sense, the United Nations Development Programme (UNDP) highlighted the importance of governments adopting general standards or regional or international frameworks for the protection of sensitive data, guaranteeing privacy and confidentiality to citizens (UNDP, 2020).

[1] Technology that allows contact tracing to locate individuals infected with COVID-19 and their contacts and measure the spread of the disease (Gomes, 2022).

In Brazil, in 2018, the first general regulation on the subject was enacted. The Brazilian General Data Protection Law (LGPD) established the guidelines for the processing of data in physical and digital media by individuals and organizations, including public authorities. In addition to the general requirements, a separate chapter was inserted into the law with specific provisions for government organizations.

While the new legislation defined principles and limits, it also enabled greater security when using personal data to improve services, by including the execution of public policies as one of the uses for data processing. With the enactment of the LGPD, the expansion of actions related to privacy and data protection became one of the main challenges for the public administration. This aspect is even more relevant in the context of the implementation of government programs, since a balance must be achieved between processing personal data to improve the operation of the public sector and minimizing potential risks to citizens, such as security incidents involving personal data, discriminatory or stigmatizing actions resulting from the implementation of automated systems, and undue surveillance.

In some contexts, the protection of personal data also receives special legal provisions because of the risks to data subjects should their information be misused. Of these, it is worth highlighting the collection and processing of personal data of children and sensitive data concerning the health of citizens. This generates the need for greater caution in terms of data processing, especially in public policies that commonly use this information, such as those related to health and education. It is also necessary that the professionals who work in the collection and analysis of this type of data are aware of and comply with security and privacy requirements, as recommended by the LGPD.

Considering this scenario, the objective of this analysis of results is to provide an overview of data protection in the context of public policies in Brazil, including the adoption of practices by government organizations, healthcare facilities, and schools. Initially, it analyzes the adoption by federal and state government organizations and local governments of measures to protect citizens' data. Next, it focuses on the health sector, specifically on the compliance of public healthcare facilities with LGPD requirements. Finally, it presents the results on privacy and personal data protection in the education sector, focusing on public Basic Education institutions. The analyses are based on the results of the ICT Electronic Government 2021, ICT in Health 2021, and ICT in Education 2020 surveys, carried out 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).

Federal and state government organizations and local governments

With the growing concern about privacy and personal data protection and the coming into force of the LGPD in the second half of 2020, the ICT Electronic Government 2021 survey (CGI.br, 2022) included a new module to investigate how Brazilian government organizations are structuring themselves to adapt to the new legislation. Questions were included for both federal and state government organizations and local governments to measure the presence of actions aimed at implementing the guidelines and requirements in the law.

Although the LGPD does not detail the need to create specific structures or departments, public and private organizations have been urged to carry out various actions to adapt to the law. An example is the encouragement of the creation of personal data governance programs to support activities related to data protection (Crespo, 2021). To meet this provision, the Ministry of Economy (2020) made a recommendation for federal organizations to establish a specific organizational structure for personal data protection governance and management.

According to the results of the ICT Electronic Government 2021 survey, more federal organizations (89%) had persons or areas responsible for the implementation of the LGPD than state organizations (55%). Among the branches, the government organizations of the judiciary (94%) and the Public Prosecutor's Office (73%) stood out. On the other hand, only a little more than half of the organizations of the executive (56%), and 68% of the legislative branch, mentioned the presence of persons or areas responsible for the implementation of this legislation. The federal public administration[2] and the judiciary (through the National Council of Justice[3]), already have a series of regulations and recommendations regarding the implementation of the LGPD, which may explain the greater institutionalization of the topic in these organizations.

Among Brazilian local governments, only 28% reported having persons or areas responsible for the implementation of the LGPD, which was more frequent among capital cities (66%) and in municipalities with more than 500,000 inhabitants (62%), as shown in Chart 1.

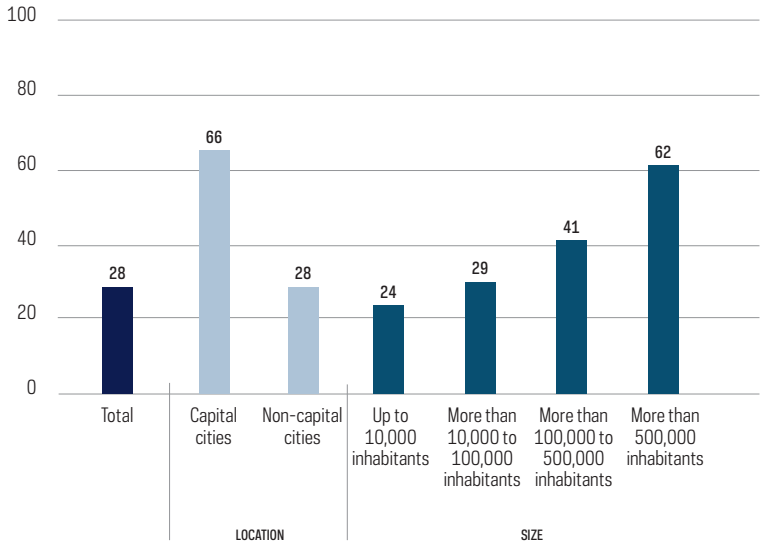
[2] More information available at https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados

[3] More information available at https://atos.cnj.jus.br/atos/detalhar/3668 and https://atos.cnj.jus.br/atos/detalhar/3432

CHART 1

LOCAL GOVERNMENTS BY WHETHER THERE WERE 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)

Total number of local governments (%)

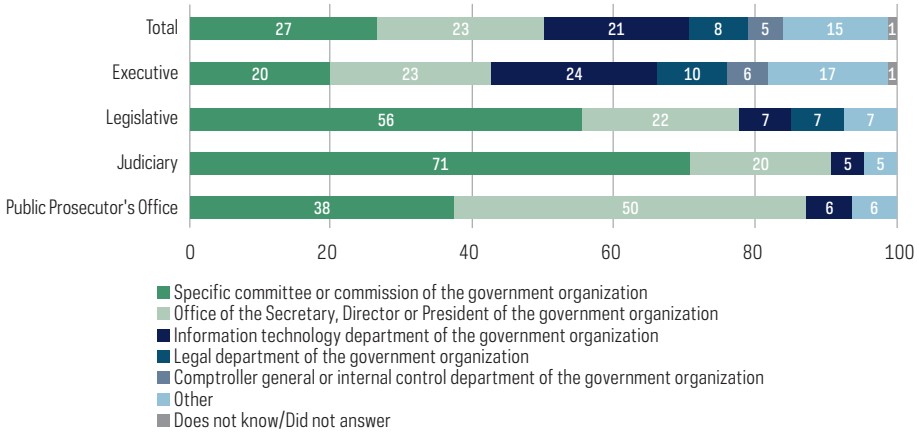


The ICT Electronic Government 2021 survey also identified in which sectors of government organizations this topic was being addressed. A variety of sectors were responsible for implementing the law among the branches. While in the executive branch, no one sector predominated (Chart 2), in the judiciary and legislative branches, the implementation of the LGPD was usually assigned to specific committees or commissions. In organizations of the executive branch, the implementation of the LGPD was divided mainly between information technology (IT) departments (24%), the offices of secretaries, directors, or presidents (23%), and specific committees or commissions (20%) of the government organizations. In the Public Prosecutor's Office, the most mentioned sectors – by half of the government organizations in this branch – were the offices of secretaries, directors, or presidents of the government organizations (50%), followed by specific committees or commissions (38%).

