



Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

Educação e Capacitação
em Proteção de Dados

GTT 1

2025





Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT1 – Educação e Capacitação em Proteção de Dados

Relatório Final

Membros:

Rodrigo Borges Valadão (Coordenador)

Alexandre Zago Boava

Ana Paula Moraes Canto de Lima

Gabrielle Bezerra Sales Sarlet

Gisela Carvalho de Freitas

Isabella Vieira Machado Henriques

Tiago Lopes de Aguiar

14 de fevereiro de 2025

SUMÁRIO

Considerações Preliminares.....	4
1. Maturidade (Geral e Específica)	5
1.1. Panorama Normativo.....	6
1.2. Panorama Fático	10
1.3. Educação em Matéria de Proteção de Dados Pessoais	13
1.3.1. Conscientização.....	13
1.3.2. Capacitação.....	14
2. Desafios	15
2.1. Mudança de Cultura.....	16
2.2. Complexidade do Tema	17
2.3. Desigualdade Econômica	18
2.4. Tecnologia e Infraestrutura	19
2.6. Desigualdades estruturais da realidade brasileira e públicos vulneráveis	21
2.7. Desafios Especiais para a Proteção Integral de Crianças e Adolescentes.....	23
3. Coleta de Subsídios	26
3.1. Plano Institucional de Ações Educativas da ANPD.....	26
3.2. Relatório da 1ª Composição do CNPD	28
3.3. Iniciativas Relevantes.....	30
3.3.1. Plano Institucional de Ações Educativas.....	30
3.3.2. Política Nacional de Educação Digital (PNED).....	31
3.3.3. Estratégia Brasileira de Educação Midiática	31
3.3.4. Educação Conectada	32
3.3.5. Resolução n. 245 do CONANDA	33
3.3.6. Estratégia Brasileira de Transformação Digital (E-Digital)	33
3.3.7. Estratégia Nacional do Governo Digital (2024-2027)	34
3.3.8. Escola de Dados	34

3.3.9. Escola Nacional de Administração Pública.....	35
3.3.10. Aula Digital	36
3.3.11. Data_Labe	36
3.3.12. Prato do Dia	36
3.3.13. Cadê meu Dado?	37
3.3.14. Canal de Ajuda da SaferNet Brasil.....	37
3.3.15. Data Privacy Brasil.....	38
3.4. Participação da Sociedade Civil.....	38
3.4.1. Mesa Redonda com Especialistas	38
3.4.2. Contribuições por Escrito de Entidades	40
4. Quadro Geral das Iniciativas e Sugestões	45
4.1. Parcerias e Colaborações Institucionais.....	45
4.2. Realização de Eventos e Atividades Interativas:	48
4.3. Produção e Disseminação de Conteúdo:	50
4.4. Integração Curricular e Capacitação Profissional	52
4.5. Campanhas de Conscientização e Engajamento Público	55
4.6. Desenvolvimento de Plataformas e Recursos Digitais.....	57
5. Recomendações	59
5.1. Criação da Escola Nacional da Proteção de Dados (ENAD).....	60
5.2. Semana da Privacidade	61
5.3. Parceria com o MEC.....	61
5.4. Revisão do Plano Nacional de Educação (PNE).....	63
5.5. Parceria com entidades reguladoras setoriais e outros órgãos públicos	64
5.6. Criação de conteúdos específicos sobre proteção de dados para grupos vulneráveis	65
5.7. Parceria com a ENAP	66
5.8. Parceria com a OAB-Nacional	67
5.9. Encontros Profissionais	68
5.10. Parceria com influenciadores digitais:	69
ANEXO I	
SUMÁRIO DOS DADOS DE APOIO PARA A CONSTRUÇÃO DO RELATÓRIO	70
A. Descrição do Documento.....	71
B. Metodologia da Pesquisa.....	71
C. Indivíduos.....	71

a. Atividades mais realizadas para gerenciar o acesso aos seus dados pessoais	71
b. Leitura de “Políticas de Privacidade”	71
c. Busca de canais de atendimento para realizar solicitações	72
d. Preocupação com dados pessoais	72
D. Empresas	72
a. Capacidades Internas	73
b. Adequação à LGPD	73
E. Setor Público	73
a. Capacidades Internas	74
b. Saúde.....	76
c. Educação	77

ANEXO II

MINUTA DO OFÍCIO ENCAMINHADO ÀS ENTIDADES DA SOCIEDADE CIVIL	81
--	----

ANEXO III

CONTRIBUIÇÕES ESCRITAS	83
A. Cadê meu Dado?.....	84
B. Câmara de Educação Superior do Conselho Nacional de Educação (MEC)	85
C. Data Privacy Brasil.....	86
D. Centro de Estudos Avançados em Proteção de Dados (CEAPD)	87

Considerações Preliminares

A proteção de dados pessoais e da privacidade é uma questão crucial na sociedade atual. Reconhecendo essa importância, o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD) estabeleceu sete grupos de trabalho temáticos¹ para coletar informações sobre temas específicos. Esses grupos atuam em sinergia com o artigo 55 da Lei Geral de Proteção de Dados Pessoais (LGPD), auxiliando a Autoridade Nacional de Proteção de Dados (ANPD) na elaboração de diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade, cujo objetivo principal é promover estratégias eficazes e abrangentes para conscientizar a sociedade e os titulares de dados sobre a importância da proteção à privacidade e o uso responsável de dados pessoais.

O Grupo de Trabalho 1 (GT1) tem como finalidade específica apresentar subsídios na temática da **“Educação e Capacitação em Proteção de Dados Pessoais”**. A relevância da tarefa atribuída ao presente GT1 é evidenciada pelo baixo nível de cultura de proteção de dados em nossa sociedade, incluindo titulares de dados, profissionais e, principalmente, agentes de tratamento (controladores e operadores). Essa situação é particularmente preocupante considerando que a LGPD foi publicada há seis anos e que a Emenda Constitucional n. 115 elevou a proteção de dados pessoais ao status de direito fundamental. Portanto, o GT1 desempenha um papel crucial na promoção da educação e da capacitação nessa área, visando elevar o nível de conscientização e de competência em relação à proteção de dados pessoais no Brasil.

Para cumprir a sua função, este GT1 trabalhou intensamente.² Suas atividades iniciaram-se no dia 14 de outubro de 2024 e se prolongaram até o dia 14 de fevereiro de 2025.³ Ao todo, foram realizadas doze reuniões virtuais,⁴ nas quais pontos críticos foram trazidos, debatidos, analisados, ponderados e decididos. Isso sem prejuízo do trabalho assíncrono realizado durante todo o período, no qual

¹ A saber: a) GT1: educação e capacitação em proteção de dados, b) GT2: mecanismos, instâncias e práticas de conformidade de proteção de dados c) GT3: governança de dados (I), d) GT4: governança de dados (II), e) GT5: dados pessoais para o desenvolvimento econômico, tecnológico e a inovação, f) GT6: LAI & LGPD: dados abertos como infraestrutura crítica em conformidade com LGPD e g) GT7: Regimento Interno. Ver: BRASIL. Autoridade Nacional de Proteção de Dados. Grupos de trabalho. Disponível em: <https://www.gov.br/anpd/pt-br/cnpd-2/grupos-de-trabalho>. Acesso em: 5 dez. 2024.

² Não se pode deixar de registrar aqui a inestimável colaboração de Emanuella Ribeiro Halfeld Maciel e Renato Godoy de Toledo, do Instituto Alana, na coleta dos dados que subsidiam o presente relatório, bem como nossos agradecimentos à Conselheira Isabella Henriques, Diretora Executiva do referido instituto, por gentilmente disponibilizar seu pessoal para essa tarefa.

³ Registre-se, aqui, que, o presente relatório já estava praticamente pronto no termo final estipulado para a sua entrega (04 de fevereiro de 2025). No entanto, os membros deste GT concordaram que mais alguns dias seriam necessários para aprimorá-lo e promover alguns ajustes finos. Atendendo ao pedido do GT1, a Presidente do CNPD, Dra. Lilian Manoela Monteiro Cintra de Melo, gentilmente, autorizou que a entrega fosse realizada no dia 14 de fevereiro.

⁴ A ata dessas reuniões, geradas por inteligência artificial e mediante autorização de todos os participantes, titulares e convidados, foram encaminhadas à ANPD para arquivamento. As gravações foram prontamente eliminadas assim que as minutas de atas foram geradas.

os membros puderam apresentar seus pontos de vista e debater questões específicas de menor complexidade, seja por meio de aplicativo de mensagem instantânea, seja na redação colaborativa de documento que serviu de *draft* ao presente relatório.

O relatório é dividido em 5 capítulos. O **capítulo 1** é dedicado à análise da maturidade da proteção de dados pessoais no Brasil em 3 (três) dimensões: a) o marco regulatório, b) o nível geral de adequação à LGPD e c) o conhecimento geral do tema, na sociedade e entre os profissionais que, em qualquer medida, realizam tratamentos de dados pessoais. Já o **capítulo 3** tem por finalidade identificar os principais desafios a serem enfrentados para a melhora do ambiente de proteção de dados no Brasil. No **capítulo 3**, foram coletados subsídios em matéria de acultramento em proteção de dados pessoais, a saber: a) o Plano Institucional de Ações Educativas da ANPD (referente ao biênio 2024-25), b) as propostas apresentadas pela 1ª composição do CNPD sobre o tema para a ANPD, c) as iniciativas relevantes em matéria de educação em proteção de dados nos âmbitos público, privado e no terceiro setor e d) as sugestões de especialistas e de entidades com reconhecida representatividade no tema. No **capítulo 4**, foi feito um resumo das iniciativas educacionais em curso e das novas iniciativas que poderiam ser apoiadas e desenvolvidas pela ANPD. Por fim, **capítulo 5** são apresentadas as sugestões de quais iniciativas devem ser mantidas, aperfeiçoadas, reavaliadas, descontinuadas ou iniciadas pela Autoridade Nacional de Proteção de Dados (ANPD) na formulação da sua Política Pública em matéria de proteção de dados pessoais, indicando-se, também, quais deveriam, sob ótica deste GT1, ser priorizadas.

Ao final, espera-se que este relatório colabore de maneira efetiva para promover a educação de proteção de dados pessoais no Brasil, contribuindo para uma sociedade mais consciente e responsável para o exercício da cidadania digital.

1. Maturidade (Geral e Específica)

A Lei Geral de Proteção de Dados Pessoais (LGPD), instituída pela Lei Federal nº 13.709/2018, inaugurou um novo paradigma para o tratamento de dados pessoais no Brasil. Desde sua implementação, organizações públicas e privadas têm buscado adequar-se às exigências legais, apesar de um quadro geral de baixo nível de conformidade com essas normas⁵, especialmente quando comparado a outros subsistemas jurídicos, como o Código de Defesa do Consumidor. Paralelamente, a conscientização dos indivíduos e da sociedade civil sobre a importância, o funcionamento e a aplicação das

⁵ De modo geral, a pesquisa produzida pelo CGI aponta que houve avanços na conformidade com a LGPD entre as médias e grandes empresas, inclusive em diferentes setores econômicos, mas há espaço para uma maior presença de boas práticas de proteção de dados pessoais, principalmente entre os negócios de menor porte. Mas, em relação ao poder público foi identificada uma grande discrepância com relação às medidas adotadas pelas empresas privadas e entre os diversos órgãos, especialmente no que se refere aos dados de saúde. De qualquer sorte, em relação a sensibilização acerca do tema, segundo o estudo, os brasileiros se preocupam com o fornecimento de seus dados biométricos em maiores proporções do que com outros tipos de dados pessoais sensíveis, tais como orientação sexual e cor ou raça. Ver: NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR (NIC.br); CENTRO REGIONAL DE ESTUDOS PARA O DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO (CETIC.br). Privacidade e proteção de dados pessoais 2023: perspectivas de indivíduos, empresas e organizações públicas no Brasil. São Paulo: Comitê Gestor da Internet no Brasil, 2024. Disponível em: <https://cetic.br/pt/publicacao/privacidade-e-protecao-de-dados-2023/>. Acesso em 9 jan. 2025.

normas de proteção de dados pessoais ainda não atingiram um nível satisfatório, permanecendo restrita a alguns círculos especializados. Destaque-se, para além disso, que o Poder Público, em todas as esferas, tem sistematicamente atuado em dissonância com o que se extrai da LGPD.

Este relatório analisa o atual nível de maturidade e os desafios enfrentados para o desenvolvimento quantitativo e qualitativo da conscientização em matéria de proteção de dados pessoais no Brasil. Consideram-se as especificidades dos setores público e privado, incluindo as diferenças entre grandes e pequenas empresas e as segmentações de mercado. Conforme será demonstrado, a análise da maturidade em proteção de dados pessoais revela um cenário de avanços normativos significativos, expressando, por outro lado, um quadro com desafios concretos em termos de adesão por parte dos agentes de tratamento (o que não será objeto deste relatório), conscientização dos titulares e capacitação dos diversos atores que operam com dados pessoais. A seguir, apresenta-se uma análise preliminar do contexto brasileiro.

1.1. Panorama Normativo

Historicamente, o tratamento de dados pessoais no Brasil era regulado por um conjunto fragmentado de normas que abordam aspectos específicos do tema. Entre essas legislações estão o Código de Defesa do Consumidor (“CDC”, Lei nº 8.078/1990), a Lei do Habeas Data (Lei nº 9.507/1997), o Marco Civil da Internet (“MCI”, Lei nº 12.965/2014), a Lei Geral de Telecomunicações (Lei nº 9.472/1997), a Lei de Acesso à Informação (“LAI”, Lei nº 12.527/2011) e a Lei do Cadastro Positivo (Lei nº 12.414/2011), além de outras normas setoriais.

Influenciado por tendências globais, o Brasil decidiu substituir este modelo fragmentado por uma regulação centralizada em matéria de proteção de dados pessoais. Inspirada no Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, a LGPD (Lei Federal nº 13.709/2018) surgiu para unificar e harmonizar essas regras, consolidando a proteção de dados pessoais no Brasil em uma estrutura moderna e abrangente. Desde então, o tratamento de dados pessoais é regulado de forma apropriada, com aplicabilidade ampla para agentes públicos e privados, consagrando princípios, hipóteses legais que legitimam o tratamento de dados pessoais, os direitos dos titulares, além de parâmetros para governança e para fiscalização.

O reconhecimento da proteção de dados pessoais como direito fundamental autônomo ocorreu em um momento posterior. Na decisão da ADI 6393, impetrada contra a Medida Provisória n. 954/20, que obrigava as empresas de telefonia a fornecerem ao Instituto Brasileiro de Geografia e Estatística (IBGE) dados como nome, número de telefone e endereço dos usuários, o Supremo Tribunal Federal (STF) reconheceu a autodeterminação informacional como princípio constitucional implícito, derivado da dignidade humana e do direito ao livre desenvolvimento da personalidade. Subsequentemente, o Poder Constituinte Derivado inseriu expressamente o direito à proteção de dados no art. 5º da Constituição Federal, por meio do inciso LXXIX: “É assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.”

A Autoridade Nacional de Proteção de Dados (ANPD), por sua vez, desempenha papel central na regulamentação e fiscalização da LGPD. Criada em 2019 como órgão vinculado à Presidência da

República, foi transformada em autarquia de regime especial pela Medida Provisória nº 1.124/2022 (convertida na Lei nº 14.460/2022). Algumas medidas em curso, como a realização de concurso público⁶ e o reforço da sua autonomia,⁷ podem vir a colaborar, em breve, para o fortalecimento da Autoridade. Dentre outras competências, a ANPD é hoje responsável pela: a) edição de normas complementares e regulamentos (art. 55, J, XII da LGPD), b) fiscalização e aplicação de sanções administrativas (art. 55, J, IV da LGPD), c) fomento à cultura de proteção de dados a partir da promoção de conhecimento das normas, políticas públicas e medidas de segurança sobre a matéria (art. 55, J, VI), d) coordenação com outras entidades regulatórias setoriais.

Desde sua criação em 2019, a ANPD vem atuando na regulamentação da LGPD. Já foram regulamentados, por exemplo: (a) o processo de fiscalização,⁸ (b) a definição e o regime jurídico dos agentes de pequeno porte,⁹ (c) a dosimetria das sanções,¹⁰ (d) a notificação de incidentes,¹¹ (e) a atuação dos encarregados¹² e, mais recentemente, (f) a transferência internacional de dados.¹³

No entanto, no âmbito normativo, ainda persistem algumas lacunas regulatórias significativas e, no campo do *enforcement*, uma atuação mais decisiva e consolidada dos agentes públicos que, em alguma medida, atuam com a proteção de dados. Especialmente sobre (a) tratamento de dados de crianças e adolescentes; (b) relatório de impacto à proteção de dados pessoais (RIPD);¹⁴ (c) manejo de

⁶ Atualmente, não há um concurso público em andamento para cargos efetivos na ANPD. Contudo, projetos estão em curso. De um lado, foi autorizada a realização de um processo seletivo simplificado para a contratação de 213 profissionais temporários, conforme a Portaria Conjunta MGI/MJSP nº 99, publicada em 18 de novembro de 2024 pelo Ministério da Gestão e da Inovação em Serviços Públicos. Paralelamente, o Projeto de Lei Orçamentária Anual (PLOA) 2025 prevê a criação de 48 vagas efetivas para a ANPD, sinalizando a possibilidade de um futuro concurso público para cargos permanentes. Essas ações demonstram que a ANPD está em processo de estruturação de seu quadro de pessoal, combinando soluções temporárias com planos para um quadro efetivo a longo prazo. Vide: BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos; Ministério da Justiça e Segurança Pública. Portaria Conjunta MGI/MJSP nº 99, de 10 de outubro de 2024. Autoriza a contratação temporária de até 213 profissionais para a Autoridade Nacional de Proteção de Dados (ANPD). Diário Oficial da União, 18 nov. 2024; BRASIL. Projeto de Lei Orçamentária Anual (PLOA) 2025. Prevê a criação de 48 vagas efetivas para a Autoridade Nacional de Proteção de Dados (ANPD). Brasília, DF, 2024.

⁷ O PL nº 615/2024, apresentado pelo Senador Ângelo Coronel (PSD-BA), em 6 de março de 2024, propõe alterar a Lei nº 13.848, de 25 de junho de 2019, conhecida como "Lei das Agências", para reforçar a autonomia da ANPD. Vide: BRASIL. Senado Federal. Projeto de Lei nº 615, de 2024. Altera a Lei nº 13.848, de 25 de junho de 2019, para garantir autonomia à Autoridade Nacional de Proteção de Dados (ANPD). Autor: Senador Ângelo Coronel (PSD-BA). Apresentado em 6 de março de 2024.

⁸ BRASIL. Autoridade Nacional de Proteção de Dados. Resolução CD/ANPD nº 1, de 28 de outubro de 2021. Aprova o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados.

⁹ BRASIL. Autoridade Nacional de Proteção de Dados. Resolução CD/ANPD nº 2, de 27 de janeiro de 2022. Aprova o Regulamento de aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) para agentes de tratamento de pequeno porte.

¹⁰ BRASIL. Autoridade Nacional de Proteção de Dados. Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023. Aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas.

¹¹ BRASIL. Autoridade Nacional de Proteção de Dados. Resolução CD/ANPD nº 15, de 26 de abril de 2024. Aprova o Regulamento de Comunicação de Incidente de Segurança.

¹² BRASIL. Autoridade Nacional de Proteção de Dados. Resolução CD/ANPD nº 18, de 16 de julho de 2024. Estabelece o regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais.

¹³ BRASIL. Autoridade Nacional de Proteção de Dados. Resolução CD/ANPD nº 19, de 23 de dezembro de 2024. Aprova o Regulamento de Transferência Internacional de Dados.

¹⁴ BRASIL. Autoridade Nacional de Proteção de Dados. *Relatório de impacto à proteção de dados pessoais (RIPD)*. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd. Acesso em: 22 jan. 2025.

algumas bases legais, como o consentimento; (d) procedimentos de anonimização e pseudonimização de dados;¹⁵ e (e) dados de trabalhadores e da atividade laboral.

Fora do âmbito normativo, a atuação da ANPD também é bastante rica. Desde sua criação foram expedidas, por exemplo, diversos “Guias Orientativos”¹⁶ e Notas Técnicas,¹⁷ que são documentos oficiais que servem como ferramentas essenciais para esclarecer, orientar e analisar questões complexas relacionadas à proteção de dados pessoais. Elaboradas por especialistas da ANPD, esses documentos oferecem *insights* valiosos sobre a aplicação prática da lei, examinam a legalidade de práticas específicas de tratamento de dados, fornecem recomendações para setores públicos e privados, e contribuem para o desenvolvimento de políticas e de regulamentações futuras. Assim, ao divulgar os entendimentos e as análises detalhadas, esses documentos não apenas promovem a transparência na atuação da ANPD, mas também auxiliam os titulares de dados, os agentes de tratamento e a sociedade em geral a navegar pelo complexo cenário da proteção de dados pessoais no país, fomentando uma cultura de privacidade e de segurança da informação. Em janeiro de 2025, a ANPD

¹⁵ Sobre o tema, a ANPD já realizou uma consulta pública. Ver: BRASIL. Autoridade Nacional de Proteção de Dados. ANPD abre consulta à sociedade sobre o guia de anonimização e pseudonimização. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-abre-consulta-a-sociedade-sobre-o-guia-de-anonimizacao-e-pseudonimizacao>. Acesso em: 22 jan. 2025.

¹⁶ BRASIL. Autoridade Nacional de Proteção de Dados. [Glossário de Proteção de Dados Pessoais](#), de 23 de maio de 2025; Guia orientativo [“Como Proteger seus Dados Pessoais”](#), em parceria com o Ministério da Justiça e Segurança Pública (MJSP), s.d., traduzido para Espanhol e Inglês; Guia orientativo [“Aplicação da Lei Geral de Proteção de Dados Pessoais \(LGPD\) por agentes de tratamento no contexto eleitoral”](#), em parceria com o Tribunal Superior Eleitoral (TSE), de 2021; Guia orientativo [“sobre segurança da informação para agentes de tratamento de pequeno porte”](#), de outubro de 2021; [Guia orientativo “para definições dos agentes de tratamento de dados pessoais e do encarregado”](#), publicado em maio de 2021 e atualizado em abril de 2022; Guia orientativo [“Cookies e proteção de dados pessoais”](#), de outubro de 2022; Guia Orientativo [“Tratamento de dados pessoais pelo Poder Público”](#), 2ª ed. de junho de 2023; [“Tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas”](#), de junho de 2023 e [“Atuação do encarregado pelo tratamento de dados pessoais”](#), de dezembro de 2024. Acesso em 26 jan. 2025.

¹⁷ BRASIL. Autoridade Nacional de Proteção de Dados. Nota Técnica nº 1/2021/CGN/ANPD, de 24 de março de 2021. Regulamentação da aplicação da LGPD para microempresas, empresas de pequeno porte, startups e pessoas físicas que tratam dados pessoais com fins econômicos; BRASIL. Autoridade Nacional de Proteção de Dados. Nota Técnica nº 68/2022/CGF/ANPD, de 13 de maio de 2022. Análise da Portaria RFB nº 167 de 19 de abril de 2022; BRASIL. Autoridade Nacional de Proteção de Dados. Nota Técnica nº 20/2022/CGN/ANPD, de 15 de julho de 2022. Proposta de realização de Tomada de Subsídios para regulamentação de transferência internacional de dados pessoais; BRASIL. Autoridade Nacional de Proteção de Dados. Nota Técnica nº 92/2022/CGF/ANPD, de 29 de agosto de 2022. Manifestação sobre a transparência e publicização das listas de requerentes e beneficiários dos auxílios emergenciais para taxistas e transportadores autônomos de carga; BRASIL. Autoridade Nacional de Proteção de Dados. Nota Técnica nº 12/2023/CGF/ANPD, de 17 de março de 2023. Avaliação dos Relatórios de Impacto à Proteção de Dados elaborados pelo INEP para adequação da divulgação dos microdados do censo escolar e do Enem à LGPD; BRASIL. Autoridade Nacional de Proteção de Dados. Nota Técnica nº 16/2023/CGTP/ANPD, de 21 de abril de 2023. Sugestões sobre o Projeto de Lei nº 2338/2023, que trata do marco regulatório da inteligência artificial; BRASIL. Autoridade Nacional de Proteção de Dados. Nota Técnica nº 19/2023/CGF/ANPD, de 5 de maio de 2023. Atividades de monitoramento da ANPD sobre o mercado financeiro e de telecomunicações; BRASIL. Autoridade Nacional de Proteção de Dados. Nota Técnica nº 22/2023/CGN/ANPD, de 2 de junho de 2023. Proposta do Regulamento de Transferência Internacional de Dados e o modelo de Cláusulas-Padrão Contratuais; BRASIL. Autoridade Nacional de Proteção de Dados. Nota Técnica nº 175/2023/CGF/ANPD, de 14 de julho de 2023. Compartilhamento e tratamento de dados pessoais no contexto do Projeto Estádio Seguro; BRASIL. Autoridade Nacional de Proteção de Dados. Nota Técnica nº 2/2024/FIS/CGF/ANPD, de 15 de janeiro de 2024. Oferta ativa de serviços de crédito a partir do tratamento de dados pessoais dos beneficiários do INSS por instituições financeiras e correspondentes bancários.

criou a página institucional “Centrais de Conteúdo”, repositório de documentos e iniciativas produzidos pelo órgão, buscando facilitar o acesso cidadão¹⁸.

A atividade fiscalizatória da ANPD vem sendo igualmente desempenhada de forma regular e consistente.¹⁹ Ela é de suma importância para a efetiva implementação da LGPD, pois demonstra que a ANPD está cumprindo seu papel fiscalizatório e regulatório, incentivando as organizações a adotarem práticas adequadas à proteção de dados. Como ponto positivo desta atuação, destaca-se a abordagem gradual e educativa, considerando as circunstâncias atenuantes e a cooperação dos infratores.²⁰ Contudo, há críticas quanto à demora na aplicação de sanções mais robustas e à falta de clareza em alguns aspectos do processo administrativo sancionador.²¹ A efetividade das autuações ainda está em fase de avaliação, mas já se observa a preocupação das empresas com a conformidade à LGPD.²² É fundamental, diante do atual cenário, que a ANPD continue aprimorando seus procedimentos e ampliando sua atuação para garantir uma agenda voltada para uma cultura de proteção de dados mais abrangente e eficaz no país.

Além disso, a complexidade a que se refere a coordenação e a harmonização de um ambiente regulatório composto por uma regulação horizontal, produzida pela ANPD, com diversas regulações setoriais, representa um desafio significativo para o cenário brasileiro de proteção de dados e, inclusive, de regulação da inteligência artificial (doravante IA).

A ANPD, como órgão central regulatório em matéria de dados pessoais, enfrenta a árdua tarefa de alinhar as diferentes abordagens e as competências de órgãos como Anatel, Cade, Anvisa, ANS,

¹⁸ BRASIL. Autoridade Nacional de Proteção de Dados. Centrais de Conteúdo. Disponível em: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo>. Acesso em 27 jan 2025.

¹⁹ Estas são algumas das sanções administrativas aplicadas pela ANPD até o momento: BRASIL. Autoridade Nacional de Proteção de Dados. Decisão nº 1/2023/CGF/ANPD. Aplicação da primeira sanção por descumprimento à LGPD à empresa Telekall Infoservice, com multa total de R\$ 14.400,00 e advertência. Publicado em 6 de julho de 2023; BRASIL. Autoridade Nacional de Proteção de Dados. Decisão nº 2/2024/CGF/ANPD. Aplicação de sanção a órgão público por exposição indevida de dados cadastrais e de saúde de 3.030 menores e seus responsáveis. Publicado em fevereiro de 2024; BRASIL. Autoridade Nacional de Proteção de Dados. Decisão nº 3/2024/CGF/ANPD. Aplicação de sanção a órgão público por falha na comunicação de incidentes de segurança envolvendo dados pessoais. Publicado em fevereiro de 2024; BRASIL. Autoridade Nacional de Proteção de Dados. Decisão nº 4/2023/CGF/ANPD. Aplicação de sanção à Secretaria de Saúde do Estado de Santa Catarina por violações aos artigos 48, 49 e 38 da LGPD e ao artigo 5º do Regulamento de Fiscalização. Publicado em 18 de outubro de 2023. Uma lista completa da sua atividade sancionatória recente pode ser encontrada aqui: BRASIL. Autoridade Nacional de Proteção de Dados. Relatório de Sanções 2023-2024. Aplicação de 17 sanções no período, sendo 6 a novos agentes de tratamento, com destaque para violações relacionadas à comunicação de incidentes de segurança envolvendo dados pessoais. Publicado em 2024.

²⁰ OLIVEIRA, Lucas Sávio; CUNHA, Henrique. Regulamento de dosimetria e aplicação de sanções administrativas da ANPD. *Consultor Jurídico*, 11 mar. 2023. Disponível em: <https://www.conjur.com.br/2023-mar-11/oliveira-cunha-aplicacao-sancoes-administrativas-anpd/>. Acesso em: 10 dez. 2024.

²¹ Há críticas na literatura quanto à adequação da norma de fiscalização para regulamentação das sanções administrativas da ANPD às prerrogativas alinhadas aos princípios basilares do processo civil e administrativo brasileiros. Ver PYRRHO, Beatriz; IZAY, Carolina; KESSLER, Daniela. Resolução de fiscalização da ANPD: aplicação de sanções e a segurança jurídica. *Migalhas*, 2021. Disponível em: <https://www.migalhas.com.br/depeso/350971/resolucao-de-fiscalizacao-da-anpd>. Acesso em: 1 dez. 2024. Ainda, entidades da sociedade civil têm questionado questões como a falta de mecanismos de participação dos interessados em procedimentos de fiscalização e sancionatórios e a atribuição de sigilo absoluto aos procedimentos em curso, dificultando o controle social dos agentes regulados e próprio ente regulador por atores externos. Ver: IDEC. *Caso WhatsApp*. IDEC, 2024. Disponível em: <https://idec.org.br/caso-whatsapp>. Acesso em 27 jan. 2025.

²² ANPD: entenda a importância da agência para LGPD. *Inteligov*, 2023. Disponível em: <https://www.blog.inteligov.com.br/anpd>. Acesso em: 10 dez. 2024.

Senacon e CGI. E esse desafio será ainda maior caso seja aprovado a proposta contida no PL 2338/23 e seu substitutivo, apresentado pelo senador Eduardo Gomes (PL/TO), que transforma a ANPD no órgão central do Sistema Nacional de Regulação e Governança de Inteligência Artificial (SIA).²³ Esse cenário exigirá da ANPD uma capacidade ainda mais robusta de liderança, comunicação e articulação interinstitucional para evitar sobreposições, conflitos normativos e garantir uma aplicação coerente e eficaz das regulações.

Verifica-se, assim, que o ambiente regulatório brasileiro, embora bem estruturado, ainda está em formação. No panorama geral, é possível afirmar que o Brasil possui um marco regulatório robusto em matéria de proteção de dados pessoais, embora haja necessidade de aperfeiçoamento do quadro normativo vigente, bem como da regulamentação e atuação mais efetiva em matérias importantes²⁴. Entende-se que a adesão às tecnologias embarcadas de Inteligência Artificial (IA) tende a performar um incremento exponencial, implicando uma expansão compatível dos esforços em políticas públicas que assegurem e implementem a cidadania digital. Em face do que foi esboçado, como é de conhecimento geral, faltam investimentos e iniciativas mais consistentes para melhor aparelhar a ANPD e, de fato, consolidar um sistema de proteção de dados e da privacidade no Brasil.

1.2. Panorama Fático

Embora o Brasil possua já possua elevado nível de maturidade normativa em matéria de proteção de dados pessoais, ele enfrenta desafios significativos na implementação efetiva da LGPD. A adequação às exigências legais envolve não apenas a conformidade jurídica formal, mas também a proteção e garantia efetiva dos direitos dos cidadãos e a segurança das informações em um contexto cada vez mais digitalizado.²⁵

No setor público, a implementação da LGPD tem sido marcada por uma adaptação desigual entre os órgãos governamentais. Enquanto entidades federais²⁶ demonstram um nível relativamente

²³ BRASIL. Senado Federal. Comissão Temporária de Inteligência Artificial. Parecer do Senador Eduardo Gomes (PL/TO) sobre o PL 2338/2023. Propõe a formalização da Autoridade Nacional de Proteção de Dados (ANPD) como órgão de coordenação do Sistema Nacional de Regulação e Governança de Inteligência Artificial (SIA). Apresentado em 18 de abril de 2024.

²⁴ Como, por exemplo: a) inclusão digital efetiva, b) políticas de dados abertos confiáveis, seguras e robustas, c) literacia popularizada entre os vários estratos da população, d) políticas de cibersegurança, e) políticas de transparência do poder público no que se refere ao emprego de ferramentas de IA e ao tratamento de dados, f) políticas de harmonização de instrumentos regulatórios, sobretudo em áreas estratégicas, g) políticas de apoio e de proteção às crianças e adolescentes em ambientes digitais.

²⁵ Este panorama fático de adesão à LGPD pode ser encontrado em diversas fontes. Ver: SARAIVA, Juliana; SOUZA, Cleidson de; SOARES, Sérgio. Desafios de Compliance da LGPD: Implantação na Indústria de Software Brasileira. *Washes*, 2024. DOI: <https://doi.org/10.5753/washes.2024.3079>. Acesso em: 5 dez. 2024. DURÃO, Fernando. *Proteção de dados: desafios e tendências para 2024*. Estadão. Disponível em: https://www.estadao.com.br/tipo_conteudo/analise/protecao-de-dados-desafios-e-tendencias-para-2024/. Acesso em: 5 dez. 2024. BUCCO, Rafael. 5 anos de LGPD: sociedade aponta desafios dos próximos anos. *Telesintese*, 2024. Disponível em: <https://telesintese.com.br/5-anos-de-lgpd-sociedade-aponta-desafios-dos-proximos-anos/>. Acesso em: 5 dez. 2024.

²⁶ Em um relatório publicado em 2021, por exemplo, o Tribunal de Contas da União (TCU) constatou que 76,7% das organizações públicas federais permaneciam nos graus inexpressivo ou inicial de adequação à LGPD. Uma nova rodada de fiscalização, prevista para 2024, ainda não teve seus resultados publicados. Ver: TRIBUNAL DE CONTAS DA UNIÃO. *TCU verifica risco alto à privacidade de dados pessoais coletados pelo governo*. TCU, 2024. Disponível em: <https://portal.tcu.gov.br/im-prensa/noticias/tcu-verifica-risco-alto-a-privacidade-de-dados-pessoais-coletados-pelo-governo>. Acesso em: 5 dez. 2024.

maior de conformidade com a lei, Estados e, principalmente, Municípios frequentemente enfrentam dificuldades significativas.²⁷ Esses desafios incluem limitações orçamentárias, falta de infraestrutura tecnológica adequada e escassez de pessoal qualificado²⁸ em proteção de dados.

Ainda, em que pese o maior nível de adequação em nível Federal, destaca-se haver uma necessidade de atenção para ações do Executivo, que possui menor nível de ações em relação à implementação da LGPD do que o Poder Legislativo e Judiciário. A pesquisa “Privacidade e Proteção de Dados Pessoais 2023”, do Comitê Gestor da Internet no Brasil, demonstra que, dentre os órgãos do Executivo, mais da metade sequer chegou a implementar quaisquer medidas de adequação à LGPD²⁹. A mesma pesquisa demonstra a necessidade de que órgãos públicos garantam atenção adequada para a implementação de planos de resposta a incidentes de segurança da informação relacionados a dados pessoais, garantindo a existência de medidas técnicas e administrativas capazes de minimizar riscos de incidentes ou reagir à possíveis incidentes de segurança identificados³⁰, em conformidade com o Capítulo VII, “Da Segurança e Boas Práticas”, da LGPD.

A ausência de políticas padronizadas e de coordenação eficaz entre os diferentes níveis governamentais agrava a situação, resultando em uma aplicação fragmentada e insuficiente das normas de proteção de dados pessoais no setor público³¹. Essa realidade evidencia a necessidade de estratégias mais abrangentes, inclusivas, robustas e integradas para promover a governança de dados em todas as esferas governamentais.

No setor privado, o cenário também é de grande variedade. Grandes empresas, principalmente aquelas que atuam em setores altamente regulados, como setores financeiro,³² exibem maior

²⁷ Sobre a situação nos Estados e nos Municípios, confira-se, por exemplo, as situações dos Estados de Rondônia, Santa Catarina e Rio de Janeiro, respectivamente, ver: TRIBUNAL DE CONTAS DO ESTADO DE RONDÔNIA (TCE-RO). *TCE apresenta resultado de ações para implementação da LGPD nos municípios de Rondônia*. Disponível em: <https://tcero.tc.br/2024/11/01/tce-apresenta-resultado-de-aco-es-para-implementacao-da-lgpd-nos-municipios-de-rondonia/>. Acesso em: 10 dez. 2024; TRIBUNAL DE CONTAS DO ESTADO DO PARANÁ (TCE-PR). *TCE-PR audita adequação à LGPD em órgãos de administração e previdência do estado*. Disponível em: <https://www1.tce.pr.gov.br/noticias/tce-pr-audita-adequacao-a-lgpd-em-orgaos-de-administracao-e-previdencia-do-estado/11495/N>. Acesso em: 10 dez. 2024; TRIBUNAL DE CONTAS DO ESTADO DO RIO DE JANEIRO (TCE-RJ). *TCE aponta risco à privacidade de dados pessoais processados pelos municípios jurisdicionados*. 2023. Disponível em: https://www.tcerj.tc.br/portalnovo/noticia/tce_aponta_risco_a_privacidade_de_dados_pessoais_processados_pelos_municipios_jurisdicionados. Acesso em: 10 dez. 2024.

²⁸ INSTITUTO RUI BARBOSA. *LGPD: Recomendações de segurança da informação para municípios de pequeno porte*. Disponível em: <https://irbcontas.org.br/artigos/lgpd-recomendacoes-de-seguranca-da-informacao-para-municipios-de-pequeno-porte/>. Acesso em: 11 dez. 2024.

²⁹ NIC.br; CETIC.br, 2024a, *op. cit.*, p. 89.

