PROPOSTA
POLÍTICA NACIONAL DE PROTEÇÃO DE DADOS

Junho de 2026

DataPrivacyBR

DataPrivacyBR Research

FICHA TÉCNICA

A **Data Privacy Brasil** é uma organização de ensino, pesquisa e incidência que produz conhecimento e forma pessoas para um ecossistema informacional justo. Por meio da educação, construção de saberes e mobilização da sociedade, buscamos uma sociedade democrática na qual as tecnologias estejam a serviço da autonomia, dignidade das pessoas e redução de assimetrias de poder.

Direção
Bruno Bioni, Mariana Rielli e Rafael Zanatta

Coordenação
Carla Rodrigues, Jaqueline Pigatto, Pedro Martins, Pedro Saliba e Victor Barcellos

Equipe
Ana Luiza Serafini, Bárbara Yamasaki, Bianca Marques, Eduardo Mendonça, Gabriela Vergili, Gabriel Franco, Giovanna Amaral, Giovana Andrade, João Paulo Vicente, Larissa Pacheco, Louise Karczeski, Luize Ribeiro, Matheus Arcanjo, Natasha Nóvoa, Paula Uematsu, Pedro Henrique Santos, Rafael Guimarães, Rodolfo Rodrigues e Vanessa Nobre.

Imprensa
Para esclarecimentos sobre o documento e entrevistas, entrar em contato pelo e-mail imprensa@dataprivacy.br.org

Contexto da PNPD e Itinerário Metodológico

A proteção de dados é um direito fundamental essencial para o desenvolvimento da cidadania, manutenção da democracia e garantia da autodeterminação e autonomia de cada cidadão. Nos anos recentes, a importância deste direito tem se intensificado cada vez mais com o surgimento de novas tecnologias com maior capacidade e processamento de informações e com a redução do espaço entre o real e o virtual, como a digitalização de serviços privados e públicos.

Foi considerando este cenário que a Lei nº 13.709/2018, Lei Geral de Proteção de Dados (LGPD), e a Emenda Constitucional nº 115/2022, que inseriu o direito à proteção de dados no rol do art. 5º, da Constituição Federal, foram aprovadas. Contudo, a legislação explícita sobre o tema não é o único passo necessário para estabelecer uma cultura de proteção de dados no país.

É preciso definir ações para alcançar o cumprimento e devida implementação da LGPD, como programas para garantir a proteção de dados em circunstâncias diversas, potenciais interações e cooperações entre Agências, programas de educação e capacitação em proteção de dados dentro de órgãos públicos, etc. É para isso que serviria uma política nacional de proteção de dados, para a materialização das de todas as aspirações normativas supracitadas e, em última análise, a promoção de uma cultura em privacidade e proteção de dados nacionalmente.

O processo de desenvolvimento dessa política se iniciou no final de 2024 quando o Conselho Nacional de Proteção de Dados Pessoais e Privacidade (CNPD) tomou medidas para propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade (PNPD), cumprido com suas atribuição previstas no art. 58-B, inciso I, da LGPD.

As membras e membros conselheiros, representantes de diversos setores, que compunham o CNPD, elencaram tópicos de análise designados a Grupos de Trabalho Temporários (GTTs) para que estes oferecessem subsídios para a PNPD, nos termos das Portarias CNPD nº 1 6/2024. As temáticas selecionadas foram: (i) educação e capacitação em proteção de dados; (ii) mecanismos, instâncias e práticas de conformidade de proteção de dados; (iii) governança de dados (tema dividido por dois GTTs);(iv) dados pessoais para o desenvolvimento econômico, tecnológico e a inovação; e (v) LAI & LGPD: dados abertos como infraestrutura crítica em conformidade com LGPD. O processo de trabalho dos GTTs foi desenvolvido entre outubro de 2024 e janeiro de 2025, culminando em 6 relatórios por GTTs e um relatório geral que compilou todos os subsídios[1]. Na segunda formação (Portaria nº 2, CNPD/2026), houve os grupos de Proteção de dados no contexto laboral, Proteção de dados de crianças e adolescentes, Coordenação interinstitucional e eficiência administrativa na proteção de dados, Proteção de dados e inteligência artificial, Proteção ao

1 CNPD. Subsídios para elaboração da política nacional de proteção de dados pessoais e da privacidade 2025. CNPD. Brasília: jun. 2025. Disponível em: https://www.gov.br/anpd/pt-br/cnpd-2/subsidios-para-elaboracao-da-pdpp.pdf

crédito e prevenção a fraudes usando dados pessoais, e Implementação do ECA Digital (Estatuto Digital da Criança e do Adolescente em ambientes digitais).

A presente proposta visa reforçar subsídios já elencados pelos GTTs, mas também formular um conteúdo mais concreto sobre temas que deve ser contidos na PNPD. Para tanto, ao longo de 6 meses, construiu-se as seguintes etapas metodológicas até que se chegasse nas formulações de textos normativas a seguir. Além de, minimamente, descrever as estratégias de investigação, a listagem abaixo tem por objetivo abrir os dados para outras pesquisas sobre esta ou outros políticas nacionais:

- Mapeamento e entabulamento de outras políticas nacionais com temas correlatos ao da proteção de dados: ao todo 39 políticas foram mapeadas, o que permitiu uma análise quantitativa e qualitativa da seguinte ordem cuja análise observou aspectos como cooperação institucional, integração federativa, direitos individuais, monitoramento de políticas públicas, transparência, entre outros pontos.

- Revisão bibliográfica sobre o tema das políticas nacionais, bem como sobre proteção de dados desde que com recorte sobre proposições voltadas à formulação, implementação e monitoramento da agenda enquanto vetor de políticas pública. Adotou-se, respectivamente, como referenciais teóricos: a) geral sobre políticas nacionais: Marcelo Sodré[2]; b) sobre privacidade e proteção de dados: Miriam Wimmer[3]; Bruno Bioni[4]

- Entrevista com Marcelo Sodré, apontando sua participação na formulação, implementação e monitoramento de outras políticas nacionais.

- Oficina interna com pesquisadoras e pesquisadores da Data Privacy Brasil, na qual compartilhamos uma versão prévia e fizemos apontamentos coletivos sobre o tema. Agradecemos a Ana Serafini, Rodolfo Rodrigues, Carla Rodrigues, Eduardo Mendonça, Jaqueline Pigatto, Luize Ribeiro, Mariana Rielli, Paula Uematsu, Victor Barcellos, Rafael Zanatta e Vanessa Nobre.

O itinerário metodológico da proposta foi organizado de modo progressivo, partindo da identificação de referências normativas e institucionais já consolidadas, passando pela escuta qualificada de atores relevantes e culminando na formulação de recomendações e propostas de texto para a Política Nacional de Proteção de Dados Pessoais e da Privacidade.

Em primeiro lugar, buscou-se compreender de onde a proposta poderia se inspirar. Para isso,

2 SODRÉ, Marcelo. Formação do Sistema Nacional de Defesa do Consumidor. 32 edição. São Paulo: Editora Revista dos Tribunais. 2007.