CHART 2

FEDERAL AND STATE GOVERNMENT ORGANIZATIONS BY SECTORS OF THE AREAS OR PERSONS RESPONSIBLE FOR THE IMPLEMENTATION OF THE LGPD (2021)

Total number of federal and state government organizations with areas or persons responsible for the LGPD (%)



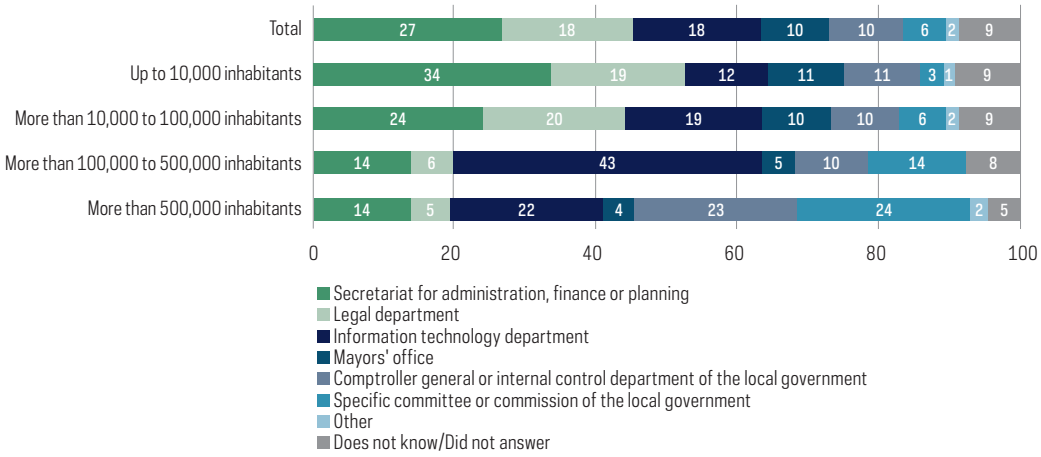
In the case of local governments, multiple sectors were responsible for ensuring compliance with the LGPD. Among the municipalities with up to 100,000 inhabitants, the most common areas included secretariats for administration, finance or planning; legal departments; and IT departments (Chart 3). In municipalities with a population of more than 100,000 to 500,000 inhabitants, almost half of the local governments said that IT departments were responsible for implementing the LGPD. Among local governments of municipalities with a population of more than half a million inhabitants, no pattern was observed among the responsible sectors. Approximately one-quarter of the local governments mentioned specific committees or commissions; 23% pointed to comptrollers general or internal control departments; and 22% indicated IT departments.

It is worth noting that the structures of local governments also differ in terms of the presence of certain departments or sectors and their organizational capacities, which could explain the higher incidence of certain areas as being responsible for LGPD compliance. It is also important to note that just under half of Brazilian local governments had IT areas or departments, in contrast with capital cities and municipalities with more than 100,000 inhabitants, in which almost all local governments had these sectors as part of their organizational structure (CGI.br, 2022).

CHART 3

LOCAL GOVERNMENTS BY SECTORS OF THE AREAS OR PERSONS RESPONSIBLE FOR THE IMPLEMENTATION OF THE LGPD (2021)

Total number of local governments with areas or persons responsible for the LGPD (%)



The ICT Electronic Government 2021 survey also investigated whether the government organizations appointed data protection officers (DPOs)[4]. Appointing a DPO took place more often among federal (81%) than in state government organizations (33%). Among the branches, it was most mentioned by organizations of the judiciary (81%) and the Public Prosecutor's Office (73%). Less than half of organizations of the legislative (40%) and executive branches (34%) had appointed a DPO at the time of the survey.

Among local governments, this was the least mentioned action measured by the survey (Chart 4), with only 14% having appointed these professionals. Even among the local governments of municipalities with the largest populations, less than half of those with more than 500,000 inhabitants had appointed a DPO. The proportions were even lower in municipalities with a population of more than 100,000 to 500,000 inhabitants: only two out of ten local governments had DPOs.

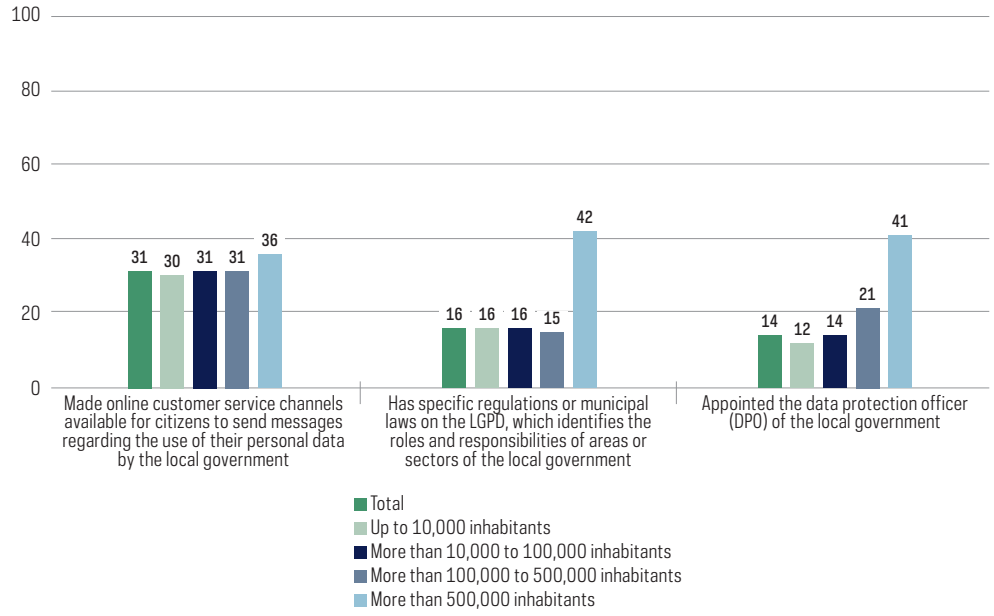
Therefore, even though Article 23, item III of the LGPD requires the public authority to appoint a DPO when processing personal data, this appointment is still very incipient among the government organizations investigated by the ICT Electronic Government 2021 survey. It should also be noted that in the future, the Brazilian National Data Protection Authority (ANPD) may eventually present guidelines and specifications for appointing a DPO according to the different characteristics of government organizations, such as the decision of exempting small data processing agents from this obligation (ANPD, 2022c).

[4] Persons named to act as channels of communication between controllers, the subjects of data, and the Brazilian National Data Protection Authority (ANPD) (Article 5, item VIII). Responsible for ensuring the organizations' compliance with the LGPD (ANPD, 2022a).

CHART 4

LOCAL GOVERNMENTS BY ACTIONS RELATED TO THE LGPD, TOTAL AND SIZE (2021)

Total number of local governments (%)



One of the principles of the LGPD is transparency regarding the processing of personal data, guaranteeing data subjects access to clear, precise, and easily accessible information about this data processing[5] and assigning to the public authority the responsibility for making this information available in easily accessible forms, preferably online (ANPD, 2022b). Among other actions, this includes providing channels for individuals to contact government organizations to obtain information and clarification on the processing of their personal data. Law No. 14129/2021 reinforces this point, indicating that digital government platforms must allow citizens to make requests to the government organizations that control their data.