³⁰ A existência efetiva de um Plano de Conformidade é mais presente em órgãos do Judiciário (60%), em comparação ao Executivo (29%), Legislativo (38%) e Ministério Público (32%). NIC.br; CETIC.br, 2024, *op. cit.*, p. 89.

³¹ Apesar da existência de normas e regulamentos para a conformidade no setor público, a implementação de ações de privacidade e proteção de dados ocorre de forma independente entre os diferentes níveis de governo, especialmente em entidades estaduais. Ver: NIC.br; CETIC.br, 2024a, *op. cit.*, p. 86.

³² GODOI, Everton. *Proteção de dados e governança: o papel da LGPD no setor financeiro*. TI Inside, 24 out. 2024. Disponível em: <https://tiinside.com.br/24/10/2024/protecao-de-dados-e-governanca-o-papel-da-lgpd-no-setor-financeiro/>. Acesso em: 10 dez. 2024.

maturidade na implementação de medidas de proteção de dados, impulsionados por atuação no âmbito internacional, por vezes, no mercado europeu, regulamentações anteriores e pelo impacto reputacional³³ que possíveis violações podem causar

Por outro lado, pequenas empresas³⁴ frequentemente não conseguem arcar com os custos dessas adaptações e enfrentam dificuldades relevantes na adequação à LGPD,³⁵ especialmente na proteção de dados pessoais sensíveis. Essa disparidade e a falta de uniformidade na governança de dados também pode ocorrer entre diferentes segmentos econômicos. Poucas empresas brasileiras integram políticas de proteção de dados em suas estratégias de governança, refletindo uma percepção limitada da proteção de dados como um princípio ético ou diferencial competitivo,³⁶ vendo-a apenas como um requisito legal³⁷, e não como um instrumento de garantia de direitos. A proteção de dados, de qualquer sorte, ainda não se tornou uma questão prioritária no contexto brasileiro.

No campo tecnológico, a infraestrutura obsoleta de muitas organizações, públicas e privadas, representa um grande obstáculo à implementação de medidas modernas de segurança, como pseudonimização (criptografia) e anonimização de dados, ou processos e procedimentos de transparência adequados. Simultaneamente, o aumento na sofisticação dos ataques cibernéticos expõe outra vulnerabilidade: muitas organizações carecem de recursos financeiros e humanos para investir em tecnologias adequadas de mercado que garantam a segurança dos dados pessoais armazenados e processados, porém a segurança da informação não tem apenas como pilar o aparato tecnológico, é fundamental que ações como treinamentos e orientações de práticas seguras no trabalho como os acessos e seus níveis, formas de autenticação como senhas e segundo fator e compartilhamento de informações sensíveis.

Por fim, a criação de uma cultura organizacional voltada à proteção de dados é tão importante quanto os investimentos tecnológicos. Isso inclui treinamentos regulares para colaboradores, auditorias frequentes e o estabelecimento de planos de resposta a incidentes. Combinando tecnologia, processos bem definidos e conscientização humana, as organizações podem mitigar riscos e fortalecer sua resiliência contra ameaças cibernéticas em um cenário cada vez mais complexo e sofisticado.

³³ MARCONDES, Lucélia Bastos Gonçalves. A privacidade como diferencial competitivo. *Migalhas*, 2023. Disponível em: <https://www.migalhas.com.br/depeso/379597/a-privacidade-como-diferencial-competitivo>. Acesso em: 11 dez. 2024.

³⁴ NIC.br; CETIC.br, 2024a, *op. cit.*, p. 71-72.

³⁵ ESTEVES, Maurício Brum. Jornada da Adequação à LGPD: os três maiores desafios. *Migalhas*, 2021. Disponível em: <https://www.migalhas.com.br/depeso/357267/jornada-da-adequacao-a-lgpd-os-tres-maiores-desafios>. Acesso em: 11 dez. 2024.

³⁶ FATTORI, Marcelo. A urgência da governança em proteção de dados nas empresas brasileiras. *Fattori*, 10 out. 2024. Disponível em: <https://fattori.com.br/2024/10/10/a-urgencia-da-governanca-em-protecao-de-dados-nas-empresas-brasileiras/>. Acesso em: 11 dez. 2024.

³⁷ FERRAZ, Paula; SIROTHEAU, Débora. A importância da conscientização sobre a proteção dos dados pessoais. *Consultor Jurídico*, 2021. Disponível em: <https://www.conjur.com.br/2021-out-02/opiniao-conscientizacao-protecao-dados-pessoais/>. Acesso em: 11 dez. 2024.

1.3. Educação em Matéria de Proteção de Dados Pessoais

A educação em matéria de proteção de dados pessoais é fundamental para melhorar o panorama atual. Ela engloba iniciativas destinadas a informar, a instruir e a preparar indivíduos e as organizações para lidar adequadamente com dados pessoais, assegurando a privacidade e a segurança das informações conforme as exigências legais e éticas.³⁸ É elementar também para que os cidadãos possam se proteger de possíveis abusos de controladores, aprender a reivindicar, de forma autônoma, os seus direitos e lidar com seus próprios dados de forma crítica, garantindo uma cultura de proteção de dados pessoais alinhada ao pleno desenvolvimento da pessoa humana, como preconiza o art. 205 da Constituição Federal.³⁹ Os desafios relacionados à educação em proteção de dados pessoais estão profundamente enraizados em aspectos culturais, éticos, técnicos e estruturais, além de serem influenciados por desigualdades socioeconômicas e regionais.

1.3.1. Conscientização

A conscientização em proteção de dados pessoais se refere ao processo de informar e de sensibilizar indivíduos e organizações sobre a importância da privacidade, da segurança das informações pessoais, dos aspectos culturais e econômicos da produção e proteção de dados, das dimensões técnicas, éticas e objetivas da existência de um dado e das dimensões subjetivas que atravessam o imaginário popular e senso comum.

Envolve a divulgação de conceitos fundamentais, tais como: os riscos associados ao tratamento inadequado de dados pessoais, os direitos e as obrigações estabelecidos pela LGPD, as infraestruturas necessárias para que um dado seja produzido, tratado e armazenado e os principais atores envolvidos nesses processos. Se o principal objetivo de um plano de ação é a criação de uma cultura que valorize a proteção de dados pessoais, promovendo atitudes proativas e responsáveis entre todos os envolvidos, os titulares de dados devem ser a sua base.⁴⁰

³⁸ A própria ANPD entende que medidas educativas são essenciais para a promoção da proteção de dados no Brasil. Em sendo assim, em janeiro de 2024, a entidade divulgou o seu Plano Institucional de Ações Educativas, contendo orientação e procedimentos para o fortalecimento da proteção de dados pessoais no país. Ver: BRASIL. Autoridade Nacional de Proteção de Dados. *ANPD divulga Plano Institucional de Ações Educativas*. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-plano-institucional-de-acoes-educativas>.

³⁹ CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO (CNMP). Nos seis anos da LGPD, conselheiro do CNMP destaca que o Brasil possui uma norma preocupada em proteger um direito fundamental do cidadão: os dados pessoais. Disponível em: <https://www.cnmp.mp.br/portal/todas-as-noticias/17774-nos-seis-anos-da-lgpd-conselheiro-do-cnmp-destaca-que-o-brasil-possui-uma-norma-preocupada-em-protetor-um-direito-fundamental-do-cidadao-os-dados-pessoais>. Acesso em: 11 dez. 2024.

⁴⁰ Note-se que este entendimento é compartilhado pela ANPD, que no seu Plano Institucional de Ações Educativas, evidencia os titulares como centro das suas atividades. Ver: BRASIL. Autoridade Nacional de Proteção de Dados. *ANPD divulga Plano Institucional de Ações Educativas*. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-plano-institucional-de-acoes-educativas>. Acesso em: 5 fev. 2025.

No Brasil, a conscientização sobre os direitos previstos na LGPD ainda enfrenta grandes desafios. Uma parcela significativa da população sequer conhece a existência desse direito⁴¹ e, entre aqueles que têm conhecimento, poucos compreendem sua extensão e os instrumentos jurídicos e administrativos disponíveis para sua proteção. Embora brasileiros demonstrem preocupação com o uso indevido de seus dados pessoais, a atenção nacional é mais centrada nos possíveis danos financeiros decorrentes do uso indevido de dados e poucos sabem efetivamente como se proteger, fazer valer seus direitos ou exercer prerrogativas como o acesso, a correção e o controle do uso de suas informações pessoais.⁴² Cabe destacar que a própria referência da ANPD enquanto órgão responsável pela matéria de proteção de dados pessoais no Brasil é frágil no imaginário da população, sendo o órgão menos procurado pela população na formalização de notificações sobre o tema.⁴³

A falta de entendimento, de letramento e de conscientização limita a capacidade dos cidadãos de prevenir, de identificar e de reagir às violações ao direito fundamental à proteção de dados,⁴⁴ deixando-os vulneráveis às estratégias e às práticas danosas. Isso perpetua um ambiente permissivo para abusos, dificultando o exercício dos direitos previstos na LGPD, a participação ativa na fiscalização do uso de seus dados e, por fim, impossibilitando o exercício da cidadania digital. Ademais, a disseminação de informações sobre proteção de dados pessoais tem se concentrado em áreas urbanas e entre públicos especializados, criando um fosso de entendimento em regiões periféricas e rurais.

Portanto, sem campanhas e iniciativas educativas eficazes, permanentes e acessíveis, inclusive acerca do letramento algorítmico, o tema permanece distante para grande parte da população, dificultando a construção de uma cultura que valorize a privacidade e promova o uso responsável dos dados pessoais no país. Percebe-se, em vista disso, a urgência em encetar uma agenda nacional que oportunize um debate que, de modo inclusivo, atraia, engaje e sensibilize todos os extratos da população.

1.3.2. Capacitação

A capacitação diz respeito ao treinamento técnico, ético, jurídico e, em particular, no que concerne ao desenvolvimento de habilidades específicas necessárias para a implementação efetiva das

⁴¹ Uma pesquisa da Kaspersky, divulgada em novembro de 2023, revelou, por exemplo, que 20% dos brasileiros não têm qualquer conhecimento sobre a LGPD. KASPERSKY. *Pesquisa da Kaspersky revela que 20% dos brasileiros não tem conhecimento sobre a LGPD*. 2023. Disponível em: <https://www.kaspersky.com.br/about/press-releases/pesquisa-da-kaspersky-revela-que-20-dos-brasileiros-nao-tem-conhecimento-sobre-a-lgpd>. Acesso em: 11 dez. 2025.

⁴² NIC.br; CETIC.br, 2024a, op. cit., p. 28.

⁴³ Dentre os canais de atendimento mais buscados para tratar de questões relativas a seus dados pessoais, estima-se que o brasileiro busca a própria empresa ou órgão público (80%), sites de reclamação relativos à direito do consumidor como ReclameAqui e Consumidor.org (69%), órgãos de defesa do consumidor, como Procon (51%), a polícia (40%), a justiça (40%) e o Ministério Público (37%) com maior recorrência do que a ANPD (35%). Os dados apontam para cenário de subnotificação em relação à Autoridade, possivelmente devido ao desconhecimento de suas competências e funções e, ainda, apontam para a importância de parcerias estratégicas com órgãos, em especial, do Sistema Nacional do Consumidor e das áreas de justiça e segurança pública. Ver: NIC.br; CETIC.br, 2024a, op. cit., p. 54.

⁴⁴ No seu relatório anual, a Verizon revelou que 68% das violações de dados ocorridas em 2024, como *ransomware* e *phishing*, teve pelo menos um componente humano envolvido. Ver: VERIZON BUSINESS. *2024 Data Breach Investigations Report*. Verizon. Disponível em: <https://www.verizon.com/business/resources/reports/dbir/>. Acesso em: 11 dez. 2024.

práticas em proteção de dados. Inclui a instrução detalhada sobre o quadro normativo, incluindo, interpretação e manejo da legislação, dos procedimentos, das ferramentas e das metodologias para cumprir os parâmetros constitucionais, os requisitos legais e regulatórios. A capacitação habilita os profissionais, mas, sobretudo, as pessoas em geral, a executar tarefas como a realização de avaliações de impacto, relatórios de impacto de risco, gestão de incidentes de segurança, manutenção de sistemas de proteção, desenvolvimento de metodologias de transparência e de comunicação. Enquanto a conscientização busca gerar sensibilização, entendimento e comprometimento geral, a capacitação fornece conhecimentos e competências técnicas para a aplicação prática das medidas de proteção de dados.

No que diz respeito à formação profissional em proteção de dados pessoais, as lacunas são evidentes. As disciplinas de proteção de dados ainda não estão amplamente incorporadas nos currículos escolares ou universitários, dificultando a formação de uma nova geração de profissionais cientes de seus deveres. Além disso, embora haja uma grande oferta de cursos, públicos e privados, sobre diversos aspectos teóricos e práticos do direito à proteção de dados pessoais, a incipiente sistematização dessa disciplina pode levar à incorporação de conceitos e de práticas estrangeiras, que necessitam de adaptação para congruência com o ordenamento jurídico brasileiro e para a aplicação contextual de acordo com a realidade nacional. No que diz respeito ao setor público e às empresas de micro/pequeno/médio porte, embora instituições como a Escola Nacional de Administração Pública (ENAP) e entidades do Sistema S (SENAI, SENAC) promovam valiosos treinamentos, respectivamente, sua abrangência ainda é limitada em comparação à demanda por profissionais qualificados na proteção à privacidade e à proteção de dados.

Ademais, entende-se a importância de que os trabalhadores que estão envolvidos na produção de tecnologias digitais, como desenvolvedores de aplicações, processadores de dados, *designers* de usabilidade, desenvolvedores de produtos e implementadoras de infraestrutura, além de serem sensibilizados e conscientizados quanto à relevância da garantia de direitos do titular de dados, também tenham capacidade técnica e autonomia para aplicar as melhores práticas para que os dispositivos da LGPD sejam atendidos de forma integral e adequada.

Comparativamente, apesar de o Brasil ter avançado ao adotar uma legislação abrangente como a LGPD, sua implementação prática ainda está aquém de países europeus como Alemanha e França. Pode-se inferir, em princípio, que a diferença reflete a ausência de uma estrutura consolidada para oportunizar a capilaridade e a escalabilidade do tema, bem como para monitorar adequadamente a efetividade das políticas de proteção de dados e a falta de relatórios periódicos de impacto, práticas comuns em jurisdições mais maduras. Esses fatores apontam para a necessidade de maior articulação e de investimento para consolidar a proteção de dados pessoais como elemento estratégico no país.

2. Desafios

O desenvolvimento do direito à proteção de dados pessoais enfrenta uma miríade de desafios que vão além da simples adequação legal. Desde o modelo de negócio das empresas, até o dia a dia das pessoas. A conscientização e a capacitação em matéria de proteção de dados são fundamentais

para garantir que os indivíduos e as organizações, inclusive os agentes do Poder Público, compreendam a sua proeminência e saibam como proteger os dados pessoais. Importa ainda, nessa altura, reconhecer a persistência do vácuo referente às possibilidades de convergência entre o escopo da LAI e da LGPD o que gera insegurança e imaturidade no processo de consolidação de um sistema de proteção de dados. Nesta seção, serão analisados os principais desafios para um projeto nacional de educação e de capacitação em proteção de dados pessoais, destacando suas implicações e os possíveis caminhos para superação.

2.1. Mudança de Cultura

Um dos principais desafios é promover uma mudança cultural em relação à importância da proteção de dados pessoais, tanto na sociedade quanto nas organizações.⁴⁵ No Brasil, a privacidade e a proteção de dados não receberam historicamente a mesma atenção que em outros países, refletindo-se na falta de atenção generalizada para com o compartilhamento de informações pessoais. Muitas vezes, indivíduos e organizações não compreendem os riscos associados ao tratamento inadequado de dados, dificultando a adoção de práticas adequadas.⁴⁶ Apesar de alguns avanços já se tornarem evidentes, a população brasileira, de modo geral, não está consciente da necessidade de observar e de controlar o modo como ocorrem os fluxos informacionais, razão pela qual não tem atentado e nem resistido à coleta, ao monitoramento e ao compartilhamento inadequados.

Uma prova da ausência de informação, foi o caso da *Tools for Humanity* que coletou dados biométricos de brasileiros para finalidade não muito clara. Do ponto de vista ético, o uso comercial de dados biométricos, dados sensíveis, levanta preocupações quanto à desigualdade digital e à vulnerabilidade de populações em situação de maior necessidade econômica. A compensação oferecida pode ser interpretada como uma forma de exploração, especialmente se as informações sobre os riscos e os direitos dos titulares não forem adequadamente comunicadas. Mais de 1 milhão de brasileiros já baixaram o *World App*, aplicativo que inclui uma carteira de criptoativos para armazenamento do WLD e da identidade digital dos usuários. Desse total, 500 mil se submeteram ao processo.

Importa lembrar que a ANPD havia emitido uma medida preventiva proibindo a *Tools for Humanity* de oferecer incentivos financeiros aos cidadãos brasileiros que aderissem à World Network. A Autoridade determinou que o procedimento de coleta de dados biométricos não precisaria ser interrompido até a conclusão das investigações, mas suspendeu a distribuição de incentivos financeiros de aproximadamente R\$700,00, efetuados por meio da criptomoeda *Worldcoin* (WLD). A Coordenação-Geral de Fiscalização da ANPD entendeu que a compensação financeira por meio de criptomoedas

⁴⁵ DAMÁSIO. *LGPD: quais os desafios enfrentados pelo Brasil na sua aplicação*. 2023. Disponível em: <https://blog.damasio.com.br/lgpd-quais-os-desafios-enfrentados-pelo-brasil-na-sua-aplicacao>. Acesso em: 5 dez. 2025. e DRUMOND, Thomaz Carneiro. LGPD e os desafios no setor público: uma necessária virada cultural. *Conjur*, 2022. Disponível em: <https://www.conjur.com.br/2022-out-05/thomaz-drumond-lgpd-desafios-setor-publico/>. Acesso em: 10 dez. 2025.

⁴⁶ REIS, Rafael. Os desafios da implementação da LGPD em empresas brasileiras. *Becker Direito Empresarial*, 2024. Disponível em: <https://www.direitoempresarial.com.br/os-desafios-da-implementacao-da-lgpd-em-empresas-brasileiras>. Acesso em: 11 dez. 2024.

pode interferir na livre manifestação de vontade dos indivíduos, especialmente em casos de vulnerabilidade social e econômica.⁴⁷ Tem-se, portanto, que vulnerabilidades socioeconômicas do contexto nacional podem influir em uma percepção transacional de dados pessoais, negociados pelo titular a partir da perspectiva de compensação econômica direta pelo compartilhamento de dados, sem clareza sobre riscos.

Outro ponto relevante é que estima-se que 58% dos brasileiros sempre ou quase sempre concordam com as Políticas de Privacidade sem realizar sua leitura e que apenas 24% da população com mais de 16 anos de idade já buscou canais de atendimento para solicitações, reclamações ou denúncias em relação aos seus dados pessoais, sendo este número ainda menor para mulheres (22%) em relação aos homens (27%) e menor para aqueles que possuem Ensino Médio (22%) ou Fundamental (23%) completo comparado com os que possuem Ensino Superior (29%)⁴⁸.

Nas organizações, especialmente em empresas e órgãos públicos, há uma tendência a tratar a proteção de dados pessoais como uma obrigação legal a ser cumprida minimamente, em vez do cumprimento de um dever constitucionalmente previsto e de um valor intrínseco ou de diferencial competitivo. Muitos agentes públicos e privados ainda enxergam dados pessoais como meros recursos mercantilizáveis, priorizando interesses econômicos e organizacionais em detrimento dos direitos dos titulares. Essa mentalidade limita o engajamento dos agentes envolvidos no processo de tratamento dos dados, a implementação de políticas efetivas de proteção de dados e a incorporação de medidas de segurança nos processos e decisões estratégicas.

A mudança cultural exige tempo, esforços contínuos e recursos aplicados à educação e à sensibilização sobre o tema, bem como aplicação de medidas efetivas de *enforcement*. É necessário desenvolver campanhas de conscientização para informar sobre os princípios, as bases legais, os direitos e as responsabilidades estabelecidas pela LGPD, promovendo a valorização da privacidade e, sobretudo, da proteção dos dados pessoais como direitos fundamentais. Indispensável, nesse caso, estabelecer uma agenda nacional dinâmica, engajando os extratos populacionais, na qual a proteção de dados seja um ponto nuclear para a ação conjunta dos agentes públicos e particulares, dispondo, sobretudo, acerca do cumprimento do rol dos deveres e das obrigações que são decorrentes do reconhecimento desse direito fundamental.

2.2. Complexidade do Tema

A proteção de dados pessoais é um tema complexo que envolve aspectos jurídicos, éticos, tecnológicos, organizacionais, dentre outros. A LGPD, por sua vez, introduziu novos conceitos e obrigações para a maioria das organizações, exigindo conhecimentos especializados e interdisciplinares. Essa complexidade dificulta a compreensão geral do tema, tanto por parte dos profissionais responsáveis quanto dos titulares dos dados.

⁴⁷ JOBIM, Caio. World mantém compensações em criptomoedas a usuários brasileiros por meio de recurso encaminhado à ANPD. *Cointelegraph*, 2025. Disponível em: <<https://br.cointelegraph.com/news/world-upholds-cryptocurrency-compensation-for-brazilian-users-in-appeal-to-anpd>>. Acesso em: 03 fev. 2025.

⁴⁸ NIC.br; CETIC.br, 2024a, op. cit., p. 27.

Muitas organizações carecem de pessoal qualificado para lidar com as exigências legais e técnicas de proteção de dados. A interpretação das bases legais para o tratamento de dados, a realização de avaliações de impacto e a implementação de medidas de segurança adequadas requerem expertise nem sempre disponível. Além disso, a rápida evolução tecnológica, as constantes atualizações nas práticas de cibersegurança, a consolidação de bases de dados massivas por empresas e órgãos públicos e vazamentos dessas bases tornam o tema ainda mais desafiador.

As organizações precisam acompanhar as tendências e ter consciência quanto às ameaças emergentes, exigindo investimentos contínuos em capacitação e na atualização de conhecimentos. Sem uma compreensão clara e atualizada da complexidade envolvida, as medidas de proteção podem ser insuficientes ou inadequadas. De fato, a proteção de dados pessoais no atual cenário implica em estratégias de ação em rede, na qual tanto o poder público quanto o setor privado devem agir em sinergia, sob pena de não se alcançar os objetivos almejados.

2.3. Desigualdade Econômica

A desigualdade entre diferentes agentes e setores econômicos também representa um desafio. Setores que já lidam com regulamentações rigorosas, como os setores financeiro e de telecomunicações, possuem maior sensibilidade quanto à importância da segurança da informação, relacionamento com titulares de dados, canais de transparência, políticas de privacidade mais criteriosas e, por isso, tendem a estar mais avançados na implementação de práticas de proteção de dados. Da mesma forma, grandes conglomerados ou gigantes do atacado e do varejo têm condições muito mais propícias, notadamente recursos financeiros e humanos, para realização de investimento em capacitação e infraestrutura adequada.

Em contraste, os agentes de micro, pequeno e médio porte, mesmo lidando com variadas quantidades de dados pessoais e sensíveis, muitas vezes não possuem a mesma capacidade de investimento ou não priorizam a proteção de dados em suas estratégias. Normalmente, os aportes financeiros necessários para a adequação à LGPD, somados a outros desafios como tempo e esforço com treinamento, interesse em obter o conhecimento e a necessária mudança de cultura que vem por derivação desses investimentos, acabam sendo desafiadores diante da priorização de implementação de medidas tidas como mais urgentes, por terem relação com a respectiva sobrevivência econômica no curto prazo. Esses agentes acabam postergando indefinidamente a adoção dessas medidas, sem compreender os benefícios a longo prazo. Essa desigualdade econômica cria um ambiente em que a proteção de dados é inconsistente, com áreas críticas ficando vulneráveis.

Quanto a isso, ressalta-se que, em 2023, apenas 25% das empresas brasileiras declararam possuir área específica ou funcionários responsáveis pelo tema de proteção de dados pessoais, número estável desde 2021. Esses números são significativamente mais reduzidos para empresas pequenas (22%) em relação às médias (43%) e grandes (56%) mas, ainda assim, demonstram uma falta

de estrutura de governança consolidada geral para tratar do tema de proteção de dados pessoais no setor econômico brasileiro⁴⁹.

Ainda, apenas 35% das empresas brasileiras realizam reuniões internas sobre proteção de dados pessoais. Há uma disparidade entre pequenas (32%), médias (55%) e grandes (73%) empresas, além de uma queda na realização dessa atividade entre as médias (de 59% em 2021 para 55% em 2023) e grandes empresas (de 73% em 2021 para 65% em 2023)⁵⁰. Nesse sentido, além da atenção para desigualdades econômicas e para a capacidade de estruturação de atividades de governança efetivas para implementação da LGPD em relação às empresas pequenas e médias, é necessário incentivo contínuo para práticas de monitoramento, atualização e continuidade por grandes empresas, buscando o incentivo à uma cultura de proteção de dados pessoais perene e duradoura.

Destaca-se, ainda, que treinamentos e capacitações pela matéria são, em sua maior parte, promovidos pela estrutura interna das próprias empresas⁵¹, havendo pouca adesão de treinamentos oferecidos pelo governo e por agentes econômicos de todos os portes - possível janela de oportunidades para disseminação de ações já existentes que contemplem as necessidades de pequenas empresas sem acarretar ônus financeiro inexequível.

2.4. Tecnologia e Infraestrutura

A infraestrutura tecnológica é um componente essencial para a proteção de dados, mas muitas organizações no Brasil operam com sistemas obsoletos, desatualizados ou inadequados⁵². A falta de investimento e conhecimento em tecnologias básicas e modernas impede a implementação de medidas de diferentes níveis de complexidade como as de segurança e prevenção,⁵³ como criptografia robusta, sistemas de detecção de intrusões e técnicas de pseudonimização e anonimização de dados, mas também de atualização de sistemas, transparência, livre acesso e prestação de contas como portal de acesso ao titular de dados e tecnologias que permitam também a comunicação constante e de qualidade com as pessoas. Além disso, a falta de interoperabilidade entre sistemas modernos e antigos dificulta o cumprimento dos requisitos de transparência e portabilidade da LGPD.

⁴⁹ NIC.br; CETIC.br, 2024a, op. cit., p. 73.

⁵⁰ NIC.br; CETIC.br, 2024a, op. cit., p. 72.

⁵¹ NIC.br; CETIC.br, 2024a, op. cit., p. 75.

⁵² Estima-se que 97% das empresas de Pequeno e Médio porte no setor nacional estejam vulneráveis a ataques cibernéticos devido à falta de recursos para manter equipe dedicada à segurança cibernética e ao uso de soluções tecnológicas desatualizadas ou improvisadas, ampliando a exposição a riscos de incidentes de segurança. Dentre os setores mais vulneráveis, destacam-se escritórios de advocacia, clínicas médicas, hospitais, oficinas e hotéis, que costumam tratar dados sensíveis. Ver: TI INSIDE. 97% das PMEs estão mais vulneráveis a ataques cibernéticos, estima o grupo Ivy. *TI Inside*. 28 jan. 2025. Disponível em: <https://tiinside.com.br/28/01/2025/97-das-pmes-estao-mais-vulneraveis-a-ataques-ciberneticos-estima-grupo-ivy/>. Acesso em: 1 fev. 2025. Ver também: DINO. Uso de sistemas legados é motivo de alerta em empresas. *Valor Econômico*, 2024. Disponível em: <https://valor.globo.com/patrocinado/dino/noticia/2024/05/09/uso-de-sistemas-legados-e-motivo-de-alerta-em-empresas.ghtml>. Acesso em: 5 fev. 2025.

⁵³ REIS, Rafael. Os desafios da implementação da LGPD em empresas brasileiras. Becker Direito Empresarial, 2024. Disponível em: <https://www.direitoempresarial.com.br/os-desafios-da-implementacao-da-lgpd-em-empresas-brasileiras>. Acesso em: 11 dez. 2024.

Especialmente no setor público, nota-se uma falta de disponibilização de portais para o exercício de direitos de titulares de dados pessoais do cidadão, mais contundente ainda na área da saúde⁵⁴. Ainda, o uso de sistemas antigos e desatualizados no âmbito da administração municipal pode torná-la mais vulnerável a ataques cibernéticos, e a falta de atualizações e manutenção adequada aumenta os riscos⁵⁵. A migração para tecnologias mais modernas, adequadas e seguras pode ser custosa e complexa, exigindo planejamento e investimento que nem sempre estão priorizados ou disponíveis.

O cenário é agravado pelo aumento na sofisticação dos ataques cibernéticos. Hackers utilizam técnicas avançadas para explorar vulnerabilidades, e sem uma infraestrutura adequada, as organizações não conseguem se defender efetivamente. A título de exemplo, o Brasil é o sétimo país do mundo mais afetado por ataques de sequestro de dados (*ransomwares*)⁵⁶, principal alvo de ataques da América Latina e estima-se que o país esteja sujeito a 1.379 ataques cibernéticos por minuto, com um prejuízo estimado de 71.4 bilhões de reais por ano⁵⁷. Isso não só coloca em risco os dados pessoais, mas também a continuidade dos negócios e a confiança dos consumidores.

2.5. Falta de Incentivos Governamentais

A ausência de incentivos governamentais robustos para promover a conscientização e a capacitação em proteção de dados é outro desafio significativo. Embora a LGPD estabeleça obrigações legais, faltam políticas públicas que apoiem as organizações na implementação das exigências, especialmente para aquelas com recursos limitados.⁵⁸ A própria ANPD conta com orçamento insuficiente para atender à demanda de fiscalização, capacitação e regulamentação necessárias para o desenvolvimento adequado da proteção de dados.

⁵⁴ Menos da metade das prefeituras municipais oferecem canal de atendimento para exercício de direitos dos titulares no Brasil. Tem-se também uma falta de Canais de Atendimento para o titular de dados no setor da saúde, presente em apenas 17% das Unidades Básicas de Saúde (UBS), principal forma de entrada da população mais vulnerável socioeconomicamente ao sistema de saúde, com uma diferença significativa entre os estabelecimentos das capitais (24%) e de cidades do interior (16%). Ver: NIC.br; CETIC.br, 2024a, op. cit., p. 54 e 95.

⁵⁵ Há casos de incidentes de segurança na administração pública pelo uso de sistemas obsoletos ou desatualizados, denotando falhas em Políticas de Segurança da Informação e exposição a riscos. Ver: CAMBORIÚ NEWS. Site da prefeitura de BC é invadido por hacker que cobra resgate. *Camboriú News*, 30 jan. 2025. Disponível em: <https://camboriu.news/site-da-pre-feitura-de-bc-e-invadido-por-hacker-que-cobra-resgate/>. Acesso em: 5 fev. 2025. Ver também: OLIVEIRA, Mariana. Falta de infraestrutura e capacitação são desafios para criação de cidades inteligentes no Brasil. *O Globo*, 16 maio 2024. Disponível em: <https://oglobo.globo.com/mundo/g20-no-brasil/noticia/2024/05/16/falta-de-infraestrutura-e-capacitacao-sao-desafios-para-criacao-de-cidades-inteligentes-no-brasil.ghtml>. Acesso em: 5 fev. 2025.

⁵⁶ O relatório Relatório “The State of Cybersecurity”. da Check Point Software Technologies Ltd aponta que a técnica de extorsão por ameaça de vazamento de dados é a mais usada nessa modalidade de ataque, que atinge, principalmente, os setores de serviço, varejo, manufatura e saúde. Ver: CHECK POINT SOFTWARE TECHNOLOGIES. *Cyber Security Report 2024*. 2024. Disponível em: <https://www.checkpoint.com/resources/report-3854/report--cyber-security-report-2024>. Acesso em 4 fev 2025.

⁵⁷ KASPERSKY. *Panorama de Ameaças na América Latina 2024*. 2024. Disponível em: <https://www.kaspersky.com.br/blog/panorama-ameacas-latam-2024/22888/>. Acesso em: 4 fev 2025.

⁵⁸ QUEIROZ, Luiz. A necessária promoção da educação em proteção de dados. *Capital Digital*, 2024. Disponível em: <https://capitaldigital.com.br/a-necessaria-promocao-da-educacao-em-protecao-de-dados/>. Acesso em: 11 fev. 2025.

A conscientização, capacitação e adoção de práticas adequadas poderiam ser estimuladas por programas de subsídios, incentivos fiscais ou linhas de crédito para investimentos em tecnologia, notadamente para micro e pequenas empresas. Além disso, iniciativas governamentais para oferecer ferramentas digitais, treinamentos e materiais educativos ajudariam a disseminar o conhecimento e a importância da privacidade. O baixo suporte governamental mina a capacidade das organizações de se adequarem à LGPD, perpetuando um ciclo de conformidade superficial e falta de accountability.

2.6. Desigualdades estruturais da realidade brasileira e públicos vulneráveis

Os desafios relativos à educação em proteção de dados no Brasil estão profundamente conectados às questões estruturais relacionadas aos desafios da educação formal e para a fruição de direitos no Brasil. Em primeiro lugar, tem-se que apenas 54,5% da população do Brasil com 25 anos ou mais concluíram o Ensino Básico completo⁵⁹, tendo atingido-se recorde nacional em evasão escolar no ano de 2023, sendo os dois principais fatores para evasão a necessidade de trabalhar para complementar a renda familiar e a falta de interesse⁶⁰. As taxas de evasão escolar são mais elevadas nas regiões Norte e Nordeste em comparação ao Sudeste, Sul e Centro-Oeste⁶¹.

Conforme demonstram os dados do Programa Internacional de Avaliação de Estudantes (Pisa), de 2022, o Brasil possui baixo desempenho nas categorias “Leitura” (52º lugar dos 81 países participantes do ranking internacional) e na categoria “Ciências” (62º lugar)⁶². O analfabetismo funcional atinge 12,3% da população⁶³, que possui dificuldades para ler textos e aplicar conceitos, o que impacta negativamente a própria apreensão de noções de direitos e empoderamento do cidadão enquanto titulares de dados⁶⁴. A realidade nacional também é marcada por um déficit de leitura, estimando-se que apenas 52% dos brasileiros têm o costume de ler e, nesse contexto, que entre 2019 e 2023, o país perdeu 6.7 milhões de leitores⁶⁵.

Constata-se, ainda, que os dados do cenário nacional demonstram um panorama de adoecimento mental dos professores da Educação Básica. 21,5% professores brasileiros classificam a própria

⁵⁹ IBGE – INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. *PNAD Contínua – Educação 2023: Informativo*. Rio de Janeiro: IBGE, 2024. p. 1. Disponível em: https://biblioteca.ibge.gov.br/visualizacao/livros/liv102068_informativo.pdf. Acesso em

⁶⁰ VIECELI, Leonardo. 1 em cada 5 jovens do país abandona escola antes de concluir educação básica. *Folha de São Paulo*, 2024. Disponível em: <https://www1.folha.uol.com.br/educacao/2024/12/1-em-cada-5-jovens-do-pais-abandona-escola-antes-de-concluir-educacao-basica.shtml>. Acesso em: 5 fev. 2025.

⁶¹ IBGE, 2024, op. cit., p. 9.

⁶² O Pisa deve também passar a avaliar competências digitais em suas próximas edições.

⁶³ INEP – INSTITUTO NACIONAL DE ESTUDOS E PESQUISAS EDUCACIONAIS ANÍSIO TEIXEIRA. *Relatório do quinto ciclo de monitoramento das metas do Plano Nacional de Educação*. Brasília, DF: INEP, 2024. Disponível em: https://download.inep.gov.br/publicacoes/institucionais/plano_nacional_de_educacao/relatorio_do_quinto_ciclo_de_monitoramento_das_metas_do_plano_nacional_de_educacao.pdf. Acesso em: 5 fev. 2025.

⁶⁴ As taxas refletem desigualdades regionais e etárias, com índices mais elevados nas regiões Norte, Nordeste e Centro-Oeste. IBGE, 2024, op. cit., p. 2.

⁶⁵ INSTITUTO PRÓ-LIVRO. *Retratos da Leitura no Brasil – 2024*. 2024. Disponível em: https://www.prolivro.org.br/wp-content/uploads/2024/11/Apresentac%C3%A7%C3%A3o_Retratos_da_Leitura_2024_13-11_SITE.pdf. Acesso em:

saúde mental como “ruim” ou “muito ruim”⁶⁶ e 71% dos professores da escola pública do Brasil sentem-se estressados no trabalho⁶⁷. O país também conta com índices elevados de professores que são afastados da rede pública de ensino em razão de transtornos mentais e comportamentais⁶⁸, atrelados ao enfrentamento de desafios como sobrecarga e desvalorização da profissão⁶⁹ - fatores que devem ser considerados no desenho e na implementação de Políticas Públicas, considerando suporte material, humano e financeiro para os educadores nacionais.

Os desafios nacionais relativos à qualidade da educação brasileira atingem, diretamente, a população nacional em múltiplas competências - incluindo no exercício de direitos enquanto titulares de dados e na capacitação para atuar com a matéria. No que diz respeito à proteção de seus dados pessoais, o cenário nacional revela um aumento de golpes digitais, como de clonagem de cartão, fraude na Internet e invasão de contas, associado a um baixo letramento digital das vítimas e à baixa capacidade do Estado em investigar as ocorrências e garantir a responsabilização⁷⁰. Esse tipo de golpe tende a prejudicar parcela da população já vulnerável socioeconomicamente, o que também explica o fato de a maior preocupação dos brasileiros quanto aos seus dados pessoais estar relacionado a golpes, fraudes ou roubos de identidade⁷¹. Tem-se, ainda, que golpes digitais são mais comuns de serem praticados contra idosos e mulheres⁷², havendo uma tendência de subnotificação às autoridades públicas⁷³.