3 WIMMER, Miriam. Os desafios do enforcement na LGPD: fiscalização, aplicação de sanções administrativas e coordenação intergovernamental. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luis.. (Org.). Tratado de Proteção de Dados Pessoais. 1ed.Rio de Janeiro: Forense, 2021, v. 1, p. 375–388.

4 BIONI, Bruno. Accountability no desenho (design) da regulação de dados pessoais: virtudes e vicissitudes. 2021. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2021.

foram selecionadas políticas nacionais brasileiras com pertinência temática, estrutural ou normativa em relação à proteção de dados pessoais. Essa etapa permitiu observar como outras agendas públicas organizaram seus objetivos, princípios, diretrizes, instrumentos de governança, mecanismos de cooperação institucional, formas de monitoramento e estratégias de implementação. A análise dessas políticas serviu não apenas como fonte de inspiração de estrutura, mas também como referência para a construção de dispositivos com vocação normativa. Agradecemos ao Instituto Alana pela compilação de dados de políticas nacionais e compartilhamento com a equipe da Data Privacy Brasil. Muitas das reflexões foram fruto do trabalho realizado pelo Instituto, que também compõe o CNPD.

Entre as políticas analisadas, destacam-se a: Política Nacional de Informática, a Política de Dados Abertos do Poder Executivo Federal, a Política Nacional de Inovação Tecnológica na Saúde, a Política Nacional de Segurança de Infraestruturas Críticas, a Política Nacional de Segurança da Informação, o Plano Nacional de Internet das Coisas, a Política Nacional de Governo Aberto, a Política Nacional de Inovação e a Política Nacional do Meio Ambiente. A pertinência dessas referências decorre de três dimensões principais: a proximidade temática com a agenda de proteção de dados; a capacidade de oferecer modelos de estruturação de políticas públicas nacionais; e a possibilidade de servirem como fonte para a redação de comandos normativos.

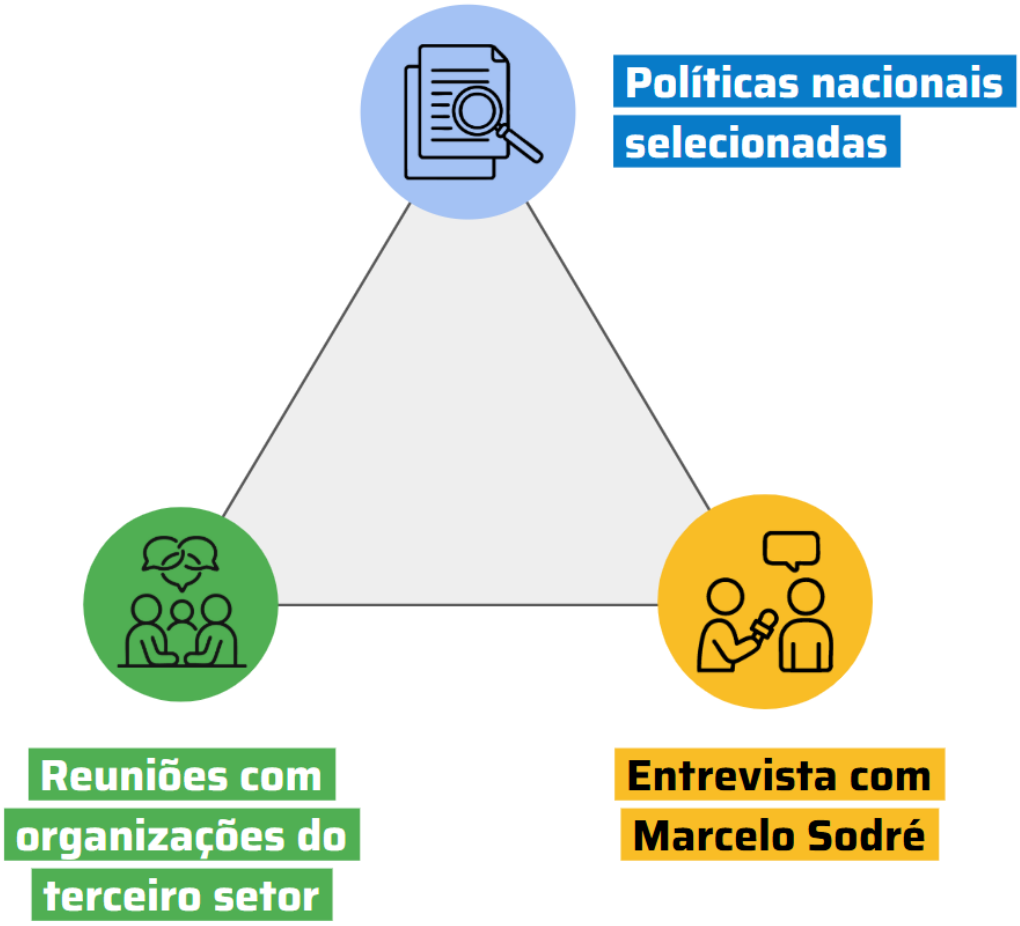
Em segundo lugar, a proposta incorporou uma etapa de escuta e diálogo com organizações da sociedade civil e especialistas. Essa etapa teve como objetivo captar diferentes percepções sobre os desafios de implementação da proteção de dados no Brasil, especialmente a partir de atores que acompanham de perto os impactos sociais, institucionais e econômicos da agenda. Foram considerados mais de quatro encontros com a sociedade civil realizados entre 2024 e 2025, cujas contribuições ajudaram a identificar prioridades, lacunas regulatórias, riscos de implementação e pontos de atenção para a formulação da política.

Além desses encontros, foi realizada entrevista com Marcelo Sodré em 2026, com o objetivo de compreender experiências anteriores de formulação, implementação e monitoramento de políticas nacionais. A entrevista contribuiu para qualificar a compreensão sobre os desafios práticos de uma política pública dessa natureza, especialmente quanto à necessidade de combinar diretrizes substantivas, desenho institucional, coordenação federativa, participação social e mecanismos de acompanhamento[5].

Em terceiro lugar, os materiais levantados foram organizados e analisados a partir de uma lógica de triangulação metodológica. De um lado, o mapeamento de políticas nacionais permitiu identificar padrões de estrutura normativa e institucional. De outro, os encontros com a sociedade civil trouxeram contribuições situadas sobre demandas, preocupações e prioridades concretas. Por fim, a entrevista especializada auxiliou na compreensão dos elementos necessários para transformar uma agenda normativa em uma política pública passível de implementação e monitoramento.

5 Entrevista em fase de revisão, a ser publicada em breve

A partir da triangulação de tais unidades de pesquisa, constatou-se que, normalmente, a discussão sobre políticas públicas organiza-se a partir de dois grandes vetores. De conteúdo, procurando-se responder o porquê e para o quê servirá tal política pública. De arranjo e cooperação institucional, procurando-se responder **quem e como**[6] será implementada e monitorada tal política pública. A presente contribuição está justamente sistematizada dessa forma, as recomendações são pontuais e não têm a pretensão de esgotar o que viria a ser integralmente a PNPD.