However, there is still little availability of online customer service channels for data subjects to send messages regarding the processing of their personal data and exercise the rights provided for in the LGPD. While 65% of federal organizations had these types of online channels, they were present in only one-third of state organizations. Among the branches, once again emphasis goes to the organizations of the judiciary, in which three out of four had online customer services for this purpose.

Less than one-third of the local governments made online customer service channels available for citizens to send messages regarding the use of their personal data. Even among local governments of municipalities with more than 500,000 inhabitants, only

[5] Article 6, item VI.

36% provided these types of services, highlighting the need for digital channels that are prepared to receive these types of demands.

On the other hand, data from ICT Electronic Government 2021 survey show that online channels, including those for receiving requests from society, were already present in a large part of government organizations in the country. More than 80% of federal and state government organizations and 71% of local governments had online ombudsmen in 2021 (CGI.br, 2022). It was also common for government organizations to make contact forms available for citizens on their websites, such as information about e-mail addresses, channels for making online reports, and services to request access to information. Thus, experiences of online customer service channels in other areas could be used to help expand contact channels for data subjects on issues related to the LGPD.

Finally, one of the dimensions associated with the implementation of a culture of respect for privacy and personal data protection in organizations is raising awareness of employees about actions related to the topic and existing regulations. Article 50 of the LGPD establishes that privacy governance programs may include educational actions as one of their activities. Emphasizing the importance of this topic, the *Guia de Elaboração de Programa de Governança em Privacidade* (Guide to Developing a Privacy Governance Program), created by the federal government, points to the need for educational programs aimed at employees to inform them about privacy protection policies and practices (Ministry of Economy, 2021).

The ICT Electronic Government 2021 survey investigated whether government organizations offered any training programs or courses for information technology personnel on the LGPD. Among federal and state organizations that had IT departments (87%), these types of actions were more frequent in organizations of the judiciary (91%) and the Public Prosecutor's Office (82%) – those that already had persons or areas responsible for implementing the LGPD to a greater extent. About half of the government organizations of the executive and legislative branches conducted this type of training among IT department employees.

At the local level, the local governments of capital cities (63%) offered training programs or courses on the LGPD for IT personnel more often than those located in non-capital cities (24%). Among local governments of municipalities with a population greater than 500,000 inhabitants, three out of four offered some training on the law to IT departments.

The indicators collected from government organizations showed disparities in the institutionalization of the LGPD, especially between state government organizations and local governments, and in the executive and legislative branches, when compared to those in other branches. Although the LGPD has only been in force two years since its enactment, and its provisions only took effect starting in August 2021, government organizations in the country still seem to be in the early stages of complying with the legislation.

In addition to dealing with the impacts of the COVID-19 pandemic, which has directed the efforts of government organizations since 2020, it should be noted that adaptation to the law involves actions in various aspects and sectors of organizations,

including organizational, technological and cultural changes in favor of actions focused on data protection (Crespo, 2021). In this regard, increasing understanding of the different structures and capacities of government organizations is essential to understanding the challenges related to the implementation of the LGPD. This is especially relevant for organizations responsible for monitoring compliance with the law, such as the ANPD, in order for them to target their actions toward the most challenging dimensions, for public authorities to guarantee the privacy and protection of citizens' personal data.

Public healthcare facilities

In recent years, health care and management have undergone a broad transformation. This process can be observed in the advancement of digital health, which includes the expansion of infrastructure for information and communication technologies (ICT) in healthcare facilities, the development of digital applications by the health public and private sectors, and their appropriation by professionals in the area.

This transformation has led to a rapid growth in the variety and volume of patient information available electronically. Furthermore, this information is increasingly being collected in electronic health records and telehealth activities, and is exchanged between healthcare facilities and institutions. Therefore, it is fundamental to standardize and regulate these activities to ensure the safe processing of digitally generated data.

In this direction, the Pan American Health Organization (PAHO) established eight guiding principles for the digital transformation in the sector, and one is dedicated to establishing mechanisms of trust and information security for the public health digital environment. One of the suggested actions is the adoption of regulatory instruments about health data processing and access. This includes safeguarding the privacy, confidentiality, and security of information; defining access profiles based on the actions users must perform; and training all actors involved in the flow of health information on security guidelines and associated risks. In addition, it refers to the adoption of monitoring mechanisms that allow the detection of security incidents in health information systems; informed consent instruments for access, registration, and protection of confidential information, among others (PAHO, 2021).

The internationally recommended guidelines are convergent with the provisions of the LGPD in Brazil. In the case of the healthcare sector, the law requires deep adaptation of facilities in this area, ranging from pharmaceutical companies and clinical research centers to public and private research bodies that control sensitive personal data concerning health (Dallari & Monaco, 2021).

For the purposes of regulating data processing activities, the law makes a distinction between personal data and sensitive personal data. Personal data consists of "information regarding an identified or identifiable natural person" (Article 5, item I), while sensitive data is defined as "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 "(Article 5, item II) (Mulholland, 2018).

The data concerning patients' health conditions is protected as sensitive data, including medical history, diseases, treatments performed, and use of medications, among others. This data is classified in this way because it presents a greater potential risk to its subjects in the event of abusive or unlawful processing, because it refers to characteristics of the subjects that have a greater probability of leading to prejudice, discrimination, or other forms of abuse. This data may reveal situations of vulnerability, and its improper use may cause damage to the fundamental rights of people, especially those related to privacy, equality, intimacy, and dignity of humans (Botelho & Camargo, 2021).

However, personal data can become sensitive data due to existing processing tools, allowing the correlation of data with a purpose and identifying its subject (Bioni, 2018). In this direction, it is possible to extend this interpretation to data that initially is not classified as sensitive, but that later become so depending on their processing context, as foreseen in Article 11, paragraph 1 of the LGPD. This interpretative extension requires contextual analysis of the processing of personal data, and factors such as illegality, discrimination, vulnerability of the subjects and potential damage must be observed (Costa, 2022).

Consequently, the LGPD has determined that more cautious protection is required for the processing of sensitive personal data that may cause harm to the subjects (patients). The use of this data requires consent of the subjects, except for cases involving the protection of their life or of third parties or the protection of health, the execution of public policies provided for in laws or regulations, and in studies carried out by research organizations, among others. Whenever possible, data processing must ensure anonymity.

For effective protection of personal data, the LGPD defines some concepts and stipulates some measures that must be adopted by the institutions holding the information. For the health sector, data subjects are patients, controllers are healthcare facilities; and processors are those who process the data on behalf of controllers, such as organizations hired to carry out third-party services. The employees of healthcare facilities are not defined as processors, because they process the data by virtue of subordinate work and cannot be held responsible for the decisions of controllers. Data protection officers are persons appointed by healthcare facilities to act as a communication channel between the facilities, subjects-patients, and the ANPD, the organization that oversees compliance with this law (Hawryliszyn et al., 2021). Because of this bias toward public interest, the LGPD prohibits the communication or shared use between controllers of sensitive personal data concerning health for the purpose of economic advantage, apart from cases involving the provision of health services, and pharmaceutical and health care (Botelho & Camargo, 2021).