Por fim, destaca-se que desigualdades históricas, econômicas e estruturais demandam olhares transversais para iniciativas de educação, de capacitação e de conscientização na matéria de proteção de dados pessoais. De acordo com levantamento do Ministério de Educação, dos 2.3 milhões de discentes sem infraestrutura mínima escolar, 86% são pretos, pardos ou indígenas. Das 100 escolas mais pobres do país, 100% delas são majoritariamente negras e não dispõem de quadra de esportes, biblioteca, tampouco laboratório de informática. Tem-se, também, que os índices de evasão escolares são maiores entre a população preta e parda (71,6%) em relação à população branca (27,4%), bem

⁶⁶ LYRA, Thaís. Pesquisa revela que saúde mental dos professores piorou em 2022. *Nova Escola*, 2022. Disponível em: <https://novaescola.org.br/conteudo/21359/pesquisa-revela-que-saude-mental-dos-professores-piorou-em-2022>. Acesso em: 5 fev. 2025.

⁶⁷ TODOS PELA EDUCAÇÃO. *Pesquisa com professores: resultados nacionais*. 2023. Disponível em: <https://todospelaeducacao.org.br/wordpress/wp-content/uploads/2023/02/pesquisa-com-professores-resultados-nacionais-todos-ip-is-pd.pdf>. Acesso em: 5 fev. 2025.

⁶⁸ MOUHAMAD, Letícia; SARAIVA, Mariana. Afastamentos acendem alerta para saúde mental nas escolas públicas. *Correio Braziliense*, 2024. Disponível em: <https://www.correiobraziliense.com.br/cidades-df/2024/03/6826783-afastamentos-acendem-alerta-para-saude-mental-nas-escolas-publicas.html>. Acesso em: 2 fev. 2025.

⁶⁹ ÁVILA, Lucas. Saúde mental dos educadores. *Revista Educação*, 2023. Disponível em: <https://revistaeducacao.com.br/2023/05/22/saude-mental-educadores/>. Acesso em: 5 fev. 2025.

⁷⁰ FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. *Anuário Brasileiro de Segurança Pública 2024*. 2024. Disponível em: <https://forumseguranca.org.br/wp-content/uploads/2024/07/anuario-2024.pdf>. Acesso em: 3 fev. 2025.

⁷¹ NIC.br; CETIC.br, 2024a, op. cit., p. 57.

⁷² AGÊNCIA BRASIL. *Golpes pela internet aumentam contra a população idosa*. 2024. Disponível em: <https://agenciabrasil.ebc.com.br/radioagencia-nacional/direitos-humanos/audio/2024-06/golpes-pela-internet-aumentam-contra-populacao-idosa>. Acesso em: 5 fev. 2025.

⁷³ CNN BRASIL. *Datafolha: país tem mais de 45 mil tentativas de golpe financeiro por hora*. 2024. Disponível em: <https://www.cnnbrasil.com.br/nacional/datafolha-pais-tem-mais-de-45-mil-tentativas-de-golpe-financeiro-por-hora/>. Acesso em: 5 fev. 2025.

como a população preta e parda possui uma desigualdade de acesso generalizado ao Ensino Superior em relação à população branca⁷⁴.

Diante desse cenário, percebe-se que a educação em proteção de dados no Brasil não pode ser dissociada do enfrentamento das desigualdades estruturais que afetam a qualidade do ensino e a garantia de direitos no país. As dificuldades de acesso à educação básica, os altos índices de evasão escolar, o déficit de leitura e a vulnerabilidade digital demonstram que a capacitação da população para lidar com a proteção de seus dados pessoais enfrenta desafios significativos. Além disso, o impacto do adoecimento mental dos professores e a precarização da infraestrutura escolar reforçam a necessidade de políticas públicas que contemplem não apenas a inclusão da proteção de dados no currículo escolar, mas também prevejam melhorias estruturais na educação como um todo. Sem iniciativas concretas e transversais que reduzam as desigualdades educacionais e promovam o letramento digital, a população brasileira seguirá vulnerável às ameaças cibernéticas e à exclusão digital, o que reforça a urgência de investimentos em formação, conscientização, valorização da educação e dos educadores e acesso à informação como pilares fundamentais para o exercício pleno da cidadania no mundo digital.

2.7. Desafios Especiais para a Proteção Integral de Crianças e Adolescentes

O público de crianças e adolescentes possui uma presença assídua no ambiente digital, tendo o primeiro acesso de forma cada vez mais precoce. Dados da pesquisa TIC Kids Online (2024) mostram que 93% das crianças e adolescentes de 9 a 17 anos utilizam a internet, e a idade do primeiro acesso é em média 6 anos. 83% deste público declara possuir perfis em redes sociais - ainda que, muitas vezes, essas redes prevejam, em seus Termos de Uso, restrição etária por pessoas com menos de 13 anos de idade⁷⁵. Tal qual é construído hoje, o ambiente digital não é sensível às necessidades especiais dessas pessoas que vivenciam um período peculiar de desenvolvimento biopsicossocial. Se os Termos de Privacidade e de Uso de aplicações online não são amigáveis para a compreensão razoável de um adulto médio, são ainda menos adequados para que uma criança ou adolescente compreenda os riscos e as condições de tratamento de seus dados pessoais, embora seja um direito explícito garantido pelo art. 14, §6º da LGPD e no art. 5, LXXIX da Constituição da República.

O uso de aplicações inadequadas para a faixa etária, além de afetar o desenvolvimento de crianças e adolescentes, expondo-os aos riscos consideráveis, pode implicar em coleta e tratamento ilegítimos de seus dados pessoais - em especial, de seus dados comportamentais para fins de direcionamento de conteúdos orgânicos e pagos. Ainda, expõe o público infantil a riscos relevantes no que diz respeito à exposição indevida de suas informações pessoais, vazamento de fotografias e de informações sensíveis ou contato com adultos e pessoas mal-intencionadas.

⁷⁴ OBSERVATÓRIO DA BRANQUITUDE. *A cor da infraestrutura escolar: diferenças entre escolas brancas e negras*. 2024. Disponível em: <https://observatoriobranquitude.com.br/a-cor-da-infraestruturura-escolar-diferencas-entre-escolas-brancas-e-negras/>. Acesso em:

⁷⁵ CETIC.br. *Resumo Executivo* - Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil - TIC Kids Online Brasil 2023. Disponível em: https://cetic.br/media/docs/publicacoes/2/20240913122405/resumo_executivo_tic_kids_online_2023.pdf. Acesso em: 5 fev. 2025.

Problemas de privacidade e a proteção da intimidade de crianças e adolescentes são mais graves com tecnologias emergentes, como a geração de imagens sintéticas de abuso e exploração sexual via IA generativa. Esse conteúdo ilegal e abusivo, muitas vezes compartilhado entre pares, está entre os fatores que explicam um número recorde de denúncias à Central Nacional de Crimes Cibernéticos em 2023⁷⁶. Também, de acordo com dados do Canal de Ajuda da organização SaferNet Brasil, destinado a apoiar crianças e adolescentes em matérias de direitos digitais, a principal demanda reportada no canal é, justamente, de problemas relacionados aos dados pessoais (212 atendimentos), seguidas de exposição de imagens íntimas (183 atendimentos), fraudes, golpes e e-mails falsos (161 atendimentos) e *cyberbullying* (115 atendimentos), denotando uma necessidade de uma educação básica que apoie, efetivamente, uma cultura de resiliência, de conscientização e de proteção de dados pessoais entre os mais jovens⁷⁷.

Ressalte-se ainda que, com a pandemia do Covid-19, houve uma tendência de digitalização e de acesso ainda mais precoce, por este público, às aplicações digitais, fato que aumenta o volume e a complexidade de dados deste público que são tratados por uma rede diversa de controladores⁷⁸. Em que pese a responsabilidade das famílias, educadores e cuidadores de zelar pela proteção de dados pessoais de crianças e adolescentes, muitas vezes os adultos também não possuem a capacidade ou os conhecimentos técnicos e jurídicos para compreender e tomar decisões bem-informadas sobre atividades de tratamento de dados pessoais, a forma como os dados são tratados e o impacto dessas atividades em curto, médio e longo prazo⁷⁹.

Mesmo que crianças e adolescentes não sejam usuárias diretas de uma aplicação digital, o funcionamento das redes faz com que seja possível uma exposição indevida de suas informações pessoais sem sua ciência ou consentimento. É o caso, por exemplo, do *sharenting*, fenômeno em que familiares e responsáveis legais realizam o compartilhamento excessivo de informações e de registros audiovisuais de crianças e adolescentes, expondo-os a possíveis riscos e danos.

É necessário destacar, também, o avanço do uso de tecnologias no âmbito da educação básica, também acelerada no contexto de isolamento social da pandemia. Em 2023, 61% das escolas estaduais e gestores declararam usar plataformas educacionais digitais, como o *Google Classroom*,

⁷⁶ AGÊNCIA BRASIL. *Exploração sexual infantil na internet bate recorde em 2023*. Agência Brasil, 5 fev. 2024. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2024-02/exploracao-sexual-infantil-na-internet-bate-recorde-em-2023>. Acesso em: 5 fev. 2025.

⁷⁷ SAFERNET BRASIL. *Helpline: visualização de indicadores*. Disponível em: <https://indicadores.safernet.org.br/helpline/helplineviz/helpchart-page.html>. Acesso em: 5 fev. 2025.

⁷⁸ A série histórica de dados da pesquisa TIC Kids Brasil demonstra uma redução da idade de primeiro acesso à Internet do brasileiro, que ocorria predominantemente na faixa etária de 10-12 anos até 2020 e passou a ocorrer, predominantemente, antes dos 6 anos de idade a partir de 2021. CETIC.br – CENTRO DE ESTUDOS SOBRE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO. Indicador A3 - Crianças e Adolescentes, por idade do primeiro acesso à internet. Disponível em: https://data.cetic.br/explore/?pesquisa_id=13&unidade=Crian%C3%A7as%20e%20Adolescentes. Acesso em: 5 fev. 2025.

⁷⁹ Dados apontam que 73% das redes municipais de ensino não possuem área ou equipe específica dedicada ao planejamento e à implementação de ações para tecnologias digitais, tendo a região Norte o melhor índice nacional. Em 55% da rede municipal, não há profissionais dedicados a garantir equipamentos, serviços e informações sobre o uso de tecnologias digitais nas unidades de ensino. Ver: UNDIME. *Relatório do 5º ciclo de monitoramento das metas do Plano Nacional de Educação – 2024*. Disponível em: https://undime.org.br/uploads/documentos/phpIWgA0C_64622c469d0ff.pdf. Acesso em: 5 fev. 2025.

evidenciando uma permanência do uso de plataformas virtuais de aprendizagem⁸⁰ sem a devida diligência e cuidado.

Atualmente, o principal critério para a escolha de uma plataforma educacional por gestores escolares da rede pública é a gratuidade da aplicação (69%), superior aos outros critérios relevantes como adequação ao currículo e aos objetivos de aprendizagem (63%), acessibilidade e adequação às necessidades de alunos com deficiências (62%), avaliação e aprovação por professores (59%), adoção de medidas de proteção de dados e da identidade digital dos alunos (58%), minimização da coleta de dados pessoais (44%) ou licença aberta ou livre (36%)⁸¹. A necessidade de gratuidade atrelada às insuficiências de recurso disponíveis pode privilegiar a contratação de aplicações aparentemente gratuitas, mas cujo modelo de negócios baseia-se na coleta e no uso secundário de dados de estudantes para fins comerciais, em oposição à garantia de tratamento de dados no melhor interesse dos estudantes, preconizada no art. 14, *caput* da LGPD.

Ainda no que se refere aos desafios, destaca-se haver uma assimetria entre o poder das escolas e dos gestores escolares em relação às empresas provedoras de tecnologias educacionais. Muitas vezes, contratos padrão assimétricos permitem às empresas a coleta e o tratamento de grandes volumes de dados, indicando uma premente necessidade de capacitação adequada dos gestores escolares para tomada de decisões sobre a implementação de uma tecnologia que garanta, de fato, a proteção de dados pessoais da comunidade escolar. Por sua vez, os dados coletados por este tipo de aplicação, muitas vezes, atendem aos interesses privados da empresa fornecedora e não são disponíveis para a própria comunidade escolar, que deles poderiam beneficiar-se a partir de perspectivas de gestão cidadã de dados e para “analisar mais profundamente os processos de ensino e de aprendizagem e de gestão das instituições, de forma a aprimorar a garantia do direito de acesso à educação para os estudantes”.⁸²

Ressalte-se que outra matéria de preocupação, no âmbito da educação, está relacionada à expansão de tecnologias de coleta de dados biométricos no ambiente escolar. Em que pese apenas 1% das escolas públicas mencionarem usar sistema de identificação pela digital ou palma da mão e 4% mencionarem usar sistema de reconhecimento facial, a proporção é significativamente maior para escolas localizadas nas regiões Sul (12%) e Centro-Oeste (7%), com destaque para os Estados de Goiás (28%) e Paraná (17%)⁸³. Trata-se, aqui, da coleta e do tratamento de dados de caráter extremamente

⁸⁰ NIC.br; CETIC.br, 2024a, op. cit., p. 99.

⁸¹ Em 2023, a pesquisa “Brasil: ferramentas de educação online coletam dados de crianças”, promovida pela Human Rights Watch, evidenciou que plataformas educacionais privadas adotadas pelo setor público estariam monitorando e compartilhando dados de navegação de crianças e adolescentes com parceiros privados para fins de direcionamento de publicidade, havendo, neste caso, um grande indício de desvio de finalidade das atividades de tratamento de dados e de um tratamento invisível realizado por meio de rastreadores ocultos - fato que dificulta, ainda mais, a possibilidade de agência de indivíduos e responsáveis. HUMAN RIGHTS WATCH. *Brazil: Online Learning Tools Harvest Children's Data*. 2023. Disponível em: <https://www.hrw.org/pt/news/2023/04/03/brazil-online-learning-tools-harvest-childrens-data#:~:text=A%20inves-tiga%C3%A7%C3%A3o%20conduzida%20pela%20Human,de%20rastreamento%20projetadas%20para%20publicidade>. Acesso em: 22 jan. 2025.

⁸² NIC.br; CETIC.br, 2024a, op. cit., p. 100.

⁸³ NIC.br; CETIC.br, 2024a, op. cit., p. 101.

sensível, sendo *softwares* de reconhecimento facial reconhecidos pela existência de vieses e discriminação algorítmica de pessoas negras.

Outro aspecto desafiador está atrelado ao uso de tecnologias de biometria facial e de IA para fiscalizar e monitorar comportamentos e emoções dos alunos. Tal é o caso ‘*Educatron*’, tecnologia implementada em 1.7 mil escolas da rede pública pela Secretaria de Educação do Paraná, em 2023⁸⁴. Em um projeto piloto de implementação, a tecnologia buscava monitorar a atenção e a dispersão de alunos para medir a qualidade das aulas e o foco. Esse tipo de uso disseminado, entretanto, pode gerar riscos consideráveis que vão desde o uso comercial dos dados obtidos, à pouca eficiência e acurácia notável de ferramentas de reconhecimento de emoções, até à sensação de vigilância e monitoramento invasivo nos estudantes⁸⁵.

3. Coleta de Subsídios

Delimitado o escopo dos trabalhos e identificados os principais desafios à promoção da educação em matéria de proteção de dados no país, este GT buscou identificar iniciativas, boas práticas e sugestões que possam embasar a formulação de estratégias para o seu desenvolvimento. Nessa etapa, foi mapeado o maior número possível de ações relevantes, implementadas ou meramente idealizadas, que, devido ao seu potencial, possam servir de fonte de inspiração ou possam ser incorporadas na política pública a ser formulada pela ANPD.

O trabalho iniciou-se pela análise do Plano Institucional de Ações Educativas da ANPD para o biênio 2024/25, aproveitou o conhecimento acumulado pelo GT2 da primeira composição do CNPD (que tinha objeto bastante semelhante), mapeou práticas já implementadas e bem-sucedidas nos setores público, privado e no terceiro setor, e, por fim, coletou sugestões de especialistas (por meio de consulta pública) e de entidades da sociedade civil que atuam em matéria de educação em proteção de dados. Diante disso, ao final, pretende-se apresentar um panorama abrangente que sirva como base para recomendações futuras, promovendo uma abordagem inclusiva e bem fundamentada para a conscientização e capacitação em proteção de dados pessoais.

3.1. Plano Institucional de Ações Educativas da ANPD

No dia 18 de janeiro de 2024, a própria ANPD publicou o seu “Plano Institucional de Ações Educativas”, por meio do qual buscava promover a cultura de proteção de dados pessoais no país e difundir conhecimento acerca das normas e das políticas públicas relacionadas ao tema.⁸⁶ As ações

⁸⁴ AUDI, Amanda. *Reconhecimento facial no Paraná impõe monitoramento de emoções em escolas*. Agência Pública, out. 2023. Disponível em: <https://apublica.org/2023/10/reconhecimento-facial-no-parana-impoe-monitoramento-de-emocoes-em-escolas/>. Acesso em: 5 fev. 2025.

⁸⁵ TAVARES, Clarice; SIMÃO, Bárbara; MARTINS, Fernanda K.; SANTOS, Blenda; ARAÚJO, Anna Martha. *Educação na mira: a vigilância e o tratamento de dados pessoais nas escolas*. InternetLab, jun. 2023. Disponível em: https://internetlab.org.br/wp-content/uploads/2023/06/Educacao-na-mira-PT_06.pdf. Acesso em: 5 jan. 2025.

⁸⁶ BRASIL. Autoridade Nacional de Proteção de Dados. *ANPD divulga Plano Institucional de Ações Educativas*. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-plano-institucional-de-aco-es-educativas>. Acesso em: 5 fev. 2025.

previstas no documento⁸⁷ eram abrangentes, contemplando uma variedade de ações, que podem ser agrupadas da seguinte forma:

Eixo 1: Parcerias

- Desenvolver parceria com o MEC para promoção da cultura de proteção de dados pessoais.
- Aproximar-se, produzir e revisar conteúdos da ENAP para capacitação de servidores públicos.

Eixo 2: Webinários e Seminários

- Realizar webinário sobre compartilhamento de dados no poder público para servidores públicos.
- Realizar webinário sobre tratamento de dados pessoais de crianças e adolescentes.
- Realizar evento em comemoração ao aniversário da LGPD.
- Realizar webinário em parceria com o Sebrae sobre segurança da informação para agentes de tratamento de pequeno porte.

Eixo 3: Produção de Conteúdo

- Produzir e divulgar material sobre Regulamento de Direito dos Titulares.
- Produzir e divulgar material sobre Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais.
- Produzir e divulgar material sobre Regulamento de Encarregado de Tratamento de Dados.
- Produzir e divulgar conteúdos sobre o Guia Orientativo sobre Tratamento em Larga Escala.
- Elaborar material educativo sobre temas prioritários vinculados ao processo de fiscalização.
- Produzir e divulgar conteúdos sobre Cookies.

Eixo 4: Celebrar Datas Comemorativas

- Dia Internacional de Proteção de Dados (28/01)
- Aniversário da LGPD (14/08).
- Dia da Informática (15/08)
- Dia Nacional do Idoso (01/10)
- Dia das Crianças (12/10)

⁸⁷ No total, foram previstas 25 ações para o ano de 2024.

- Aniversário da ANPD (06/11)

Eixo 5: Desenvolvimento da sua Plataforma

- Criar página no site da ANPD para os titulares de dados.
- Atualizar a seção de Perguntas Frequentes da ANPD.

3.2. Relatório da 1ª Composição do CNPD

Note-se, diante de sua relevância, que este não foi o primeiro GT instituído pelo CNPD para coleta de subsídios e apresentação de propostas na matéria objeto do presente relatório.⁸⁸ Por meio da Portaria CNPD n. 2, de 1º de abril de 2022, o CNPD instituiu o Grupo de Trabalho 2 (GT2), formado por alguns conselheiros da primeira sua composição⁸⁹ e dedicado à proposição de ações educativas e fomento à cultura de proteção de dados e da privacidade. O objetivo principal do GT2 era desenvolver estratégias para disseminar o conhecimento sobre proteção de dados pessoais e privacidade para a população em geral, alinhando-se com uma das atribuições fundamentais do CNPD.⁹⁰

A análise e aproveitamento, no que for possível, do trabalho anteriormente realizado pelo mencionado GT2 é mais do que importante: é fundamental. De fato, a falta de continuidade do trabalho produzido por grupos subsequentes sobre o mesmo objeto pode gerar diversos problemas significativos. A *uma*, há o risco de perda de conhecimento acumulado e memória institucional, levando à repetição de esforços e desperdício de recursos. A *duas*, a falta de comunicação do novo relatório com o anterior pode resultar em reversão de prioridades e metas, causando confusão e ineficiência na implementação de políticas e projetos. A *três*, essa descontinuidade também pode levar à descrença e desmotivação por parte dos conselheiros e *stakeholders* envolvidos, uma vez que o trabalho anterior pode vir a ser desconsiderado ou subutilizado. A *quatro*, a possível fragmentação de informações dificulta a tomada de decisões embasadas e o acompanhamento do progresso ao longo do tempo. A *cinco* e por fim, a falta de continuidade mínima entre relatórios pode comprometer a credibilidade e eficácia das iniciativas, prejudicando a confiança dos *stakeholders* e a capacidade de alcançar objetivos de longo prazo.

As propostas educativas e de cultura de privacidade presentes nos documentos produzidos pelo mencionado GT2 tinham como objetivo central a promoção da conscientização social sobre a proteção de dados pessoais e a privacidade no Brasil. Essas iniciativas foram abrangentes, destacando-se, a seguir, as principais:

⁸⁸ Registra-se, aqui, o agradecimento especial à ex-conselheira Patrícia Peck, que gentilmente forneceu a este GT todo o material produzido pelo GT2 da primeira composição do CNPD.

⁸⁹ O GT2 era composto pelos seguintes Conselheiros: *Patrícia Peck Garrido Pinheiro* (coordenadora), *Bruno Ricardo Bioni*, *Cláudio Eduardo Lobato Abreu Rocha*, *Cláudio Simão de Lucena Neto*, *Hartmut Richard Glaser*, *Michele Nogueira Lima* e *Taís Carvalho Serralva*.

⁹⁰ Portaria CNPD n. 2, de 1º de abril de 2022. Não foi possível localizar este documento na internet. Registre-se, aqui, mais uma vez, o agradecimento à ex-conselheira Patrícia Peck por ceder cópia do referido documento.

- Criação do Dia Nacional da Proteção de Dados Pessoais, com o intuito de estabelecer um marco anual para debates e ações voltadas à conscientização sobre a importância da privacidade. Além disso, foram identificadas outras datas relevantes para campanhas educativas, como o Dia Internacional da Proteção de Dados (28 de janeiro) e o Dia Mundial do Backup (31 de março), que buscam sensibilizar a população para temas específicos relacionados à segurança digital e à proteção de informações.
- Elaboração e disseminação de materiais educativos. A proposta incluía tanto a criação de conteúdos inéditos quanto a indexação e a disponibilização de materiais já existentes nos setores público e privado. Esses recursos seriam acessíveis por meio de um Portal Educacional ou Biblioteca Virtual no site do CNPD, concebido como um repositório digital para informações sobre privacidade e proteção de dados.
- Formação de parcerias institucionais, especialmente com o Ministério da Educação. O objetivo seria inserir conteúdos sobre proteção de dados nos currículos escolares e promover audiências públicas para discutir e ampliar a relevância do tema. Paralelamente, sugeriu-se a criação de cursos específicos para capacitar agentes públicos sobre a proteção de dados no exercício de suas funções, reforçando a disseminação de boas práticas em diversos níveis da administração pública.
- Realização de eventos nacionais e internacionais, com foco em reunir especialistas para debater melhores práticas e desenvolver estratégias de comunicação eficazes. Essas iniciativas buscam engajar não apenas a sociedade civil, mas também o setor privado e o poder público em uma abordagem integrada.
- Reversão de recursos provenientes de multas aplicadas pela ANPD em iniciativas educativas. Essa abordagem visaria garantir a sustentabilidade financeira de ações voltadas à promoção da cultura de privacidade e proteção de dados no país.
- Criação de um subdomínio específico para o CNPD no portal da ANPD, onde seriam centralizadas informações e campanhas educativas. Também foi sugerida a publicação de conteúdos regulares em redes sociais e canais oficiais, com linguagem acessível e atrativa, para alcançar o maior público possível.
- No que diz respeito especificamente ao tratamento de dados de crianças e adolescentes, foi proposta (a) a elaboração de enunciados que orientem o tratamento de dados pessoais de crianças e adolescentes, construídos com base nos resultados da consulta pública e nos estudos da ANPD e (b) criação de materiais de conscientização voltados especificamente ao público infantil e juvenil, promovendo a educação desde cedo, por meio de materiais adequados à faixa etária e a inclusão de temas nos currículos escolares.

3.3. Iniciativas Relevantes

A identificação de iniciativas bem-sucedidas nas áreas pública, privada e do terceiro setor é fundamental para a construção de um plano nacional eficaz sobre proteção de dados pessoais. Essas iniciativas servem como exemplos práticos que demonstram a viabilidade de estratégias e de abordagens que promovem a conscientização e a capacitação em relação à proteção de dados. Ao analisar o que já foi realizado, é possível extrair lições valiosas e adaptar práticas que se mostraram eficazes em diferentes contextos, garantindo que o plano nacional seja embasado em experiências concretas.

Além disso, essas iniciativas podem proporcionar *insights* sobre as necessidades e os desafios enfrentados por diferentes segmentos da sociedade. Ao compreender como organizações de diversos setores abordam a educação em proteção de dados, é possível identificar lacunas no conhecimento e áreas que requerem maior atenção. Essa análise permite que o plano nacional seja mais inclusivo e direcionado, atendendo às especificidades de cada público-alvo, desde empresas até cidadãos comuns.

Por fim, a colaboração entre os setores público, privado e terceiro setor é essencial para o sucesso de um plano nacional sobre proteção de dados pessoais. A troca de experiências e boas práticas não apenas enriquece o debate, mas também fortalece a rede de apoio e engajamento em torno da proteção de dados. Essa sinergia pode resultar em campanhas mais abrangentes e eficazes, além de fomentar uma cultura de respeito à privacidade e à segurança da informação em toda a sociedade.

Durante as suas atividades, o GT1 mapeou e analisou diversas iniciativas por todo o Brasil em matéria de educação, de conscientização e de capacitação em proteção de dados. Dentre as iniciativas analisadas, algumas merecem destaque, a saber:

3.3.1. Plano Institucional de Ações Educativas

O Plano Institucional de Ações Educativas da ANPD representa um marco significativo na estratégia de promoção da cultura de proteção de dados pessoais no Brasil. Lançado em janeiro de 2024, o documento traduz o compromisso institucional de estimular o conhecimento sobre normas e políticas públicas relacionadas ao tratamento de dados, com uma abordagem abrangente e multifacetada.

Concebido para alcançar diferentes segmentos da sociedade, o plano contempla 25 atividades que dialogam com diversos públicos, desde estudantes até profissionais de diferentes setores. Entre suas iniciativas mais relevantes estão a realização de eventos técnicos, o desenvolvimento de materiais instrutivos, a produção de conteúdos específicos para grupos vulneráveis como crianças, adolescentes e idosos, e parcerias estratégicas com instituições educacionais, como o Ministério da Educação.

O documento não apenas prevê ações educativas, mas também busca promover transparência e empoderamento dos cidadãos. Destaca-se a criação de uma página dedicada aos titulares de dados no site da ANPD, a elaboração de material explicativo sobre processos de fiscalização e o Concurso de Monografias Danilo Doneda, que visa estimular a produção acadêmica sobre proteção de dados. Essas iniciativas refletem o compromisso da Autoridade em construir uma cultura nacional de

proteção de dados, fundamentada no conhecimento, na transparência e no respeito aos direitos individuais.

3.3.2. Política Nacional de Educação Digital (PNED)

A Política Nacional de Educação Digital (PNED)⁹¹ consiste em uma iniciativa crucial do governo brasileiro, estabelecida pela Lei nº 14.533/2023, que busca transformar o cenário educacional do país por meio da integração de tecnologias digitais. Esta política abrangente visa não apenas promover o uso de ferramentas digitais no ensino, mas também garantir que todos os cidadãos, especialmente aqueles em situação de vulnerabilidade, tenham acesso a recursos e práticas digitais essenciais para o mundo contemporâneo.

No cerne da PNED estão objetivos ambiciosos que incluem a promoção da inclusão digital em todos os níveis educacionais, o aprimoramento da qualidade do ensino por meio do uso eficaz de tecnologias, a preparação dos estudantes para as demandas do mercado de trabalho do século XXI e a capacitação de professores e gestores escolares para utilizarem eficientemente as tecnologias digitais em suas práticas pedagógicas. Para alcançar esses objetivos, a política se estrutura em quatro eixos fundamentais: Inclusão Digital, Educação Digital Escolar, Capacitação e Especialização Digital, e Pesquisa e Desenvolvimento em Tecnologias da Informação e Comunicação.

A implementação da PNED prevê uma série de ações concretas e inovadoras. Entre elas, destacam-se a promoção de competências digitais, midiáticas e informacionais; o treinamento específico em habilidades digitais, com foco especial em grupos vulneráveis; o desenvolvimento de ferramentas para autoavaliação de competências digitais; a criação de processos de certificação nessas competências; a implantação de infraestrutura de conectividade nas escolas; e a formação continuada de professores e gestores para o uso efetivo de tecnologias digitais no ambiente escolar. Essas iniciativas visam não apenas modernizar o sistema educacional brasileiro, mas também preparar a população para os desafios e oportunidades da era digital, promovendo assim uma sociedade mais inclusiva e tecnologicamente capacitada.

3.3.3. Estratégia Brasileira de Educação Midiática

A Estratégia Brasileira de Educação Midiática (EBEM)⁹² é um importante documento elaborado pela Secretaria de Comunicação Social da Presidência da República (SECOM), que reúne uma série de iniciativas do Governo Federal voltadas para a promoção da educação midiática entre a população brasileira. Essa estratégia tem como principais objetivos conscientizar a sociedade sobre a

⁹¹ BRASIL. *Lei nº 14.533, de 11 de janeiro de 2023*. Dispõe sobre o regime jurídico de proteção de dados pessoais no Brasil e outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Lei/L14533.htm. Acesso em: 5 dez. 2024.

⁹² BRASIL. Secretaria de Comunicação Social (SECOM). *Estratégia Brasileira de Educação Midiática*. 1ª versão, 2023. Disponível em: https://www.gov.br/secom/pt-br/assuntos/noticias/2023/10/estrategia-brasileira-de-educacao-midiatica-apresenta-as-politicas-publicas-voltadas-para-a-populacao/2023_secom-spdigi_estrategia-brasileira-de-educacao-midiatica.pdf. Acesso em: 5 dez. 2024.

relevância da educação midiática e da cultura digital para a cidadania e para a democracia, além de qualificar profissionais da educação e multiplicadores que atuam nesse campo.

Um dos focos da EBEM é promover o ensino e a aprendizagem de habilidades que permitam uma leitura crítica e participativa das mídias. Para isso, o documento foi construído a partir de uma consulta pública que recebeu mais de 400 contribuições, refletindo a diversidade de opiniões e experiências do país. A estratégia está alinhada com a Base Nacional Comum Curricular e com a Política Nacional de Educação Digital, buscando integrar essas abordagens no sistema educacional brasileiro.

Entre as ações previstas pela EBEM, destaca-se a formação de 300 mil educadores e 400 mil trabalhadores da saúde, com o intuito de combater a desinformação. Além disso, a estratégia propõe iniciativas para incorporar a educação midiática nos currículos escolares e incentivar a criação de conteúdos que reflitam a diversidade cultural e social do Brasil. Dessa forma, a EBEM busca capacitar pessoas de todas as idades para compreender, analisar e produzir conteúdo de forma crítica na era digital, promovendo uma sociedade mais informada e participativa.

3.3.4. Educação Conectada

O Programa de Inovação Educação Conectada⁹³ é uma iniciativa do Ministério da Educação (MEC) que visa transformar o cenário educacional brasileiro por meio da integração de tecnologias digitais. Lançado em 2017 e posteriormente transformado em política pública pela Lei nº 14.180 de 2021, o programa tem como objetivo principal apoiar a universalização do acesso à internet de alta velocidade e fomentar o uso pedagógico de tecnologias digitais na educação básica.

O programa se estrutura em quatro dimensões complementares: visão, formação, recursos educacionais digitais e infraestrutura. Suas ações incluem a preparação do ambiente escolar para receber conexão de internet, capacitação de professores para utilizar novos conteúdos educacionais e proporcionar aos alunos o contato com tecnologias educacionais inovadoras.

A implementação do programa foi planejada em três fases: indução (2017-2018), expansão (2019-2021) e sustentabilidade (2022-2024). O objetivo final é alcançar 100% dos alunos da educação básica, transformando o programa em uma política pública permanente de inovação e educação conectada. Para isso, o MEC trabalha em parceria com estados, municípios e o Distrito Federal, oferecendo apoio técnico e financeiro para a aquisição de equipamentos, contratação de serviços de internet e desenvolvimento de recursos educacionais digitais.

Além da conectividade, o programa também engloba iniciativas como a Plataforma Integrada de Recursos Educacionais Digitais (MEC RED) e a plataforma AVAMEC para cursos a distância. Essas ferramentas visam enriquecer o processo de ensino-aprendizagem e preparar os estudantes para os desafios do século XXI, promovendo a inclusão digital e o uso consciente e pedagógico das tecnologias na educação básica brasileira.

⁹³ BRASIL. Ministério da Educação. *Educação Conectada*. Disponível em: <https://educacaoconectada.mec.gov.br/o-programa/sobre>. Acesso em: 5 dez. 2024.

3.3.5. Resolução n. 245 do CONANDA

O Conselho Nacional dos Direitos da Criança e do Adolescente (Conanda) publicou, em 5 de abril de 2024, a Resolução 245⁹⁴, que dispõe sobre a promoção e a proteção dos direitos de crianças e adolescentes no ambiente digital.

A resolução dá vazão à garantia dos direitos da criança e do adolescente com absoluta prioridade no Brasil, prevista no artigo 227 da Constituição Federal e faz uma leitura sistemática do arcabouço legal do país para o ambiente digital, notadamente o Estatuto da Criança e do Adolescente (ECA), o Marco Legal da Primeira Infância, o Código de Defesa do Consumidor (CDC), o Marco Civil da Internet, a Lei Geral de Proteção de Dados Pessoais (LGPD), além da própria Carta Magna.

A norma também considerou os conteúdos do Comentário Geral 25 sobre os direitos de crianças e adolescentes no ambiente digital e do Comentário Geral 14 sobre o melhor interesse de crianças e adolescentes, ambos emanados pelo Comitê dos Direitos da Criança da ONU, em consonância com a Convenção sobre os Direitos da Criança da ONU, que possui status constitucional no país (Decreto 99.710/90).

O Conselho estabeleceu, por meio da resolução, a necessidade da criação de uma política nacional de proteção dos direitos da criança e do adolescente no ambiente digital, a ser desenvolvida e coordenada pela Secretaria Nacional dos Direitos da Criança e do Adolescente do Ministério dos Direitos Humanos e da Cidadania e pelo próprio Conanda. No que tange à educação e à proteção de dados, compete à política: “a promoção do uso equilibrado e positivo de equipamentos digitais, manutenção e fortalecimento de vínculos familiares e comunitários, inclusão digital, cultura de proteção de dados e educação midiática”. Ainda prevê, em conformidade com o ordenamento jurídico vigente, que empresas publiquem relatórios, ao menos anuais, acerca “de esforços envidados para educação e promoção de direitos e uso consciente, saudável e responsável dos ambientes e serviços digitais”.

Nesse sentido, e em demais dispositivos da norma, há o intuito do conselho de efetivar a noção da responsabilidade compartilhada pela garantia dos direitos de crianças e adolescentes ao determinar que o poder público, as famílias e toda a sociedade, incluindo as empresas provedoras de produtos e serviços digitais, devem zelar por esta garantia também no ambiente digital.

3.3.6. Estratégia Brasileira de Transformação Digital (E-Digital)

A Estratégia Brasileira para a Transformação Digital (E-Digital), instituída pelo decreto 9.319 de 21 de março de 2018, é uma iniciativa coordenada pelo Ministério da Ciência, Tecnologia e Inovação. De acordo com o próprio MCTI, a E-Digital visa promover a harmonização das iniciativas do Executivo Federal ligadas ao ambiente digital, com o objetivo de aproveitar o potencial das tecnologias

⁹⁴ BRASIL. Conselho Nacional dos Direitos da Criança e do Adolescente (Conanda). *Resolução CONANDA nº 245, de 5 de abril de 2024*. Disponível em: <https://www.lex.com.br/resolucao-conanda-no-245-de-5-de-abril-de-2024/>. Acesso em: 5 dez. 2024.

digitais para promover o desenvolvimento econômico e social sustentável e inclusivo, com inovação, aumento de competitividade, de produtividade e dos níveis de emprego e renda no país.

A E-Digital é estruturada em eixos, entre os quais um guarda ampla relação com o tema deste GT, o eixo D: “Educação e capacitação profissional”. Segundo o MCTI, o eixo tem o intuito de “promover a formação da sociedade para o mundo digital, com novos conhecimentos e tecnologias avançadas, e prepará-la para o trabalho do futuro”⁹⁵.

No ciclo de ações estratégicas de 2022-2026, há 15 ações referentes ao eixo D “Educação e capacitação profissional”, que vão desde questões como o aprimoramento curricular, a fim de adequá-los às novas tecnologias da informação e comunicação, passando por questões relacionadas à tecnologia assistiva, para promover o direito à educação de pessoas com deficiência até a concessão de bolsas de pesquisa, desenvolvimento, inovação, intercâmbio e extensão tecnológica nos níveis técnico, de graduação e pós-graduação nos temas de transformação digital, a fim de atender demandas do setor produtivo.

3.3.7. Estratégia Nacional do Governo Digital (2024-2027)

A Estratégia Nacional de Governo Digital é um conjunto de recomendações estratégicas que tem por objetivo articular e direcionar as iniciativas de governo digital entre todos os entes federados, de modo a ampliar e simplificar o acesso do cidadão aos serviços públicos. A iniciativa tem como objetivo promover a transformação digital do setor público, visando aprimorar a eficiência, a transparência, a acessibilidade e o impacto positivo dos serviços governamentais, além de fortalecer ferramentas de participação cidadã e impulsionar a inovação tecnológica.