6 SODRÉ, Marcelo. Formação do Sistema Nacional de Defesa do Consumidor. 32 edição. São Paulo: Editora Revista dos Tribunais. 2007.

PARTE 1
PNPD – Por quê e para quê

Fundamentos, Objetivos e Princípios da PNPD

Sugestão de Redação

> Art. X: Fica instituída a Política Nacional de Proteção de Dados Pessoais e Privacidade com **a finalidade de assegurar os direitos fundamentais à privacidade e à proteção de dados pessoais** que têm por fundamento **o pleno exercício da cidadania e para a promoção de um ecossistema informacional justo**.

A Política Nacional de Proteção de Dados (PNPD) deve estar ancorada no marco constitucional e infraconstitucional brasileiro, reconhecendo a proteção de dados pessoais como direito fundamental e condição estrutural para o exercício da cidadania, para a autonomia individual e coletiva e para a soberania tecnológica do país.

A Constituição Federal de 1988 estabelece, no art. 5º, após a Emenda Constitucional nº 115/2022, o direito fundamental à proteção de dados pessoais, de modo a garantir o livre desenvolvimento da personalidade, a autodeterminação informacional e a limitação do uso de dados pessoais pelo poder público ou agentes privados. A proteção de dados integra a proteção da dignidade da pessoa humana, sendo pressuposto para que indivíduos e coletividade possam participar da vida pública de forma consciente, informada e autônoma.

A definição legal da finalidade da PNPD não pode ser lida isoladamente de seus fundamentos: é precisamente o entrelaçamento entre o para quê da política — assegurar os direitos fundamentais à privacidade e à proteção de dados — e o por quê que a sustenta — o pleno exercício da cidadania e a promoção de um ecossistema informacional justo — que confere densidade normativa ao texto e o transforma em vetor interpretativo capaz de orientar a aplicação concreta de suas disposições. O conceito de ecossistema informacional justo cumpre papel central nesse ponto. Ele desloca a proteção de uma visão fragmentada, que trata privacidade, proteção de dados, liberdade de expressão e governança de algoritmos como temas isolados, para uma perspectiva mais ampla e atenta às relações de poder entre empresas, Estado e cidadãos. Com isso, a proteção de dados deixa de se limitar ao titular individual e passa a alcançar também dimensões coletivas, comunitárias e socioambientais. Esse ecossistema também não se restringe ao mundo digital. A proteção da privacidade e dos dados alcança igualmente o universo analógico e offline, já que a coleta e a circulação de informações produzem efeitos concretos na vida das pessoas: no acesso ao crédito, ao trabalho, aos serviços públicos e à participação democrática. A justiça do ecossistema informacional é, assim, condição para que a proteção de dados sirva a um propósito mais amplo, ancorado na dignidade humana, na redução das desigualdades e na

sustentabilidade[7].

O direito fundamental à proteção de dados permite também que inovações no setor público sejam pensadas para lidar com os desafios da sociedade brasileira de forma responsável. Isso significa dizer que tal direito fundamental visa permitir o uso de dados para iniciativas que visam promover o desenvolvimento socioeconômico, cultural e ambiental, o desenvolvimento do sistema produtivo nacional e regional. Tudo isso prezando pela autonomia tecnológica do país e sua inserção e competitividade nos mercados interno e internacional. Iniciativas como a Nuvem Soberana encarnam esse desenvolvimento de uma autonomia em relação à gestão de dados pessoais no Brasil e redução de dependência em uma infraestrutura tão crítica.

Sugestão de Redação

Art. X: São diretrizes e objetivos da Política Nacional de Proteção de Dados:

X - fomentar o desenvolvimento e a adoção de tecnologias que facilitem o exercício dos direitos dos titulares;

x - a autodeterminação informativa junto à participação e controle social por meio da transparência ativa e passiva de informações públicas

X - precaução que por meio da promoção de um ambiente colaborativo, participativo e transparente na cognição, mitigação e gerenciamento dos riscos em prol da proteção da liberdade e direitos fundamentais;

X - a observância da sustentabilidade socioambiental no tratamento de dados pessoais, mediante a promoção de práticas que considerem os impactos ambientais decorrentes do tratamento em larga escala e da infraestrutura a ele associada, bem como os efeitos diferenciados sobre comunidades e grupos vulneráveis

A PNPD deverá consolidar mecanismos para garantir que todos os titulares, independentemente de nível educacional, condição socioeconômica ou grau de letramento digital, possam exercer plenamente os direitos previstos na LGPD, fortalecendo a autodeterminação informacional, reduzindo assimetrias de poder e aumentando a confiança social nos tratamentos de dados.

O conjunto de direitos previstos na LGPD formam um sistema integrado de garantias que precisa ser promovido pela PNPD, que inclui o direito de confirmação e acesso aos dados (art. 18, I

7 Veja mais em: https://www.dataprivacybr.org/en/beyond-digital-rights-towards-a-fair-information-ecosystem/

e II, LGPD), permitindo ao titular conhecer quais dados são tratados, para quais finalidades, por quais agentes e com quais compartilhamentos; o direito de correção dos dados (art. 18, III, LGPD), que possibilita a correção de informações inexatas ou desatualizadas; e o direito de eliminação (art. 18,VI, LGPD), aplicável em situações em que a manutenção do dado não se justifica, garantindo aderência à necessidade e finalidade do tratamento.

A precaução é essencial como diretriz porque trata a gestão de riscos como um processo contínuo, transparente e participativo, e não como simples supressão do tratamento diante da incerteza[8]. A proposta de diretriz estimula um uso responsável dos dados pessoais por entes federativos e diferentes organizações, propondo que a coleta, tratamento e eliminação seja precedida de cautela a respeito de seus potenciais riscos.

A PNPD também deve reforçar a operacionalização do direito de portabilidade dos dados (art. 18, V, LGPD), que promove autonomia do usuário na circulação de seus próprios dados e favorece ambientes competitivos. A revogação do consentimento (art. 18, IX, LGPD) deve ser facilitada, sem ônus ou barreiras de design, assegurando que permissões de tratamento de dados concedidas possam ser retiradas de forma simples, informada e contínua.

O direito de oposição (art. 18, §2°, LGPD) é central para impedir usos ilegais, incompatíveis, excessivos ou que violem expectativas legítimas do titular. Esta prerrogativa ganha importância especial em cenários de decisões automatizadas, perfis comportamentais de usuários, uso de dados sensíveis e tratamentos que promovem grandes assimetrias de poder, devendo a PNPD estabelecer diretrizes específicas para que titulares possam contestar, solicitar revisão e exigir intervenção humana quando decisões os afetarem de maneira relevante, principalmente considerando o design de aplicações.

A política deve avançar também na definição de padrões mínimos para canais de atendimento, que deverão ser acessíveis, gratuitos, multicanal (digital, presencial e telefônico), com linguagem simples e adaptada a populações vulneráveis ou com baixo letramento digital. Tais canais devem garantir transparência sobre prazos de resposta, mecanismos de acompanhamento e possibilidade de encaminhamento para supervisão da ANPD em caso de resposta inadequada ou omissão por parte do agente de tratamento.