In this context, before the enactment of the law, the ICT in Health survey had already investigated actions aimed at data protection carried out by healthcare facilities, such as the implementation of information security policies and training of employees on the subject, in addition to the adoption of information security tools. According to the survey results, in 2021, only 21% of public and 38% of private healthcare facilities had an information security policy (Chart 5). There has been little variation among public healthcare facilities throughout the survey's historical series: In 2015, the percentage was 19%, showing that the validity of the law had not

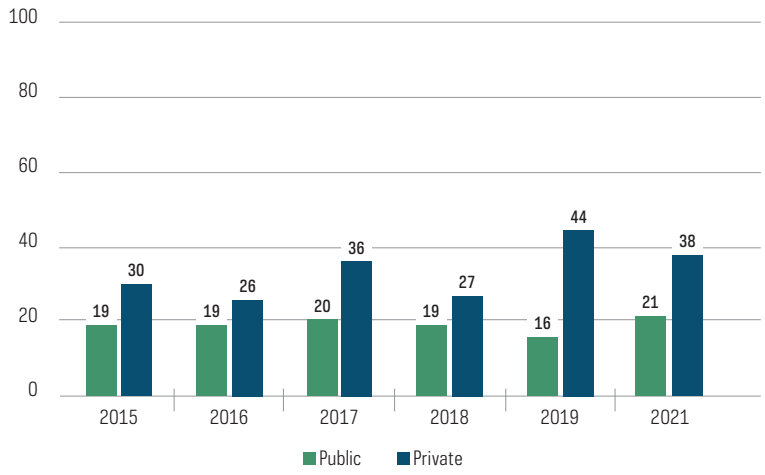
yet significantly impacted the presence of information security policies in public healthcare systems.

The survey also investigated the information security training of employees of healthcare facilities. In 2021, 69% of facilities that had information security policies provided some type of training on the topic, with higher percentages among private (72%) than public facilities (62%).

CHART 5

HEALTHCARE FACILITIES WITH AN INFORMATION SECURITY POLICY (2021)

Total number of healthcare facilities that used the Internet in the last 12 months (%)



Therefore, the results show a low percentage of healthcare facilities that had institutionalized security and privacy policies for sensitive patient information. In the facilities that had this policy, most managers reported that their personnel were trained on the subject. Comprehensive information security policies should consider, not only security tools and data controllers, but also the training of personnel to improve the use of these tools and applications in health.

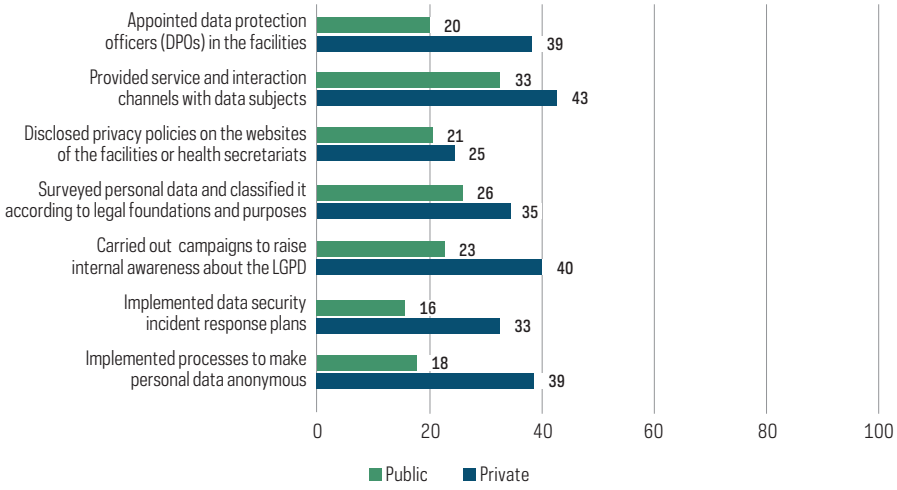
Given the relevance of the LGPD for the sector, in its 2021 edition, the ICT in Health survey included a new indicator to investigate the compliance of healthcare facilities with the terms established by law. With interviews conducted in the first half of 2021, the results allow to monitor the measures implemented by facilities when the law came into force.

Thus, the ICT in Health survey began to measure the appointment of DPOs in healthcare facilities, whose activities include accepting complaints and communications from data subjects, providing explanations and adopting measures; receiving communications from the national authority and adopting measures; orienting entity's employees and contractors regarding practices to be taken in relation to personal data protection (Article 41). In relation to this requirement set forth in the law, only 20% of public and 39% of private healthcare facilities had adapted to this measure (Chart 6).

CHART 6

HEALTHCARE FACILITIES BY MEASURES ADOPTED REGARDING THE LGPD (2021)

Total number of healthcare facilities that used the Internet in the last 12 months (%)



The LGPD also requires that personal data processing be done for legitimate, specific, and explicit purposes informed to the data subject, in accordance with Article 6, item I. In the case of public facilities, only 26% surveyed personal data and classified it according to legal foundations and purposes. In the private sector, this survey was carried out by 35% of facilities.

Another point that, in addition to complying with the law, also impacts the transparency of use of subjects' data is the need to provide service and interaction channels for data subjects to ensure greater transparency of operations (Article 6, items IV and VI). This measure presented the highest percentage of both public (33%) and private (43%) healthcare facilities that reported having made channels available for this purpose.

The law also recommends the preparation of plans with rules for good practices and governance relative to privacy that considers, in relation to data processing, the nature, scope, purpose, and probability and seriousness of the risks and benefits that will result from data processing, in accordance with Article 50. These plans should include internal processes and policies that ensure compliance with standards and good practices related to the protection of personal data, establishing transparent relationships, and guaranteeing mechanisms for data subjects to participate, with plans for incident responses and solutions, among other resources necessary to ensure and guarantee the protection of these data. Furthermore, the plans must be published and updated periodically.

As for these recommendations, a large proportion of public healthcare facilities were still not compliant. Only 21% disclosed their privacy policies on the websites of the facilities or health secretariats. In this regard, the results for private facilities (25%) were very close to those for public facilities. In relation to other measures

investigated, a higher percentage of private healthcare facilities had adapted to the provisions of the law in comparison with public facilities. Only 18% of the public facilities had implemented processes to make personal data anonymous, and 16% had implemented data security incident response plans, while private facilities presented rates of 39% and 33%, respectively.

For the adopted processes and internal policies to ensure comprehensive compliance with the standards and good practices related to the protection of personal data, it is necessary for all the actors involved at all levels of care and management to be familiar with them and aware of their importance. Despite the importance of carrying out campaigns to raise internal awareness about the LGPD, these types of measures were carried out by 23% of public and 40% of private facilities. It is essential that these measures be expanded so that all healthcare facility employees and professionals are engaged and recognize the importance of compliance with the LGPD, since from the moment patients enter reception until they are discharged, sensitive data are being processed, making the health sector one of the most directly and widely impacted by the new legislation.

The results indicate that healthcare facilities face major challenges in adapting to the requirements of the law. The onset of the COVID-19 pandemic demanded emergency measures from facilities in other areas of care and management, which may have compromised the progress on taking measures in relation to the LGPD. However, it is paramount that healthcare facilities comply with the law and ensure the security of information and the right to privacy of the subjects.

Public Basic Education schools

At the start of 2021, the United Nations (UN) held the global launch of *General comment No. 25 on children's rights in relation to the digital environment* (UN, 2021), a document that extends the scope of application of the Convention on the Rights of the Child to digital spaces. Privacy is understood in the document as one of the aspects relevant to the digital rights of children, which must be preserved using appropriate means in favor of their best interests.