Segundo o Ministério da Gestão e da Inovação em Serviços Públicos, o objetivo central da estratégia é promover uma administração pública mais moderna, ágil e centrada no cidadão. A estratégia prevê a capacitação contínua dos servidores públicos em temas relacionados à transformação digital, com o treinamento em novas tecnologias, em promoção de habilidades digitais, gestão pública digital e na formação de uma governança digital em consonância com a Lei Geral de Proteção de Dados.

3.3.8. Escola de Dados

A Escola de Dados,⁹⁶ programa de alfabetização de dados da Open Knowledge Brasil, é uma iniciativa dedicada a promover o uso eficaz de dados para resolver problemas reais e contribuir para sociedades mais conscientes, sustentáveis e justas. Esta rede abrangente tem como objetivo capacitar indivíduos e organizações, fornecendo-lhes as habilidades necessárias para compreender criticamente

⁹⁵ BRASIL. Ministério da Ciência, Tecnologia e Inovação. *Estratégia Brasileira para a Transformação Digital (E-Digital)*. Disponível em: <https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/estrategia-digital-aco-es-2022-2026>. Acesso em: 5 dez. 2024.

⁹⁶ ESCOLA DE DADOS. *Sobre a Escola de Dados*. Disponível em: <https://escoladedados.org/>. Acesso em: 5 dez. 2024.

seu ambiente, responder a questões importantes e engajar-se em ações que gerem impacto social positivo.

Desde sua fundação em 2013, a Escola de Dados tem desempenhado um papel crucial na formação de milhares de pessoas, tanto em atividades presenciais quanto online. Seu alcance é notável, tendo impactado mais de 30 mil pessoas por meio de suas diversas atividades, eventos e cursos. A iniciativa tem sido particularmente influente no campo do jornalismo, tendo treinado editores e repórteres de alguns dos maiores veículos de comunicação do país.

A abordagem da Escola de Dados é multifacetada, focando em três áreas principais: capacitação, conhecimento e comunidade. No âmbito da capacitação, a escola oferece treinamentos presenciais e online, contando com uma rede diversificada de especialistas com vasta experiência no uso de dados. Em termos de conhecimento, a iniciativa desenvolve tutoriais, realiza pesquisas e cria metodologias de aprendizagem, além de promover discussões sobre dados e suas implicações sociopolíticas. No que diz respeito à comunidade, a Escola de Dados organiza eventos, facilita encontros e conecta redes diversas de atores interessados ou já atuantes no campo de dados.

Mediante essas atividades, a Escola de Dados não apenas fornece habilidades técnicas, mas também promove uma compreensão mais profunda do potencial transformador dos dados na sociedade contemporânea. Seu trabalho é fundamental para democratizar o acesso ao conhecimento sobre dados e fomentar uma cultura de tomada de decisões baseada em evidências em diversos setores da sociedade.

3.3.9. Escola Nacional de Administração Pública

A Escola Nacional de Administração Pública (ENAP)⁹⁷ tem se destacado por suas iniciativas voltadas à capacitação em proteção de dados pessoais, refletindo seu compromisso com a formação de servidores públicos e a promoção de boas práticas no setor. Entre as principais ações desenvolvidas, estão os cursos online gratuitos, que incluem temas como "Proteção de Dados Pessoais no Setor Público" (15h), "Introdução à Lei Brasileira de Proteção de Dados Pessoais" (10h) e "Fundamentos da Lei Geral de Proteção de Dados" (15h). Esses cursos, com carga horária variada, visam fornecer uma base sólida sobre a legislação e suas implicações.

Além disso, a ENAP oferece uma trilha de aprendizagem chamada "Privacidade e Segurança da Informação", disponível na plataforma Escola Virtual de Governo (EV.G). Essa trilha abrange uma gama de tópicos relevantes, como a Lei Geral de Proteção de Dados (LGPD), governança, segurança da informação e resposta a incidentes, totalizando 212 horas de conteúdo. Essa abordagem abrangente permite que os participantes adquiram conhecimentos essenciais para lidar com as demandas contemporâneas relacionadas à proteção de dados.

A ENAP também tem estabelecido parcerias significativas, como com a Autoridade Nacional de Proteção de Dados (ANPD), promovendo eventos como o 1º Encontro ANPD de Encarregados. Além disso, a escola realiza seminários e palestras online em colaboração com a Escola da Advocacia-Geral

⁹⁷BRASIL. *Governo Digital*. Disponível em: <https://www.gov.br/governodigital/pt-br>. Acesso em: 5 dez. 2024.

da União (AGU), ampliando o alcance da capacitação. Por fim, destaca-se o Programa de Governança em Privacidade da Enap (PGP-ENAP), elaborado em conformidade com a LGPD, que visa assegurar a proteção de dados e a privacidade nos processos internos e externos da escola. Essas iniciativas demonstram o empenho da Enap em fomentar uma cultura de proteção de dados no setor público brasileiro.

3.3.10. Aula Digital

O Aula Digital⁹⁸ é um programa educacional que visa promover a inovação nas escolas por meio da tecnologia e de novas metodologias de ensino e aprendizagem. Lançado no Brasil em 2017, o programa faz parte da iniciativa ProFuturo,⁹⁹ atua em parceria com secretarias de educação municipais e estaduais, e tem como objetivos fortalecer e ampliar práticas pedagógicas para inovação educativa e o uso de recursos digitais nas redes de ensino. Ele também oferece formação para educadores, focando em temas como educação digital e uso de tecnologias em sala de aula e trabalha para aproximar as tecnologias digitais do ensino, potencializando avanços no cenário educacional.

3.3.11. Data_Labe

O data_labe¹⁰⁰ é um laboratório de dados e narrativas localizado na favela da Maré, no Rio de Janeiro. Ele é composto por uma equipe de jovens moradores de territórios populares que utilizam dados para contar histórias e abordar questões sociais relevantes. O projeto busca dar visibilidade às realidades das favelas, promovendo uma perspectiva crítica e inclusiva por meio do uso de dados e narrativas que refletem as experiências desses territórios.

3.3.12. Prato do Dia

"Prato do Dia"¹⁰¹ é uma iniciativa digital inovadora, realizada pela Rede Transfeminista de Cuidados Digitais, que funciona como um "restaurante dos cuidados digitais", no qual os usuários podem explorar e "consumir" conteúdos e práticas relacionadas ao bem-estar digital. Nesse conceito, os visitantes têm a liberdade de escolher entre um menu diversificado de "pratos", cada um abordando diferentes aspectos da segurança e saúde no ambiente online. A proposta visa promover uma relação mais consciente e responsável com a tecnologia. Com uma abordagem lúdica e educativa, a iniciativa busca conscientizar as pessoas sobre a importância de adotar práticas saudáveis ao utilizar ferramen-

⁹⁸ FUNDAÇÃO TELEFÔNICA VIVO. *Aula Digital 2 - Profuturo*. Disponível em: <https://www.fundacaotelefonica vivo.org.br/aula-digital-2-profuturo/>. Acesso em: 5 dez. 2024.

⁹⁹ PROFUTURO. *Quem somos*. Disponível em: <https://profuturo.education/pt-br/quem-somos/>. Acesso em: 5 dez. 2024.

¹⁰⁰ DATALABE. *Datalabe - Proteção de Dados e Privacidade*. Disponível em: <https://datalabe.org/>. Acesso em: 5 dez. 2024.

¹⁰¹ PRATO DO DIA. *Plataforma Prato do Dia*. Disponível em: <https://pratododia.org/pt/>. Acesso em: 05 dez. 2024.

tas digitais. Ao experimentar essas "refeições", os participantes são incentivados a desenvolver hábitos que garantam sua segurança e confiança no mundo online, tornando-se mais informados e empoderados em sua interação com a tecnologia.

3.3.13. Cadê meu Dado?

A plataforma "Cadê meu Dado"¹⁰² é uma iniciativa digital voltada para a promoção da transparência e proteção de dados pessoais, com o objetivo principal de dar visibilidade a eventos que possam comprometer a Lei Geral de Proteção de Dados Pessoais (LGPD). Funcionando como um canal de comunicação entre os diversos atores do ecossistema de proteção de dados, a plataforma oferece um espaço gratuito e colaborativo para que cidadãos, organizações e especialistas possam se engajar na discussão sobre privacidade.

Entre as principais funcionalidades da plataforma, destaca-se um canal para denúncias relacionadas a violações de privacidade e proteção de dados, além de uma ferramenta de busca que permite aos usuários verificarem se seus e-mails estão envolvidos em algum vazamento de dados. A "Cadê meu Dado" também serve como um repositório de artigos, notícias e informações relevantes sobre o tema, contribuindo para o amadurecimento da discussão sobre privacidade no Brasil. Com essa abordagem, a plataforma visa promover a conscientização e fornecer recursos para que os cidadãos possam exercer seus direitos digitais de modo mais informado e ativo.

3.3.14. Canal de Ajuda da SaferNet Brasil

O Canal de Ajuda da SaferNet Brasil,¹⁰³ também conhecido como HelpLine, é um serviço gratuito e confidencial criado para orientar crianças e adolescentes sobre o uso seguro e responsável da internet. Desenvolvido em parceria com a Secretaria de Direitos Humanos da Presidência da República, o canal oferece atendimento especializado por meio de chat ou e-mail, realizado por uma equipe de psicólogos experientes. O serviço está disponível em horários específicos durante a semana e aborda uma ampla gama de temas relacionados à segurança online.

Seu objetivo principal é fornecer suporte e orientação para situações de risco na internet, como cyberbullying, sexting, exposição indesejada de imagens íntimas, assédio online e uso seguro das redes sociais. Além de atender crianças e adolescentes, o serviço também oferece informações e recursos para pais e educadores, auxiliando-os na orientação sobre o uso seguro da internet. A SaferNet utiliza técnicas de criptografia e desenvolveu seu próprio sistema de chat web para garantir a segurança e o anonimato dos usuários.

Com abrangência nacional, o Canal de Ajuda da SaferNet Brasil se estabelece como um recurso crucial na proteção de crianças e adolescentes no ambiente digital. O serviço não recebe denúncias formais, mas orienta os usuários sobre como proceder em casos de violações dos direitos humanos

¹⁰² CADE MEU DADO. *Plataforma Cadê Meu Dado?*, Disponível em: <https://cademeudado.com.br/>. Acesso em: 05 dez. 2024.

¹⁰³ SAFERNET BRASIL. *Helpline SaferNet*. Disponível em: <https://new.safernet.org.br/helpline>. Acesso em: 25 jan. 2025.

na internet. Ao oferecer suporte profissional, confidencial e acessível, o Canal de Ajuda contribui significativamente para enfrentar os desafios e riscos da internet, promovendo um uso mais seguro e responsável das tecnologias digitais entre os jovens brasileiros.

3.3.15. Data Privacy Brasil

Data Privacy Brasil é uma organização que nasce da união entre uma escola e uma associação civil em prol da promoção da cultura de proteção de dados e direitos digitais no Brasil e no mundo. Para isso, com o apoio de uma equipe multidisciplinar, realiza formações, eventos, certificações, consultorias, conteúdos multimídia, pesquisas de interesse público e auditorias cívicas para promoção de direitos em uma sociedade datificada marcada por assimetrias e injustiças. Por meio da educação, da sensibilização e da mobilização da sociedade, almeja uma sociedade democrática onde as tecnologias estejam a serviço da autonomia e dignidade das pessoas.

Entre outros cursos, possui o de PPD - Privacidade e Proteção de Dados, que, a partir de uma linguagem acessível busca apresentar uma visão completa do ecossistema de privacidade e proteção de dados. O curso tem como objetivo capacitar os alunos e alunas a assessorar empresas e organizações públicas no desenvolvimento e na supervisão das suas práticas de proteção de dados e segurança da informação. Fomentar a aquisição e a ampliação de habilidades necessárias para desenvolver modelos de negócio e políticas públicas inovadoras, tornando-os capazes de lidar com os mais novos desafios regulatórios e jurídicos de uma sociedade cada vez mais movida e orientada por dados (*data-driven society*). Coloca em perspectiva a Lei Geral de Proteção de Dados (LGPD) e as normas setoriais brasileiras de proteção de dados em relação à General Data Protection Regulation (GDPR), fornecendo uma visão geral de todo o ecossistema de governança e regulação de dados.

3.4. Participação da Sociedade Civil

Com a finalidade de ampliar a participação da sociedade civil, este GT1 convidou diversos especialistas para que apresentassem propostas concretas para o desenvolvimento de uma política pública de educação em proteção de dados pessoais. Essa iniciativa foi dividida em 2 (duas) etapas: a realização de uma mesa redonda e o envio de convites para apresentação de colaboração por escrito.

3.4.1. Mesa Redonda com Especialistas

Para a mesa redonda, realizada virtualmente no dia 16 de dezembro de 2024, foram convidados 16 (dezesesseis) especialistas.¹⁰⁴ Estiveram presentes os Conselheiros Rodrigo Valadão (Coordenador), Alexandre Boava, Ana Paula Canto, e Gabrielle Sarlet e os seguintes convidados especialistas:

¹⁰⁴ Alessandra Borelli (Instituto Educando Direito), Ana Frazão (UnB), Bruna Diniz Franqueira (MTST), Bruno Bioni (Data Privacy), Carlos Affonso Souza (ITS-Rio), Fabiano Menke (UFRGS), Haidée Svab (Open Knowledge Brasil), Jamile Santana (Escola de Dados), Leonardo Parentoni (UFMG), Patrícia Blanco (Palavra Aberta), Patricia Peck (Advogada), Priscila Cruz (Todos pela Educação), Priscila Gonzales (EducaDigital), Rafael Zanatta (Data Privacy), Rodrigo Pinho Gomes (CTS/FGV-Rio) e Viviane Maldonado (New Law Institute).

Alessandra Borelli (Instituto Educando Direito), Bruna Diniz Franqueira (MTST), Haidée Svab (Open Knowledge Brasil), Patrícia Blanco (Palavra Aberta), Patricia Peck e Rodrigo Pinho Gomes (CTS/FGV-Rio).¹⁰⁵

No início da reunião, foram estabelecidas algumas premissas. As propostas e os respectivos debates deveriam levar em conta a exigência de que as ações educativas tivessem o *maior impacto* e o *menor custo* possíveis, em razão, respectivamente, do baixo nível de aculturação da sociedade da matéria e das atuais limitações estruturais e orçamentárias da ANPD. Todos os conselheiros e especialistas presentes concordaram com este ponto de partida, principalmente por estar em sintonia com o *princípio da eficiência*, constante no artigo 37, *caput* da Constituição da República. Em linhas gerais, foram apresentadas as seguintes sugestões:

- No que diz respeito aos limites orçamentários, foi sugerido que, para alavancar seus projetos, a ANPD busque linhas de financiamento junto a agências de fomento nacionais (eg. BNDES, FINEP etc.) e internacionais (eg. Banco Mundial, BID, CAF).
- A principal linha de ação sugerida foi a busca de sinergia com as redes já consolidadas e integradas por outras instituições, seja do setor público estatal (eg. ANATEL, ANVISA, CGI, ENAP, Sebrae etc.) ou paraestatal (eg. OAB), seja privada (eg. universidades privadas), seja em organizações da sociedade civil.¹⁰⁶
- Da mesma forma, o fortalecimento de laços com escolas de governo (e.g. ENAP), com a produção e a disseminação de novos cursos sobre proteção de dados e matérias correlatas poderia alavancar sobretudo a capacitação dos servidores públicos. Inclusive, no que diz respeito à abertura de dados, foi sugerida a criação de cursos específicos para ajudar os servidores públicos a conciliarem a aplicação da LGPD e da LAI, sanando dúvidas e unificando entendimentos sobre o tema.
- Outra sugestão relevante para uma maior conscientização foi a inserção da temática de proteção de dados pessoais em currículos escolares e universitários, o que também iria exigir ações voltadas à capacitação dos profissionais da área da educação na matéria.
- Também foi sugerida a intensificação da presença da ANPD nas mídias sociais, inclusive com o apoio de influenciadores digitais para difundir conteúdo educacional.

¹⁰⁵ Registre-se, por oportuno, que todos os demais especialistas convidados responderam o email enviado, agradecendo, mas, por força de compromissos previamente agendados, informaram que lamentavelmente não poderiam participar.

¹⁰⁶ As vantagens são óbvias. A celebração de convênios com outras instituições pode trazer mais eficiência, devido à combinação de múltiplos fatores. A uma, porque essas instituições possuem especialização temáticas que poderiam ser acopladas ao tema da proteção de dados, gerando conteúdo específico e direcionando as ações educacionais de acordo com a realidade e a necessidade dos *stakeholders* de cada rede. A duas, porque permite que a ANPD se comunique diretamente com os *stakeholders* das mais variadas redes, as quais, sozinha, ela teria muita dificuldade em acessar.

- Por fim, foi sugerido que este GT levasse em consideração as propostas apresentadas pelo GT2 da composição anterior do CNPD.¹⁰⁷

Em síntese, para que os titulares de dados compreendam e possam exercer seus direitos, é crucial a implementação de uma vasta campanha de sensibilização, que inclua informações transparentes e de fácil acesso sobre a LGPD, seus direitos e os meios para comunicar problemas, empregando canais de comunicação que alcancem diversas idades e estratos sociais. Ações educacionais podem ser realizadas em plataformas como televisão, rádio e redes sociais, atingindo um público vasto. Adicionalmente, a ANPD poderia realizar parcerias com entidades de defesa do consumidor, organizações civis e empresas privadas, expandindo a disseminação de informações. Outra ação relevante seria a incorporação do assunto ao currículo escolar e universitário. Incorporar temas de proteção de dados e privacidade desde a educação básica até o ensino superior pode capacitar as novas gerações a interagirem de maneira mais consciente e segura no universo digital. Portanto, as crianças, os adolescentes e os adultos teriam um entendimento claro de seus direitos e estariam preparados para demandar transparência de empresas e instituições. Com uma educação sólida em proteção de dados desde a infância, as próximas gerações estarão mais bem equipadas para enfrentar os desafios de um mundo digital e terão uma participação ativa na supervisão dos seus próprios dados.¹⁰⁸

3.4.2. Contribuições por Escrito de Entidades

Inicialmente, foi permitido que os especialistas convidados, mas ausentes no debate virtual, pudessem enviar contribuições por escrito. A mesma oportunidade foi dada a diversas instituições representativas acerca do tema, escolhidas pelos conselheiros, por meio de ofício enviado via email, no dia 03 de janeiro de 2025. Originalmente, o prazo final da apresentação dessas contribuições por escrito era o dia 13 de janeiro de 2025, todavia, o prazo foi prorrogado por decisão do GT1 para o dia 17 de janeiro do mesmo ano, tendo todos os convidados sido informados do novo termo final por email.

Os convites continham 3 (três) quesitos, rogando que as entidades trouxessem informações sobre (a) situações concretas e dados estatísticos que demonstrem o déficit educacional e a necessidade de melhora nos índices de conscientização e capacitação em matéria de proteção de dados pessoais, (b) iniciativas ou práticas que poderiam ser *replicadas* ou *difundidas* pela ANPD para melhorar os índices de conscientização e capacitação em matéria de proteção de dados pessoais e (c) iniciativas ou práticas que poderiam ser *adotadas* ou *patrocinadas* pela ANPD para melhorar os índices de conscientização e capacitação em matéria de proteção de dados pessoais?

Foram convidadas as seguintes instituições: *Cadê meu Dado?*, *Centro de Inovação para a Educação Brasileira (CIEB)*, *CEPI/FGV-SP*, *Data_Labe*, *Data Privacy Brasil*, *EducaDigital*, *Internet Lab*, *ITS-*

¹⁰⁷ Findo o debate, a especialista Patrícia Peck, integrante da composição anterior, enviou as referidas propostas ao coordenador do GT1, que prontamente compartilhou os arquivos com os demais conselheiros.

¹⁰⁸ QUEIROZ, Luiz. *A necessária promoção da educação em proteção de dados*. Capital Digital, 2024. Disponível em: <https://capitaldigital.com.br/a-necessaria-promocao-da-educacao-em-protecao-de-dados/>. Acesso em: 11 dez. 2025.

Rio, LAPIN, Legal Grounds Institute, MEC, Palavra Aberta, SaferNet Brasil, UFMG e UFRGS. Apenas 3 (três) delas atenderam à convocação deste GT, apresentando suas colaborações por escrito, a saber: a) *Cadê meu Dado?*, b) *Câmara de Educação Superior do Conselho Nacional de Educação (MEC)* e c) *Data Privacy Brasil*. Por fim, também houve envio espontâneo de contribuições pelo (d) *Centro de Estudos Avançados em Proteção de Dados (CEAPD)*.

3.4.2.1. Contribuições da “Cadê meu Dado?”

Embora a resposta da “Cadê meu Dado?” tenha sido enviada apenas no dia 20 de janeiro de 2025, portanto fora do prazo estipulado, o GT1 deliberou por receber suas contribuições e incluí-las no presente relatório, diante da ausência de prejuízo na intempestividade. Depois de descrever o papel da respectiva plataforma na promoção da privacidade e proteção de dados no Brasil, o documento apresentou dados sobre o déficit educacional no tema sob análise¹⁰⁹ e as sugestões concretas para a ANPD:

Iniciativas a serem replicadas pela ANPD:

- Realização de campanhas massivas de conscientização, inspiradas na abordagem do Regulamento Geral de Proteção de Dados, da União Europeia.
- Realização de parcerias com o Ministério da Educação para inclusão da proteção de dados nos currículos escolares e universitários.
- Criação de cursos online gratuitos (MOOCs) para diferentes públicos.
- Divulgação de guias práticos em linguagem acessível.

Iniciativas a serem adotadas ou patrocinadas pela ANPD:

- Promoção de hackathons e premiações para incentivar soluções tecnológicas educacionais.
- Criação de kits de treinamento simplificados para micro e pequenas empresas.
- Realização de workshops gratuitos em parceria com associações locais e sindicatos.
- Apoio financeiro a ONGs e projetos comunitários que promovam conscientização em matéria de proteção de dados pessoais.
- Implementação de um sistema de monitoramento e avaliação contínua das iniciativas.
- Destaque de ações e posturas positivas sobre o tema para incentivar outras instituições.

¹⁰⁹ O documento apresentou dados estatísticos e situações concretas que demonstram a falta de conhecimento sobre proteção de dados no Brasil. Destaca-se que apenas 28% dos entrevistados em uma pesquisa do Cetic.br em 2023 afirmaram conhecer a LGPD, enquanto 67% nunca receberam treinamento sobre o tema. Além disso, mencionou que 60% dos servidores públicos desconhecem suas responsabilidades no manejo de dados pessoais.

Por fim, o documento reafirma o compromisso da plataforma "Cadê Meu Dado?" com a melhoria da proteção de dados no Brasil.

3.4.2.2. Contribuições da “Câmara de Educação Superior do Conselho Nacional de Educação (MEC)”

O segundo órgão que atendeu à convocação deste GT1 foi a Câmara de Educação Superior do Conselho Nacional de Educação (MEC), por meio de ofício enviado por email, enviado no dia 17 de janeiro de 2025. Inicialmente, o documento¹¹⁰ (a) destaca a importância da Revolução 4.0 e seu impacto nas relações sociais, especialmente no contexto educacional, (b) enfatiza a necessidade do “letramento digital”, sobretudo diante da crescente adoção de plataformas tecnológicas no sistema educacional, (c) apresenta dados alarmantes sobre violações de privacidade em plataformas educacionais brasileiras¹¹¹ e (d) aborda a falta de formação adequada sobre segurança digital e proteção de dados nas escolas brasileiras.¹¹²

Sugestões encaminhadas:

- Implementação de um programa de Alfabetização Digital para Proteção de Dados, inspirado no modelo europeu *Safer Internet Programme*.
- Criação de material didático oficial sobre a LGPD para distribuição gratuita em instituições de ensino.
- Estabelecimento de parcerias institucionais com universidades e centros de pesquisa para fomentar a produção de conhecimento sobre proteção de dados.
- Inclusão de educação em proteção de dados na Base Nacional Comum Curricular (BNCC).
- Desenvolvimento de uma plataforma pública e gratuita de capacitação em proteção de dados.
- Lançamento de editais públicos para fomentar pesquisa e inovação em proteção de dados.

¹¹⁰ Assinado pela Conselheira Mônica Sapucaia.

¹¹¹ O documento cita uma investigação da *Human Rights Watch* que revelou a coleta e transmissão indevida de dados de estudantes para fins publicitários, destacando, inclusive, que sites operados por Secretarias de Educação estaduais estavam envolvidos nessas práticas questionáveis. Sobre o tema: HUMAN RIGHTS WATCH (HRW). *Brazil: Online Learning Tools Harvest Children's Data*. 3 abr. 2023. Disponível em: <https://www.hrw.org/news/2023/04/03/brazil-online-learning-tools-harvest-childrens-data>. Acesso em: 28 jan. 2025.

¹¹² O documento cita a pesquisa TIC Educação 2023, que mostra que apenas 55% das escolas de ensino fundamental e médio possuíam políticas de proteção de dados. Sobre o tema: NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR (NIC.br). *Pesquisa sobre o uso das tecnologias de informação e comunicação nas escolas brasileiras: Pesquisa TIC Educação, ano 2023*. 2024. Disponível em: <https://cetic.br/pt/arquivos/educacao/2023/escolas>. Acesso em: 24 jan. 2025.

No final, o documento enfatiza a importância da atuação proativa do CNPD para fortalecer a cultura de privacidade e segurança digital no Brasil, afirmando que tanto a Câmara de Educação Superior do Conselho Nacional de Educação (MEC), quanto a sua subscritora estão à disposição para contribuir no desenvolvimento de políticas públicas voltadas à proteção de dados e à educação digital.

3.4.3.3. Contribuições da “Data Privacy Brasil”

A última colaboração escrita enviada dentro do prazo estipulado foi apresentada pela Data Privacy Brasil.¹¹³ Inicialmente, o documento (a) apresenta uma visão geral da estrutura educacional brasileira, utilizando dados da OCDE de 2021¹¹⁴ e abrangendo desde a educação infantil até o ensino superior, incluindo programas de doutorado, (b) enfatiza a complexidade da governança educacional no Brasil, que envolve três níveis federativos (municípios, estados e federação) e (c) destaca a necessidade de combinar arranjos institucionais existentes com estratégias inovadoras de educação em direitos.

Em seguida, o documento aborda o 5o Ciclo de Monitoramento do Plano Nacional de Educação (PNE) e suas metas para 2024,¹¹⁵ focando especialmente na Meta 2, que visa universalizar o acesso ao ensino fundamental para a população de 6 a 14 anos. São apresentados dados do Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep) que mostram os avanços e retrocessos nessa área, incluindo o impacto da pandemia de COVID-19 nos índices educacionais. O texto também discute a Meta 8 do PNE, que busca elevar a escolaridade média dos jovens entre 18 e 29 anos para 12 anos de estudo até 2024. São apresentados dados que mostram a evolução desse indicador, destacando as disparidades regionais e socioeconômicas persistentes no país. Nesse particular, a contribuição enfatiza 3 (três) pontos cruciais para qualquer discussão sobre políticas de educação no Brasil: as desigualdades territoriais, as desigualdades entre pobres e ricos, e o não cumprimento das principais metas do PNE para 2024.

Respostas às perguntas formuladas:

- Quanto à primeira questão, foi destacada a importância da educação em direitos humanos como um processo sistemático e multidimensional, citando a Constituição Federal, a Lei de Diretrizes e Bases da Educação Nacional e o Plano Nacional de Educação em Direitos Humanos. Foram apresentados dados do Comitê Gestor da Internet no Brasil (CGI.br)¹¹⁶ sobre a percepção da população brasileira em relação ao gerenciamento de acesso a dados pessoais. O texto também menciona pesquisas como a TIC

¹¹³ E assinada pelos coordenadores Bruno Bioni, Mariana Rielli, Rafael Zanatta e Pedro Saliba.

¹¹⁴ OECD. *Education in Brazil: An International Perspective*. Paris: OECD Publishing, 2021. Disponível em: <https://doi.org/10.1787/60a667f7-en>. Acesso em: 24 jan. 2025.

¹¹⁵ BRASIL. Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira. Relatório do 5º ciclo de monitoramento das metas do Plano Nacional de Educação – 2024. Brasília, DF: Inep, 2024. Disponível em: https://download.inep.gov.br/publicacoes/institucionais/plano_nacional_de_educacao/relatorio_do_quinto_ciclo_de_monitoramento_das metas_do_plano_nacional_de_educacao.pdf. Acesso em: 24 jan. 2025.

¹¹⁶ NIC.br; CETIC.br, 2024a, *op. cit.*

Kids Online e TIC Educação, que fornecem informações sobre o uso de ferramentas digitais por crianças e adolescentes no contexto doméstico e escolar.

- Quanto à segunda questão, foi sugerida a realização de cursos avançados de proteção de dados pessoais para atores do sistema de justiça, como Defensorias Públicas e Procons, bem como a criação de uma “Escola de Formação em Proteção de Dados Pessoais”, reunindo profissionais do setor público e lideranças comunitárias.
- Quanto à terceira questão, foram sugeridas as seguintes iniciativas: a) uso de educação midiática, incluindo a produção de podcasts e parcerias com veículos de comunicação, bem como o investimento em mecanismos de disseminação de direitos por meio de rádios, dada a ampla penetração desse meio de comunicação no Brasil, b) celebração de parcerias com influenciadores digitais especializados em divulgação científica, promoção de concursos culturais, bem como o diálogo com lideranças comunitárias através de eventos regionais. Em ambos os casos, foi enfatizada a importância de utilização de instrumentos populares já existentes para transmitir a mensagem e efetivar o direito à proteção de dados como uma garantia fundamental.

Ao final, o documento reitera a disposição da Data Privacy Brasil em contribuir com os trabalhos deste GT1, do CNPD e da ANPD.

3.4.3.4. Contribuições do “Centro de Estudos Avançados em Proteção de Dados (CEAPD)”

Além das contribuições acima mencionadas, que trouxeram respostas e sugestões aos quesitos constantes no ofício convocatório, houve também a apresentação espontânea de sugestões pelo Centro de Estudos Avançados em Proteção de Dados (CEAPD). Em ofício encaminhado no dia 28 de janeiro de 2025, o seu Diretor-Acadêmico Fabrício da Mota Alves apresentou uma única proposta: a criação da “Escola Nacional de Proteção de Dados (ENAD)”, visando “preencher uma lacuna crítica na formação de profissionais e servidores públicos na área de proteção de dados”.

De acordo com o signatário, a criação da ENAD estaria triplamente justificada. A uma, porque a simples conformidade da sua atuação administrativa com o ordenamento jurídico nacional impõe à União Federal o dever de manter escolas de governo para capacitação de servidores. A duas, porque em cumprimento ao princípio da eficiência administrativa, a ENAD permitiria a padronização de diretrizes pedagógicas e centralização de parcerias com instituições relevantes. Por fim, porque atende demandas regulatórias emergentes, considerando que a Agenda Regulatória 2025-2026 da ANPD prioriza temas complexos que demandam capacitação especializada.

Além disso, a ENAD poderia, segundo o entendimento do signatário, se estabelecer como um centro de formação certificada, alinhando-se com normas internacionais como a ISO/IEC 27701. Isso permitiria o desenvolvimento de programas de certificação técnica e profissional reconhecidos nacionalmente, contribuindo para a formação de uma rede de especialistas qualificados em proteção de dados.

O ofício solicita que a proposta de criação da ENAD seja incluída como pauta prioritária nas deliberações do GT1 e recomenda a formação de um grupo de estudo para elaborar estudos de viabilidade e uma minuta de decreto presidencial. Ao final, informa que o CEAPD se coloca à disposição para fornecer esclarecimentos adicionais e colaborar na elaboração de estudos técnicos complementares para subsidiar esta importante iniciativa para o avanço da proteção de dados no Brasil.

4. Quadro Geral das Iniciativas e Sugestões

Durante os trabalhos realizados pelo GT1, diversos subsídios foram coletados, iniciativas foram identificadas e sugestões foram recebidas. Algumas delas já estão em curso, outras têm previsão de serem implementadas e mais um punhado ainda são meras ideias. Além disso, muitas delas apresentam algumas semelhanças ou, no mínimo, uma razoável dose de superposição. Para auxiliar na compreensão da grande quantidade e variedade das ideias coletadas durante a instrução deste relatório, apresenta-se uma tentativa de sistematizar, organizar e sistematizar essas ideias informações em 6 (seis) categorias principais, cada uma delas contando com propostas específicas.

4.1. Parcerias e Colaborações Institucionais

Nesta categoria, as iniciativas e sugestões mapeadas têm por objetivo fortalecer e expandir as iniciativas educacionais em proteção de dados por meio de parcerias estratégicas com diversas instituições. Seu objetivo principal é criar uma rede colaborativa que abranja diferentes setores da sociedade, incluindo o governo, a academia, o setor privado e organizações da sociedade civil. Essas parcerias buscam integrar a proteção de dados nos currículos escolares e universitários, capacitar servidores públicos e empresas, fomentar pesquisas acadêmicas, disseminar informações ao público em geral e promover a conscientização jurídica. Ao estabelecer essas colaborações, pretende-se criar um ecossistema educacional abrangente e eficaz, que possa alcançar diversos públicos e níveis de ensino, promovendo assim uma cultura de proteção de dados mais sólida e disseminada em todo o país.

- **Aproximação com a ENAP:** A colaboração com a Escola Nacional de Administração Pública visa produzir e revisar conteúdos para capacitação de servidores públicos. Isso inclui cursos online e presenciais sobre a LGPD, boas práticas de proteção de dados no serviço público e gestão de incidentes de segurança. Um exemplo concreto é o Programa de Governança em Privacidade da ENAP (PGP-ENAP), elaborado em conformidade com a LGPD.
- **Parcerias com universidades e centros de pesquisa:** O objetivo é fomentar a produção de conhecimento sobre proteção de dados. Isso envolve o financiamento de pesquisas, a criação de grupos de estudo interdisciplinares e a promoção de intercâmbios acadêmicos focados em privacidade e segurança de dados. Também inclui o lançamento de editais públicos para fomentar pesquisa e inovação em proteção de dados.
- **Colaboração com entidades de defesa do consumidor e organizações civis:** Esta iniciativa visa expandir a disseminação de informações. Inclui a produção conjunta de

materiais educativos, a realização de campanhas de conscientização e o estabelecimento de canais de comunicação para esclarecer dúvidas do público.

- **Parcerias com o Sebrae:** Esta colaboração visa a capacitação de micro e pequenas empresas em proteção de dados, incluindo a criação de kits de treinamento simplificados para esse público específico.
- **Colaborações com a OAB-Nacional e Escolas de Governo** (eg. Escola da Advocacia-Geral da União - AGU): Esta parceria envolve a realização de seminários e palestras online sobre temas relacionados à proteção de dados no contexto jurídico e governamental.
- **Fortalecimento de parcerias e ações com o Sistema de Garantia de Direitos e com o MEC, Comunidade Escolar e Conselhos da área:** O fortalecimento da colaboração envolve desenvolvimento de materiais didáticos oficiais, inserção do tema nos currículos, definição de indicadores de monitoramento, promoção de estratégias de conscientização, criação de instrumentos regulatórios de apoio para gestores escolares, ampliação da fiscalização da proteção de dados em plataformas educacionais ou grandes plataformas com tecnologias que atraem crianças e adolescentes e fomento à um ambiente de inovação seguro, adequado à idade e em prol da educação.

RECOMENDAÇÃO	O QUE A ANPD TEM PREVISTO OU REALIZADO ?
Aproximação com a ENAP: A colaboração com a Escola Nacional de Administração Pública visa produzir e revisar conteúdos para capacitação de servidores públicos. Isso inclui cursos online e presenciais sobre a LGPD, boas práticas de proteção de dados no serviço público e gestão de incidentes de segurança. Um exemplo concreto é o Programa de Governança em Privacidade da ENAP (PGP-ENAP), elaborado em conformidade com a LGPD.	Em parceria com a ENAP, a ANPD realizou o 1º Encontro ANPD de Encarregados , em 1 de agosto de 2024. O evento, que deve ser recorrente, tem enfoque na discussão das atividades do encarregado de dados pessoais . Além disso, o Plano de Ações Educativas 2023-2024 da ANPD previu, em seu item 8, a aproximação, produção e revisão de conteúdo da ENAP para capacitação de servidores públicos.
Parcerias com universidades e centros de pesquisa: O objetivo é fomentar a produção de conhecimento sobre proteção de dados. Isso envolve o financiamento de pesquisas, a criação de grupos de estudo interdisciplinares e a promoção de intercâmbios acadêmicos focados em privacidade e segurança de dados. Também inclui o lançamento de editais públicos para fomentar pesquisa e inovação em proteção de dados.	Em 2024, em parceria com o PNUD, a ANPD publicou <u>editais para projeto de Sandbox de Inteligência Artificial e Proteção de Dados</u> , credenciando instituições públicas de ensino superior que realizem pesquisas na área de Ambiente Regulatório Experimental e Inteligência Artificial.