A PNPD deve incentivar mecanismos alternativos de solução de conflitos, como mediação, ouvidorias especializadas, plataformas públicas de resolução e instrumentos cooperativos entre ANPD, Procons e Ministério Público, assegurando respostas céleres a violações de direitos. Além disso, a política pode prever iniciativas que auxiliem titulares na compreensão dos impactos sociais e coletivos do uso de dados, reforçando a leitura de que os direitos não se referem apenas à esfera individual e podem ser a chave para a proteção de grupos expostos a riscos discriminatórios.

Assim, os direitos dos titulares constituem não apenas garantias individuais, mas instrumentos

8 BIONI, B. R.; LUCIANO, M. . O Princípio da Precaução na Regulação de Inteligência Artificial: Seriam as Leis de Proteção de Dados o seu Portal de Entrada?. In: Ana Frazão; Caitlin Mulholland. (Org.). Inteligência Artificial e Direito – Ética, Regulação e Responsabilidade. 1ed.São Paulo: Thomson Reuters, 2019, v. , p. 207–231.

estruturantes para a proteção de dados no Brasil, devendo a PNPD assegurar sua plena efetividade como condição indispensável para a construção de um ecossistema informacional justo, seguro e centrado na proteção das pessoas.

Educação, Capacitação e Cultura de Proteção de Dados

CAPÍTULO X

DA EDUCAÇÃO, CAPACITAÇÃO E CULTURA DE PROTEÇÃO DE DADOS PESSOAIS E PRIVACIDADE

Art. X. A Política Nacional de Proteção de Dados Pessoais promoverá a educação, a conscientização e o desenvolvimento de uma cultura de proteção de dados pessoais e privacidade, bem como tecnologias que facilitem o exercício dos direitos dos titulares.

Art. X. Constituem objetivos da política de educação, capacitação e cultura em proteção de dados e privacidade:

I – ampliar a compreensão da população acerca dos direitos fundamentais à privacidade e à proteção de dados pessoais;

II – fomentar o exercício dos direitos dos titulares;

III – promover o tratamento de dados pessoais de forma ética, segura e responsável;

IV – fortalecer capacidades institucionais para a implementação da legislação de proteção de dados;

V – estimular a pesquisa, a inovação e a produção de conhecimento em proteção de dados pessoais.

Art. X. O Poder Público promoverá a integração progressiva de conteúdos relacionados à privacidade, proteção de dados pessoais, segurança da informação e adoção responsável de tecnologias nas diretrizes curriculares da educação básica e da educação superior.

§ 1º A inclusão dos conteúdos observará o princípio da transversalidade curricular e poderá ocorrer de forma interdisciplinar nas diferentes etapas e modalidades de ensino.

§ 2º O Ministério da Educação, em articulação com a Agência Nacional de Proteção de Dados – ANPD o Conselho Nacional de Educação e o Comitê Gestor

da Internet, poderá elaborar referenciais curriculares, materiais pedagógicos e orientações para implementação dos conteúdos previstos neste artigo.

Art. X+3. Os órgãos e entidades da administração pública deverão promover programas permanentes e recorrentes de capacitação e atualização de agentes públicos.

Art. X+4. A União fomentará programas de capacitação destinados a profissionais dos setores público e privado, pesquisadores, educadores, organizações da sociedade civil e demais atores envolvidos em atividades de tratamento de dados pessoais.

Art. X. Por ocasião do Dia Nacional da Privacidade e Proteção de dados, órgãos e entidades da administração pública deverão promover anualmente ações de conscientização, educação e divulgação dos direitos dos titulares de dados pessoais.

Parágrafo único. Durante a semana em que ocorrer a data comemorativa, os órgãos e entidades públicas poderão promover campanhas educativas, seminários, concursos, atividades escolares e iniciativas de engajamento social relacionadas à proteção de dados pessoais.

Art. X. A ANPD poderá desenvolver, em cooperação com instituições públicas e privadas, programas nacionais de educação e conscientização voltados à proteção de dados pessoais e aos direitos dos titulares.

O fortalecimento de uma cultura nacional de proteção de dados exige ações estruturadas, contínuas e multissetoriais, voltadas tanto à formação técnica quanto à conscientização pública ampla. A PNPD deve ser o instrumento capaz de promover iniciativas, estabelecer prioridades e criar mecanismos de coordenação nacional de iniciativas de letramento digital, autonomia informacional e práticas seguras de tratamento de dados em toda a sociedade.

A política pode instituir programas nacionais de conscientização pública, com foco em comunicação acessível, linguagem simples, campanhas educativas, produção de materiais didáticos, ações voltadas a escolas, adolescentes, populações vulneráveis e comunidades tradicionais, além de iniciativas cooperativas com organizações da sociedade civil. O objetivo é disseminar noções de privacidade, proteção de dados, riscos do ambiente digital, direitos dos titulares, uso seguro de tecnologias e impactos sociais e coletivos associados ao tratamento de dados pessoais.

No setor público, é fundamental implementar formações e treinamentos permanentes para servidores e profissionais, com trilhas de capacitação alinhadas aos princípios da LGPD, boas práticas de governança de dados, prevenção de riscos e accountability. A profissionalização da governança de dados de dados deve integrar carreiras estratégicas da administração pública,

com incentivos à criação de equipes e estruturas institucionais de proteção de dados.

A PNPD também deve incentivar a pesquisa científica e tecnológica sobre proteção de dados, segurança da informação, inteligência artificial, soberania tecnológica, governança de dados e impactos sociais do tratamento massivo de dados. Programas de financiamento, centros de pesquisa e cooperação acadêmica são instrumentos essenciais para o fortalecimento da autonomia tecnológica nacional e precisam ser fortalecidos pela PNPD.

Por fim, a política deve promover cooperação com instituições de ensino, articulando universidades, escolas e organizações especializadas em educação e comunicação do tema da proteção de dados. Essa integração poderia ampliar a legitimidade pública da PNPD e assegurar que a cultura de proteção de dados se torne parte da formação cidadã de todo brasileiro.

CAPÍTULO X

DO FOMENTO À INOVAÇÃO E ÀS TECNOLOGIAS DE PROTEÇÃO DE DADOS

Art. X. O Poder Público promoverá o desenvolvimento, a adoção e a difusão de tecnologias, metodologias e soluções voltadas à proteção de dados pessoais, à privacidade, à segurança da informação e à governança responsável de dados.

Parágrafo único. As ações de fomento deverão priorizar soluções que promovam a proteção dos direitos fundamentais dos titulares de dados pessoais, a inovação tecnológica, a competitividade econômica e a autonomia tecnológica do país.