Since 2000, the discussion on privacy, security, and data protection of children, especially in digital environments, has been present in the Children's Online Privacy Protection Act (COPPA) (U.S. Congress, 1998), legislation enacted by the United States with the main objective of preventing the exposure of this public to online risks, especially pornography. The General Data Protection Regulation (GDPR) (European Union, 2018), implemented by the European Union in 2018, also pays special attention to the topic of data protection for children. Since 2018, the countries of the European bloc have striven to develop specific guidelines, especially regarding the provision of online services for this audience, such as applications, games, websites, and social networks. In Brazil, Section III, Chapter II of the LGPD is especially aimed at the processing of children's data, assigning parents and legal guardians the task of controlling data processing operations through specific consent.

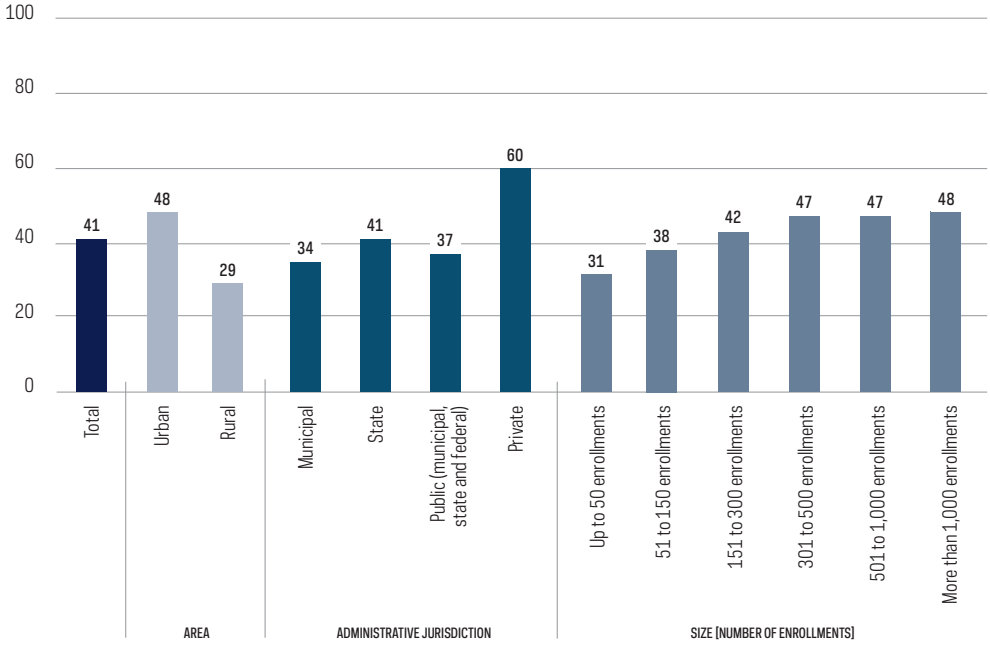
Although discussions about the privacy of children have become more important, especially in the last two decades, the practical application of these principles is still quite complex. One of the challenges lies in the diversity in how the personal data of children is collected, because it involves, not only information consciously shared by them or their caregivers (parents, legal guardians, educational institutions, and teachers, among others), but also information derived from their online practices. This challenge is made clear when analyzing the educational context, especially the context of public Basic Education schools, whose responsibility for the collection and protection of student data must be shared with public administration organizations, such as secretariats and directorates of education.

According to data from the ICT in Education 2020 survey (CGI.br, 2021a), 41% of Basic Education schools in Brazil had documents that defined the information security and data protection policies of the institutions, a percentage that was 60% among private schools and 37% among public schools (municipal, state, and federal) (Chart 7). However, the ecosystem of technology use in the educational field has become increasingly broad and diverse, making it difficult for educational institutions to predict all types and forms of personal data processed, directly or indirectly, based on the activities carried out by school communities.

CHART 7

SCHOOLS WITH DOCUMENTS THAT DEFINE THE INFORMATION SECURITY AND DATA PROTECTION POLICIES OF THE INSTITUTIONS (2020)

Total number of schools (%)



Personal data of children can be categorized into three types (van der Hof, 2016; Livingstone et al., 2019; OECD, 2020a):

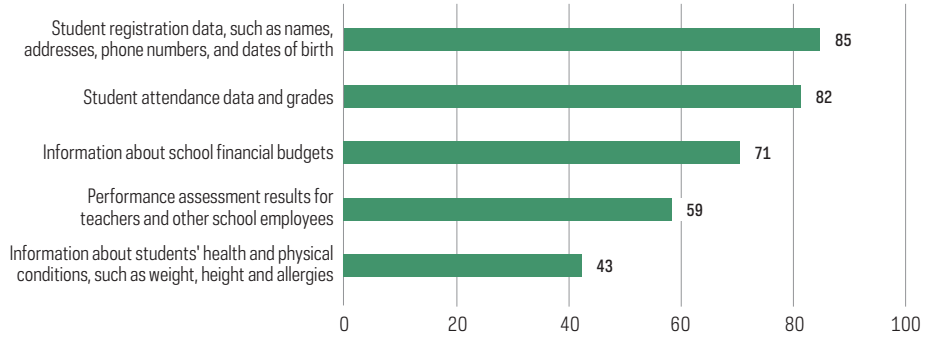
- **Data given**, i.e., data knowingly contributed by children, their parents, or educational institutions.
- **Data traces**, a result of the data left by children online, such as cookies, fingerprinting, location data, and the use of search engines and websites.
- **Inferred data**, which is the information derived from analyzing data given and data traces left during the use of applications.

Regarding data given, 82% of public schools with Primary and Secondary Education classes recorded and consulted student attendance data and grades in electronic format, and 85% recorded and consulted student registration data, such as names, addresses, phone numbers, and dates of birth. In addition to the collection and storage of this data, 43% of public schools recorded or consulted information about students' health and physical conditions, such as weight, height and allergies, in electronic formats (Chart 8).

CHART 8

PUBLIC SCHOOLS THAT RECORDED AND CONSULTED STUDENT AND SCHOOL DATA IN ELECTRONIC FORMAT (2020)

Total number of schools (%)



In addition to the data stored in the institutions' management systems, schools also use other systems that can collect sensitive information from students. According to the 2020 edition of the ICT in Education survey, a small percentage of public schools used fingerprint or palmprint identification systems for students (2%); however, the use of biometric data has intensified among education systems[6]. Furthermore, 30% of the public schools had internal video camera systems, a percentage that reached 59% among state schools and 71% among public schools with more than 1,000 students enrolled.