<p>Colaboração com entidades de defesa do consumidor e organizações civis: Esta iniciativa visa expandir a disseminação de informações. Inclui a produção conjunta de materiais educativos, a realização de campanhas de conscientização e o estabelecimento de canais de comunicação para esclarecer dúvidas do público.</p>	<p>Acordo de Cooperação Técnica com a SENACON para troca de informações. Em outubro de 2021, ANPD e Senacon assinaram acordo de cooperação técnica com o objetivo de compartilhar informações e reclamações sobre Proteção de Dados Pessoais e apoiar interpretações dos casos que tocam a matéria, parte do Planejamento Estratégico 2021-2023.</p> <p>Também há um histórico de campanhas e ações de comunicação junto a entidades de defesa do consumidor.</p>
<p>Parcerias com o Sebrae: Esta colaboração visa a capacitação de micro e pequenas empresas em proteção de dados, incluindo a criação de kits de treinamento simplificados para esse público específico.</p>	<p>O Plano de Ações Educacionais da ANPD demonstra, no Eixo 2 - Webinários e Seminários, a meta de “realizar webinar em parceria com o Sebrae sobre segurança da informação para agentes de tratamento de pequeno porte.”.</p> <p>Ainda, o Sistema S e a ANPD tem realizado eventos em conjunto, como a participação da Autoridade no SEBRAE do Paraná em evento sobre IA e Proteção de Dados ou debate promovido sobre adequação de pequenos negócios.</p> <p>O SEBRAE também possui curso de formação denominado “ANPD: cultura de proteção de dados”, curso introdutório com objetivo de capacitar cidadãos no exercício de direitos enquanto titulares de dados e possui cartilhas PDF sobre o tema, mas não foi identificado materiais no formato de caixas de ferramenta práticas para atividades como inventário de dados pessoais.</p>
<p>Colaborações com a OAB-Nacional e Escolas de Governo (eg. Escola da Advocacia-Geral da União - AGU): Esta parceria envolve a realização de seminários e palestras online sobre temas relacionados à proteção de dados no contexto jurídico e governamental.</p>	<p>A Escola da AGU já ofertou palestras para privacidade e proteção de dados pessoais e seminários no tema.</p>
<p>Fortalecimento de parcerias e ações com o Sistema de Garantia de Direitos e com o MEC, Comunidade Escolar e Conselhos da área. O fortalecimento da colaboração envolve desenvolvimento de materiais didáticos oficiais, inserção do tema nos currículos, definição de indicadores de monitoramento, promoção de estratégias de conscientização, criação de instrumentos regulatórios de apoio para gestores escolares, amplia-</p>	<p>O Plano de Ações Educativas 2023-2024 previu o desenvolvimento de parceria com o MEC para o 1º Semestre de 2024. Apesar disso, até a data dessa pesquisa, não foi possível encontrar instrumento de celebração de cooperação entre as instituições.</p> <p>Também não consta no plano estratégias de ações com o Sistema de Garantia de Direitos, Conselho Nacional de Direitos da Criança e do Adolescente ou Conselhos de Educação.</p> <p>Há exemplos de materiais relevantes sobre proteção de</p>

ção da fiscalização da proteção de dados em plataformas educacionais ou grandes plataformas com tecnologias que atraem crianças e adolescentes e fomento à um ambiente de inovação seguro, adequado à idade e em prol da educação.	dados e educação, como o ‘Manual de LGPD para Gestores e Gestoras Públicas Educacionais’ do CIEB.
--	---

4.2. Realização de Eventos e Atividades Interativas:

As iniciativas e sugestões apresentadas nessa categoria têm como objetivo principal promover o engajamento direto e o aprendizado prático sobre proteção de dados por meio de uma variedade de eventos e iniciativas interativas. Estas propostas visam criar oportunidades para que diferentes públicos - desde profissionais e especialistas até estudantes e o público em geral - possam aprofundar seus conhecimentos e habilidades práticas em proteção de dados. Através de webinários, seminários, hackathons, workshops, encontros profissionais e eventos comemorativos, busca-se fomentar a troca de experiências, o desenvolvimento de soluções inovadoras e a aplicação prática dos conceitos de proteção de dados em diversos contextos. Essas atividades não só disseminam conhecimento, mas também incentivam a participação ativa, o pensamento crítico e a formação de *networks*, contribuindo para a formação de uma comunidade mais engajada e capacitada em questões de privacidade e segurança de dados.

- **Realização de seminários nacionais e internacionais:** Estes eventos reúnem especialistas para debater melhores práticas, podendo ser realizados presencial ou virtualmente. Incluem conferências, mesas redondas e sessões de networking para promover a troca de conhecimentos e experiências entre profissionais do setor.
- **Organização de workshops gratuitos:** Em parceria com associações e sindicatos, estes workshops oferecem treinamento prático sobre como implementar medidas de proteção de dados em diferentes contextos profissionais.
- **Promoção de hackathons e premiações:** Esta iniciativa incentiva o desenvolvimento de soluções tecnológicas educacionais. Os participantes criam aplicativos, jogos ou plataformas que ajudem a ensinar conceitos de proteção de dados de forma interativa e acessível.
- **Realização de encontros de redes de profissionais:** Como exemplo do 1º Encontro ANPD de Encarregados que, realizado em parceria com a ENAP, reuniu os encarregados de proteção de dados de diferentes organizações e de todo o território nacional.
- **Organização de evento em comemoração ao aniversário da LGPD:** Este evento anual serve como um marco para avaliar o progresso na implementação da lei e discutir desafios futuros.

RECOMENDAÇÃO	O QUE A ANPD TEM PREVISTO OU REALIZADO ?
<p>Realização de seminários nacionais e internacionais: Estes eventos reúnem especialistas para debater melhores práticas, podendo ser realizados presencial ou virtualmente. Incluem conferências, mesas redondas e sessões de networking para promover a troca de conhecimentos e experiências entre profissionais do setor.</p>	<p>O Plano de Ações Educativas 2023-2024 previu a participação em eventos e a organização de Webinários (<i>Sebrae - Agentes de Pequeno Porte, Poder Público, Crianças e Adolescentes, Evento TJBA - Comitê Gestor LGPD do Judiciário e Futurecom</i>).</p> <p>A ANPD tem realizado eventos e tido participação em eventos internacionais. Destaca-se, por exemplo, a promoção do Encontro de Encarregados em 2024, que agregou diversos setores, e as participações da Autoridade em Fóruns Internacionais, como o Internet Governance Forum.</p>
<p>Organização de workshops gratuitos: Em parceria com associações e sindicatos, estes workshops oferecem treinamento prático sobre como implementar medidas de proteção de dados em diferentes contextos profissionais.</p>	<p>Em que pese haver registro de participação da ANPD em workshops, não encontrou-se iniciativas de realização desse tipo de atividade pela Autoridade.</p>
<p>Promoção de hackathons e premiações: Esta iniciativa incentiva o desenvolvimento de soluções tecnológicas educacionais. Os participantes criam aplicativos, jogos ou plataformas que ajudem a ensinar conceitos de proteção de dados de forma interativa e acessível.</p>	<p>No Plano de Ações Educativas 2023-2024, não constava realização de Hackatons ou estratégias de engajamento e inovação com juventudes e comunidade escolar a partir de uma perspectiva de engajamento comunitário e criação de soluções locais.</p> <p>Há Prêmios promovidos pela Autoridade regularmente, com público-alvo academia e juventudes, como o Prêmio Danilo Doneda.</p> <p>Enquanto estratégia de desenvolvimento e fomento à inovação segura, destacam-se as iniciativas de Sandbox.</p>
<p>Realização de encontros de redes de profissionais: Como exemplo do 1º Encontro ANPD de Encarregados que, realizado em parceria com a ENAP, reuniu os encarregados de proteção de dados de diferentes organizações e de todo o território nacional.</p>	<p>Destaca-se previsão de participação no evento “TJBA - Comitê Gestor LGPD do Judiciário” e organização do Encontro de Encarregados, já citados.</p>
<p>Organização de evento em comemoração ao aniversário da LGPD: Este evento anual serve como um marco para avaliar o progresso na implementação da lei e discutir desafios futuros.</p>	<p>Em 2023, a ANPD comemorou 5 anos de LGPD no Brasil com evento presencial em Brasília.</p> <p>Em 2024, a ANPD comemorou o 4º ano da Autoridade, com evento no Palácio da Justiça, transmitido online.</p>

4.3. Produção e Disseminação de Conteúdo:

As iniciativas e sugestões aqui apresentadas têm como objetivo principal a criação e distribuição de materiais educativos em diversos formatos, visando alcançar um público amplo e diversificado com informações sobre proteção de dados. Essa abordagem multifacetada inclui a elaboração de guias práticos, cursos online gratuitos, material didático oficial, podcasts, e conteúdos específicos para diferentes públicos e setores. A variedade de formatos - desde livros didáticos e apostilas até recursos digitais e midiáticos - busca atender às diferentes preferências de aprendizagem e níveis de conhecimento, garantindo que a informação seja acessível e compreensível para todos. Além disso, há um foco especial em criar conteúdos adaptados para grupos específicos, como pequenas empresas, organizações que lidam com grandes volumes de dados e grupos vulneráveis, assegurando que as orientações sobre proteção de dados sejam relevantes e aplicáveis a diversos contextos e necessidades.

- **Elaboração de materiais educativos:** Inclui a produção de guias práticos, kits de treinamento para micro e pequenas empresas, e conteúdos sobre temas específicos como cookies e regulamentos da ANPD. Estes materiais são adaptados para diferentes níveis de conhecimento e setores da economia.
- **Criação de cursos online gratuitos (MOOCs):** Esses cursos cobrem desde conceitos básicos de proteção de dados até tópicos avançados como criptografia e análise de risco. São acessíveis a diferentes públicos, incluindo estudantes, profissionais e o público em geral.
- **Desenvolvimento de material didático oficial sobre a LGPD:** Este material é destinado à distribuição gratuita em instituições de ensino. Inclui livros didáticos, apostilas e recursos digitais adaptados para diferentes faixas etárias e níveis educacionais.
- **Produção de podcasts e parcerias com veículos de comunicação:** Esta iniciativa utiliza educação midiática para disseminar informações. Os podcasts abordam temas atuais relacionados à proteção de dados, enquanto as parcerias com a mídia resultam em séries de artigos ou programas especiais sobre o tema.
- **Elaboração e divulgação de material educativo sobre o Regulamentos e Guias Orientativos editados pela ANPD:** Esse material visa promover a informação dos documentos oficiais produzidos pela ANPD de forma mais simples e acessível ao grande público.
- **Criação de conteúdos específicos sobre proteção de dados para grupos vulneráveis:** Esses materiais são adaptados para as necessidades específicas de crianças, adolescentes e idosos, garantindo que esses grupos compreendam seus direitos e responsabilidades no ambiente digital.

RECOMENDAÇÃO	O QUE A ANPD TEM PREVISTO OU REALIZADO ?
Elaboração de materiais educativos: Inclui a produção de guias práticos, kits de treinamento para micro	Destaca-se a publicação dos seguintes materiais educativos pela Autoridade:

RECOMENDAÇÃO	O QUE A ANPD TEM PREVISTO OU REALIZADO ?
e pequenas empresas, e conteúdos sobre temas específicos como cookies e regulamentos da ANPD. Estes materiais são adaptados para diferentes níveis de conhecimento e setores da economia.	<p>Glossário de Proteção de Dados Pessoais, lançado em 2024 com abertura contínua para contribuições, o Glossário representa iniciativa de sistematização de termos e expressões e apoia um vocabulário comum na matéria de proteção de dados pessoais no Brasil.</p> <p>Fascículos "Segurança para Internet", publicados em julho de 2021, com conteúdo relacionados à práticas de segurança da informação e exercício de direitos de titulares de dados. Fruto de parceria com o Núcleo de Informação e Coordenação do Ponto BR.</p> <p>Guia "Como Proteger Seus Dados Pessoais", lançado em 2021 em conjunto com a Secretaria Nacional de Defesa do Consumidor (Senacon), também publicado em inglês e espanhol.</p> <p>Radar Tecnológico, série de publicações técnicas que debate tecnologias emergentes, potencialidades e perspectivas de futuro, com foco no cenário brasileiro, buscando tornar temas de proteção de dados pessoais didáticos e acessíveis ao público.</p> <p>Lançamento de Guias Orientativos, incluindo o Guia de Cookies.</p>
Criação de conteúdos específicos sobre proteção de dados para grupos vulneráveis: Esses materiais são adaptados para as necessidades específicas de crianças, adolescentes e idosos, garantindo que esses grupos compreendam seus direitos e responsabilidades no ambiente digital.	<p>Destaca-se, especialmente, o material:</p> <p>Mangá sobre exercício de direitos dos titulares de dados, lançado em 2025 em parceria com a Comissão Nacional de Informática e Liberdade da França (CNIL) e a Comissão de Proteção de Informações Pessoais da Coreia do Sul (PIPC), que usa de recursos criativos como contação de histórias e ilustrações.</p>
Criação de cursos online gratuitos (MOOCs): Esses cursos cobrem desde conceitos básicos de proteção de dados até tópicos avançados como criptografia e análise de risco. São acessíveis a diferentes públicos, incluindo estudantes, profissionais e o público em geral.	<p>Não foi encontrado curso na temática proteção de dados pessoais na plataforma AVAMEC - Ambiente Virtual de Aprendizagem do Ministério da Educação.</p> <p>Realização de parcerias para revisão de cursos na perspectiva de capacitação de gestores (ver <i>Parceria Institucional - Sebrae</i>).</p>
Desenvolvimento de material didático oficial sobre a LGPD: Este material é destinado à distribuição gratuita em instituições de ensino. Inclui livros didáticos, apostilas e recursos digitais adaptados para diferentes faixas etárias e níveis educacionais.	<p>Não foi encontrada menção à proteção de dados pessoais no Plano Nacional de Educação Digital, em tramitação no Senado Federal, que irá decidir metas para educação nos próximos 10 anos.</p>

RECOMENDAÇÃO	O QUE A ANPD TEM PREVISTO OU REALIZADO ?
Produção de podcasts e parcerias com veículos de comunicação: Esta iniciativa utiliza educação midiática para disseminar informações. Os podcasts abordam temas atuais relacionados à proteção de dados, enquanto as parcerias com a mídia resultam em séries de artigos ou programas especiais sobre o tema.	Apesar de não ter sido encontrado projetos de pílulas de podcasts, foram encontrados projetos nesse modelo do Ministério das Comunicações , do TCMRJ e de organizações da sociedade civil e jornalistas no tema. Também foram encontradas pílulas sobre proteção de dados para rádio realizadas pelo TJ-MG e diversas entrevistas sobre o tema em rádios, em especial, no dia 28 de janeiro, Dia Internacional da Proteção de Dados.
Elaboração e divulgação de material educativo sobre o Regulamentos e Guias Orientativos editados pela ANPD: Esse material visa promover a informação dos documentos oficiais produzidos pela ANPD de forma mais simples e acessível ao grande público.	A ANPD publicou Guias Orientativos nos temas: Encarregado; Legítimo Interesse; Tratamento de dados pessoais para fins de pesquisa; Tratamento de Dados pelo Poder Público; Cookies e Proteção de Dados; Segurança da Informação para Agentes de Tratamento de Pequeno Porte e Tratamento de Dados no Contexto Eleitoral.

4.4. Integração Curricular e Capacitação Profissional

As iniciativas e sugestões que se seguem visam institucionalizar o ensino sobre proteção de dados em diferentes níveis educacionais e profissionais. Estas iniciativas buscam integrar o tema nos currículos escolares e programas de formação, adaptando o conteúdo para diversas faixas etárias e níveis de ensino. Ao propor a inclusão deste tema nos padrões educacionais, busca-se criar uma base sólida de conhecimento sobre privacidade e segurança de dados, preparando o mercado e as futuras gerações para os desafios do mundo digital.

- **Inclusão da proteção de dados na grade curricular:** Esta iniciativa busca integrar a proteção de dados nos currículos escolares e universitários. Isso pode envolver a criação de módulos específicos sobre privacidade e segurança digital, adaptados para diferentes níveis educacionais, desde o ensino fundamental até o superior. A parceria também visa incluir a proteção de dados na Base Nacional Comum Curricular (BNCC), garantindo que o tema seja abordado de forma sistemática em todo o país.
- **Implementação de um programa de Alfabetização Digital para Proteção de Dados:** Inspirado no modelo europeu *Safer Internet Programme*, este programa ofereceria recursos educacionais, ferramentas de avaliação e suporte para escolas e famílias na promoção de hábitos digitais seguros.
- **Criação de cursos específicos para capacitar agentes públicos:** Esses cursos devem focar na proteção de dados no exercício de suas funções. Abordam temas como gestão de dados governamentais, segurança da informação no setor público e atendimento aos direitos dos titulares de dados.

- **Implementação do Programa de Governança em Privacidade da ENAP (PGP-ENAP):** Esse programa visa capacitar servidores públicos em práticas de governança de dados e privacidade.
- **Criação de uma "Escola de Formação em Proteção de Dados Pessoais":** Voltada para profissionais do setor público e privado, esta escola poderá oferecer programas de formação continuada, certificações e oportunidades de especialização em proteção de dados.
- **Desenvolvimento de cursos específicos sobre a conciliação entre a aplicação da LGPD e da LAI:** Destinados a servidores públicos, ajudando-os a navegar pelas complexidades de ambas as leis no contexto do serviço público.
- **Programas de Acreditação:** Definir parâmetros técnicos a serem seguidos por profissionais que atuam com proteção de dados, credenciando entidades e organismos que pretendam emitir certificados.¹¹⁷

RECOMENDAÇÃO	O QUE A ANPD TEM PREVISTO OU REALIZADO ?
<p>Inclusão da proteção de dados na grade curricular: Esta iniciativa busca integrar a proteção de dados nos currículos escolares e universitários. Isso pode envolver a criação de módulos específicos sobre privacidade e segurança digital, adaptados para diferentes níveis educacionais, desde o ensino fundamental até o superior. A parceria também visa incluir a proteção de dados na Base Nacional Comum Curricular (BNCC), garantindo que o tema seja abordado de forma sistemática em todo o país.</p>	<p>A “Cultura Digital” é a quarta Competência Geral da BNCC.</p> <p>Na BNCC-Computação, há uma trilha de conhecimento contínuo na Educação Básica em prol do desenvolvimento de competências sobre alfabetização digital (compreensão sobre dados e algoritmos, gestão de requisitos, avaliação crítica e cidadã, pesquisa, práticas de privacidade e prevenção de golpes). No Ensino Médio, a habilidade EM13CO26¹¹⁸ faz referência explícita à LGPD.</p> <p>Apesar disso, não consta menção específica à Proteção de Dados Pessoais no Plano Nacional de Educação em discussão no Senado Federal.</p> <p>É relevante compreender se há ações planejadas no escopo da Política Nacional do Livro Didático, destinada a disponibilizar obras didáticas, pedagógicas e literárias de forma sistemática, regular e gratuita.</p>
<p>Implementação de um programa de Alfabetização Digital para Proteção de Dados: Inspirado no modelo europeu <i>Safer Internet Programme</i>, este programa</p>	<p>Há exemplos de projetos de empoderamento em proteção de dados pessoais, alfabetização digital e participação de crianças e adolescentes no Brasil. Dentre</p>

¹¹⁷ Em consonância com o artigo 35, §3º da LGPD.

¹¹⁸ Esta habilidade visa a orientar os estudantes sobre questões que se referem ao respeito a Lei Geral de Proteção de Dados e outras correlacionadas, seja nas oportunidades de interação e colaboração online (navegação nas redes sociais, organização de grupos de trabalho etc.), seja na produção de uma pesquisa científica (autoria na produção de materiais, por exemplo) ou mesmo no desenvolvimento de um software, onde é necessário avaliar que tipo de informação é possível coletar de um usuário e o que pode ser feito com ela.

RECOMENDAÇÃO	O QUE A ANPD TEM PREVISTO OU REALIZADO ?
<p>ofereceria recursos educacionais, ferramentas de avaliação e suporte para escolas e famílias na promoção de hábitos digitais seguros.</p>	<p>eles, tem-se: o CONANDA e o Conselho de Participação de Adolescentes, que atuou no desenvolvimento da Resolução n.º 2.45, as estruturas de Conselhos de Participação Estaduais e Municipais e programas promovidos por ONGs (ex. <i>Criativos na Escola</i>, do Instituto Alana; <i>Cidadão Digital</i>, da SaferNet Brasil em parceria com a Meta).</p> <p>Há, também, Políticas relevantes em curso, a exemplo da Política Nacional de Proteção da Criança e do Adolescente no Ambiente Digital (MDHC e Conanda), Política de Educação Midiática (SECOM-PR), o Programa Nacional do Livro Didático (MEC), a Estratégia para Eliminar a Violência Contra Crianças e Adolescentes (MJSP), estruturas que favorecem Políticas integradas com o empoderamento da comunidade escolar e famílias, cuja temática de Privacidade e Proteção de Dados é relevante.</p> <p>Apesar disso, não encontrou-se iniciativas em estrutura e escalabilidade nacional, com engajamento da ANPD, para promoção de programas de empoderamento de jovens e da comunidade escolar.</p>
<p>Criação de cursos específicos para capacitar agentes públicos: Esses cursos devem focar na proteção de dados no exercício de suas funções. Abordam temas como gestão de dados governamentais, segurança da informação no setor público e atendimento aos direitos dos titulares de dados.</p>	<p>Parcerias com a ENAP para revisão de cursos (<i>ver item 4.1 - ENAP</i>).</p> <p>Realização de webinários formativos no tema.</p>
<p>Implementação do Programa de Governança em Privacidade da ENAP (PGP-ENAP): Esse programa visa capacitar servidores públicos em práticas de governança de dados e privacidade.</p>	<p><i>Ver item 4.1 - ENAP e item 4.6 - Trilhas Formativas.</i></p>
<p>Criação de uma "Escola de Formação em Proteção de Dados Pessoais": Voltada para profissionais do setor público e privado, esta escola poderia oferecer programas de formação continuada, certificações e oportunidades de especialização em proteção de dados.</p>	<p>Não há registro de iniciativa de Escola de Formação em Proteção de Dados.</p> <p>Há previsão e concretização de parcerias para disponibilização de cursos em plataformas existentes (<i>ver item 4.1 - ENAP</i>).</p> <p>Um exemplo interessante é o modelo da Escola de Governança da Internet, do NIC.br e CGI.br e dos programas Educativos e para Intercâmbio de Conhecimento entre profissionais da EDPB.</p>

RECOMENDAÇÃO	O QUE A ANPD TEM PREVISTO OU REALIZADO ?
Desenvolvimento de cursos específicos sobre a conciliação entre a aplicação da LGPD e da LAI: Destinados a servidores públicos, ajudando-os a navegar pelas complexidades de ambas as leis no contexto do serviço público.	ANPD e CGU formalizaram, em 2023 , Acordo de Cooperação Técnica , que tem, em seu objeto, a elaboração conjunta de cursos de capacitação e formação relacionados à transparência e proteção de dados pessoais.
Programas de Acreditação: Definir parâmetros técnicos a serem seguidos por profissionais que atuam com proteção de dados, credenciando entidades e organismos que pretendam emitir certificados. ¹¹⁹	A Resolução CD/ANPD nº 18 de 16 de julho de 2024 dispõe, em seu art. 18, da dispensa de certificação para profissionais encarregados de dados.

4.5. Campanhas de Conscientização e Engajamento Público

Nesse seguimento, as iniciativas e sugestões mapeadas buscam aumentar a visibilidade do tema da proteção de dados e engajar o público de forma mais ampla e acessível. Utilizando uma variedade de estratégias de comunicação, como campanhas de conscientização, celebração de datas comemorativas, parcerias com influenciadores digitais e presença intensificada nas mídias sociais, o objetivo é informar e educar diversos segmentos da sociedade sobre seus direitos e responsabilidades relacionados à proteção de dados. Essas abordagens buscam tornar o tema mais relevante e compreensível para diferentes públicos, promovendo uma cultura de proteção de dados mais abrangente e participativa.

- **Realização de campanhas massivas de conscientização:** Inspiradas na abordagem do GDPR europeu, estas campanhas utilizam múltiplos canais de comunicação para informar o público sobre seus direitos e responsabilidades em relação à proteção de dados.
- **Celebração de datas comemorativas:** Eventos como o Dia Internacional de Proteção de Dados (28/01), o aniversário da LGPD (14/08), o Dia da Informática (15/08), o Dia Nacional do Idoso (01/10), o Dia das Crianças (12/10) e o aniversário da ANPD (06/11) são utilizados para promover atividades especiais, como feiras de informação, concursos e debates públicos.
- **Parcerias com influenciadores digitais:** Visando a divulgação científica e a promoção de concursos culturais. Influenciadores criam conteúdo educativo sobre proteção de dados em formatos acessíveis e atrativos para diferentes públicos.
- **Intensificação da presença da ANPD nas mídias sociais:** Envolve a criação de séries de posts informativos, vídeos explicativos e sessões de perguntas e respostas ao vivo.

¹¹⁹ Em consonância com o artigo 35, §3º da LGPD.

RECOMENDAÇÃO	O QUE A ANPD TEM PREVISTO OU REALIZADO ?
<p>Realização de campanhas massivas de conscientização: Inspiradas na abordagem do GDPR europeu, estas campanhas utilizam múltiplos canais de comunicação para informar o público sobre seus direitos e responsabilidades em relação à proteção de dados.</p>	<p>Identificou-se realização de campanha de alerta ao consumidor em 2021, sob o lema “Proteja Seus Dados: Não Compartilhe”, realizada junto ao Consumidor.Gov e MJSP.</p> <p>Além disso, há campanhas no tema desenvolvidas por outros órgãos relevantes, como CNMP (campanha de prevenção à fraudes na Black Friday), TJSP e MPSC (campanha CPF para quê?) e organizações da sociedade civil (Tira Meu Rosto da Sua Mira) e Coalizão Direitos na Rede (Seus Dados São Você).</p>
<p>Celebração de datas comemorativas: Eventos como o Dia Internacional de Proteção de Dados (28/01), o aniversário da LGPD (14/08), o Dia da Informática (15/08), o Dia Nacional do Idoso (01/10), o Dia das Crianças (12/10) e o aniversário da ANPD (06/11) são utilizados para promover atividades especiais, como feiras de informação, concursos e debates públicos.</p>	<p>Em 2024, a ANPD comemorou o Dia Internacional da Proteção de Dados Pessoais como data simbólica para entrega de projetos, realização de <i>lives</i> e divulgação de materiais na busca de conscientização sobre exercício de direitos dos titulares.</p> <p>Em 2025, uma das ações centrais de celebração do dia envolveu o evento "Importância da Segurança para a Proteção de Dados", em parceria com o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), do Núcleo de Informação e Coordenação do Ponto BR (NIC.br).</p> <p>Outras datas relevantes, como o Aniversário da LGPD, o Dia da Informática, o Dia Nacional da Pessoa Idosa, o Dia das Crianças e o Aniversário da ANPD foram incluídas no Plano Institucional de Ações Educativas da Autoridade.</p> <p>Tem-se também o PL 2076/2022, já aprovado no Senado Federal, institui o Dia Nacional da Proteção de Dados Pessoais em 17 de Julho. Está pronto para Pauta em Plenário na Câmara dos Deputados, já tendo passado pelo rito de tramitação nas Comissões e tendo tido parecer favorável.</p>
<p>Parcerias com influenciadores digitais: Visando a divulgação científica e a promoção de concursos culturais. Influenciadores criam conteúdo educativo sobre proteção de dados em formatos acessíveis e atrativos para diferentes públicos.</p>	<p>Não foi identificada ação de parceria com influenciadores digitais enquanto estratégia de conscientização no Plano de Ações Educativas 2023-2024 ou no Balanço de 4 anos da ANPD. Há projetos modelo no Supremo Tribunal Federal e previstos na Estratégia Brasileira de Educação Midiática da SECOM-PR.</p>
<p>Intensificação da presença da ANPD nas mídias sociais: Envolve a criação de séries de posts informativos,</p>	<p>Hoje, a ANPD tem presença na rede Instagram, fazendo postagens regulares de divulgação de materiais, novidades e resultados de casos de fiscalização.</p>

RECOMENDAÇÃO	O QUE A ANPD TEM PREVISTO OU REALIZADO ?
vídeos explicativos e sessões de perguntas e respostas ao vivo.	Há também na rede uso de estratégia de vídeos curtos e falas de evento no Recurso Reels, Fixado de divulgação de Notícias, Prêmios, Guias, Denúncias e Petições e postagem regular de divulgações no <i>feed</i> (a título de exemplo, foram 9 postagens realizadas no mês de Janeiro de 2025).

4.6. Desenvolvimento de Plataformas e Recursos Digitais

Por fim, este grupo de iniciativas e sugestões têm por meta criar infraestruturas digitais para suportar e ampliar o alcance das ações educativas sobre proteção de dados. Estas propostas incluem o desenvolvimento de plataformas online, páginas web informativas, sistemas de monitoramento e avaliação, e recursos digitais educacionais. O objetivo é facilitar o acesso à informação, oferecer capacitação gratuita, e promover o engajamento contínuo dos cidadãos em relação à proteção de dados. Por meio dessas iniciativas digitais, busca-se criar um ambiente online abrangente e interativo que apoie efetivamente as ações de educação nesta área, tornando-as mais acessíveis e eficazes para diversos públicos.

- **Criação de uma página no site da ANPD para os titulares de dados:** Visando facilitar o acesso à informação. Inclui seções como "Conheça seus direitos", "Como fazer uma reclamação" e "Perguntas frequentes".
- **Desenvolvimento de uma plataforma pública e gratuita de capacitação:** Focada em proteção de dados, esta plataforma oferece cursos, materiais de estudo e ferramentas de avaliação para diferentes públicos.
- **Implementação de um sistema de monitoramento e avaliação contínua:** Este sistema permite acompanhar a eficácia das iniciativas educacionais. Inclui métricas de engajamento, testes de conhecimento e pesquisas de satisfação.
- **Criação de um subdomínio específico para o CNPD no portal da ANPD:** Este subdomínio serve para centralizar informações e campanhas educativas. Inclui um repositório de recursos educacionais, um calendário de eventos e um fórum para discussões sobre proteção de dados.
- **Atualização regular da seção de Perguntas Frequentes no site da ANPD:** Essa seção deve ser constantemente atualizada para refletir as dúvidas mais comuns dos cidadãos e fornecer informações atualizadas sobre proteção de dados.
- **Criação de uma trilha de aprendizagem chamada "Privacidade e Segurança da Informação":** Disponibilizada na plataforma Escola Virtual de Governo (EV.G), oferecendo uma série de cursos interconectados sobre proteção de dados e segurança da informação.

RECOMENDAÇÃO	O QUE A ANPD TEM PREVISTO OU REALIZADO ?
Criação de uma página no site da ANPD para os titulares de dados: Visando facilitar o acesso à informação. Inclui seções como "Conheça seus direitos", "Como fazer uma reclamação" e "Perguntas frequentes".	Ação prevista no Plano de Ações Educacionais 2023-2024 , há página no Portal da ANPD com explicações básicas sobre proteção de dados, dicas sobre proteção de dados, direitos dos titulares de dados e ferramentas de denúncia e petição.
Criação de um subdomínio específico para o CNPD no portal da ANPD: Este subdomínio serve para centralizar informações e campanhas educativas. Inclui um repositório de recursos educacionais, um calendário de eventos e um fórum para discussões sobre proteção de dados.	Há página que indexa ações do CNPD dentro do website da ANPD, mas seu objetivo não é, necessariamente, a divulgação de materiais educativos. A ANPD transformou a página de Publicações e Documentos em uma "Central de Conteúdo" , agregando materiais destinados para titulares de dados e agentes de tratamento sobre o tema.
Atualização regular da seção de Perguntas Frequentes no site da ANPD: Essa seção deve ser constantemente atualizada para refletir as dúvidas mais comuns dos cidadãos e fornecer informações atualizadas sobre proteção de dados.	Hoje, a ANPD possui página de Perguntas Frequentes , ação prevista no Plano de Ação Educacional
Desenvolvimento de uma plataforma pública e gratuita de capacitação: Focada em proteção de dados, esta plataforma oferece cursos, materiais de estudo e ferramentas de avaliação para diferentes públicos.	Não previsto no Plano de Ações Educacionais. Estratégia tem sido a articulação com plataformas existentes, como as parcerias com a ENAP.
Implementação de um sistema de monitoramento e avaliação contínua: Este sistema permite acompanhar a eficácia das iniciativas educacionais. Inclui métricas de engajamento, testes de conhecimento e pesquisas de satisfação.	Hoje, o monitoramento de Ações Educativas da ANPD dá-se por instrumento de planejamento publicado no website sem acesso, na página de publicação, de mecanismo para download dos dados, o que dificulta trabalhos de monitoramento social de indicadores.
Criação de uma trilha de aprendizagem chamada "Privacidade e Segurança da Informação": Disponibilizada na plataforma Escola Virtual de Governo (EV.G), oferecendo uma série de cursos interconectados sobre proteção de dados e segurança da informação.	Hoje, não há Trilha de Aprendizagem no tema na Plataforma da Escola Virtual de Governo da ENAP, mas há Cursos de Proteção de Dados Pessoais, inclusive com conteudistas, órgãos públicos e institutos de pesquisa.

Estas iniciativas e sugestões formam um conjunto abrangente de ações e abordam diferentes aspectos da educação e conscientização, garantindo que todos os setores da sociedade sejam alcançados e, se implementadas de forma coordenada, têm o potencial de criar um ecossistema educacional robusto e eficaz em proteção de dados no Brasil.

5. Recomendações

No capítulo anterior, foi apresentado um quadro geral de todas as iniciativas identificadas e sugestões coletadas para desenvolver o acultramento em proteção de dados pessoais no Brasil. Elas refletem o acúmulo de conhecimento e as discussões realizadas ao longo dos trabalhos deste GT, levando em consideração as análises sobre a maturidade da proteção de dados no Brasil, os desafios identificados e os subsídios coletados de diversas fontes. Além de coletar esses subsídios, entende este GT que deve apresentar recomendações do GT1 para a ANPD na formulação de sua política pública em matéria de educação e capacitação em proteção de dados pessoais.

De fato, não se pode ignorar o caráter técnico-político do CNPD, no geral, e deste GT, em particular. Ambos são órgãos colegiados formados por especialistas em proteção de dados que atuam como representantes de diversos setores da sociedade civil e do Estado. Essa composição híbrida garante que as respectivas discussões e decisões do considerem tanto o conhecimento técnico especializado quanto às diferentes perspectivas e interesses dos diversos segmentos da sociedade brasileira. Não se deve esquecer que, em conformidade com o artigo 55 da LGPD e seu regimento interno, o CNPD tem a função de assessorar a ANPD na elaboração de diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade. Assim, o CNPD se posiciona como um ator fundamental na construção de uma política de proteção de dados que seja ao mesmo tempo tecnicamente sólida e socialmente relevante.

As recomendações a seguir visam auxiliar a ANPD a definir as prioridades para suas ações em matéria de educação e capacitação, indicando quais iniciativas devem ser mantidas, aperfeiçoadas, reavaliadas, descontinuadas ou iniciadas, sob a ótica deste GT1. A escolha das prioridades é fundamental para garantir que os recursos da ANPD sejam direcionados para as áreas de maior impacto e relevância para a sociedade brasileira. Espera-se que estas sugestões contribuam para o desenvolvimento de uma política pública eficaz e abrangente, capaz de promover a conscientização e o conhecimento sobre a importância da proteção de dados pessoais em toda a sociedade brasileira, preparando cidadãos e organizações para o exercício pleno da cidadania digital. Ao promover a educação e a capacitação em proteção de dados, a ANPD investirá no futuro de uma sociedade mais justa, transparente e democrática.

Diante deste quadro, sem prejuízo da adoção de outras iniciativas em sua Política Pública, os membros do GT1 recomendam à ANPD que, dentre as diversas iniciativas e sugestões mapeadas, priorize:

5.1. Criação da Escola Nacional da Proteção de Dados (ENAD)

A criação de uma Escola Nacional de Proteção de Dados permitirá que a ANPD consolide e sistematize os esforços de educação e capacitação em proteção de dados, garantindo a qualidade e a padronização dos conteúdos e das metodologias. Além disso, a Escola Nacional poderá atuar como um centro de referência e de excelência em proteção de dados, promovendo a pesquisa, a inovação e o desenvolvimento de novas tecnologias e soluções para a proteção da privacidade.

Ações Sugeridas

- **Definição da estrutura e do modelo de gestão:** Definir a estrutura organizacional da Escola Nacional, incluindo a composição do corpo docente, a forma de financiamento e os mecanismos de governança.
- **Criação de um catálogo de cursos e de programas de capacitação:** Elaborar um catálogo de cursos e de programas de capacitação abrangente e diversificado, que contemple diferentes níveis de conhecimento e diferentes áreas de atuação, desde cursos básicos de conscientização até programas de especialização e de pós-graduação.
- **Desenvolvimento de materiais didáticos e de recursos educativos:** Produzir materiais didáticos e recursos educativos de alta qualidade, utilizando diferentes formatos e linguagens, como guias, cartilhas, vídeos, podcasts, jogos, entre outros.
- **Estabelecimento de parcerias com instituições de ensino e de pesquisa:** Firmar parcerias com universidades, centros de pesquisa e outras instituições de ensino para oferecer cursos e programas de capacitação, realizar pesquisas e desenvolver projetos de inovação em proteção de dados.
- **Promoção de eventos e de atividades de divulgação:** Organizar eventos, seminários, workshops e outras atividades de divulgação para promover a conscientização e o conhecimento sobre a proteção de dados.
- **Certificação de profissionais e de organizações:** Criar um sistema de certificação de profissionais e de organizações que atuam na área de proteção de dados, visando garantir a qualidade e a competência dos serviços prestados.

5.2. Semana da Privacidade

A criação da "Semana da Privacidade" permitirá que a ANPD concentre seus esforços de comunicação e educação em um período específico do ano, gerando maior impacto e visibilidade para o tema da proteção de dados. Além disso, o evento servirá como um espaço para reconhecer e premiar as iniciativas de destaque na área, incentivando a adoção de boas práticas e o aprimoramento contínuo da proteção de dados pessoais no Brasil.

Ações Sugeridas

- **Definição do período e da temática:** Definir o período do ano em que será realizada a "Semana da Privacidade", considerando datas relevantes para a proteção de dados, bem como a temática geral do evento, que deverá ser renovada a cada ano, buscando abordar os temas mais relevantes e atuais da proteção de dados.
- **Criação de um comitê organizador:** Formar um comitê organizador com representantes da ANPD e do CNPD, visando garantir a diversidade de perspectivas e a qualidade das atividades.
- **Realização de outros concursos:** à semelhança do que já ocorre com o “Prêmio Danilo Doneda”, criar concursos com outros formatos e temáticas (eg. tutela de vulneráveis etc.), possibilitando a participação mais ampla de interessados no tema da privacidade.
- **Distribuição de prêmios e comendas:** Criar categorias de premiação para reconhecer diferentes tipos de iniciativas (pública, privada, acadêmica etc.) e estabelecer critérios claros e transparentes para a seleção dos premiados. Promover uma cerimônia de premiação durante a "Semana da Privacidade", com ampla divulgação na mídia e nas redes sociais.
- **Incentivo à participação da sociedade civil:** Estimular a participação da sociedade civil na organização e na realização das atividades da "Semana da Privacidade", oferecendo apoio financeiro e técnico para projetos e iniciativas inovadoras.