Art. X. Constituem objetivos da política de fomento à inovação em proteção de dados:

I – estimular a pesquisa científica e tecnológica em proteção de dados pessoais;

II – promover o desenvolvimento de Tecnologias de Facilitação da Privacidade – Privacy Enhancing Technologies (PETs);

III – incentivar soluções que implementem os princípios de privacidade desde a concepção e por padrão;

IV – incentivar o desenvolvimento de soluções nacionais voltadas à governança, anonimização, pseudonimização, auditoria, rastreabilidade e direito de revi-

são em meio a processos de decisões automatizadas.

Art. X. A União poderá instituir programas de apoio financeiro, técnico e institucional destinados ao desenvolvimento, à validação, à adoção e à escalabilidade de tecnologias de proteção de dados pessoais.

§ 1º Os programas poderão contemplar:

I – pesquisa científica básica e aplicada;

II – projetos de inovação tecnológica;

III – empresas de base e nascentes de tecnologia;

IV – laboratórios de pesquisa e desenvolvimento;

V – projetos de transferência tecnológica;

VI – programas de capacitação e formação de recursos humanos especializados.

§ 2º Os programas deverão observar critérios de transparência, impacto social, potencial inovador, mitigação de riscos e contribuição para a proteção dos direitos fundamentais.

Art. X. Os instrumentos de implementação desta Política poderão incluir linhas de financiamento, crédito, investimento, subvenção econômica, encomenda tecnológica e incentivos à pesquisa e inovação operacionalizados por instituições públicas federais.

§ 1º A União buscará articular a implementação desta Política com os instrumentos de fomento administrados pelo Banco Nacional de Desenvolvimento Econômico e Social – BNDES, pela Financiadora de Estudos e Projetos – FINEP, pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico – CNPq, pela Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – CAPES e por demais entidades públicas de apoio à inovação.

§ 2º Os fundos públicos destinados ao desenvolvimento científico, tecnológico e industrial poderão contemplar programas e projetos relacionados à proteção de dados pessoais, à privacidade, à segurança da informação e às tecnologias de facilitação da privacidade.

§ 3º Os órgãos competentes poderão estabelecer programas prioritários para o desenvolvimento e adoção de Tecnologias de Facilitação da Privacidade – Privacy Enhancing Technologies (PETs), incluindo técnicas de anonimização, criptografia avançada e outras tecnologias destinadas à redução de riscos aos titula-

res de dados.

Art. X. Nas contratações públicas de soluções digitais intensivas em tratamento de dados pessoais, os órgãos e entidades da administração pública deverão considerar, sempre que tecnicamente viável, a adoção de tecnologias e arquiteturas que incorporem mecanismos de proteção de dados desde a concepção e por padrão, observadas as diretrizes da ANPD.

Para que a proteção de dados cumpra essa função de vetor de desenvolvimento, a PNPD não deve se limitar a uma lógica regulatória punitiva e descendente, mas combiná-la com instrumentos de incentivo a comportamentos desejáveis, induzindo a corregulação a partir das próprias práticas dos agentes. Como se observa no debate sobre o Plano Nacional de Internet das Coisas, a privacidade pode deixar de ser percebida como mero custo de conformidade e passar a constituir elemento de competitividade e vantagem econômica, sobretudo quando a proteção de dados desde a concepção (*privacy by design*) é estimulada por normas, como o direito ambiental faz ao conceder benefícios a tecnologias menos poluentes[9]. É nessa direção que se propõe articular a implementação da Política com os instrumentos de fomento à inovação, de modo que a adoção de boas práticas de proteção de dados possa ser estimulada no âmbito do financiamento público à pesquisa e ao desenvolvimento tecnológico.

9 BIONI, Bruno. Como o brasil pode ter um plano nacional de IOT inovador para a proteção de dados pessoais?. In: Proteção de dados: contexto, narrativa e elementos fundantes. 2021.

PARTE 2
PNPD – Quem e como

Cooperação e Arranjos Institucionais

Sugestão de Redação

CAPÍTULO X

DO SISTEMA NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE

Art. X. Fica instituído o Sistema Nacional de Proteção de Dados Pessoais e da Privacidade – SNPDP, com a finalidade de promover a coordenação federativa, a articulação institucional, a cooperação regulatória e a implementação integrada da Política Nacional de Proteção de Dados Pessoais e da Privacidade.

§ 1º O Sistema Nacional de Proteção de Dados Pessoais e da Privacidade será composto por:

I – a Agência Nacional de Proteção de Dados;

II – a Secretaria Nacional de Direitos Digitais;

III – o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade;

IV – o Fórum Nacional de Proteção de Dados Pessoais e da Privacidade;

V – demais instituições públicas e entidades colaboradoras definidas em regulamento.

§ 2º O Sistema Nacional tem por objetivos:

I - a implementação coordenada, harmônica e integrada da Política Nacional de Proteção de Dados Pessoais e da Privacidade em todo o território nacional;

II - promover a cooperação institucional entre os órgãos e entidades responsáveis pela proteção de dados pessoais;

III - promover ações integradas de educação e conscientização pública e formação técnica em proteção de dados pessoais;

IV - fomentar o desenvolvimento de tecnologias que facilitem a conformidade à legislação de proteção de dados, bem como exercício dos direitos pelos titulares

A proteção de dados pessoais no Brasil envolve uma pluralidade de órgãos e entidades, em diferentes esferas federativas, cujas competências se cruzam sem que exista, hoje, uma estrutura formal de coordenação entre elas. A ANPD exerce a função regulatória e fiscalizatória; a Secretaria Nacional de Direitos Digitais conduz a formulação da política no âmbito do Executivo federal; o CNPD atua como instância consultiva e multissetorial; e conselhos, comitês e autoridades

estaduais e municipais vêm assumindo responsabilidades próprias. A instituição de um Sistema Nacional de Proteção de Dados Pessoais e da Privacidade tem como objetivo organizar essa rede em um arranjo institucional comum, que assegure implementação coordenada, harmônica e integrada da política em todo o território nacional. A solução acompanha a tradição do direito administrativo brasileiro, que se vale de sistemas nacionais, como o Sistema Nacional do Meio Ambiente, para articular entes e instâncias em torno de uma política pública transversal, sem suprimir as competências e a autonomia de cada um.

A estruturação do SNPDP é também condição para a efetividade da PNPD. Sem mecanismos estáveis de articulação, persiste o risco de sobreposição de esforços, de lacunas de atuação e de interpretações divergentes entre os órgãos, comprometendo a segurança jurídica e a coerência da proteção de dados no país. A criação do Sistema estabelece as bases para a cooperação institucional, o compartilhamento de boas práticas, a integração das ações de educação e conscientização e o fomento ao desenvolvimento de tecnologias de conformidade e de exercício de direitos pelos titulares. Trata-se, portanto, de instrumento que confere capilaridade e governança à política, traduzindo as diretrizes nacionais em uma atuação coordenada de múltiplos atores.