[6] Public schools in a municipality in Bahia use facial recognition to control student attendance (*Escolas públicas de município baiano usam reconhecimento facial para controlar frequência dos alunos*). (February 9, 2022). https://g1.globo.com/jornal-nacional/noticia/2022/02/09/escolas-publicas-de-municipio-baiano-usam-reconhecimento-facial-para-controlar-frequencia-dos-alunos.ghtml

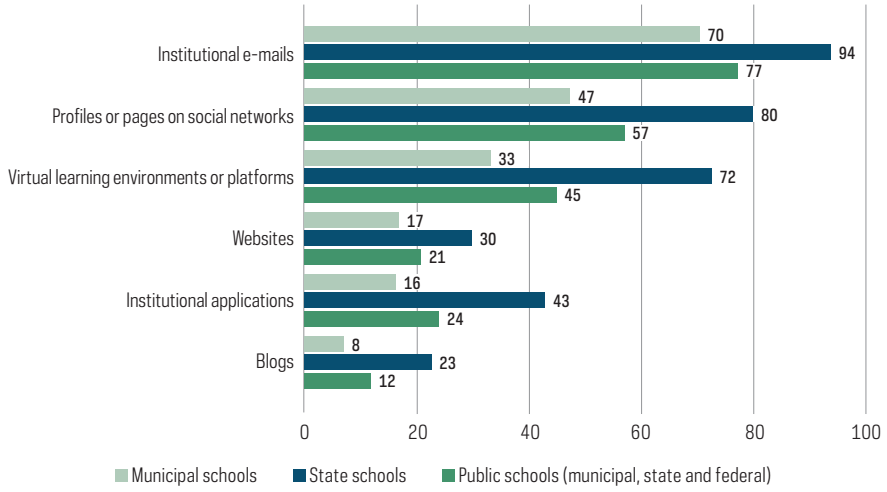
One-quarter of public schools had institutional apps for mobile phones or tablets, and of these, 6% allowed for the monitoring of students via access to school video cameras. In 12% of public schools, these applications also allowed for tracking records of students' daily activities, such as eating, behavior, mood, or participation.

Schools also collect and store a large amount of tracking data, which can also be a source of information for inferred data. Overall, the largest flow of information about students occurs on virtual learning environments and platforms and on social network applications and platforms. According to the ICT in Education survey, in 2020, 45% of public Basic Education schools used virtual learning environments or platforms, a percentage that varied according to the schools' level of connectivity, with higher levels present among urban schools (61%), those in capital cities (71%), those with more than 1,000 enrollments (79%), and among state schools (72%), where there was a greater presence and use of systems, platforms and social networks (Chart 9).

CHART 9

PUBLIC SCHOOLS BY PRESENCE AND USE OF DIGITAL SYSTEMS, PLATFORMS AND SOCIAL NETWORKS AND ADMINISTRATIVE JURISDICTION (2020)

Total number of public schools (%)



The health measures adopted to face the COVID-19 pandemic, such as social distancing and the consequent school closings, with the implementation of remote educational activities, further boosted the use of platforms, environments, applications, and digital networks in Basic Education, with increasing participation of the private sector in the provision of these resources. According to the ICT in Education 2020 survey, conducting remote classes through videoconferencing platforms, for example, was cited by 59% of public school managers as a measure adopted for giving continuity to pedagogical activities during the pandemic, and the use of social networks and instant messaging applications for this purpose reached 90%.

In most cases, virtual learning environments or platforms were used by public school teachers to administer tests and exercises to students (42%), for students to send completed activities to their teachers (41%), and to allow students to ask their teachers questions via videoconferencing (38%). However, the availability of tools based on Artificial Intelligence techniques may offer other options for using student data collected from these resources, such as the possibility of students testing their own performance and creating individualized study plans, which was less mentioned by schools (29%), or providing teachers and school managers with access to students' performance reports (39%).

Learning analytics is another area that has been improved with the use of virtual learning environments and platforms. For 41% of public school managers, the educational platforms used allowed educators to analyze how students learn, 39% said they could assess the students' learning progress, and 29% reported that it was possible to analyze students' emotional characteristics, such as anxiety, sadness or enthusiasm.

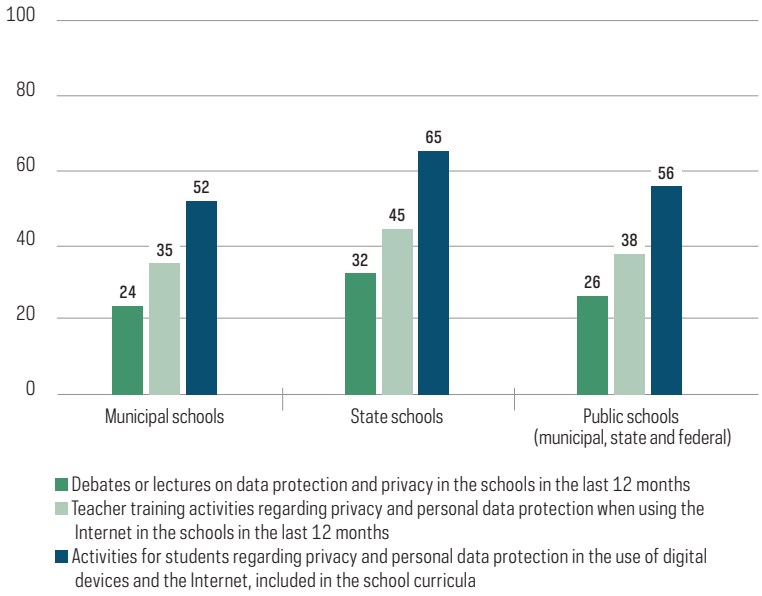
A large part of the traces left by students and teachers in virtual environments can become a source of inferred data, i.e., the basis for analyses of the personal characteristics of users. In addition to schools, students and teachers having no control over the data collected in these environments, one of the risks associated with the use of platforms, applications, and networks is the sharing of user data by technology enterprises with digital marketing services, advertising based on behavioral and contextual analyses, and the creation of audience segmentation and profiling to recommend personalized content (United Nations Educational, Scientific and Cultural Organization [UNESCO], 2022; Human Rights Watch, 2022).

Some actions to confront such risks, documents and analyses of privacy and data protection in the educational field (Henriques & Hartung, 2021; Laterça, et al., 2021; UNESCO, 2022) highlight the importance of legally guaranteeing students' rights and encouraging greater involvement of technology enterprises in the development of applications that respect these rights by design, i.e., that include in their computational models ethical principles in relation to the well-being of children.

CHART 10

PUBLIC SCHOOLS BY TRAINING ACTIVITIES CARRIED OUT BY THE INSTITUTIONS (2020)

Total number of public schools (%)



In addition to these actions, institutions involved in the defense of children's digital rights also emphasize the importance of the involvement of educational actors in the promotion of more appropriate digital spaces. In 2020, 26% of public schools mentioned organizing debates or lectures on data protection and privacy in the 12 months prior to the survey (Chart 10). It is important that such initiatives be disseminated to a greater number of schools. The development of digital skills and critical thinking among students, educators, and parents and legal guardians is extremely relevant to raising awareness about the various ways that personal data is collected and used, in addition to taking measures that can provide greater security and protection during the use of digital resources.

Final considerations: Agenda for public policies

While technological development has made it possible to incorporate ICT in the most diverse activities in public organizations, including the use of citizens' data for many different purposes, this development has also brought to light the importance of ensuring the security of privacy and the protection of personal data. In addition, the increase in digitization of the public sector has shone a spotlight on the inequalities among government organizations and institutions in terms of their readiness to handle this type of data, especially in emergency situations such as the COVID-19 pandemic. With the widespread attention of national and international organizations on the subject and the enactment of the LGPD in Brazil, public institutions began to

have many responsibilities when processing personal data. In this regard, this analysis provided an overview of privacy and data protection in public organizations in the country, based on survey indicators collected by Cetic.br|NIC.br.