5.3. Parceria com o MEC

A parceria com o MEC permitirá que a ANPD alcance muitos estudantes, professores e gestores escolares em todo o país, disseminando o conhecimento sobre a LGPD e a proteção de dados de forma eficaz e abrangente. Essa parceria poderá garantir que as futuras gerações estejam preparadas para lidar com os desafios da proteção de dados no mundo digital.

Ações Sugeridas

- **Criação de materiais didáticos oficiais sobre a LGPD para distribuição gratuita em instituições de ensino:** Elaborar materiais didáticos em diferentes formatos (livros, cartilhas, vídeos, jogos etc.) e adaptados para diferentes faixas etárias e níveis de ensino, que abordem os principais conceitos da LGPD e da proteção de dados.
- **Incentivo à inclusão da educação em proteção de dados na Base Nacional Comum Curricular (BNCC):** Articular com o MEC para incluir a educação em proteção de dados na BNCC e monitorar as capacidades previstas na BNCC-Computação, garantindo que o tema seja abordado de forma transversal e interdisciplinar em todas as etapas da educação básica, estabelecendo indicadores e estrutura de monitoramento público.
- **Desenvolvimento de programas de capacitação para professores em proteção de dados e privacidade:** Oferecer cursos, workshops e treinamentos para os professores e os gestores escolares, visando capacitá-los para lidar com os desafios da proteção de dados no ambiente educacional e para transmitir o conhecimento sobre a LGPD aos alunos, tanto em formato presencial quanto formação à distância, a exemplo da plataforma Avamec.
- **Promoção de eventos e debates sobre proteção de dados nas universidades:** Realizar eventos, seminários e debates sobre a proteção de dados nas universidades, visando estimular a pesquisa, extensão e o desenvolvimento de soluções inovadoras para a proteção da privacidade, inclusive com financiamento e editais públicos de incentivo.
- **Fortalecimento de parcerias e ações com o Sistema de Garantia de Direitos e com o MEC, Comunidade Escolar e Conselhos da área:** Desenvolver materiais didáticos oficiais, inserir o tema nos currículos, definir indicadores de monitoramento, promover estratégias de conscientização, criar instrumentos regulatórios de apoio para gestores escolares, ampliar a fiscalização da proteção de dados em plataformas educacionais ou grandes plataformas com tecnologias que atraem crianças e adolescentes e fomentar um ambiente de inovação seguro, adequado à idade e em prol da educação.
- **Criação de um programa de Alfabetização Digital para Proteção de Dados:** Inspirado no modelo europeu Safer Internet Programme, oferecendo recursos educacionais, ferramentas de avaliação e suporte para escolas e famílias na promoção de hábitos digitais seguros, inclusive abordando questões como direito à privacidade de crianças e adolescentes, compartilhamento excessivo ou abusivo de informações

de pares ou por responsáveis e prevenção de abuso e exploração sexual no contexto de tecnologias emergentes.

- **Promoção de Hackathons e Desafios de Inovação.** A realização de competições voltadas para o desenvolvimento de soluções tecnológicas e criativas, temáticas, que acompanhassem a agenda regulatória da ANPD, o que incentivaria a inovação e a participação de jovens talentos. Os eventos poderiam ser realizados em parceria com ONGs, universidades, startups e empresas de tecnologia.
- **Incentivo à participação dos cidadãos na fiscalização do uso de seus dados:** Implementar ações que promovam o conhecimento e a conscientização para uma participação mais ativa no controle dos dados pessoais.

5.4. Revisão do Plano Nacional de Educação (PNE)

A participação ativa da ANPD nos debates sobre a revisão do PNE permitirá que a Autoridade contribua com sua expertise e conhecimento técnico para influenciar o conteúdo do plano e garantir que ele reflita as melhores práticas e as mais recentes tendências em matéria de proteção de dados. Além disso, essa participação fortalecerá a imagem da ANPD como um órgão de referência e de vanguarda na proteção da privacidade e dos dados pessoais no Brasil.

Ações Sugeridas

- **Acompanhamento das discussões:** Acompanhar de perto os debates públicos no Senado Federal sobre a revisão do PNE, identificando os pontos de maior relevância para a proteção de dados pessoais.
- **Elaboração de propostas de aprimoramento:** Elaborar propostas de aprimoramento do PNE, com base na LGPD e nas melhores práticas internacionais, visando integrar a proteção de dados de forma transversal e interdisciplinar em todas as etapas e modalidades de ensino.
- **Articulação com outros atores relevantes:** Articular com outros atores relevantes, como o Ministério da Educação (MEC), as universidades, as organizações da sociedade civil e os parlamentares, visando construir um consenso em torno das propostas de aprimoramento do PNE.
- **Participação e organização de audiências públicas e debates:** Participar ativamente das audiências públicas promovidas pelo Senado Federal para debater a revisão do PNE, apresentando as propostas da ANPD e defendendo a importância da proteção de dados pessoais para a educação no Brasil, bem como realizar eventos para fomentar a construção de conhecimento e agenda na temática.

- **Divulgação das propostas:** Divulgar amplamente as propostas da ANPD para a revisão do PNE, utilizando os seus canais de comunicação (site, redes sociais, imprensa) e buscando o apoio da mídia especializada e da sociedade civil.

5.5. Parceria com entidades reguladoras setoriais e outros órgãos públicos

A colaboração com órgãos reguladores setoriais permitirá que a ANPD otimize seus recursos, aproveitando a expertise e a infraestrutura já existentes em cada setor. Além disso, essa abordagem garante que as ações educativas sejam mais direcionadas e relevantes para cada público, aumentando sua efetividade e o impacto na conscientização e na adoção de boas práticas em proteção de dados pessoais. Recomenda-se, portanto, que a ANPD estabeleça parcerias estratégicas com órgãos reguladores setoriais, tais como Anatel, Anvisa, ANS, Senacon, Secom, MCTI, dentre outros, para a criação conjunta de conteúdo educativo e campanhas de conscientização sobre proteção de dados pessoais, direcionadas aos respectivos *stakeholders*.

Ações Sugeridas

- **Mapeamento de órgãos reguladores setoriais e outros órgãos públicos relevantes:** Identificar os órgãos com maior interface com o tema da proteção de dados e com potencial para colaboração na disseminação de informações e boas práticas (eg. Anatel, Anvisa, ANS, Senacon, Secom, MCTI etc.).
- **Definição de áreas temáticas prioritárias:** Estabelecer, em conjunto com os órgãos parceiros, as áreas temáticas mais relevantes para cada setor, considerando as especificidades de cada atividade e os riscos envolvidos no tratamento de dados pessoais.
- **Criação de grupos de trabalho interinstitucionais:** Formar grupos de trabalho com representantes da ANPD e dos órgãos parceiros para o desenvolvimento conjunto de materiais educativos, como guias, cartilhas, vídeos, podcasts, entre outros.
- **Realização de eventos e treinamentos:** Promover eventos, seminários e treinamentos em parceria com os órgãos reguladores setoriais, visando capacitar os agentes de tratamento e os titulares de dados sobre seus direitos e obrigações.
- **Desenvolvimento de campanhas de conscientização:** Elaborar campanhas de conscientização direcionadas aos respectivos stakeholders, utilizando linguagem acessível e formatos variados, como posts em redes sociais, vídeos explicativos, banners em sites, entre outros.
- **Integração de conteúdos nos canais de comunicação dos órgãos:** Utilizar os canais de comunicação dos órgãos reguladores setoriais para disseminar os materiais educativos e as campanhas de conscientização, ampliando o alcance das ações.

5.6. Criação de conteúdos específicos sobre proteção de dados para grupos vulneráveis

A criação de conteúdos específicos e adaptado para grupos vulneráveis (crianças, adolescentes, idosos, mulheres, PCDs, pessoas racializadas e LGBTQIAPN+ etc.), garantindo que esses grupos compreendam seus direitos e responsabilidades no ambiente digital e permitindo o acesso à informação sobre proteção de dados de forma clara, acessível e relevante. Esses conteúdos devem levar em consideração as necessidades e características específicas de cada grupo, utilizando linguagem simples, formatos variados e exemplos práticos para facilitar a compreensão e o engajamento. Ao capacitar os grupos vulneráveis para proteger seus dados pessoais, a ANPD contribuirá para a construção de uma sociedade mais justa, igualitária e democrática.

Ações Sugeridas

- **Realização de pesquisas e consultas:** Realizar pesquisas e consultas com representantes dos diferentes grupos vulneráveis para identificar suas necessidades e desafios específicos em relação à proteção de dados pessoais.
- **Adaptação da linguagem e dos formatos:** Adaptar a linguagem e os formatos dos conteúdos sobre proteção de dados para atender às necessidades de cada grupo vulnerável, utilizando linguagem simples e clara, evitando jargões técnicos e jurídicos, e explorando diferentes formatos, como vídeos, animações, jogos, cartilhas ilustradas,¹²⁰ podcasts, entre outros.
- **Criação de materiais de conscientização voltados especificamente ao público infantil e juvenil:** Desenvolver materiais adequados à faixa etária para a educação em proteção de dados desde cedo, com a criação de personagens e histórias que representem abordem situações cotidianas em que seus dados pessoais podem estar em risco, visando promover a identificação e o engajamento com o tema.
- **Promoção de campanhas de conscientização:** Desenvolver campanhas de conscientização específicas para cada grupo vulnerável, utilizando os canais de comunicação mais adequados para alcançar cada público (redes sociais, rádio, televisão, jornais, revistas, eventos comunitários, inserção do tema em produções audiovisuais nacionais, entre outros).

¹²⁰ Nesse particular, convém registrar a recente publicação, pela da ANPD, em parceria com a Comissão Nacional de Informática e Liberdade da França (CNIL) e a Comissão de Proteção de Informações Pessoais da Coreia do Sul (PIPC), do mangá educativo *"Meus Dados, Meus Direitos"* em português. Esta iniciativa visa a sensibilizar jovens acerca de seus direitos em matéria de proteção de dados pessoais, promovendo uma cultura de privacidade e de uso responsável de seus dados. Sobre o tema: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-cnil-e-pipc-promovem-conscientizacao-sobre-protecao-de-dados-entre-jovens-por-meio-de-manga>. Acesso em 14 fev 2025.

- **Estabelecimento de parcerias:** Estabelecer parcerias com organizações da sociedade civil e do poder público que atuam em defesa e atendimento aos direitos dos grupos vulneráveis e do consumidor, visando ampliar o alcance e o impacto das ações de educação e conscientização nos territórios.
- **Criação de um guia de boas práticas:** Elaborar um guia de boas práticas para a criação de conteúdos sobre proteção de dados para grupos vulneráveis, contendo orientações sobre linguagem, formatos, exemplos e outras dicas úteis para garantir a acessibilidade e a relevância da informação, além de serviços para denúncia e modelos para garantia de mecanismos de exercício de direitos dos titulares de dados.
- **Elaboração de enunciados que orientem o tratamento de dados pessoais dos grupos vulneráveis:** Construir, com base nos resultados da consulta pública e nos estudos da ANPD, enunciados que orientem o tratamento de dados pessoais de grupos vulneráveis.

5.7. Parceria com a ENAP

O fortalecimento da parceria com a ENAP permitirá que a ANPD aproveite a expertise e a infraestrutura da escola para alcançar um maior número de servidores públicos e promover uma cultura de proteção de dados em toda a administração pública. Além disso, essa parceria garantirá a qualidade e a padronização dos conteúdos e das metodologias de ensino, contribuindo para a formação de profissionais capacitados e comprometidos com a proteção da privacidade.

Ações Sugeridas

- **Desenvolvimento de uma grade curricular abrangente:** Elaborar, em conjunto com a ENAP, uma grade curricular abrangente e diversificada, que contemple diferentes níveis de conhecimento e diferentes áreas de atuação, desde cursos básicos de conscientização até programas de especialização e de pós-graduação.
- **Criação de cursos online e presenciais:** Oferecer cursos online e presenciais sobre a LGPD, as boas práticas de proteção de dados no serviço público, a gestão de incidentes de segurança e outros temas relevantes para a atuação dos servidores públicos.
- **Promoção da trilha de aprendizagem "Privacidade e Segurança da Informação":** Divulgar e incentivar a participação dos servidores públicos na trilha de aprendizagem "Privacidade e Segurança da Informação" da Escola Virtual de Governo (EV.G), que oferece uma variedade de cursos e recursos sobre o tema.

- **Desenvolvimento de cursos específicos:** Criar cursos específicos para atender as necessidades específicas dos servidores públicos (e.g. compatibilização entre LAI e LGPD).
- **Realização de eventos e seminários conjuntos:** Promover eventos, seminários e workshops em parceria com a ENAP, visando debater temas relevantes para a proteção de dados no setor público e disseminar boas práticas e experiências.
- **Incentivo à produção de pesquisas e estudos:** Apoiar a produção de pesquisas e estudos sobre a proteção de dados no setor público, visando gerar conhecimento e subsidiar a formulação de políticas públicas.

5.8. Parceria com a OAB-Nacional

A parceria com a OAB-Nacional permitirá que a ANPD alcance muitos advogados em todo o país, disseminando o conhecimento sobre a LGPD e a proteção de dados de forma eficaz e abrangente. Essa iniciativa poderá garantir a formação de profissionais qualificados e comprometidos com a defesa dos direitos dos titulares de dados.

Ações Sugeridas

- **Desenvolvimento de materiais educativos específicos para advogados:** Elaborar materiais didáticos, como guias, cartilhas, vídeos e cursos online, que abordem os principais aspectos da LGPD e da proteção de dados, com foco nas questões jurídicas e nas responsabilidades dos advogados.
- **Realização de eventos e seminários sobre proteção de dados para a comunidade jurídica:** Promover eventos, seminários e workshops em parceria com a OAB-Nacional, visando debater temas relevantes para a proteção de dados no âmbito jurídico, disseminar boas práticas e apresentar casos práticos.
- **Criação de um programa de certificação em proteção de dados para advogados:** Desenvolver um programa de certificação para advogados que atuam na área de proteção de dados, visando reconhecer e valorizar a sua expertise e o seu comprometimento com a privacidade.
- **Inclusão obrigatória de questões sobre proteção de dados no Exame de Ordem:** Articular com a OAB-Nacional para incluir questões sobre a LGPD e a proteção de dados no Exame de Ordem, tornando o tema obrigatório na prova e incentivando o estudo e a especialização dos futuros advogados nessa área.
- **Apoio à criação de comissões de proteção de dados nas seccionais da OAB:** Incentivar a criação de comissões de proteção de dados nas seccionais da OAB em todo o

país, visando promover o debate, a pesquisa e a disseminação do conhecimento sobre a LGPD e a proteção de dados no âmbito local.

5.9. Encontros Profissionais

O sucesso do I Encontro ANPD de Encarregados, que demonstrou a importância da troca de experiências e do diálogo entre os profissionais responsáveis pela proteção de dados nas organizações. A necessidade de ampliar o alcance da conscientização e da capacitação em proteção de dados para outros públicos-alvo que também atuam no tratamento de dados pessoais, como programadores, desenvolvedores e outros. A realização de encontros com diferentes públicos-alvo permitirá que a ANPD compreenda as necessidades e os desafios específicos de cada grupo, adaptando suas ações de educação e capacitação para atender às demandas de cada setor. Além disso, esses encontros promoverão a troca de experiências e o debate sobre as melhores práticas em proteção de dados, incentivando a inovação e a colaboração entre os profissionais.

Ações Sugeridas

- **Identificação dos públicos-alvo:** Identificar os públicos-alvo mais relevantes para a proteção de dados pessoais, considerando os diferentes setores, áreas de atuação, esferas da administração pública e os diferentes níveis de conhecimento sobre o tema (e.g., programadores, desenvolvedores etc.).
- **Definição dos temas e formatos:** Definir, em conjunto com os públicos-alvo, os temas e os formatos mais adequados para cada encontro, considerando as necessidades e os interesses de cada grupo (e.g., workshops, palestras, painéis de debate, estudos de caso etc.).
- **Realização de eventos temáticos:** Organizar eventos específicos para cada público-alvo, abordando temas relevantes para suas áreas de atuação e promovendo a troca de experiências e o debate sobre os desafios e as oportunidades da proteção de dados em diferentes contextos.
- **Promoção da interação entre os participantes:** Estimular a interação entre os participantes, criando espaços para o networking, a troca de informações e a colaboração em projetos e iniciativas conjuntas.
- **Divulgação das boas práticas:** Divulgar as boas práticas e as soluções inovadoras encontradas pelos profissionais, incentivando a adoção de medidas de proteção de dados desde a concepção dos produtos e serviços.
- **Promoção de intercâmbio entre entidades e órgãos públicos com disseminação de boas práticas.** Criar um programa de intercâmbio entre entidades e órgãos públicos

para compartilhar experiências e soluções eficazes na implementação de políticas de proteção de dados, estimulando a cooperação nacional, regional e local.

5.10. Parceria com influenciadores digitais:

A parceria com influenciadores digitais permitirá que a ANPD atinja um público mais amplo e diversificado, utilizando a linguagem e os formatos que são mais eficazes para engajar diferentes segmentos da sociedade. Além disso, essa estratégia contribuirá para desmistificar o tema da proteção de dados, tornando-o mais acessível e relevante para o dia a dia dos titulares e da sociedade.

Ações Sugeridas

- **Mapeamento de influenciadores relevantes:** Identificar influenciadores que atuem em diferentes áreas (tecnologia, direito, educação, cultura etc.) e que possuam um público engajado e alinhado com os objetivos da ANPD.
- **Definição de temas e formatos:** Definir, em conjunto com os influenciadores, os temas e os formatos mais adequados para abordar a proteção de dados, considerando as características do público-alvo e as tendências das redes sociais.
- **Produção de conteúdo educativo:** Elaborar materiais educativos em formatos variados, como vídeos, posts, stories, podcasts, infográficos, memes, entre outros, utilizando linguagem clara e acessível.
- **Realização de campanhas de conscientização:** Desenvolver campanhas de conscientização em parceria com os influenciadores, utilizando hashtags, desafios, sorteios e outras estratégias para aumentar o engajamento e a participação do público.
- **Participação em eventos, podcasts e lives:** Participar de eventos *online*, podcasts e *lives* com a participação dos influenciadores, visando debater temas relevantes para a proteção de dados e responder às dúvidas do público.

As recomendações apresentadas neste capítulo representam um esforço concentrado para orientar a ANPD na formulação de uma política pública robusta e eficaz em matéria de educação e capacitação em proteção de dados pessoais. Priorizando a parceria setorial, a criação de uma escola nacional, o fortalecimento de laços com outras instituições e a produção de conteúdo direcionado a grupos vulneráveis, a ANPD poderá otimizar seus recursos e alcançar um impacto significativo na conscientização e no conhecimento sobre a importância da proteção de dados em toda a sociedade brasileira, preparando cidadãos e organizações para o exercício pleno da cidadania digital e para a construção de uma sociedade mais justa, transparente e democrática.

ANEXO I

SUMÁRIO DOS DADOS DE APOIO PARA A CONSTRUÇÃO DO RELATÓRIO

A. Descrição do Documento

A partir do Relatório Prévio elaborado pelo GT1 do CNPD, foi feito um fichamento dos dados da pesquisa “[Privacidade e Proteção de Dados Pessoais 2023](#)”, do Comitê Gestor da Internet no Brasil, buscando apoiar o trabalho de complementação e enriquecimento das contribuições já realizadas pelos Conselheiros.

Privacidade e Proteção de Dados Pessoais 2023: Perspectivas de Indivíduos, empresas e organizações públicas no Brasil. Núcleo de Informação e Coordenação do Ponto BR. São Paulo: Comitê Gestor da Internet no Brasil, 2024. <https://cetic.br/media/docs/publicacoes/2/20240901120340/privacidade-e-protecao-de-dados-2023.pdf>

B. Metodologia da Pesquisa

Entrevistou, via questionário online, 2.618 usuários de Internet com 16 anos ou mais, em dezembro de 2023, bem como 2075 empresas entre agosto e dezembro de 2023.

C. Indivíduos

a. Atividades mais realizadas para gerenciar o acesso aos seus dados pessoais

- Verificação de segurança de páginas ou aplicativos (67%) (p. 49)
- Recusa de permissão de uso de seus dados para publicidade personalizada (66%) (p. 49)
- Solicitar a exclusão de dados junto a agentes de tratamento é a prática menos apontada (45%) - menor indicador, depende da existência de um canal de atendimento e da ciência do direito (p. 49)
- Para todas as atividades realizadas, indivíduos que usam a Internet exclusivamente por telefone celular apresentaram proporções inferiores àquelas dos que combinam telefone celular com computador (p. 49)

b. Leitura de “Políticas de Privacidade”

- 58% dos usuários de Internet sempre ou quase sempre concordam com as Políticas de Privacidade sem realizar sua leitura (p. 27)
- A proporção é maior para a faixa etária de 25 a 34 anos (39%) e menor para a faixa etária de 45 a 59 anos e 60 anos ou mais (28%) (p. 27)

c. Busca de canais de atendimento para realizar solicitações

- 24% dos usuários de Internet com 16+ buscaram canal de atendimento para solicitações, reclamações ou denúncias em relação aos seus dados pessoais (p. 53)
- Há um recorte de gênero, sendo a proporção maior para usuários do gênero masculino (27%) em relação ao feminino (22%) (p. 53)
- Há, também, um recorte educacional, sendo maior a proporção daqueles que têm Ensino Superior (29%) comparado com os de menor escolaridade (23% até Ensino Fundamental, 22% até Ensino Médio) (p. 53)
- ANPD não é um órgão muito buscado, usuários de Internet tendem a vincular reclamações com relações de consumo ou ocorrências policiais (p. 53)

d. Preocupação com dados pessoais

- Maior nível de preocupação está atrelado a comprar pela Internet por páginas e aplicativos (29% muito preocupados e 27% preocupados), indicando uma percepção de potencial de dano relacionado a dados de transações financeiras, destacando-se a preocupação com impressão digital, reconhecimento facial (p. 55)
- A categoria de dado que gera maior preocupação no compartilhamento é o dado biométrico, a qual 32% disseram estar muito preocupados e 28% preocupados (p. 58)
- Outra categoria relevante engloba os dados de saúde, havendo 24% muito preocupados e 27% preocupados (p. 58)
- Maior nível de preocupação dos usuários, na transmissão de dados biométricos, com instituições financeiras (37% muito preocupados e 46% preocupados), órgãos do governo (35 e 38%) e transporte público (34 e 37%) (p. 59)
- Baixa preocupação com dados de saúde menstrual da mulher - apesar de serem *apps* que coletam enormemente dados de saúde e haver preocupação relevante geral para dados de saúde (24% muito preocupados e 27% preocupados) (p. 56)
- 68% dos usuários desinstalem aplicativos por preocupações com sua privacidade e proteção de dados, demonstrando aspecto reputacional (p. 57)
- Preocupação alta com “caminhar por espaços públicos como ruas, transporte público etc”, que pode ser relacionada com o aumento de câmeras e vigilância na segurança pública no Brasil (p. 54)
- Maior preocupação com danos de natureza financeira ou relativos à fraude do que com averiguação de práticas de governança segura e perspectiva de riscos (p. 60)

D. Empresas

- A maior parte dos dados pessoais mantidos por empresas, independentemente do porte, é de clientes e usuários ou de parceiros e fornecedores (p. 28)
- A finalidade mais indicada para manutenção de dados de usuários e clientes é o contato direto com esses (70%) e, a segunda, é a checagem de crédito (45%) (p. 28)

- Os dados de funcionário são usados para controle de entrada e saída de locais de trabalho, aumentando a proporção de manutenção de dados biométricos que foi de 24% em 2021 a 30% em 2023 (p. 69)

a. Capacidades Internas

- Em 2021, 23% das empresas possuíam área de governança interna para matérias de proteção de dados pessoais, passando para 25% em 2023 - o que reflete uma estabilidade no indicador (p. 28)
 - Estruturas organizacionais são mais presentes em grandes empresas ou naquelas que lidam com grandes volumes de dados pessoais (p. 72)
- Há convergência entre as áreas de Segurança da Informação e Proteção de Dados Pessoais, sendo que a maior parte das empresas tem a área ou pessoa responsável proveniente da área de TI (69% em 2021 e 68% em 2023) (p. 28)
- Diminuição de reuniões internas sobre proteção de dados pessoais no setor de serviços (p. 72)
- 33% das empresas realizaram ações de treinamento ou capacitações, proporção que foi de 29% em 2021. (p. 74)
- Quanto ao porte, houve, entre as duas edições, um aumento moderado entre as médias empresas. Por outro lado, houve redução na proporção de médias e grandes empresas que realizaram treinamento ou capacitação oferecida por outras empresas. (p. 74)

b. Adequação à LGPD

- Aumento significativo entre 2021 e 2023 nas práticas de adequação à LGPD por empresas, sendo elas (p. 30):
 - Alteração de contratos (de 28%, 2021, a 35%, 2023)
 - Mais proeminente nos setores de construção, transportes, alojamento e alimentação, informação e comunicação, atividades profissionais e serviços
 - Elaboração de Plano de Conformidade para Adequação (de 24%, 2021, para 32%, 2023)
- Práticas de adequação menos realizadas são realização de inventário de dados pessoais (18%) e realização do teste do legítimo interesse (16%) (p. 76)
- Diminuição das empresas que disponibilizam canal de atendimento aos titulares de dados entre 2021 (24%) e 2023 (20%) (p. 76)

E. Setor Público

- Menos da metade das prefeituras oferecem canais para solicitações acerca de dados pessoais (p. 54)
- Entidades do setor público estão entre as que mais reportaram incidentes de segurança relacionados a dados pessoais e mais receberam denúncias passíveis de serem analisadas (p. 66)

a. Capacidades Internas

- **Melhoras nas capacidades internas e na presença de atores ou setores responsáveis pelo tema da privacidade e proteção de dados no Legislativo e Ministério Público.** Aumento de 17 e de 11 pontos percentuais, respectivamente. (p. 85)
- **Necessidade de ampliar ações com Executivo e em nível federativo estadual e municipal:** “Os órgãos do Poder Judiciário (99%) e do nível federal (90%) destacam-se, como observado em 2021, ao passo que os órgãos do Poder Executivo (61%) e do nível estadual (62%) têm esse tipo de iniciativa em proporções inferiores aos demais órgãos públicos investigados pela pesquisa.” (p. 86)
- **Disparidades federais e estaduais:** “Também existem disparidades, principalmente entre os órgãos dos níveis federal e estadual, em relação à oferta de capacitação, curso ou treinamento sobre a LGPD para os funcionários de tecnologia da informação (TI) dos órgãos públicos. Enquanto 84% dos órgãos federais com área de TI reportaram ofertar cursos desse tipo, isso ocorreu em pouco mais da metade dos órgãos estaduais (53%). Ainda sobre essa oferta, foi observado um crescimento entre os órgãos do Poder Legislativo, passando de 49%, em 2021, para 75%, em 2023. Órgãos do Executivo (53%), Judiciário (90%) e Ministério Público (80%) apresentaram estabilidade em relação à 2021, com o Executivo se situando em uma proporção inferior aos demais poderes.” (p. 87)
- **Existência de ações descentralizadas.** “A despeito dessas iniciativas, a implementação de ações relacionadas à privacidade e à proteção de dados é, em geral, realizada de modo independente entre os órgãos públicos dos diferentes níveis de governo e poderes, principalmente entre as entidades estaduais. No Executivo estadual, por exemplo, as iniciativas ligadas ao tema podem ocorrer de maneiras e em momentos distintos nos 26 estados e no Distrito Federal. Entre os tribunais de contas no país, por sua vez, há grande variação nos resultados de adequação à LGPD (Holdefer, 2022). Em outro âmbito, uma análise realizada pelo Tribunal de Contas da União (TCU) entre 382 organizações públicas federais apontou que a maior parte delas ainda está em fase inicial de conformidade com a LGPD (TCU, 2022). Portanto, além de indicar desigualdades na implementação da legislação, esses estudos sinalizam o fato de que as organizações públicas ainda precisam ampliar ações voltadas para a temática.” (p. 86)
- **Nomeação de encarregados seria principal ação adotada no setor público:** “Em relação às ações de implementação da LGPD investigadas pela TIC Governo Eletrônico 2023 (CGI.br, 2024c), a nomeação de encarregado de dados pessoais foi a mais mencionada tanto por órgãos federais (83%) como estaduais (46%). Cabe destacar que houve aumento na nomeação do encarregado entre os órgãos do Executivo (de 34%, em 2021, para 46%, em 2023), do Legislativo (de 40% para 66%) e do nível estadual (de 33% para 46%). Em seguida, a disponibilização de canais de atendimento pela Internet para os cidadãos foi citada por 73% dos órgãos federais e 47% dos estaduais, ocorrendo crescimento na maior parte dos órgãos públicos. (p. 87)
- **Faltam encarregados nas Prefeituras.** Em relação às medidas da LGPD adotadas pelas prefeituras (Gráfico 4), a mais reportada é a disponibilização de canais de atendimento pela Internet sobre o uso de dados pessoais (42%), seguida pela existência de documento formalmente instituído sobre papéis e responsabilidades de áreas e setores relacionados à lei (29%), ao passo

que a nomeação do encarregado (21%) é a ação menos presente. Cabe destacar que a existência de um encarregado é exigida pela legislação, dado que esse é responsável pela transparência em processos fundamentais, como a comunicação com a ANPD e a aplicação de demandas da agência, bem como pela orientação de funcionários sobre dados pessoais e a execução de atribuições estabelecidas pelo controlador ou por normas complementares (ANPD, 2023a). (p. 90)

- **Necessidade de atenção para incidentes de segurança da informação.** “Por fim, a iniciativa menos reportada foi a implementação de um plano de resposta a incidentes de segurança da informação relacionado a dados pessoais, sendo mais presente entre os órgãos do Judiciário (60%) quando comparada aos do Executivo (29%), Legislativo (38%) e Ministério Público (32%). Também foi mais apontada entre os órgãos federais (47%) em relação aos estaduais (30%). Vale ressaltar que, conforme a LGPD, o tratamento de dados pessoais deve ser acompanhado de medidas técnicas e administrativas para minimizar a ocorrência de incidentes de segurança (ANPD, 2023a). Nesse sentido, entre boas práticas para promover a segurança digital no setor público, o governo federal criou diversas iniciativas nessa temática, incluindo um programa de privacidade e segurança da informação e a publicação de guias e modelos para apoiar práticas de segurança que podem ser utilizados ou adaptados por outras organizações públicas.” (p. 89)
- **Diferenças significativas entre capitais e municípios com mais de 100 mil habitantes em relação ao interior do país.** “No âmbito dos governos municipais, também foram observadas mudanças em relação a 2021 em todos os recortes divulgados pela TIC Governo Eletrônico 2023, com maior crescimento de iniciativas relacionadas à privacidade e à proteção de dados entre as prefeituras de capitais e em municípios com mais de 100 mil habitantes. Para a presença de pessoa ou área responsável pela implementação da LGPD em prefeituras, houve um crescimento de 66% para 82% entre 2021 e 2023 nas capitais, e de 28% para 36% nas cidades localizadas no interior. Também foram identificadas diferenças de acordo com o porte populacional do município, principalmente nas cidades de mais de 100 mil e menos de 500 mil habitantes – em que a presença de área ou pessoa responsável pela LGPD passou de 41%, em 2021, para 63%, em 2023 – e naquelas com mais de 500 mil habitantes – em que passou de 62% para 82%” (p. 89)
- **Necessidade de atenção para a região Nordeste. Aumento significativo de ações no Centro-Oeste.** “Para as regiões, o maior crescimento foi observado entre as prefeituras do Centro-Oeste, nas quais a presença de área ou pessoa responsável passa de 28% a 41%. Vale destacar que as proporções nas demais regiões são bastante próximas, com menor presença de área para o tema de privacidade e proteção de dados entre as prefeituras do Nordeste (33%).” (p. 90)
- **Diferenças regionais agravam-se na medida em que cidades maiores avançam e menores não.** “Nota-se que, assim como nas demais dimensões medidas na TIC Governo Eletrônico, o módulo de Privacidade e Proteção de Dados Pessoais indica a maior presença de iniciativas entre as prefeituras de capitais e de cidades de grande porte populacional, especialmente aquelas com mais de 100 mil habitantes. Além disso, entre 2021 e 2023, as maiores cidades também apresentaram um crescimento mais acentuado em grande parte dos indicadores

quando comparado aos resultados dos demais municípios. Um exemplo nesse sentido é a disponibilização de canais de atendimento, ação presente em proporção muito semelhante entre cidades de diferentes portes em 2021 (36% das prefeituras com mais de 500 mil habitantes e 30% das prefeituras com até 10 mil habitantes), e que passa, em 2023, a um cenário de maior presença nas cidades de 500 mil habitantes ou mais (66%) do que nas com até 10 mil habitantes (43%).” (p. 91)

- **Metade das prefeituras não possuíam quaisquer ações sobre privacidade e proteção de dados pessoais.** “Ainda sobre esse indicador, é importante destacar que nem metade das prefeituras no país possuía as ações relacionadas à LGPD investigadas pela pesquisa, apesar do crescimento observado entre 2021 e 2023. Com o avanço da adoção das tecnologias digitais no cotidiano das prefeituras e da implementação de iniciativas de cidades inteligentes, que envolvem uma intensa coleta de dados em tempo real, inclusive de dados pessoais (Bruzze-guez et al., 2024), os resultados da TIC Governo Eletrônico 2023 indicam que a maior parte das prefeituras ainda precisam avançar em ações voltadas para promoção da privacidade e proteção de dados pessoais.” (p. 91)

b. Saúde

- **Discrepância entre estabelecimentos públicos e privados.** “Esse tema tem sido investigado pela pesquisa TIC Saúde desde 2015, quando apenas 24% dos estabelecimentos de saúde tinham um documento com a política de segurança da informação definida, indicador que registrou uma melhora nos últimos anos, avançando para 40%, em 2023. No entanto, observa-se ainda uma discrepância entre os estabelecimentos públicos (24%) e privados (54%), indicando uma maior necessidade de ações dos poderes públicos nesse sentido.” (p.92)
- **Discrepância em relação entre pequenas e grandes cidades.** “Ainda sobre esse indicador, e analisando mais em detalhe os estabelecimentos públicos, aqueles com mais de 50 leitos de internação (49%) e os localizados nas capitais (46%) eram os que mais dispunham de um documento que definia a política de segurança da informação. Já do lado oposto, os com internação até 50 leitos (19%) e aqueles localizados em municípios do interior (22%) eram os que menos tinham esse documento.” (p. 92)
- **Redução de percentual de estabelecimentos com políticas de S.I. entre 2022 e 2023.** “para os estabelecimentos com até 50 leitos de internação (de 28% para 19%) e os com mais de 50 leitos (de 57% para 49%) (Gráfico 5). Ressalta-se que, nos estabelecimentos privados, cerca de metade tem um documento que define a política de segurança da informação, com destaque para os estabelecimentos com mais de 50 leitos de internação (80%) e serviço de apoio à diagnose e terapia (SADT) (62%)” (p. 92-93)
- **Apenas 1/3 de estabelecimentos de saúde forneceram treinamento para seus funcionários em 2023.** “O treinamento de profissionais da saúde é outro aspecto importante para a segurança, privacidade e proteção de dados, pois contribui para que possam identificar e mitigar possíveis riscos e assegurar melhores práticas no tratamento dos dados e no uso das informações dos pacientes. A despeito dessa relevância, apenas um terço dos estabelecimentos de saúde (31%) ofereceu esse tipo de treinamento para seus funcionários em 2023.” (p. 93)

- **Diferenças significativas entre capital e interior e entre rede pública e privada no que concerne oferta de treinamentos para profissionais de saúde.** “Verifica-se para esse indicador uma diferença considerável entre estabelecimentos públicos (16%) e privados (44%). Entre os estabelecimentos públicos, mais especificamente, 37% dos com mais de 50 leitos de internação ofereceram treinamento em segurança da informação para seus funcionários, com um aumento significativo em relação a 2022. Os demais tipos de estabelecimentos públicos, além de estarem em patamares muito inferiores, não apresentaram alteração significativa em relação ao ano anterior, conforme se observa no Gráfico 6. Nota-se, ainda, que os estabelecimentos de saúde da capital (26%) têm oferecido mais esse treinamento do que os situados nos municípios do interior (15%). Em contrapartida, na rede privada, 65% dos com mais de 50 leitos de internação, 54% dos SADT e cerca de 40% dos sem internação e dos com até 50 leitos de internação ofereceram treinamento em segurança da informação em 2023.” (p. 93)
- **Falta de medidas adequadas sobre LGPD.** “Os resultados indicam que grande parte dos estabelecimentos ainda não implementou por completo as medidas recomendadas para se adequarem à LGPD, principalmente aqueles da rede pública de saúde. Nota-se que, de maneira geral, cerca de 40% dos estabelecimentos de saúde realizaram campanha de conscientização interna sobre a LGPD e 30% nomearam um encarregado de dados pessoais, resultado que tem se mantido estável nos últimos dois anos. Ademais, a implementação de um plano de resposta a incidentes apresentou crescimento, passando de 26%, em 2022, para 30%, em 2023 (Gráfico 7). Verifica-se uma diferença significativa entre estabelecimentos públicos e privados na adoção dessas medidas, o que tem se mantido desde o início da apuração desse indicador.” (p. 94)
- **Falta de canais de atendimento para titulares de dados, em especial, nas UBS.** “O percentual de estabelecimentos públicos que disponibilizam canais de atendimento pela Internet para os titulares dos dados entrarem em contato sobre o uso de seus dados pessoais ainda é reduzido, principalmente entre as Unidades Básicas de Saúde (UBS) (17%), os sem internação (17%) e os SADT (17%). Além disso, a disparidade entre os estabelecimentos localizados nas capitais (24%) e aqueles localizados no interior (16%) é evidente. Vale destacar que, entre os direitos dos titulares dos dados, está o de ter fácil acesso a canais de atendimento, inclusive com a possibilidade de solicitar que seus dados sejam apagados nos casos cabíveis.” (p. 95)

c. Educação

- **Alta digitalização da educação.** “De acordo com a edição 2023 da pesquisa TIC Educação: 91% das escolas públicas de Ensino Fundamental e Médio registravam ou consultavam, em formato eletrônico, dados de frequência e de notas; 91%, dados cadastrais; e 53%, informações sobre condições físicas e de saúde dos alunos. Além disso, em 82% das instituições educacionais públicas (77% entre as escolas municipais e 96% entre as estaduais) havia a adoção de diário de classe online ou sistema digital de controle de matrícula, notas e frequência dos alunos, e, em 66% (59% entre as escolas municipais e 84% entre as estaduais), a utilização de um sistema de armazenamento de dados e arquivos em nuvem.” (p. 97)