Sugestão de Redação

Seção — Fórum Nacional de Proteção de Dados Pessoais e da Privacidade

Art. X. Fica instituído o Fórum Nacional de Proteção de Dados Pessoais e da Privacidade, instância permanente de articulação entre União, Estados, Municípios e Distrito Federal para cooperação e coordenação da implementação e monitoramento da política nacional de privacidade e proteção de dados em toda a federação

§ 2º O Fórum Nacional será composto por:

I – todos membros titulares do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade;

II – representantes de conselhos, comitês, autoridades, órgãos ou instâncias estaduais relacionados à proteção de dados pessoais, limitado a indicação de 01 (uma) pessoa por cada ente estadual e distrital;

III – representantes de conselhos, comitês, autoridades, órgãos ou instâncias municipais relacionados à proteção de dados pessoais, limitado a indicação de 01 (uma) pessoa por um ente municipal;

IV – representantes da Agência Nacional de Proteção de Dados;

V – poderão ser convidados representantes de entidades da sociedade civil, da comunidade científica, do setor produtivo e de instituições públicas de ensino e pesquisa, na forma do regulamento.

Art. X. Compete ao Fórum Nacional de Proteção de Dados Pessoais e da Pri-

vacidade:

I – promover a cooperação federativa em matéria de proteção de dados pessoais;

II – fomentar a disseminação de conhecimento e ferramentas tecnológicas quanto à proteção de dados, em especial quanto à intersecção com acesso à informação e com ênfase no atendimento de direitos dos titulares;

III - propor diretrizes para ações coordenadas de educação digital, conscientização pública e formação técnica em proteção de dados pessoais;

IV - contribuir para a elaboração, monitoramento e avaliação da Política Nacional de Proteção de Dados Pessoais e da Privacidade;

Art. O Fórum Nacional reunir-se-á bienalmente, na forma do regulamento.

§ 1º O Fórum Nacional poderá instituir grupos de trabalho temáticos, câmaras técnicas e redes colaborativas para o desenvolvimento de estudos, propostas e ações específicas.

§ 2º A participação no Fórum Nacional será considerada prestação de serviço público relevante, não remunerada.

Nos últimos anos, observa-se a emergência de diversos conselhos, comitês, autoridades e instâncias estaduais e municipais voltados à proteção de dados pessoais, que vêm desenvolvendo normas, projetos e boas práticas de forma autônoma e descentralizada. Esse movimento revela o amadurecimento do tema na federação, mas também produz experiências dispersas, com graus distintos de maturidade institucional e sem mecanismos estáveis de articulação entre si e com a esfera nacional.

Nos últimos anos, observa-se a emergência de diversos conselhos, comitês, autoridades e instâncias estaduais e municipais voltados à proteção de dados pessoais, que vêm desenvolvendo normas, projetos e boas práticas de forma autônoma e descentralizada. Esse movimento revela o amadurecimento do tema na federação, mas também produz experiências dispersas, com graus distintos de maturidade institucional e sem mecanismos estáveis de articulação entre si e com a esfera nacional.

Essa assimetria é especialmente relevante no nível municipal, em que os gargalos institucionais são mais evidentes. Segundo dados do Cetic.br/NIC.br, em 2023 apenas 36% das prefeituras possuíam área ou pessoa responsável por procedimentos e políticas de coleta, armazenamento ou uso de dados pessoais ou pela implementação da LGPD. O percentual era ainda menor entre municípios de até 10 mil habitantes, nos quais apenas 31% das prefeituras declararam possuir esse tipo de estrutura, enquanto chegava a 82% nas cidades com mais de 500 mil habitantes

(CGI.br, 2024, p. 90)[10] . No mesmo levantamento, menos da metade das prefeituras havia adotado ações básicas relacionadas à LGPD: 42% disponibilizavam canais de atendimento sobre uso de dados pessoais, 29% possuíam documento formal sobre papéis e responsabilidades internas e apenas 21% haviam nomeado encarregado de dados pessoais (CGI.br, 2024, p. 91)[11] .

Embora os órgãos federais disponham de maior capacidade institucional, o próprio Cetic.br aponta que 90% dos órgãos federais possuíam área ou pessoa responsável pelo tema em 2023(CGI.br, 2024, p. 86)[12], os dados do Tribunal de Contas da União indicam que a adequação à LGPD também permanece insuficiente nesse nível. Em auditoria realizada com 387 entidades, o TCU identificou que quase 60% ainda se encontravam em grau inexpressivo ou inicial de adequação, enquanto apenas 8,53% estavam em estágio aprimorado. O diagnóstico também apontou falhas estruturais relevantes: quase um terço das organizações ainda não havia concluído estudos de identificação e planejamento das medidas necessárias à adequação; 10% sequer tinham mapeado elementos básicos dos tratamentos de dados pessoais; apenas 25% haviam incluído proteção de dados em seus planos de capacitação e treinado seus colaboradores; 70% não mantinham registros de operações de tratamento; 72,35% não elaboravam Relatórios de Impacto à Proteção de Dados[13]; quase 40% não possuíam política de privacidade com visibilidade adequada ao tratamento; 23% não dispunham de mecanismos para atendimento dos titulares[14]; e cerca de 45% não haviam mapeado o compartilhamento de dados[15].

Esses dados sugerem que o desafio federativo da proteção de dados pessoais envolve a construção de capacidades institucionais mínimas, a padronização de procedimentos, a capacitação de servidores, a articulação entre transparência pública e proteção de dados e a coordenação entre União, estados e municípios. Sem mecanismos estáveis de cooperação e indução federativa, há o risco de que a implementação da LGPD avance de forma desigual, concentrando maior maturidade em alguns órgãos e entes federativos, enquanto outros permanecem sem estruturas básicas para garantir direitos dos titulares, segurança jurídica aos agentes públicos e uso responsável de dados pessoais pelo Estado.

A criação de um Fórum Nacional responde justamente a essa necessidade: oferecer um espaço permanente de cooperação federativa, capaz de integrar as iniciativas locais e regionais, harmonizar entendimentos, compartilhar boas práticas e evitar a fragmentação na implementação da política. Ao reunir União, Estados, Municípios e Distrito Federal em uma instância comum, o Fórum permite que as experiências acumuladas nos diferentes entes sejam aproveitadas de forma coordenada, fortalecendo a capacidade institucional do conjunto da federação e assegurando

10 CGI.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. p.90

11 Ibid. p. 91

12 Ibid. p. 86

13 BRASIL. Tribunal de Contas da União. Acórdão nº 1.372/2025 – Plenário. Relatório de Auditoria. TC 009.980/2024-5. Relator: Ministro Walton Alencar Rodrigues. Brasília, DF: Tribunal de Contas da União, 2025. p. 21–22

14 Ibid. p. 23–25

15 Ibid. p.26–29

coerência na proteção de dados pessoais em todo o território nacional.

Sugestão de Redação

Seção I Da Secretaria Nacional de Direitos Digitais

Art. X. Compete à Secretaria Nacional de Direitos Digitais coordenar a implementação da Política Nacional de Proteção de Dados Pessoais e da Privacidade no âmbito da administração pública federal, sem prejuízo das competências da Agência Nacional de Proteção de Dados.