The data presented indicate that, in general, the presence of structures focused on the implementation of the LGPD is still incipient in Brazilian federal and state government organizations and local governments, suggesting that they are in the initial phase of adapting to the legislation. Emphasis goes to the organizations of the judiciary branch, in which many of the structures and actions related to the LGPD measured by the survey were already in place. Moreover, to a greater extent, federal organizations also had initiatives on the subject, especially when compared to state organizations and local governments. One possible explanation for the considerable presence of the actions investigated at the federal level and in the judiciary is the greater institutionalization of recommendations and regulations on the subject in these institutions. Among the existing recommendations are a series of operational guides for adapting to the LGPD that were prepared by the Ministry of Economy, via the Secretariat of Digital Government, in addition to questionnaires to diagnose the maturity of privacy and security at the federal level[7]. Norms have also been created aimed at the implementation of the law at this level of government, such as Normative Instruction SGD/ME No.117, which provides guidelines for how to appoint DPOs. The National Council of Justice, among other initiatives, has established measures for the courts to be compliant with the LGPD (Resolution No. 363/2021, 2021).

Therefore, the results show disparities in the implementation of the LGPD in the public organizations, indicating the need for actions to better understand the main challenges faced by these organizations in meeting the requirements provided for in the law. Greater understanding of the main barriers to this adaptation can help institutions responsible for compliance with the LGPD, such as the ANPD, to direct their efforts to ensure privacy and protection of personal data in the operations of public authorities.

The results presented relative to the health sector indicate great challenges faced by public healthcare facilities in complying with the requirements established by the LGPD. To achieve progress in this area, coordination between federative entities is needed so that measures and processes can be implemented and adopted by all actors in the health sector, such as managers, employees, and professionals. This precept is a requirement, so that there will be no inappropriate use of sensitive patient data, and patients will feel increasingly confident and secure about the use of their information, being fully informed and aware of the use of this data. The penalties applicable to institutions that do not comply with the LGPD are either financial, such as in the form of fines, or the suspension of the right to collect any type of data from subjects, causing the interruption of the healthcare facility's activities and operation.

[7] More information available at https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados

The Ministry of Health has conducted studies to advance the discussion and develop a norm that includes two fundamental themes: the definition of LGPD profiles and regarding consent in the National Health Data Network (RNDS) (Ministry of Health, 2021). However, there are still gaps about how to carry out data exchange, health interoperability, and the definition of procedures for health services and professionals in the area, with knowledge to act in digital health, in the collection and use of data to be registered in electronic health records. Many challenges must be overcome to ensure the legal security that will underpin the advancement of digital health in the country and transparency about the use of subjects' information.

In the area of education, the results showed that public Basic Education schools have large amounts of student information, which includes not only personal data recorded by the schools themselves, but also data generated via activity monitoring applications, including via the images of children. However, less than half of these schools had documents that defined data protection and information security policies.

The Ministry of Education has carried out actions to map and diagnose the use of personal data internally, such as the development of the Institutional Program for the Protection of Personal Data and Privacy, the establishment of the Subcommittee on Information Security and Protection of Personal Data and of the Study Center for the Implementation of the General Data Protection Law, in addition to conducting a survey of personal data processing activities. Regarding public schools, it is necessary for secretariats of education to develop processes and adopt measures that can help these schools adopt solutions that protect student information and guarantee their privacy.

Given this scenario, there are still many challenges for public institutions to comply with the requirements set forth by the LGPD. The public sector needs to develop plans with rules of best practices and privacy governance that map the sensitive personal data used by its various institutions and determine how this data should be processed. It is also necessary to develop clear and objective protocols, as well as widespread awareness of the importance of these actions by all actors involved.

References

Bioni, B. R. (2018). *Proteção de dados pessoais: a função e os limites do consentimento*. Forense.

Bleeker, A. (2020). Creating an enabling environment for e-government and the protection of privacy rights in the Caribbean: a review of data protection legislation for alignment with the General Data Protection Regulation. *Studies and Perspectives – ECLAC Subregional Headquarters for the Caribbean*, (94).

Botelho, M. C., & Camargo, E. P. A. (2021). A aplicação da Lei Geral de Proteção de Dados na saúde. *Revista De Direito Sanitário*, *21*, e0021. https://doi.org/10.11606/issn.2316-9044.rdisan.2021.168023

Brazilian General Data Protection Law – LGPD. Law No. 13.709, of August 14, 2018. (2018). Addresses the processing of personal data, including on digital media, by natural or legal persons, of public or private law, with the goal of protecting the fundamental rights of freedom and privacy and the free development of the personality of natural persons. http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

Brazilian Internet Steering Committee. (2020). *Public notice on the processing of personal data and surveillance during the self-isolation period introduced because of the COVID-19 pandemic.* https://cgi.br/esclarecimentos/ver/public-notice-on-the-processing-of-personal-data-and-surveillance-during-the-self-isolation-period-introduced-because-of-the-covid-19-pandemic.pdf

Brazilian Internet Steering Committee. (2021a). *Survey on the use of information and communication technologies in Brazilian schools: ICT in Education* 2020 (COVID-19 edition — Adapted methodology). https://www.cetic.br/media/docs/publicacoes/2/20211124200326/tic_educacao_2020_livro_eletronico.pdf

Brazilian Internet Steering Committee. (2021b). *Survey on the use of information and communication technologies in Brazilian healthcare facilities: ICT in Health 2021* (COVID-19 edition — Adapted methodology). https://cetic.br/media/docs/publicacoes/2/20211124123911/tic_saude_2021_livro_eletronico.pdf

Brazilian Internet Steering Committee. (2022). *Survey on the use of information and communication technologies in the Brazilian public* sector*: ICT Electronic Government 2021*. https://cetic.br/media/docs/publicacoes/2/20220725170710/tic_governo_eletronico_2021_livro_eletronico.pdf

Brazilian National Data Protection Authority. (2022a). *Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado*. https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf

Brazilian National Data Protection Authority. (2022b). G*uia orientativo: tratamento de dados pessoais pelo poder público.* https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf

Brazilian National Data Protection Authority. (2022c). *Resolution CD/ANPD no. 2 of January 27, 2022.* https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019

Costa, R. (2022). Personalidade hackeada: considerações sobre proteção de dados pessoais sensíveis, vigilância digital e discriminação. In C. Teffé, & S. Branco (Coords.), *Proteção de dados e tecnologia: estudos da pós-graduação em Direito Digital* (pp. 52-78). Institute of Technology and Society of Rio de Janeiro; ITS/Obliq.

Crespo, M. (2021). Proteção de dados pessoais e o poder público: noções essenciais. In C. D. Cravo, D. Z. G. Cunda, & R. Ramos (Eds.), *Lei Geral de Proteção de Dados e o poder público* (pp. 16-28). Escola Superior de Gestão e Controle Francisco Juruena; Centro de Estudos de Direito Municipal.

Dallari, A. B., & Monaco, G. F. C. (Eds.). (2021). *LGPD na saúde*. Thomson Reuters, Revista dos Tribunais.

European Data Protection Board. (2020). *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

European Union. (2018). *General Data Protection Regulation*. https://gdpr.eu/

Gomes, M. C. O. (2022). Public policy and the data protection impact assessment: Case analysis of the NHS COVID-19 app. In Brazilian Internet Steering Committee (CGI.br). *Survey on the use of information and communication technologies in the Brazilian public sector: ICT Electronic Government 2021* (pp. 297-309). https://cetic.br/media/docs/publicacoes/2/20220725170710/tic_governo_eletronico_2021_livro_eletronico.pdf

Hawryliszyn, L. O., Coelho, N. G. S. C., & Barja, P. R. (2021). Lei Geral de Proteção de Dados (LGPD): o desafio de sua implantação para a saúde. *Revista Univap, 27*(54).