- **Aumento de Políticas de Proteção de Dados por escolas públicas.** “Na edição 2023 da pesquisa, cerca de metade das escolas públicas declararam ter um documento que define a política de proteção de dados e de segurança da informação na instituição (51%), apresentando um crescimento em relação à edição 2020 (quando essa proporção era de 37%).” (p. 97)
- **Riscos: dados rastreados e plataformas educacionais.** Além das informações fornecidas durante a matrícula ou em levantamentos de dados administrativos, como é o caso, por exemplo, do Censo Escolar da Educação Básica, cada vez mais os estudantes estão expostos ao tratamento de dados rastreados – ou seja, dados que resultam das atividades realizadas nos ambientes online, como cookies, impressão digital, dados de geolocalização, buscas em navegadores e websites, entre outros – e dados inferidos – derivados de análises realizadas a partir das informações fornecidas e dos rastros deixados durante o uso de aplicações digitais (Livingstone et al., 2019; OCDE, 2022; van der Hof, 2016). (p. 97)
- **Aumento da presença de escolas públicas em redes sociais.** “Nesse cenário, entre as edições 2020 e 2023 da pesquisa TIC Educação, a proporção de escolas públicas com perfil ou página em redes sociais passou de 57% para 68%. O crescimento na presença das escolas públicas em redes sociais foi observado em maiores patamares em escolas localizadas em áreas rurais (de 29% para 48%) e entre as escolas de pequeno a médio porte, como de 51 a 150 matrículas (de 33% para 62%) e de 151 a 300 matrículas (de 59% para 79%)” (p. 97)
- **EdTechs reduziram, pós-pandemia, mas continuam presentes.** “De acordo com a edição 2020 da pesquisa, realizada durante o primeiro ano da pandemia, 45% das instituições públicas de educação recorriam a ambientes ou plataformas de aprendizagem com os estudantes, proporção que passou para 35% na edição 2023. Todavia, de acordo com a edição 2023 da pesquisa, em 61% das escolas estaduais os gestores declararam utilizar plataformas, como o Google Classroom, o que evidencia a forte disseminação desses recursos específicos entre essas instituições no período pós-pandemia.” (p. 99)
- **Risco: necessidade de conscientização dos pais e responsáveis.** “Ademais, para além da complexidade e do volume dos dados atrelados à tendência de digitalização, grande parte da responsabilidade por acompanhar, resguardar e garantir que os direitos de crianças e adolescentes sejam respeitados é de responsáveis, educadores, cuidadores e outros indivíduos que atuam com jovens. Em relação aos atores escolares, muitas vezes eles não têm conhecimentos técnicos e jurídicos para compreenderem as formas como os dados de crianças e adolescentes são recolhidos e tratados nos ambientes digitais, quem tem acesso a eles e qual o impacto desse uso para as próprias crianças, tanto no presente quanto no futuro (Livingstone et al., 2024).” (p. 99)
- **Risco: assimetria entre escolas e empresas.** “Além das dificuldades envolvidas no reconhecimento das formas de tratamento dos dados dos estudantes realizadas pelas plataformas e aplicações, de acordo com a Digital Futures Commission (2023), haveria ainda uma assimetria entre as escolas e as empresas de tecnologia nesses contextos. Espera-se que as escolas tomem decisões informadas sobre a adoção de tecnologias e recursos educacionais digitais, e negociem contratos complexos em conformidade com as políticas de proteção de dados, assumindo a responsabilidade por mediar a adoção desses recursos junto às empresas e às famílias; no entanto, muitas vezes tais contratos são assimétricos, permitindo às empresas a

coleta e o tratamento de grandes volumes de dados (CGI.br, 2024a; Evangelista & Gonsales, 2024). Ao mesmo tempo, os dados coletados por plataformas e aplicações continuam indisponíveis para a própria comunidade escolar, que poderia deles se beneficiar para analisar mais profundamente os processos de ensino e de aprendizagem e de gestão das instituições, de forma a aprimorar a garantia do direito de acesso à educação para os estudantes (Turner et al., 2022).” (p. 100)

- **Gratuidade como principal critério na escolha de plataforma educacional.** “Segundo entrevistas realizadas com coordenadores pedagógicos de escolas públicas durante a edição 2022 da pesquisa, 36% deles afirmaram sempre participar da seleção de recursos educacionais digitais implementados nas instituições de ensino onde atuavam, 24% participavam às vezes, 15%, raramente, e 22% nunca participavam. Os coordenadores de escolas estaduais mencionaram atuar na seleção desses recursos em maiores proporções (45%) do que os coordenadores de escolas municipais (33%). Entre os critérios priorizados pelas instituições de ensino para a seleção de recursos educacionais digitais, de acordo com os coordenadores pedagógicos, a gratuidade é o aspecto mais importante, citado por 69% dos profissionais (Gráfico 11). Outros aspectos considerados muito importantes são a adequação ao currículo e aos objetivos de aprendizagem, a acessibilidade e a aprovação dos professores.” (p. 100)
- **Minimização tem menos relevância do que proteção da identidade na escolha de plataformas educacionais.** “Outro ponto que chama a atenção é o fato de os coordenadores mencionarem em maiores proporções a importância de os recursos educacionais digitais adotarem medidas de proteção aos dados e à identidade dos alunos (58%) em comparação com a importância de os recursos digitais coletarem o mínimo possível de dados pessoais dos estudantes (44%). Os dados sobre a percepção dos coordenadores pedagógicos evidenciam os desafios enfrentados pela comunidade escolar em equilibrar o uso de recursos considerados relevantes para apoiar o desenvolvimento dos estudantes com atenção às possíveis formas de violação de seus direitos.” (p. 101)
- **Aumento do uso do reconhecimento facial em escolas, com especial enfoque nos Estados de Goiás e Paraná.** “Do total de escolas públicas, 1% mencionou utilizar sistema de identificação dos estudantes pela digital ou palma da mão e 4%, por reconhecimento facial. No entanto, entre as escolas localizadas na região Sul (12%) e na região Centro-Oeste (7%), uma proporção maior de instituições declarou contar com sistemas de reconhecimento facial. Os estados de Goiás (28%) e Paraná (17%) destacaram-se com os maiores patamares de utilização desses recursos.” (p. 101)
- **Das escolas públicas, 1 em cada 3 promove debates sobre proteção de dados pessoais.** “A respeito desse aspecto, 32% das escolas públicas de Ensino Fundamental e Médio haviam realizado debates ou palestras sobre privacidade e proteção de dados nos 12 meses anteriores à realização da pesquisa. Os professores (32%) e outros funcionários da instituição (30%) destacaram-se como os principais públicos-alvo dessas iniciativas, com alunos (24%) e responsáveis (24%) citados em menores proporções. Por outro lado, 64% dos professores mencionaram terem realizado atividades com os alunos sobre temas relacionados à privacidade, à proteção de dados e à segurança na Internet. No entanto, tais atividades são abordadas princi-

palmente em conversas dos professores com os estudantes e, possivelmente, ainda não fazem parte do currículo, o que demonstra a necessidade de maior articulação entre as instâncias governamentais, de gestão escolar e pedagógicas para a promoção dessas iniciativas entre a comunidade escolar.”

ANEXO II

MINUTA DO OFÍCIO ENCAMINHADO ÀS ENTIDADES DA SOCIEDADE CIVIL

GT1 DO CNPD
EDUCAÇÃO E CAPACITAÇÃO EM PROTEÇÃO DE DADOS PESSOAIS

Entidade: #####

A/C: Representante da Entidade

Ref: Solicitação de contribuição ao CNPD (GT1)

Prezado(a),

Conforme Portaria CNPD nº 01/2024¹²¹, foi estabelecido Grupo de Trabalho **dedicado a fornecer subsídios, na temática de “Educação e Capacitação em Proteção de Dados Pessoais”, para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade**, no âmbito do Conselho Nacional de Proteção de Dados.

Diante da relevância da vossa entidade acerca do tema, caso tenham interesse, **solicitamos a gentileza de apresentar contribuições, por escrito, até o prazo máximo de 13/01/2025**, de acordo com os seguintes quesitos:

- 1) Informações sobre situações concretas e dados estatísticos que demonstrem o déficit educacional e a necessidade de melhora nos índices de conscientização e capacitação em matéria de proteção de dados pessoais;
- 2) Quais iniciativas ou práticas poderiam ser **replicadas** ou **difundidas** pela ANPD para melhorar os índices de conscientização e capacitação em matéria de proteção de dados pessoais?
- 3) Quais iniciativas ou práticas poderiam ser **adotadas** ou **patrocinadas** pela ANPD para melhorar os índices de conscientização e capacitação em matéria de proteção de dados pessoais?

O documento deverá ser encaminhado em PDF, por e-mail (xxxxxxxxxxxxxx), aos cuidados de Rodrigo Valadão (Conselheiro Coordenador do GT1). Desde já agradecemos a disponibilidade e aproveitamos a oportunidade para renovar os votos da mais elevada estima e consideração.

Atenciosamente,

Lílian Manoela Monteiro Cintra de Melo
Presidente do CNPD

Rodrigo Borges Valadão
Conselheiro e Coordenador do GT1

¹²¹ PORTARIA CNPD Nº 1, DE 4 DE OUTUBRO DE 2024. Disponível em: https://www.gov.br/anpd/pt-br/cnpd-2/portarias-gts-2a-formacao/sei_0148052_portaria_cnpd_01_2024.pdf/view. Acesso em 05 jan. 2025.

ANEXO III

CONTRIBUIÇÕES ESCRITAS

A. Cadê meu Dado?

São Paulo, 20 de janeiro de 2025.

Ao Conselho Nacional de Proteção de Dados e da Privacidade - CNPD.

Inicialmente, agradecemos o convite para colaborar na construção de um documento tão relevante que está sendo produzido, considerando seus efeitos para o fortalecimento de uma sociedade mais justa e informada sobre o tema de proteção de dados.

Nesse sentido, a plataforma "Cadê Meu Dado?" desempenha um papel significativo na promoção da privacidade e proteção de dados no Brasil, alinhando-se com os princípios da Lei Geral de Proteção de Dados Pessoais (LGPD) sem qualquer incentivo externo.

A plataforma oferece aos usuários a possibilidade de verificar se seus endereços de e-mail foram expostos em vazamentos de dados, possibilitando um controle sobre eventuais incidentes, possibilitando que alterem as senhas dos seus e-mails, alertando para eventuais golpes que possam ocorrer por desdobramento do vazamento, tudo isso sem armazenar essas informações em seu banco de dados, conforme destacado em seu aviso de privacidade.

Além disso, o site atua como um canal de comunicação entre os diversos atores do ecossistema de proteção de dados, permitindo que os usuários façam denúncias relacionadas a incidentes, ou outras práticas abusivas ou em desacordo com a LGPD.

A plataforma também disponibiliza artigos, notícias e informações relevantes sobre privacidade e proteção de dados pessoais, contribuindo para o amadurecimento do tema no país.

A plataforma possibilita que as empresas denunciadas se defendam e se manifestem, podendo, inclusive, ser um meio de composição de conflitos entre as partes, sem a necessidade de demandas judiciais, conforme possibilita a LGPD.

Como diferencial e buscando incentivar as melhores práticas, a "Cadê meu Dado?" possibilita e incentiva que os titulares façam elogios de boas práticas, não apenas denuncie. Sob nossa ótica essa postura incentiva mais práticas positivas por parte dos Agentes de Tratamento.

Dito isto, passamos a responder as questões propostas.

1) Informações sobre situações concretas e dados estatísticos que demonstrem o déficit educacional e a necessidade de melhora nos índices de conscientização e capacitação em matéria de proteção de dados pessoais:

Pesquisa Cetic.br 2023 apresentou que apenas 28% dos entrevistados afirmaram ter conhecimento sobre a LGPD, enquanto 67% indicaram nunca ter recebido qualquer tipo de treinamento ou capacitação sobre o tema.

Casos reais: Incidentes de vazamento de dados envolvendo pequenas empresas (e engenharia social) demonstram a falta de protocolos básicos de segurança, muitas vezes associados à ausência de treinamento e conscientização entre colaboradores.

Setor público: Um levantamento feito pela Controladoria-Geral da União (CGU) apontou que cerca de 60% dos servidores públicos desconhecem suas responsabilidades específicas no manejo de dados pessoais, expondo lacunas significativas na formação desses profissionais.

Esses dados indicam que há uma necessidade urgente de capacitar diversos públicos — desde funcionários públicos até usuários finais — para lidar de forma adequada com questões de privacidade e segurança.

2) Quais iniciativas ou práticas poderiam ser replicadas ou difundidas pela ANPD para melhorar os índices de conscientização e capacitação em matéria de proteção de dados pessoais?

A ANPD poderia replicar práticas bem-sucedidas aplicadas em outros contextos globais e nacionais, como:

Campanhas massivas de conscientização: Inspiradas na abordagem da GDPR (Regulamento Geral sobre a Proteção de Dados da União Europeia), campanhas de comunicação visual e digital acessíveis, disseminadas em redes sociais, televisão e rádios locais.

Educação formal: Parcerias com o Ministério da Educação para incluir temas de proteção de dados em currículos escolares e universitários, com materiais educativos e módulos obrigatórios.

Cursos online gratuitos: Criação de uma plataforma oficial da ANPD com cursos MOOC (Massive Open Online Courses), com módulos específicos para diferentes públicos (advogados, empresários, professores, etc.).

Divulgação de guias práticos: Material de fácil acesso e linguagem acessível, como cartilhas ilustrativas ou vídeos curtos explicando os direitos e deveres dos cidadãos e das empresas sob a LGPD.

3) Quais iniciativas ou práticas poderiam ser adotadas ou patrocinadas pela ANPD para melhorar os índices de conscientização e capacitação em matéria de proteção de dados pessoais?

Para maximizar o impacto, sugerimos que a ANPD adote ou patrocine as seguintes iniciativas:

Hackathons e premiações: Promover competições que incentivem a criação de soluções tecnológicas voltadas para a educação em proteção de dados, patrocinando os melhores projetos com implementação no setor público ou privado.

Educação para pequenos negócios: Criação de kits de treinamento simplificado para micro e pequenas empresas, que frequentemente enfrentam dificuldades em entender e aplicar a LGPD.

Eventos regionais: Realização de workshops gratuitos em parceria com associações locais e sindicatos, especialmente em regiões com acesso limitado a informações digitais.

Apoio financeiro a ONGs e projetos comunitários: Financiar projetos que já estejam promovendo conscientização e educação em comunidades vulneráveis.

Monitoramento e avaliação contínuos: Criação de indicadores de desempenho e métricas para acompanhar a eficácia das iniciativas implementadas, possibilitando ajustes rápidos quando necessário.

Destacar ações e posturas positivas sobre o tema incentivando outras instituições.

Permanecemos à disposição para contribuir para a maturidade da proteção de dados no Brasil.

Equipe Cadê meu Dado

B. Câmara de Educação Superior do Conselho Nacional de Educação (MEC)

CONTRIBUIÇÃO AO GRUPO DE TRABALHO DO CONSELHO NACIONAL DE PROTEÇÃO DE DADOS (GT1)

Ref.: Contribuição para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade

1. Situações concretas e dados estatísticos que demonstram o déficit educacional e a necessidade de melhoria nos índices de conscientização e capacitação em matéria de proteção de dados pessoais

A Revolução 4.0¹ introduziu de maneira disruptiva novas dinâmicas às relações sociais em virtude do uso da inteligência artificial nos processos produtivos industriais. Estamos em um período de transição que tem alterado significativamente as estruturas profissionais, e a perspectiva das novas tecnologias às dinâmicas de trabalho e educação, que demandam a produção de conhecimento sobre os mecanismos de aprendizado por meio de uma nova linguagem – a dos ambientes e plataformas digitais – e que caracteriza o chamado “letramento digital”², cujo aprendizado é absolutamente necessário para compreensão das Tecnologias de Informação e Comunicação (TIC)³, principalmente pelas crianças e adolescentes que nos últimos anos passaram a usar os ambientes digitais para alfabetização, inclusive.

Os sistemas educacionais, por sua vez, têm adotado cada vez mais plataformas tecnológicas para aprimorar as experiências de aprendizagem e expandir o acesso aos recursos educacionais. A integração de sistemas de informação educacional e plataformas de aprendizagem digital modificou o formato de interação entre estudantes e educadores.

¹ A Revolução 4.0 surgiu na Alemanha como uma política pública do Governo Federal Alemão para digitalizar a manufatura, implementada no ano de 2010 e que tem causado uma verdadeira revolução nos processos produtivos. É considerada a Quarta Revolução Industrial e, por isso, o nome “4.0”. Ver: LEDFORD, Allison Brown; HYRE, Anna et al. Origin of the Fourth Industrial Revolution: manufacturing predictions preceding Industrie 4.0. **Journal of Science and Technology Policy Management**. Publicado em 02 out. 2024. Disponível em: <https://www.emerald.com/insight/content/doi/10.1108/jstpm-03-2023-0040/full/html>. Acesso janeiro de 2025.

² O conceito de letramento digital diz respeito às práticas sociais de leitura e produção de textos em ambientes digitais, isto é, ao uso de textos em ambientes propiciados pelo computador ou dispositivos móveis, tal como celulares e tablets, em plataformas como e-mail, redes sociais na web, entre outras. In.: RIBEIRO, Ana Elisa, COSCARELLI, Carla Viana. Letramento Digital. In. **Glossário Ceale - Termos de Alfabetização, Leitura e Escrita para educadores**, Faculdade de Letras da Universidade Federal de Minas Gerais (UFMG). Disponível em: <https://www.ceale.fae.ufmg.br/glossarioceale/verbetes/letramento-digital#:~:text=Letramento%20digital%20diz%20respeito%20%C3%A0s,sociais%20na%20web%2C%20entre%20outras>. Acesso: janeiro de 2025.

³ VASCONCELOS, S.T. L. Educação digital, proteção de dados pessoais e novos espaços de trabalho jurídico. **Revista Interdisciplinar de Direito**, v. 19, n. 1, pp. 166-174, jan./jun., 2021.

Entretanto, concomitante aos benefícios da transformação digital, surgem riscos significativos, especialmente no domínio da cibersegurança.⁴

As instituições educacionais armazenam grandes quantidades de dados sensíveis, que vão desde informações de estudantes até pesquisas proprietárias, tornando-se alvos preferenciais para ataques cibernéticos. O crescimento dos ambientes de aprendizagem digital exige uma infraestrutura robusta de cibersegurança para proteger a integridade dos dados, garantir a privacidade e proteger os usuários contra possíveis ameaças. Não obstante a rápida adoção de ferramentas digitais na educação, muitas instituições ainda estão atrasadas na implementação de medidas adequadas de cibersegurança, representando uma ameaça significativa à segurança de seus sistemas e de seus usuários.⁵

A utilização das tecnologias de informação no setor educacional está suscetível a diferentes formas de ataques cibernéticos, como phishing, malware, ransomware e vazamento de dados. As lacunas ocasionadas pela desigualdade social contribuem para a precarização orçamentária de instituições de ensino, que operam com serviços limitados de TI e pouca expertise em cibersegurança, tornando essas instituições especialmente vulneráveis. Ademais, a crescente dependência de sistemas baseados em nuvem e plataformas de ensino remoto expôs ainda mais essa vulnerabilidade, reforçando a necessidade latente de estratégias abrangentes de cibersegurança adaptadas às necessidades específicas dos ambientes educacionais.⁶

Uma recente investigação conduzida pela Human Rights Watch, revisada em janeiro de 2023, trouxe à tona preocupantes violações de privacidade em plataformas educacionais direcionadas a estudantes brasileiros. Segundo o relatório, pelo menos sete sites educacionais coletaram e transmitiram dados de crianças e adolescentes para empresas terceirizadas mediante o uso de tecnologias de rastreamento, presumivelmente projetadas para fins publicitários. Entre esses sites, destacam-se o "Estude em Casa" e o "Centro de Mídias da Educação de São Paulo", ambos criados por secretarias estaduais de educação, bem como plataformas privadas como Descomplica, Escola Mais, Explicaê, MangaHigh e Stoodi.⁷

⁴ WATINI, Sri; DAVIES, George; ANDERSEN, Nicole. Cybersecurity in Learning Systems: Data protection and privacy in educational information systems and digital learning environments. **International Transactions on Education Technology** (ITEE), v. 3, n. 1, pp. 26–35, November 2024.

⁵ Ibidem.

⁶ Ibidem.

⁷ HAN, He Jung. Brazil: Online Learning Tools Harvest Children's Data. **Human Rights Watch**, April 4, 2023. Disponível em: <https://www.hrw.org/news/2023/04/03/brazil-online-learning-tools-harvest-childrens-data> Acesso em janeiro de 2024.

Outro site, o Revisa Enem, embora não tenha utilizado rastreadores específicos para anúncios, ainda assim transmitiu informações pessoais de estudantes para terceiros, sem o consentimento explícito necessário nos termos da Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709/2018). Tais plataformas não apenas monitoraram os estudantes dentro de seus ambientes virtuais de aprendizagem, mas também os acompanharam durante sua navegação em outros sites, estendendo-se para além do período letivo, em evidente violação ao direito fundamental à privacidade e à proteção de dados pessoais. A LGPD já prevê salvaguardas para a coleta e tratamento de dados de crianças e adolescentes, exigindo consentimento específico e destacado dos pais ou responsáveis legais. Entretanto, a presente investigação evidencia lacunas na fiscalização e na aplicabilidade dessas normas no ambiente educacional digital, tornando imperativa a revisão do arcabouço normativo para garantir maior proteção aos menores em contextos digitais.⁸

A pesquisa evidenciou que sites pertencentes e operados pelas próprias Secretarias de Educação de Minas Gerais e São Paulo enviaram dados pessoais de crianças e adolescentes para empresas de tecnologia de publicidade, os sites permanecem em atividade vinculando conteúdos educacionais. A Secretaria Estadual de Educação de Minas Gerais, em resposta ao Human Rights Watch removeu todo o rastreamento de anúncios do site, mas a Secretaria Estadual de Educação de São Paulo, permanece divulgando o uso de sete sites educacionais que coletam indevidamente dados pessoais de estudantes, incluindo aqueles desenvolvidos pela própria secretaria, que não respondeu aos pedidos da Organização Internacional.⁹

A investigação também comprovou que pelo menos quatro desses sites rastreiam crianças e adolescentes com mais intensidade do que normalmente um adulto é rastreado ao navegar na Internet. Os dados coletados envolvem a análise dos estudantes para prever comportamentos de venda e mecanismos de influência e foram enviados a empresas especializadas em publicidade comportamental, que desenvolve perfis e direcionamento específico para publicidade, de modo que violam de forma inadmissível a privacidade dos alunos, e são totalmente desnecessárias às funções educacionais. A prática também desempenha um papel negativo a formação de experiência dos usuários, e é determinante

⁸ HAN, He Jung. Brazil: Online Learning Tools Harvest Children's Data. **Human Rights Watch**, April 4, 2023. Disponível em: <https://www.hrw.org/news/2023/04/03/brazil-online-learning-tools-harvest-childrens-data> Acesso em janeiro de 2024.

⁹ Ibidem.

para as informações que acessam, especialmente num momento de vulnerabilidade de opiniões e cresças, oferecendo um alto risco de interferência manipuladora.¹⁰

Por se tratar de ferramenta de utilização coletiva, os estudantes não possuem a escolha de se opor a essa vigilância. Assim como não escolhem os livros didáticos, não possuem o poder de escolher sobre o uso de metodologias digitais, rapidamente adotadas a partir da pandemia de COVID. Exemplo disto foi a adoção pela Secretaria de Educação do Estado de São Paulo do website Escola Mais. Este website foi autorizado a usar recursos de gravação de sessão para que terceiros possam assistir e registrar o comportamento dos usuários, incluindo cliques do mouse e movimentos em sites, o equivalente a câmeras de monitoramento que registram sempre que a criança coça o nariz ou pela o lápis na sala de aula.¹¹

Nenhuma das secretarias de educação citadas verificou previamente se os sites que estavam utilizando eram seguros para a utilização infantil, o que evidencia o papel da Autoridade Nacional de Proteção de Dados (ANPD) para mitigar as violações aos direitos à privacidade e a necessária regulamentação em sede nacional do uso de plataformas de ensino e outras mídias digitais.¹²

Outro fator de impacto é o fato de que a maior parte dos estudantes brasileiros não recebem formação específica adequada sobre segurança digital e proteção de dados em sua trajetória acadêmica. De acordo com o TIC Educação 2023, apenas 55% das escolas de ensino fundamental e médio possuíam documentos que definem as políticas institucionais de proteção de dados e segurança da informação. Na edição de 2020, apenas 41% das instituições mencionaram possuir tais documentos, o que demonstra um aumento gradual na adaptação das escolas às diretrizes da Lei Geral de Proteção de Dados (LGPD), mas ainda um significativo déficit na Política de Proteção de Dados para a educação.¹³

Embora não exista imposição legal para a formulação de uma política específica sobre proteção de dados no âmbito das instituições de ensino, a implementação de

¹⁰ HAN, He Jung. Brazil: Online Learning Tools Harvest Children's Data. **Human Rights Watch**, April 4, 2023. Disponível em: <https://www.hrw.org/news/2023/04/03/brazil-online-learning-tools-harvest-childrens-data> Acesso em janeiro de 2024.

¹¹ Ibidem.

¹² Ibidem.

¹³ Pesquisa sobre o uso das tecnologias de informação e comunicação nas escolas brasileiras: TIC Educação, 2023 [livro eletrônico]. Survey on the use of information and communication technologies in Brazilian schools: ICT in Education 2023 / [editor] Núcleo de Informação e Coordenação do Ponto BR. -- 1. ed. -- São Paulo: **Comitê Gestor da Internet no Brasil**, 2024.

diretrizes dessa natureza constitui recomendação alinhada às boas práticas de governança institucional e que deve ser feita pela União.

Na rede pública de ensino, temáticas relacionadas à privacidade e à proteção de dados pessoais são, em alguns casos, regulamentadas diretamente por meio das secretarias e diretorias de ensino. A questão é sensível, já que pouco mais da metade dos estados possuem regulamentação normativa, na maioria de caráter precário, instituídas por portarias. Neste sentido, verificou-se que 51% das instituições públicas possuem normativas específicas sobre o tema, não havendo por óbvio uma parametrização. Dados sensíveis de crianças e adolescentes estão expostos. Entre as unidades da federação, o Distrito Federal destaca-se como a região com maior adesão a tais normativas, com 90% das instituições reportando a adoção de diretrizes específicas.¹⁴

Na rede privada de ensino, a pesquisa constatou um percentual mais elevado de segurança de dados, muito em função da entrada em vigor da Lei Geral de Proteção de Dados (LGPD, 2018). O percentual é de 74% no ensino privado.

Os dados obtidos junto aos gestores escolares evidenciam a crescente preocupação com a privacidade e a segurança de dados dos alunos no processo de seleção de ferramentas educacionais digitais. Em 2023, 29% dos gestores relataram ter deixado de implementar determinados recursos digitais, tais como plataformas, aplicativos e programas de computador, devido a preocupações com a privacidade e proteção de informações sensíveis. Essa precaução foi ainda mais acentuada no âmbito das escolas estaduais (30%) e privadas (41%). Dentre as principais motivações para essa postura cautelosa, destacam-se os riscos de vazamento ou apropriação indevida dos dados estudantis (18%) e a falta de clareza nos termos de uso acerca da destinação das informações coletadas (17%). No caso das escolas particulares, outros fatores relevantes incluem a exibição de anúncios publicitários dentro dos ambientes digitais educacionais (23%) e potenciais riscos de discriminação e exclusão social dos estudantes, baseados em critérios como raça, gênero e condição socioeconômica (22%).¹⁵

Os espaços de debate e conscientização são importantes ferramentas para ampliação do conhecimento a respeito, necessário para a tomada de decisão e redução dos riscos de violação aos direitos, em 2022 28% das escolas afirmaram que haviam

¹⁴ Pesquisa sobre o uso das tecnologias de informação e comunicação nas escolas brasileiras: TIC Educação, 2023 [livro eletrônico]. Survey on the use of information and communication technologies in Brazilian schools: ICT in Education 2023 / [editor] Núcleo de Informação e Coordenação do Ponto BR. -- 1. ed. -- São Paulo: **Comitê Gestor da Internet** no Brasil, 2024.

¹⁵ Ibidem.

promovido debates ou palestras sobre a proteção de dados no espaço acadêmico virtual, a proporção aumentou para 34% em 2023, nas escolas particulares a proporção foi de 40% no mesmo ano. Entretanto, a pesquisa aponta que o principal público alvo da formação foi de professores e outros profissionais da escola, correspondendo a 32% das palestras, apenas 24% dos eventos de formação foram destinados aos alunos, apontando para a necessidade de direcionamento do debate à parte mais vulnerável às violações da proteção de dados.¹⁶

Apesar do direcionamento majoritário aos profissionais da escola, a pesquisa revela que os professores da educação básica afirmam não ter conhecimento adequado sobre a Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709/2018). Essa lacuna na formação docente também reflete diretamente na falta de conscientização dos alunos sobre o tema. Outro destaque é para implementação de sistemas de reconhecimento facial tem avançado no ambiente escolar, impulsionada pela crescente utilização de câmeras de monitoramento, inteligência artificial e outras tecnologias de vigilância. Entre os anos de 2020 e 2023, a proporção de escolas de ensino fundamental e médio que adotaram sistemas internos de videomonitoramento aumentou de 37% para 51%, crescimento superior ao observado na adoção de dispositivos educacionais, como computadores de uso estudantil.¹⁷

Embora a utilização de biometria possa contribuir para o controle institucional, especialistas alertam para os riscos associados ao tratamento de dados sensíveis, sobretudo no que concerne à identificação equivocada e ao potencial reforço de práticas discriminatórias. A Autoridade Nacional de Proteção de Dados (ANPD) destaca que a introdução do reconhecimento facial nas escolas representa riscos acentuados, considerando que os titulares desses dados são crianças e adolescentes. Assim, recomenda-se a observância do princípio do melhor interesse do menor, conforme preconiza o artigo 14 da Lei Geral de Proteção de Dados (LGPD)¹⁸

Paralelamente, verifica-se a crescente inserção das instituições de ensino em ambientes digitais, especialmente no uso de redes sociais institucionais. Entre 2020 e 2023, a proporção de escolas que mantêm perfis ou páginas nessas plataformas aumentou

¹⁶Pesquisa sobre o uso das tecnologias de informação e comunicação nas escolas brasileiras: TIC Educação, 2023 [livro eletrônico]. Survey on the use of information and communication technologies in Brazilian schools: ICT in Education 2023 / [editor] Núcleo de Informação e Coordenação do Ponto BR. -- 1. ed. -- São Paulo: **Comitê Gestor da Internet** no Brasil, 2024.

¹⁷ Ibidem.

¹⁸ Ibidem.

de 64% para 73%, sendo esse avanço mais expressivo nas regiões Norte (de 35% para 47%) e Nordeste (de 56% para 68%), nas escolas municipais (de 47% para 60%) e em unidades situadas em áreas rurais (de 29% para 46%).¹⁹

Há uma lacuna presente também nas instituições de ensino superior públicas e privadas que em sua maioria não dispõem de disciplinas obrigatórias ou eletivas voltadas à proteção de dados pessoais em cursos das áreas de tecnologia, direito e administração. Tal situação evidencia a necessidade urgente de reformas curriculares que incluam a LGPD e temas correlatos nos programas acadêmicos, especialmente em razão da demanda crescente de utilização de dados pessoais enquanto ativos financeiros comercializado entre empresas e *Big Techs*.

2. Iniciativas ou práticas que poderiam ser replicadas ou difundidas pela ANPD para melhorar os índices de conscientização e capacitação em matéria de proteção de dados pessoais

Com base em experiências bem-sucedidas em outras jurisdições, sugere-se que a ANPD implemente, difunda e replique as seguintes iniciativas:

- a) Alfabetização Digital para Proteção de Dados: inspirado no modelo europeu do *Safer Internet Programme*, esse programa poderia incluir à Política Nacional de Educação Digital (PNED), instituída pela Lei nº 14.533/2023, campanhas massivas de conscientização voltadas para estudantes, professores e famílias, enfatizando boas práticas de segurança e privacidade na internet. O modelo europeu busca formar base segura de utilização da internet a partir do combate ao conteúdo ilegal e potencialmente perigoso para crianças e adolescentes. No contexto da iniciativa também foram criados canais diretos de denúncia para o combate de conteúdo ilegal, com alcance internacional. O financiamento de canais de denúncia em rede de cooperação por todo território europeu. A coleta de dados qualitativos e quantitativos sobre a operação dos canais. Medidas de incentivo para acelerar o processo de criação de canais e expansão da rede. A articulação de um centro de coordenação da rede, para aumentar sua visibilidade a nível europeu e melhorar a eficácia operacional. Um sistema de autorregulamentação totalmente

¹⁹ Pesquisa sobre o uso das tecnologias de informação e comunicação nas escolas brasileiras: TIC Educação, 2023 [livro eletrônico]. Survey on the use of information and communication technologies in Brazilian schools: ICT in Education 2023 / [editor] Núcleo de Informação e Coordenação do Ponto BR. -- 1. ed. -- São Paulo: **Comitê Gestor da Internet no Brasil**, 2024.

funcional é um elemento essencial para limitar o fluxo de conteúdo indesejado, prejudicial e ilegal. A autorregulamentação envolve vários componentes: consulta e representação apropriada das partes envolvidas, códigos de conduta, órgãos nacionais facilitando a cooperação em nível comunitário e avaliação nacional de estruturas de autorregulamentação. Para melhorar a autorregulamentação no setor, a Comissão está fornecendo aos órgãos nacionais de regulamentação ou autorregulamentação o Fórum da Internet Mais Segura como uma plataforma para troca de experiências.²⁰

- b) Criação de Material Didático Oficial: desenvolvimento de cartilhas, vídeos educativos e guias práticos de aplicação da LGPD, distribuídos gratuitamente para instituições de ensino fundamental, médio e superior, com incentivo à adoção curricular dessas ferramentas.
- c) Parcerias Institucionais: celebração de convênios com universidades e centros de pesquisa para fomentar a produção de conhecimento sobre proteção de dados, incentivando a pesquisa acadêmica e a formação de especialistas na área.

3. Iniciativas ou práticas que poderiam ser adotadas ou patrocinadas pela ANPD para melhorar os índices de conscientização e capacitação em matéria de proteção de dados pessoais

- d) Inclusão de Educação em Proteção de Dados na Base Nacional Comum Curricular (BNCC): junto ao MEC, promover a inclusão obrigatória de disciplinas ou módulos sobre proteção de dados pessoais na BNCC para o ensino básico e na estrutura curricular de cursos superiores, especialmente aqueles voltados à formação de professores.
- e) Plataforma de Capacitação em Proteção de Dados: criação de uma plataforma pública e gratuita, com cursos certificados sobre a LGPD, cibersegurança e direitos digitais, acessível a docentes, estudantes e profissionais de diversas áreas.
- f) Fomento à Pesquisa e Desenvolvimento: lançamento de editais públicos de fomento à pesquisa e inovação em proteção de dados, com apoio a estudos que

²⁰ EUR-Lex. Access to European Union Law. **Safer Internet Programme 2005-2008** (Safer Internet Plus). Decision No 854/2005/EC of the European Parliament and of the Council of 11 May 2005. Disponível em: <https://eur-lex.europa.eu/EN/legal-content/summary/safer-internet-programme-2005-2008-safer-internet-plus.html> Acesso em janeiro de 2024.

analisem os impactos da LGPD na sociedade e proponham soluções para aprimorar sua implementação.

As sugestões apresentadas fundamentam-se em dados concretos e práticas exitosas, sendo certo que a atuação proativa do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade poderá contribuir significativamente para o fortalecimento da cultura de privacidade e segurança digital no Brasil.

Coloco-me à disposição para eventuais esclarecimentos e para contribuir no desenvolvimento de políticas públicas voltadas à proteção de dados e à educação digital.

Monica Sapucaia Machado

Conselheira da Câmara de Educação Superior

Conselho Nacional de Educação

C. Data Privacy Brasil

São Paulo, 17 de janeiro de 2025

Ao Sr. Rodrigo Valadão,

Coordenador do GT de Políticas de Educação
Conselho Nacional de Proteção de Dados Pessoais e Privacidade
Autoridade Nacional de Proteção de Dados Pessoais

Assunto: Contribuições da Data Privacy Brasil para GT de Políticas de Educação e Capacitação em Proteção de Dados Pessoais

Caro Sr. Rodrigo Valadão,

Recebemos com satisfação sua mensagem sobre a **Portaria CNPD nº 01/2024**, que estabeleceu o Grupo de Trabalho dedicado a fornecer subsídios na temática de “Educação e Capacitação em Proteção de Dados Pessoais” para a elaboração da **Política Nacional de Proteção de Dados Pessoais e da Privacidade**, no âmbito do Conselho Nacional de Proteção de Dados.

Como entidade que se dedica à expansão da gramática dos direitos digitais no Brasil e a promoção da cultura democrática da proteção de dados pessoais, entendemos que a elaboração da Política Nacional de Proteção de Dados Pessoais e de Privacidade é crucial e um das principais razões de existência da Autoridade Nacional de Proteção de Dados Pessoais.

Entendemos, também, que a elaboração de uma Política deste porte é complexa. O Brasil é um país com realidades muito distintas. Uma república com diversidades geográficas e territoriais enormes. Ainda possuímos **grandes desafios com relação à educação**, que possui uma estrutura complexa, como aprofundaremos abaixo em nossa contribuição. A figura abaixo, elaborada no curso do relatório

Endereço
Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato
contato@dataprivacybr.org

dataprivacybr.org

sobre Educação no Brasil para **OCDE em 2021**,¹ mostra os muitos níveis de educação que possuímos, passando pela educação da primeira infância, educação infantil, o ensino médio, a educação profissionalizante e o ensino superior, que inclui graduação, mestrado e doutorado.