Art. São competências da Secretaria Nacional de Direitos Digitais:

I – promover a articulação entre órgãos e entidades da administração pública federal para implementação integrada da Política Nacional;

II – coordenar estratégias nacionais de educação e conscientização pública e formação em proteção de dados pessoais;

III – apoiar Estados, Distrito Federal e Municípios no fortalecimento de capacidades institucionais relacionadas à proteção da privacidade;

V – fomentar a adoção de boas práticas de governança de dados pessoais no setor público;

VI – promover estudos, diagnósticos, pesquisas e indicadores relacionados à proteção de dados pessoais e direitos digitais;

§ 1º Para fins do disposto no caput, a Secretaria poderá:

I – instituir comitês, grupos de trabalho e instâncias de articulação interministerial;

II – promover ações integradas entre órgãos e entidades da administração pública federal;

§ 2º A Secretaria Nacional de Direitos Digitais promoverá, em conjunto com a Secretaria Nacional do Consumidor, cooperação permanente com os órgãos integrantes do Sistema Nacional de Defesa do Consumidor, especialmente os Procons, as Defensorias Públicas e o Ministério Público, compreendendo, entre outras medidas:

I – o compartilhamento e o cruzamento de informações, estudos e diagnós-

ticos;

III – o fortalecimento da atuação dos Procons em matérias relacionadas ao tratamento de dados pessoais nas relações de consumo, especialmente quanto:

a) incidentes de segurança;

b) à publicidade comportamental e práticas de perfis comportamentais;

c) o tratamento de dados pessoais para oferta, precificação ou direcionamento de produtos e serviços;

IV – a articulação com as Defensorias Públicas e o Ministério Público para promoção do acesso à justiça, tutela coletiva e proteção de consumidores e titulares de dados;

V – o desenvolvimento de mecanismos de indicadores relacionados às políticas nacionais de proteção de dados pessoais e de defesa do consumidor, especialmente quanto:

a) à correlação entre acidentes de consumo e incidentes de segurança envolvendo dados pessoais;

b) o reconhecimento da assimetria informacional, técnica e econômica comum entre consumidores e titulares de dados pessoais;

A previsão de competências próprias da Secretaria Nacional de Direitos Digitais justifica-se pela necessidade de um órgão do Executivo federal capaz de coordenar a implementação da PNPD na administração pública, função distinta e complementar à atuação regulatória e fiscalizatória da ANPD. Enquanto a Agência preserva sua independência técnica, cabe à Secretaria articular órgãos e entidades federais, apoiar Estados e Municípios no fortalecimento de suas capacidades institucionais e conduzir estratégias nacionais de educação, governança e produção de indicadores.

Destaca-se, ainda, a cooperação permanente com o Sistema Na cional de Defesa do Consumidor — Procons, Defensorias Públicas e Ministério Público —, que reconhece a sobreposição frequente entre violações de proteção de dados e lesões a consumidores. Essa articulação dialoga diretamente com experiências já desenvolvidas pela Data Privacy Brasil para profissionais de Procons de todo o país. A iniciativa capacitou 76 alunos, incluindo representantes de Procons de todos os estados, além de promotores de justiça e defensores públicos, abordando temas como direitos dos consumidores e titulares de dados, vazamentos de dados, direito à informação, práticas abusivas e conformidade institucional à LGPD.

Essa experiência evidencia que a articulação entre proteção de dados e defesa do consumidor não é apenas desejável no plano normativo, mas também necessária para qualificar a atuação dos órgãos de linha de frente, ampliar a tutela coletiva e enfrentar as assimetrias informacionais, técnicas e econômicas que marcam o tratamento de dados pessoais em relações de consumo. Ao privilegiar a experiência do Ministério da Justiça e Segurança Pública enquanto instituição capaz de articular diferentes esferas da vida pública , consumidor, combate à criminalidade, acesso à justiça, entre outros, tal arranjo indica as conexões necessárias para uma política nacional de direitos digitais orientada à efetividade institucional e à proteção concreta de direitos.

Cooperação e Integração do Nacional Face ao Regional e ao Global

Sugestão de Redação

Art. X A Agência Nacional de Proteção de Dados atuará, em permanente articulação com o Ministério das Relações Exteriores, como órgão central de cooperação internacional para promover a inserção do país em redes regionais e globais de proteção à privacidade e de dados pessoais.

§ 1º Compete à Agência Nacional de Proteção de Dados:

I – promover a harmonização de entendimentos regulatórios internacionais com a legislação brasileira de proteção de dados pessoais;

II - promoção da convergência regulatória compatível a legislação brasileira e política nacional de proteção de dados;

III – ampliação da segurança jurídica para fluxos internacionais de dados pessoais;

IV – incentivo à cooperação internacional em investigações, enforcement e resposta a incidentes transfronteiriços de proteção de dados;

V – promoção de padrões internacionais de proteção de dados centrados na pessoa humana.

§ 3º A Agência Nacional de Proteção de Dados poderá celebrar acordos, memorandos de entendimento e instrumentos de cooperação internacional com autoridades estrangeiras e organismos internacionais, observadas as disposições legais aplicáveis e as diretrizes da política externa brasileira.

§ 4º A atuação internacional de que trata este artigo deverá ser integrada às estratégias nacionais de implementação da Política Nacional de Proteção de Dados Pessoais e da Privacidade, de forma a assegurar coerência entre a governança doméstica, a cooper

§ 5º Nos acordos celebrados, deverá ser priorizada a produção de conhecimento e cooperação dos povos da América Latina e de línguas portuguesas.

O fluxo transnacional de dados é uma realidade concreta, de modo que a cooperação e integração internacional devem estar previstas na Política Nacional de Proteção de Dados. Com vistas a isso, propõe-se a harmonização com normas internacionais, acordos de cooperação e atuação em fóruns regionais, ações já em curso pela ANPD nos últimos anos.

Monitoramento, Avaliação e Revisão da Política

O monitoramento e a avaliação da Política Nacional de Proteção de Dados devem constituir eixo permanente de sua implementação. Para isso, é importante atribuir à Agência Nacional de Proteção de Dados a responsabilidade pela definição de indicadores de desempenho capazes de mensurar a efetividade da política, identificar gargalos institucionais e orientar prioridades de capacitação, cooperação federativa, fiscalização e revisão normativa.

Esses indicadores devem dialogar com pesquisas já consolidadas, como as produzidas pelo Cetic.br/NIC.br. No setor público, a pesquisa TIC Governo Eletrônico passou a monitorar, desde 2021, ações relacionadas à privacidade e à proteção de dados pessoais em órgãos públicos federais, estaduais e municipais, permitindo acompanhar a evolução da agenda e comparar diferentes níveis de maturidade institucional ao longo do tempo[16]. A série histórica é especialmente importante porque permite verificar se as medidas adotadas produzem avanços concretos, se gargalos persistem e se há desigualdades relevantes entre União, estados, municípios e também entre diferentes setores econômicos.