Henriques, I., & Hartung, P. (2021). Children's rights by design in AI development for education. *The International Review of Information Ethics, 29*.

Human Rights Watch. (2022). *"How dare they peep into my private life?" Children's rights violations by governments that endorsed online learning during the COVID-19 pandemic*. https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments

Laterça, P., Fernandes, E., Teffé, C., & Branco, S. (2021). *Privacidade e proteção de dados de crianças e adolescentes*. Institute of Technology and Society of Rio de Janeiro; Obliq.

Law No. 14.129, of March 29, 2021. (2021). Provides for the principles, rules and instruments for digital government and for increasing public efficiency and amends Law No. 7116, of August 29, 1983, Law No. 12527, of November 18, 2011 (Access to Information Law), Law No. 12682, of July 9, 2012, and Law No. 13460, of June 26, 2017. https://www.in.gov.br/en/web/dou/-/lei-n-14.129-de-29-de-marco-de-2021-311282132

Livingstone, S., Stoilova, M., & Nandagiri, R. (2019). *Talking to children about data and privacy online: research methodology*. London School of Economics and Political Science.

Ministry of Economy. (2020). *Lei Geral de Proteção de Dados (LGPD): guia de boas práticas para implementação na administração pública federal*. https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf

Ministry of Economy. (2021). G*uia de elaboração de programa de governança em privacidade*. https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_governanca_privacidade.pdf/view

Ministry of Health. (2021). *1º Relatório de monitoramento e avaliação da estratégia de saúde digital para o Brasil 2020-2028*. https://bvsms.saude.gov.br/bvs/publicacoes/relatorio_monitoramento_estrategia_saude_digital.pdf

Mulholland, C. (2018). Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/18). *Revista de Direitos e Garantias Fundamentais, 19*(3), 159-180. https://www.sumarios.org/artigo/dados-pessoais-sens%C3%ADveis-e-tutela-de-direitos-fundamentais-uma-an%C3%A1lise-%C3%A0-luz-da-lei-geral-de

Organisation for Economic Co-operation and Development. (2020a). *Growing up online: Addressing the needs of children in the digital environment*. https://www.oecd.org/sti/ieconomy/growing-up-online.pdf

Organisation for Economic Co-operation and Development. (2020b). *Tracking and tracing COVID: Protecting privacy and data while using apps and biometrics*. http://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protectingprivacy-and-data-while-using-apps-and-biometrics-8f394636/

Pan American Health Organization. (2021). *Eight guiding principles of digital transformation of the health sector: A call to Pan American action.* https://iris.paho.org/handle/10665.2/54256

Resolution No. 363 of January 12, 2021. (2021). Establishes measures for the process of adaptation to the General Data Protection Law to be adopted by the courts. https://atos.cnj.jus.br/atos/detalhar/3668

United Nations. (2021). *General comment No. 25 on children's rights in relation to the digital environment.* United Nations Committee on the Rights of the Child. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/053/43/PDF/G2105343.pdf?OpenElement

United Nations Development Programme. (2020). *Guidance to UNDP country offices on the privacy, data protection and broader human rights dimensions of using digital technologies to combat COVID-19*. https://www.sdg16hub.org/content/covid-19-guidance-undp-country-offices-privacy-data-protection-and-digital-technologies

United Nations Department of Economic and Social Affairs. (2020). *E-government survey 2020: Digital government in the decade of action for sustainable development: With addendum on COVID-19 response*. https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf

United Nations Educational, Scientific and Cultural Organization. (2022). *Minding the data: Protecting learners' privacy and security*. https://unesdoc.unesco.org/ark:/48223/pf0000381494

U.S. Congress. (1998). *Children's online privacy protection act*. https://www.congress.gov/bill/105th-congress/senate-bill/2326/text

van der Hof, S. (2016). I agree… or do I? A rights-based analysis of the law on children's consent in the digital world. *Wisconsin International Law Journal, 34*(2), 409-445.

Lista de Abreviaturas

ANPD – Autoridade Nacional de Proteção de Dados

BID – Banco Interamericano de Desenvolvimento

Cempre – Cadastro Central de Empresas

Cetic.br – Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação

CGI.br – Comitê Gestor da Internet no Brasil

CNAE – Classificação Nacional de Atividades Econômicas

CNES – Cadastro Nacional de Estabelecimentos de Saúde

CNPD – Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

COPPA – Children's Online Privacy Protection Act

Datasus – Departamento de Informática do Sistema Único de Saúde

DPO – Data Protection Officer

EDPB – European Data Protection Board

Eurostat – Instituto de Estatísticas da Comissão Europeia

GDPR – General Data Protection Regulation

IBGE – Instituto Brasileiro de Geografia e Estatística

Idec – Instituto Brasileiro de Defesa do Consumidor

Inep – Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira

LGPD – Lei Geral de Proteção de Dados Pessoais

Mercosul – Mercado Comum do Sul

NIC.br – Núcleo de Informação e Coordenação do Ponto BR

OCDE – Organização para a Cooperação e Desenvolvimento Econômico

ONU – Organização das Nações Unidas

OPAS – Organização Pan-Americana da Saúde

PNUD – Programa das Nações Unidas para o Desenvolvimento

RNDS – Rede Nacional de Dados em Saúde

TIC – Tecnologias de informação e comunicação

UIT – União Nacional de Telecomunicações

UN DESA – Departamento das Nações Unidas para Assuntos Econômicos e Sociais

UNCTAD – Conferência das Nações Unidas sobre Comércio e Desenvolvimento

UNESCO – Organização das Nações Unidas para a Educação, a Ciência e a Cultura

List of Abbreviations

ANPD – Brazilian National Data Protection Authority

Cempre – Central Register of Enterprises

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

CGI.br – Brazilian Internet Steering Committee

CNAE – National Classification of Economic Activities

CNES – National Registry of Healthcare Facilities

CNPD – National Council for the Protection of Personal Data and Privacy

COPPA – Children's Online Privacy Protection Act

Datasus – SUS Informatics Department

DPO – Data Protection Officer

EDPB – European Data Protection Board

Eurostat – Statistical Office of the European Communities

GDPR – General Data Protection Regulation

IBGE – Brazilian Institute of Geography and Statistics

ICT – Information and communication technologies

IDB – Inter-American Development Bank

Idec – Brazilian Institute of Consumer Protection

Inep – National Institute for Educational Studies and Research "Anísio Teixeira"

ITU – International Telecommunication Union

LGPD – Brazilian General Data Protection Law

Mercosur – Southern Common Market

NIC.br – Brazilian Network Information Center

OECD – Organisation for Economic Co-operation and Development

PAHO – Pan American Health Organization

RNDS – National Health Data Network

UN – United Nations

UN DESA – United Nations Department of Economic and Social Affairs

UNCTAD – United Nations Conference on Trade and Development

UNDP – United Nations Development Programme

UNESCO – United Nations Educational, Scientific and Cultural Organization

cetic.br nic.br cgi.br

Tel 55 11 5509 3511
Fax 55 11 5509 3512

https://www.cgi.br
https://www.nic.br
https://www.cetic.br