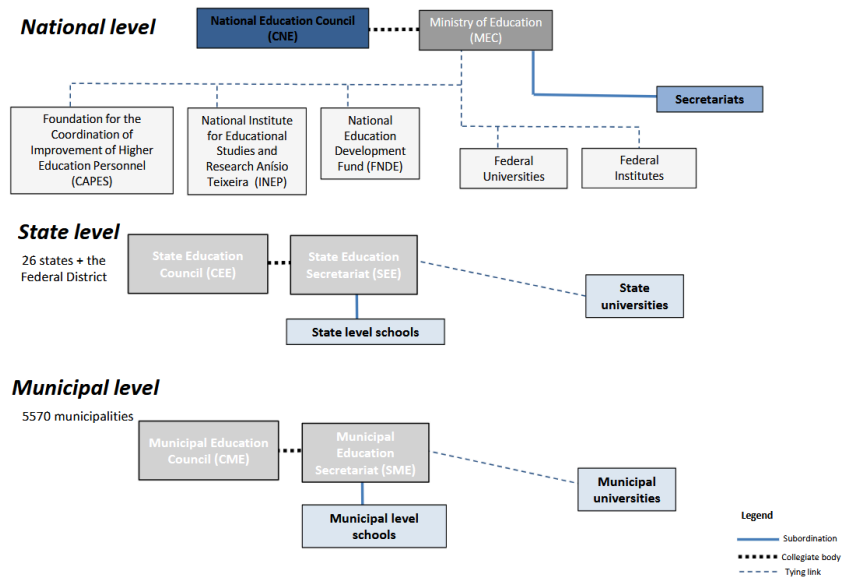
ISCED 2011	Starting age	Administrative unit (primarily responsibility)	Grade/Year	Education programme		
8	23-26	Federal government	Higher education	Doctoral degree (<i>Doutorado</i>)		
7	22			Academic Master's degree, stricto sensu (<i>Mestrado, stricto sensu</i>)	Professional Master's degree, stricto sensu (<i>Mestrado Profissional, stricto sensu</i>)	
6	18			Bachelor's degree (<i>Bacharelado</i>)	Licentiate's degree (<i>Licenciatura</i>)	Specific Professional diploma, lato sensu (<i>Curso de especialização, lato sensu</i>)
4	18	Federal government and states				Technological degree (<i>Graduação Tecnológica</i>)
3	15	States	Grade 3 Grade 2 Grade 1	Upper secondary education (<i>ensino médio</i>)		
2	11	Municipalities and states	Year 9 Year 8 Year 7 Year 6 Year 5	Lower secondary (<i>anos finais do ensino fundamental</i>)		
1	6	Municipalities	Year 4 Year 3 Year 2 Year 1	Primary (<i>anos iniciais do ensino fundamental</i>)		
0	4	Municipalities		Pre-school (<i>pré-escola</i>)		
	0			Early childhood educational development (<i>creches</i>)		

Fonte: OCDE (2021)

A governança da educação no Brasil é complexa pois envolve um arranjo federativo de três níveis: municípios, estados e federação. Portanto, o ponto de partida de uma reflexão sobre uma Política Nacional de Proteção de Dados Pessoais no Brasil com enfoque em educação é como combinar os arranjos institucionais pré-existentes e alavancar estratégias de educação em direitos de formas inovadoras, **valendo-se de experiências institucionais já em curso e que podem ser otimizadas.**

¹ OECD, **Education in Brazil: An International Perspective**. Paris: OECD Publishing, 2021. <https://doi.org/10.1787/60a667f7-en>

As funções educacionais do **governo federal** incluem: definir padrões nacionais e objetivos gerais para o país (por exemplo, o PNE); gerenciar diretamente instituições, incluindo universidades federais e escolas federais vocacionais; coordenar políticas e práticas educacionais em todos os níveis de governo; e fornecer assistência técnica e financeira a estados e municípios. O Ministério da Educação (MEC) também é responsável por regulamentar todos os níveis educacionais no Brasil, da primeira infância ao ensino superior. O MEC avalia o sistema educacional por meio do Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (INEP), que se concentra principalmente na educação pré-terciária, e da Fundação para a Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), que se concentra no ensino superior. Em colaboração com os governos estaduais e municipais, o MEC determina diretrizes curriculares (ou seja, competências e disciplinas comuns) a serem ensinadas nas escolas.



Fonte: OCDE (2021)

Endereço
 Alameda Santos, 1293
 3º Andar – Jardim Paulista
 São Paulo – SP
 CEP 01419-904

Contato
 contato@dataprivacybr.org

dataprivacybr.org

O último relatório do **quinto ciclo de monitoramento de metas do Plano Nacional de Educação (2024)**, elaborado pelo Inep, traz um balanço das várias metas definidas para políticas de

educação no Brasil. O acesso ao ensino fundamental de 9 anos e a sua conclusão na idade recomendada é o foco da Meta 2 do PNE, na qual se estabelece que, até o fim da vigência do plano, em 2024, **o Brasil universalize o acesso para toda a população de 6 a 14 anos de idade** e que a conclusão dessa etapa na idade recomendada ocorra para, pelo menos, 95% dos adolescentes.

Para aferir essa meta, por exemplo, o Inep utiliza dois indicadores: **Indicador 2A** - Percentual da população de 6 a 14 anos que frequenta ou que já concluiu o ensino fundamental (taxa de escolarização líquida ajustada); **Indicador 2B**: Percentual da população de 16 anos completos de idade com pelo menos o ensino fundamental concluído.

Nas estimativas dos dois indicadores, são utilizados os microdados da **Pnad Contínua (Pnad-c) para o período 2013-2023**, de modo a fornecer o dado mais atual disponível e suas desagregações. No último decênio, o Brasil apresentou avanços na cobertura escolar da população de 6 a 14 anos frequentando o ensino fundamental, saindo de um patamar **de 96,7% em 2012 e alcançando 97,8% em 2019**. Esse recuo ocorrido nos últimos anos, reflexo da crise sanitária enfrentada pelo País, representa, em perspectiva histórica, um retrocesso de mais de 10 anos no indicador, visto que, na linha de base do Plano Nacional de Educação (2012), **foi estimado em 96,7%.**

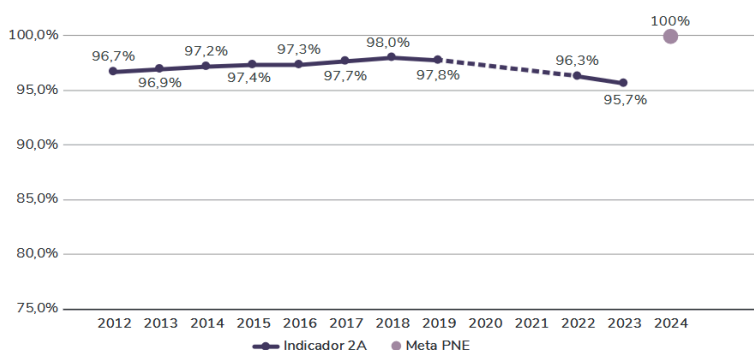


GRÁFICO 1

PERCENTUAL DA POPULAÇÃO DE 6 A 14 ANOS QUE FREQUENTA OU JÁ CONCLUIU O ENSINO FUNDAMENTAL – BRASIL – 2012-2019/2022-2023

Fonte: Elaborado pela Direção de Indicadores e Pesquisas do Inep com base em dados da Pnad-c/IBGE (2012-2019/2022-2023).

Nota: Os resultados de 2020 e 2021 foram suprimidos por recomendação do IBGE, em virtude de dificuldades na coleta de dados da Pnad-c durante a pandemia de covid-19 (IBGE, 2022).

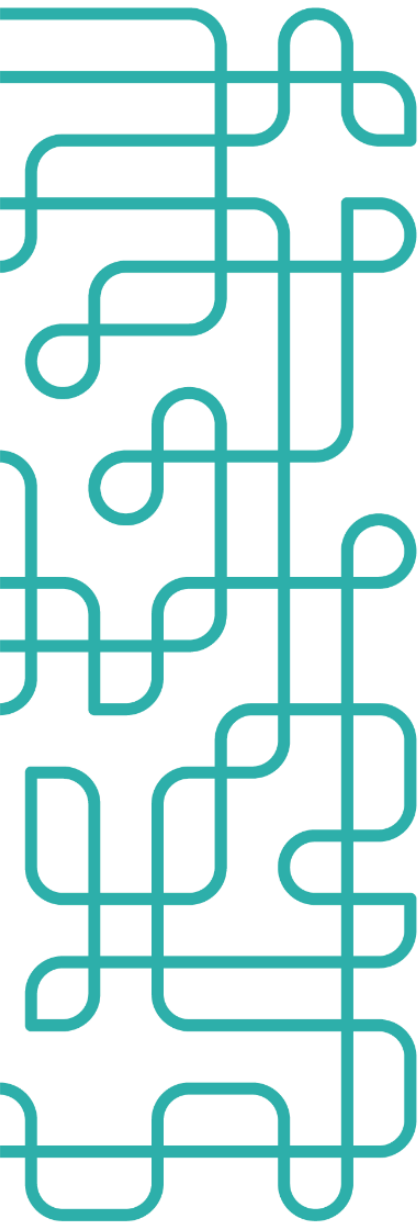
Endereço

Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato

contato@dataprivacybr.org

dataprivacybr.org



Conforme o último estudo do Inep (2024), o impacto da pandemia foi sentido em todas as regiões do País, sendo a região Sul a que observou o maior retrocesso na cobertura entre 2019 e 2023 (2,6 p.p.), seguida da região Centro-Oeste (2,3 p.p.). Ambas recuaram ao patamar de 95,4% e 95,5%, respectivamente, em 2023, ficando abaixo da linha de base do PNE em 2012. As demais regiões também recuaram para índices inferiores aos da linha de base.

Entre as unidades da Federação, o maior recuo em relação à linha de base do PNE (2012) no indicador de cobertura é observado em Roraima, que retrocedeu 4,5 p.p., chegando a 92,0% em 2023, contrastando com o índice de 96,5% em 2012. Entre as 27 unidades da Federação, 19 retrocederam no indicador de cobertura em relação à linha de base do PNE, com apenas sete apresentando índices ligeiramente superiores à linha de base e uma sem alteração, o Amazonas.

A diferença **na cobertura entre os 25% mais pobres e os 25% mais ricos é a mais proeminente entre todas as análises realizadas e cresce ao longo do tempo**. Em 2016, a diferença entre os dois grupos era de 1,3 p.p., passando a 2,3 p.p. em 2022, ano em que a população de 6 a 14 anos pertencente aos 25% mais ricos alcançaram 97,8% de cobertura no ensino fundamental, enquanto o alcance entre os 25% mais pobres foi de 95,5%. O Inep conclui que **a desigualdade na conclusão do ensino fundamental** para a população de 16 anos conforme renda domiciliar per capita é marcante em todo o período.

A Meta 8, inserida no Plano Nacional de Educação (PNE), visa elevar a escolaridade média dos jovens entre 18 e 29 anos de idade para, ao menos, 12 anos de estudo completos até 2024.

No ano de 2023, a população brasileira de 18 a 29 anos de idade apresentou uma média de escolaridade de 11,8 anos, conforme demonstrado no gráfico abaixo. Essa média reflete um crescimento gradual ao longo dos anos, visto que, em 2012, a média era de 10,7 anos, indicando um aumento total de 1,1 ano completo de estudo durante o período. Apesar da evolução, ainda não se atingiu a meta de 12 anos de estudo.

Endereço
Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato
contato@dataprivacybr.org

dataprivacybr.org

As regiões Norte e Nordeste continuaram como as de menor escolaridade em 2023, com uma média de 11,3 anos de estudo, mostrando um crescimento, mas ainda abaixo da meta. As demais regiões, por sua vez, já alcançaram ou ultrapassaram o objetivo estipulado. Em 2022, a **escolaridade média dos 25% mais pobres da população de 18 a 29 anos era de 10,3 anos, 1,7 anos abaixo da meta**, e os **25% mais ricos tinham uma média de 13,5 anos, evidenciando uma disparidade significativa**. Vale lembrar que mudanças e limitações nos dados coletados pela Pnad Contínua devido à pandemia de covid-19 impactaram o monitoramento da Meta 8, especialmente em relação à indisponibilidade de dados sobre rendimento domiciliar per capita.

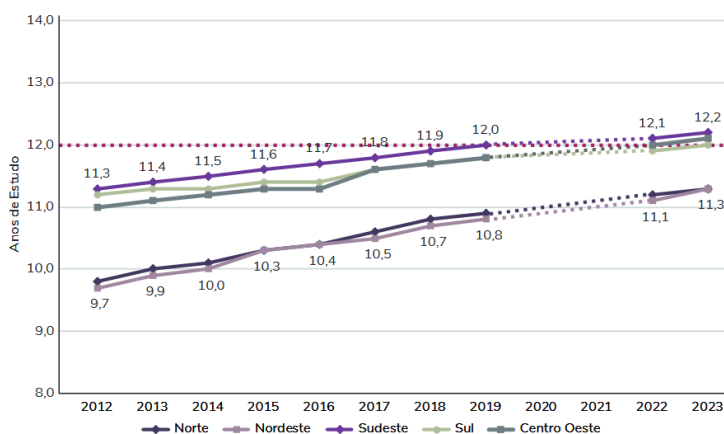


GRÁFICO 2

ESCOLARIDADE MÉDIA, EM ANOS DE ESTUDO, DA POPULAÇÃO DE 18 A 29 ANOS DE IDADE
 – GRANDES REGIÕES – 2012-2019/2022-2023

Fonte: Elaborado pela Diretd/Inep com base em dados da Pnad-c/IBGE.

Nota: Os resultados de 2020 e 2021 foram suprimidos por recomendação do IBGE, em virtude de dificuldades na coleta de dados da Pnad-c durante a pandemia de covid-19 (IBGE, 2022). Os rótulos indicam os valores das regiões com a maior e a menor escolaridade média do Sudeste e Nordeste, respectivamente.

Retomamos os dados da OCDE (2021) e do Inep (2024) apenas para reforçar três pontos cruciais em qualquer discussão sobre políticas de educação no Brasil:

- As desigualdades territoriais importam e mostram cenários muito distintos dentro do mesmo país;
- As desigualdades entre pobres e ricos importam e mostram um país com oportunidades educacionais muito distintos;
- O país não conseguiu cumprir as principais metas de 2024 de seu Plano Nacional de Educação, o que mostra a

Endereço

Alameda Santos, 1293
 3º Andar – Jardim Paulista
 São Paulo – SP
 CEP 01419-904

Contato

contato@dataprivacybr.org

dataprivacybr.org

complexidade de execução dessas políticas diante de fatores conjunturais externos, como a pandemia de Covid-19;

A seguir, oferecemos respostas às perguntas formuladas no Ofício para a Data Privacy Brasil, a partir de subsídios de pesquisas conduzidas pela organização e nossa experiência enquanto instituição de ensino que se dedica à formação e capacitação em proteção de dados pessoais.

Entendemos que uma abordagem de **educação em direitos** precisa ser executada a partir de **vetores de multiplicação** dentro do próprio sistema de justiça.

1) Informações sobre situações concretas e dados estatísticos que demonstrem o déficit educacional e a necessidade de melhora nos índices de conscientização e capacitação em matéria de proteção de dados pessoais

O problema da falta de conscientização sobre direitos de proteção de dados pessoais está associado a um problema maior no Brasil: **a formação em direitos humanos**. A educação em direitos humanos é compreendida como um processo sistemático e multidimensional que orienta a formação do **sujeito de direitos**.

A Constituição Federal de 1988 estabelece a educação como um direito de todos e um dever do Estado e da família, promovendo o pleno desenvolvimento da pessoa, o preparo para o exercício da cidadania e a qualificação para o trabalho (art. 205). A Lei de Diretrizes e Bases da Educação Nacional (LDB) - Lei nº 9.394/1996, orienta que a educação deve promover valores de **cidadania, democracia e respeito aos direitos humanos**.

A **Educação em Direitos Humanos** é uma diretriz reconhecida pelo Plano Nacional de Educação em Direitos Humanos (PNEDH), instituído em 2003. Este plano incentiva a inclusão de conteúdos relacionados a direitos humanos em todos os níveis e modalidades de ensino, priorizando práticas que promovam a dignidade, o respeito à diversidade e a justiça social. Embora o

Endereço
Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato
contato@dataprivacybr.org

dataprivacybr.org

PNEDH seja uma recomendação, não há uma obrigatoriedade explícita para todas as escolas, mas espera-se que as instituições sigam essas orientações, alinhando-se aos objetivos da Base Nacional Comum Curricular (BNCC).

Conforme relatório do **Plano Nacional de Educação em Direitos Humanos de 2018**,² são objetivos balizadores do PNEDH conforme estabelecido no artigo 2: a) fortalecer o respeito aos direitos humanos e liberdades fundamentais; b) promover o pleno desenvolvimento da personalidade e dignidade humana; c) fomentar o entendimento, a tolerância, a igualdade de gênero e a amizade entre as nações, os povos indígenas e grupos raciais, nacionais, étnicos, religiosos e linguísticos; d) estimular a participação efetiva das pessoas em uma sociedade livre e democrática governada pelo Estado de Direito; e) construir, promover e manter a paz.

Em publicações recentes, o Comitê Gestor da Internet no Brasil (CGI.br) analisou a percepção da população brasileira acima dos 16 anos sobre as práticas de gerenciamento de acesso a dados pessoais, além de riscos envolvidos, controle dos dados e tratamento de dados biométricos. No relatório³, um dos pontos de atenção é para o fato de 26% das entrevistadas afirmarem que concordam com as políticas de privacidade sem sua leitura, indicando a necessidade de atuação mais incisiva para que plataformas digitais tragam elementos de fácil compreensão quanto ao tratamento de dados. Sobre a busca de canais de atendimento para dados pessoais, **77% afirmam procurar a própria empresa, seguido de sites como Reclame Aqui e Consumidor.gov.br (69%) e Procon (51%). Polícia**

² BRASIL, Plano Nacional de Educação em Direitos Humanos. Brasília: Ministério dos Direitos Humanos, 2018.

<https://www.gov.br/mdh/pt-br/navegue-por-temas/educacao-em-direitos-humanos/DIAGRAMAOPNEDH.pdf>

³ COMITÊ GESTOR DA INTERNET NO BRASIL. Privacidade e proteção de dados pessoais 2023 [livro eletrônico] : perspectivas de indivíduos, empresas e organizações públicas no Brasil = Privacy and personal data protection 2023 : 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, 2024. Disponível em:

<https://cgi.br/media/docs/publicacoes/2/20240901120340/privacidade-e-protecao-de-dados-2023.pdf>. Acesso em: 17 jan. 2025.

(40%), Poder Judiciário (40%) e Ministério Público (40%) estão à frente da ANPD (35%), indicando potencial desconhecimento da autoridade para grande parte da população. A pesquisa traz ainda percepções interessantes sobre as maiores preocupações pelo tratamento de dados em diferentes atividades *online*, como compras, acesso em bancos, aplicativos de relacionamento, entre outros. Esses achados são relevantes para pensar estratégias de comunicação eficientes de acordo com os interesses do público.

Outros dados que podem corroborar com o tema são a pesquisa TIC Kids Online⁴ e TIC Educação⁵, ambas com resultados de 2023. Nela, há dados quantitativos sobre o uso de ferramentas digitais por crianças e adolescentes, tanto no contexto doméstico, quanto escolar. **Cerca de 95% de indivíduos entre 9 e 17 anos têm acesso à internet no Brasil, sendo 38% destes com acesso exclusivamente pelo celular.** A pesquisa indica ainda que crianças e adolescentes acessam a internet cada vez mais cedo: se em 2015 o primeiro acesso aos 6 anos era relatado por 11% das entrevistas, em 2023 esse número subiu para 24%.

A conectividade nas escolas é um ponto a ser levado em consideração em uma Política Nacional de Proteção de Dados. Apesar de 82% das escolas públicas conectadas terem acesso à internet na sala de aula, é preciso considerar os sistemas e plataformas digitais que são utilizadas para mediação do processo pedagógico, sejam elas e-mails, redes sociais, arquivos em nuvem ou

⁴ COMITÊ GESTOR DA INTERNET NO BRASIL. Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil: TIC Kids Online Brasil 2023 [livro eletrônico] = Survey on Internet use by children in Brazil: ICT Kids Online Brazil 2023 / [editor] Núcleo de Informação e Coordenação do Ponto BR. -- 1. ed. -- São Paulo: Comitê Gestor da Internet no Brasil, 2024. Disponível em: https://cgi.br/media/docs/publicacoes/2/20241104103339/tic_kids_online_2023_livro_eletronico.pdf. Acesso em: 17 jan. 2025.

⁵ Pesquisa sobre o uso das tecnologias de informação e comunicação nas escolas brasileiras: TIC Educação 2023 [livro eletrônico] = Survey on the use of information and communication technologies in Brazilian schools: ICT in Education 2023 / [editor] Núcleo de Informação e Coordenação do Ponto BR. -- 1. ed. -- São Paulo : Comitê Gestor da Internet no Brasil, 2024. Disponível em: https://cgi.br/media/docs/publicacoes/2/20241119194257/tic_educacao_2023_livro_completo.pdf. Acesso em: 17 jan. 2025.

ambientes virtuais de aprendizagem. Essas atividades refletem diretamente no tratamento de dados pessoais, especialmente de crianças e adolescentes, mas apenas 55% das escolas afirmaram ter documentos que definem a política de proteção de dados e segurança da informação na instituição.

A Data Privacy Brasil é uma organização que nasce da parceria entre uma escola e uma associação de pesquisa com o objetivo de fomentar a cultura de proteção de dados e direitos digitais no Brasil e no mundo. Nesse sentido, trabalhamos com uma série de iniciativas que podem contribuir para inspirar ações de outras instituições para uma educação em proteção de dados pessoais integrada com a cultura nacional.

Em nossos cursos de formação, **trabalhamos com uma perspectiva abrangente da proteção de dados, vinculando-a a outros direitos fundamentais**. A difusão de tecnologias digitais no cotidiano traz dificuldades no monitoramento e cumprimento da legislação, mas tem potencial para maior compreensão das pessoas sobre como o tratamento de dados afeta suas vidas. Assim, a datificação da vida pode ser um fio condutor para diferentes narrativas, demonstrando como a coleta e tratamento de dados tem relação direta com direitos de personalidade no Brasil. Outro ponto que abordamos é uma **visão pragmática sobre obrigações aos controladores dos dados, inclusive com mecanismos de supervisão, mitigação e prevenção de riscos**. Para a população, é essencial vincular esse conhecimento com abordagens práticas para exercício de direitos de titulares, conforme previstos na LGPD.

Enquanto direito fundamental autônomo, é preciso que a proteção de dados pessoais seja componente de uma **Política Nacional de Educação em Direitos Humanos**, produzindo convergências com a atuação da ANPD. Essa articulação com diferentes órgãos e ministérios tem potencial para deixar evidente a atuação da autoridade no tema, refletindo o compromisso na defesa constitucional de indivíduos no país.

Considerando as políticas existentes de educação em direitos humanos e as competências já existentes do PNEDH, é preciso uma

Endereço
Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato
contato@dataprivacybr.org

dataprivacybr.org

tomada de decisão estratégica por parte da Autoridade Nacional de Proteção de Dados Pessoais sobre como combinar a atuação da ANPD, MDH e MEC para uma concepção abrangente de capacitação em proteção de dados pessoais como um componente central dos direitos fundamentais. Considerando os dados já produzidos pelo Inep sobre as assimetrias de educação entre diferentes classes sociais, é preciso uma focalização da política pública de educação em direitos, priorizando a população mais distante dos processos de ensino-aprendizagem sobre cidadania e direitos fundamentais.

2) Quais iniciativas ou práticas poderiam ser replicadas ou difundidas pela ANPD para melhorar os índices de conscientização e capacitação em matéria de proteção de dados pessoais?

Para uma Política Nacional de Proteção de Dados efetiva, é preciso considerar quais são os atores interessados no tema e que podem trazer contribuições concretas para a educação no tópico. Alguns projetos da Data Privacy Brasil podem servir de inspiração nesse sentido.

Entre 2020 e 2022, realizamos cursos avançados de proteção de dados pessoais para Defensorias Públicas do país, especificamente nos estados do Rio de Janeiro, São Paulo e Bahia. A escolha do trabalho com defensoras e defensores públicos se deu pelo papel essencial que têm na democracia brasileira, garantindo acesso à justiça e difusão da educação em direitos no país. O trabalho trouxe resultados concretos, como reportagens direcionadas ao público leigo, ações civis públicas e mesmo oficinas com movimentos sociais no Rio de Janeiro e Salvador.

A ANPD tem papel fundamental nesse cenário e pode reproduzir esse tipo de formação, com foco em lideranças do sistema de justiça que atende diretamente cidadãs e cidadãos, trazendo capilaridade ao conhecimento. Um exemplo é a **formação de lideranças dos Procons**, acionando o Sistema Nacional de Defesa do Consumidor em uma estratégia de vetores de multiplicação. Uma

Endereço

Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato

contato@dataprivacybr.org

dataprivacybr.org

parceria da ANPD e Senacon poderia utilizar a Escola Nacional de Defesa do Consumidor – instrumento já existente dentro da Senacon – para um curso de formação presencial.

Um modelo interessante seria similar à Escola de Governança da Internet, promovido pelo CGI.br. Com duração de uma semana, as aulas aprofundam temas relevantes no campo e promovem trocas profissionais entre pessoas que normalmente não seriam reunidas para debates práticos e teóricos. Nossa experiência aponta que essas experiências promovem uma transformação de visão do mundo, além da criação de um *ethos* profissional, agregando pessoas especializadas em prol de um objetivo comum.

É preciso criar uma lógica de “formação de formadores”, multiplicando os efeitos dos investimentos públicos de capacitação em direitos fundamentais e proteção de dados pessoais. Uma “Escola de Formação em Proteção de Dados Pessoais” poderia ser criada juntando dois tipos de públicos: (i) profissionais do setor público com grande capacidade de mobilização educacional (Defensorias Públicas, membros dos Procons, membros do SUS, Promotores de Justiça, vereadores e legisladores locais) e (ii) lideranças comunitárias que atuam no território com projetos de capacitação em direitos, incluindo profissionais que atuam em escolas e projetos formativos.

3) Quais iniciativas ou práticas poderiam ser adotadas ou patrocinadas pela ANPD para melhorar os índices de conscientização e capacitação em matéria de proteção de dados pessoais?

Uma estratégia adequada é utilizar educação midiática para conscientização e capacitação em proteção de dados pessoais. Na Data Privacy Brasil, a comunicação e produção audiovisual é uma das iniciativas organizacionais para cumprir esse objetivo, sendo realizada de diferentes formas.

Em nosso podcast Dadocracia, trazemos temas sociais relevantes que se relacionam com a temática de direitos digitais, convidando especialistas para conversas profundas e de fácil

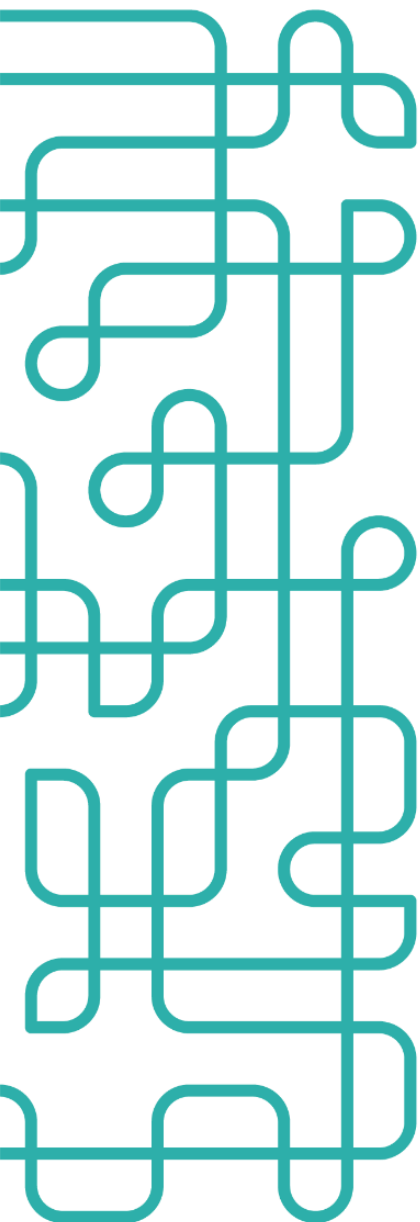
Endereço

Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato

contato@dataprivacybr.org

dataprivacybr.org



compreensão. A ANPD poderia fazer uso do setor de comunicação social para parcerias com veículos similares, colocando-se à disposição para elucidar dúvidas e questões para a população.

Segundo o estudo “Inside Áudio 2023” da Kantar IBOPE Media, o rádio é ouvido por 80% da população brasileira, sendo que cada ouvinte passa, em média, 3h55min diariamente escutando rádio. O consumo é realizado, principalmente, em casa durante atividades cotidianas (58%), no carro/moto particular (27%) e no trabalho presencial (12%). A ANPD pode investir em mecanismos de disseminação de direitos por meio de avisos de pauta e parcerias para criação de conteúdos que podem ser livremente utilizado pelas rádios no Brasil. Até o momento, não se tem notícia de nenhuma iniciativa da ANPD que tenha focalizado as rádios como meio de comunicação e disseminação de sua atuação.

Outra estratégia poderia ser parcerias com influenciadores e influenciadoras digitais que trabalham com a temática de divulgação científica e ciências sociais. Há canais especializados em divulgação científica no YouTube que podem ser mobilizados, como Manual do Mundo, Ciência Todo Dia, Canal do Schwarza, TecMundo, Nerdologia. A ANPD também pode oferecer premiações para [influenciadores de divulgação científica em plataformas como TikTok e Instagram](#). De acordo com dados de 2022 da empresa Insider Intelligence, as redes que mais cresceram em números de usuários na América Latina foram o Tiktok (11,8%) e o Instagram (3,2%). No Brasil, o Instagram contava com 113,5 milhões de usuários e o TikTok tinha cerca de 82 milhões no início de 2023, segundo dados compilados pelo site DataReportal, que reúne informações de materiais publicitários das empresas de tecnologia.

A promoção de concursos culturais, como o já realizado Prêmio Danilo Doneda, poderia alavancar o debate sobre proteção de dados pessoais utilizando pessoas que já trabalham em redes sociais, garantindo capilaridade e discurso condizente com diferentes públicos.

Por fim, acreditamos que o diálogo com lideranças comunitárias tem capacidade de promover o debate com cidadãos e

Endereço

Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato

contato@dataprivacybr.org

dataprivacybr.org

cidadãos a partir de seus interesses e necessidades imediatas. Isso poderia ser realizado com eventos regionais, nos quais a ANPD se colocasse à disposição, mostrasse o trabalho realizado e divulgasse as formas adequadas de denúncia e mitigação de riscos. Utilizar rádios comunitárias e instrumentos populares já existentes é a forma mais efetiva de transmitir a mensagem e efetivar o direito à proteção de dados enquanto uma garantia fundamental.

Desde já agradecemos pela oportunidade de contribuir com os trabalhos do GT de Políticas de Educação do Conselho Nacional de Proteção de Dados e aproveitamos para enviar-lhe nossos protestos de estima e distinta consideração.

Atenciosamente,



Bruno Bioni

Codiretor, Data Privacy Brasil

Endereço

Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato

contato@dataprivacybr.org

dataprivacybr.org



Mariana Rielli

Codiretora, Data Privacy Brasil



Rafael A. F. Zanatta

Codiretor, Data Privacy Brasil



Pedro Saliba

Coordenador de Assimetrias e Poder

Endereço

Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato

contato@dataprivacybr.org

dataprivacybr.org

D. Centro de Estudos Avançados em Proteção de Dados (CEAPD)

OFÍCIO Nº 002/2025

Ao Senhor Rodrigo Borges Valadão

Conselheiro Suplente do Conselho Nacional de Proteção de Dados e da Privacidade (CNPD)

Coordenador do Grupo de Trabalho GT1 – Educação e Capacitação em Proteção de Dados

Autoridade Nacional de Proteção de Dados

Assunto: Proposta de criação da Escola Nacional de Proteção de Dados (ENAD) vinculada à ANPD e contribuições à política pública de educação em proteção de dados

Senhor Conselheiro,

Em nome do **Centro de Estudos Avançados em Tecnologia, Privacidade e Proteção de Dados (CEAPD)**, submeto à apreciação do GT1 sugestão para fortalecimento institucional da proteção de dados no Brasil, alinhada às competências legais da Autoridade Nacional de Proteção de Dados (ANPD) e ao disposto na Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018).

A proposição consiste na criação da Escola Nacional de Proteção de Dados (ENAD), entidade vinculada à ANPD, com eixo estruturante previsto no bojo da Política Nacional de Proteção de Dados (PNPD). A iniciativa responde diretamente às atribuições do GT1 estabelecidas pela Portaria CNPD nº 01/2024 e à competência do CNPD para "disseminar conhecimento sobre proteção de dados", conforme art. 58-B, V, da LGPD, e fortaleceria, ainda, a configuração da PNPD.

A criação da ENAD surge como resposta urgente a um cenário de deficiências estruturais identificadas em âmbito nacional. Dados do Tribunal de Contas da União (Relatório TC 012/2024) revelam que 68% dos servidores públicos federais não possuem formação específica em proteção de dados, lacuna que compromete a aplicação eficaz da LGPD e a própria segurança jurídica e tecnológica do Estado. Esse diagnóstico alarmante ganha maior

relevância diante da promulgação da Emenda Constitucional nº 115/2022, que elevou a proteção de dados à categoria de direito fundamental, impondo ao poder público o dever de implementar mecanismos concretos para sua efetivação.

Nesse contexto, a proposta alinha-se a um robusto arcabouço jurídico.

A Constituição Federal, em seu art. 39, § 2º, estabelece a obrigatoriedade de a União manter escolas de governo para capacitação de servidores, princípio reforçado pela Política Nacional de Educação Digital (Lei nº 14.533/2023), que prevê a integração de competências digitais na administração pública. Ademais, o Marco Civil da Internet (Lei nº 12.965/2014) prevê, em seu art. 26, prevê o adimplemento da obrigação estatal na prestação da educação e capacitação para o uso seguro, consciente e responsável da internet como ferramenta para o exercício da cidadania, a promoção da cultura e o desenvolvimento tecnológico. Por fim, a Política Nacional de Educação Digital (Lei nº 14.533/2023) possui, como eixo estruturante e objetivo, a capacitação e especialização digital, as quais prevêem medidas estratégicas voltadas para qualificação digital de servidores e funcionários públicos, a fim de combater o déficit de competências digitais na administração pública.

Complementarmente, a Agenda Regulatória 2025-2026 da ANPD destaca a necessidade premente de formação especializada em temas complexos como governança de dados e inteligência artificial, consolidando a ENAD como instrumento estratégico para o cumprimento das metas regulatórias.

Para enfrentar esses desafios, a estrutura ora proposta para a ENAD articula-se em três dimensões complementares.

A vinculação administrativa à ANPD, regulamentada pelo Decreto nº 10.474/2020, assegura sinergia operacional com a autoridade nacional, ao mesmo tempo que estabelece modelo de governança compartilhada com o CNPD, o Ministério da Gestão e Inovação e representantes

da sociedade civil. Esse desenho institucional garante equilíbrio entre expertise técnica e participação social. Nesse contexto, também se promoveriam convênios com organizações da sociedade civil, a fim de promover capilaridade e profundidade orgânica na estratégia educacional.

No aspecto financeiro, a proposição sugere captação de recursos por meio do Fundo de Defesa de Direitos Difusos (FDD), nos termos do art. 13 da Lei nº 7.347/1985, combinados com dotação orçamentária específica da ANPD, conforme diretrizes do Decreto nº 9.203/2017 sobre governança pública. Essa dupla fonte de financiamento assegura sustentabilidade econômica sem onerar exclusivamente os cofres públicos.

Quanto à metodologia, a ENAD poderia adotar modelo híbrido de ensino (presencial e EaD), com certificação reconhecida pelo MEC para fins de progressão funcional. O currículo integrará padrões internacionais como a norma ISO/IEC 27701 de gestão de privacidade, além de parcerias estratégicas com o CGI.br e universidades públicas, conforme previsto no art. 26 do Marco Civil da Internet. Essa abordagem permitiria alinhamento na formação às melhores práticas globais, sem desconsiderar as especificidades do ordenamento jurídico brasileiro.

Como desdobramento natural desse planejamento, propõem-se três eixos prioritários de implementação. Em primeiro lugar, a inclusão da ENAD como pauta central no GT1 permitirá articular esforços institucionais para sua viabilização. Posteriormente, a criação de grupo de trabalho específico dedicado à elaboração de estudo técnico-orçamentário em conjunto com outros órgãos do Governo Federal a fim de fornecer subsídios para minuta de decreto presidencial (nos termos do art. 84, IV, da CF/1988) garantirá adequação normativa à proposta.

Por fim, o estabelecimento imediato de parcerias preliminares com instituições como o CGI.br e universidades públicas viabilizaria a estruturação pedagógica e tecnológica necessária, antecipando-se à formalização legal da escola.

Essas ações, articuladas em sequência lógica, transformarão o projeto em política pública efetiva, cumprindo o mandato constitucional de proteção de dados e respondendo às demandas identificadas pelo TCU.

Em conclusão, a proposta de criação da ENAD representa solução institucional inovadora para os desafios identificados pelo TCU e pela própria ANPD em sua Agenda Regulatória e se alinharia com as melhores práticas administrativas.

Colocamo-nos à disposição para colaborar na elaboração de estudos complementares e no diálogo com os órgãos envolvidos.

Atenciosamente,

Brasília, 12 de fevereiro de 2025



FABRICIO DA MOTA ALVES
Diretor Acadêmico

Centro de Estudos Avançados em Tecnologia, Privacidade e
Proteção de Dados (CEAPD)