Os próprios dados do Cetic.br/NIC.br evidenciam a necessidade desse acompanhamento contínuo. Em 2023, 90% dos órgãos federais possuíam área ou pessoa responsável por procedimentos e políticas de coleta, armazenamento ou uso de dados pessoais ou pela implementação da LGPD, percentual superior ao verificado nos órgãos estaduais, de 79%[17]. No nível municipal, contudo, os gargalos são mais evidentes: apenas 36% das prefeituras possuíam esse tipo de estrutura, percentual que caía para 31% nos municípios de até 10 mil habitantes e chegava a 82% naqueles com mais de 500 mil habitantes[18]. No setor privado, a TIC Empresas 2023 também revela avanços ainda limitados: apenas 33% das empresas realizaram treinamentos ou capacitações internas sobre proteção de dados pessoais, embora esse percentual tenha aumentado em relação a 2021, quando era de 29%[19]. Além disso, entre 2021 e 2023, houve crescimento nas ações de adequação à LGPD, como a alteração de contratos, que passou de 28% para 35%, e a elaboração de plano de conformidade ou adequação à proteção de dados pessoais, que passou de 24% para 32%[20].

16 CGI.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. p.85

17 Ibid. p. 86

18 Ibid. p. 90

19 Ibid. p. 74

20 Ibid. p. 30

Sugestão de Redação

Indicadores de Desempenho e Resultados

Seção X - Do Monitoramento, Avaliação e Revisão da Política Nacional

Art. X. A Agência Nacional de Proteção de Dados e Secretaria Nacional de Direitos Digitais deverão estabelecer sistema permanente de monitoramento e avaliação da Política Nacional de Proteção de Dados Pessoais e da Privacidade, mediante a definição de indicadores de desempenho, resultados e impacto destinados a aferir sua implementação e efetividade.

§ 1º Os indicadores de que trata o caput deverão considerar, entre outros aspectos:

I – o nível de conformidade com a legislação de proteção de dados pessoais;

II – a incidência, gravidade e recorrência de incidentes de segurança envolvendo dados pessoais;

III – a efetividade das medidas de prevenção, mitigação e resposta a incidentes;

IV – o nível de conscientização e educação da população acerca de seus direitos;

V – o desenvolvimento de tecnologias e a proteção de dados desde a concepção até a execução de produtos, serviços e políticas públicas e o exercício facilitado dos direitos dos titulares;

VI – o nível de cooperação dos entes federativos e dos órgãos integrantes do Sistema Nacional;

VII – a efetividade da atuação regulatória, fiscalizatória e sancionatória em matéria de proteção de dados pessoais, incluindo do Sistema Nacional de Defesa do Consumidor ;

VIII – os impactos diferenciados do tratamento de dados pessoais sobre grupos vulneráveis;

§ 2º Os indicadores de desempenho e resultados deverão ser elaborados com participação do Conselho Nacional de Proteção de Dados Pessoais e da Privaci-

dade, garantindo-se transparência, participação social e multissetorialismo.

§ 3º A metodologia, os dados agregados, os critérios de avaliação e os resultados do monitoramento deverão ser disponibilizados em formato acessível e aberto.

Art. X. A produção de dados, estudos, estatísticas e mecanismos de monitoramento da Política Nacional poderá contar com:

I - a cooperação do Comitê Gestor da Internet no Brasil e do Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (CETIC.br), especialmente para:

a) percepção social e maturidade institucional no setor público e privado sobre proteção de dados pessoais;

b) – apoio técnico à padronização de indicadores nacionais;

c) – disseminação de informações qualificadas sobre a implementação da Política Nacional.

Parágrafo único. A cooperação prevista neste artigo deverá observar a autonomia técnica e institucional das entidades envolvidas, bem como promover a integração com outras políticas públicas, tais como governo digital e a proteção integral de crianças e adolescentes;

II - entidades sociedade civil especializada na geração cidadã de dados especialmente para mensurar a percepção social e o nível de conscientização pública sobre proteção de dados

Art.. A Agência Nacional de Proteção de Dados elaborará e publicará, a cada dois anos, o Relatório Nacional de Implementação da Política Nacional de Proteção de Dados Pessoais e da Privacidade.

§ 1º O relatório deverá ser submetido ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade e ao Fórum Nacional de Proteção de Dados Pessoais e da Privacidade, garantindo-se ampla divulgação pública de seu conteúdo.

Art. X. A Política Nacional de Proteção de Dados Pessoais e da Privacidade deverá ser revisada periodicamente, em prazo não superior a quatro anos, ou sempre que houver alterações tecnológicas, regulatórias, econômicas ou sociais relevantes que impactem a proteção de dados pessoais.

P. Único O processo de revisão deverá observar mecanismos de participação social, consulta pública e diálogo multissetorial.

Segurança Pública

Ainda que não seja aplicada em sua integralidade, a Lei Geral de Proteção de Dados tem relevância para nortear o tratamento de dados pessoais na segurança pública, defesa nacional, segurança do Estado, atividades de investigação e repressão de infrações penais. Nesse sentido, é fundamental que a Política afirme expressamente em seu texto a aplicação do devido processo legal, os princípios gerais de proteção e os direitos do titular, bem como a competência da ANPD para regulação e fiscalização na área. Por fim, diante das movimentações recentes em torno do Projeto de Lei nº 1515/2022, conhecida como LGPD Penal, a Política deve prever revisão caso haja aprovação do texto.

Sugestão de Redação

Art. X: O tratamento de dados pessoais em atividades exclusivamente para segurança pública, defesa nacional, segurança do Estado, atividades de investigação e repressão de infrações penais deverão respeitar devido processo legal, os princípios gerais de proteção e os direitos do titular, cabendo à Agência Nacional de Proteção de Dados a fiscalização e regulação desses temas.

Parágrafo 1º: A Agência Nacional de Proteção de Dados poderá firmar acordos de cooperação com órgãos de segurança pública e inteligência para orientação e regulação de suas atividades, resguardado o interesse público e transparência.

Parágrafo 2º: Havendo a publicação de lei específica voltada para o tratamento de dados pessoais, esta Política deverá ser atualizada para aderência ao novo texto legal.

Transparência Pública e Proteção de Dados

A Política Nacional de Proteção de Dados deve se atentar aos movimentos recentes de harmonização da Lei de Acesso à Informação (LAI) e LGPD. A ANPD e Controladoria Geral da União têm acordos de cooperação para garantia de interpretações que não limitem a transparência pública apenas com a justificativa da proteção de dados, além dos próprios enunciados da CGU nesse sentido. Assim, a Política deve reconhecer a LAI e LGPD como instrumentos complementares de proteção de direitos fundamentais, de modo que a legislação de proteção de dados não seja utilizada de forma genérica ou automática para negar pedidos de acesso à informação pública, exigindo-se fundamentação específica, análise de risco e, quando cabível, a aplicação de técnicas de anonimização ou de acesso parcial.

Além disso, cabe incentivar a ampliação da interação institucional entre o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade e os conselhos e instâncias de transparência e controle social, com o objetivo de alinhar entendimentos, compartilhar boas práticas e promover soluções integradas que conciliem a proteção de dados pessoais com a transparência pública e a participação social.

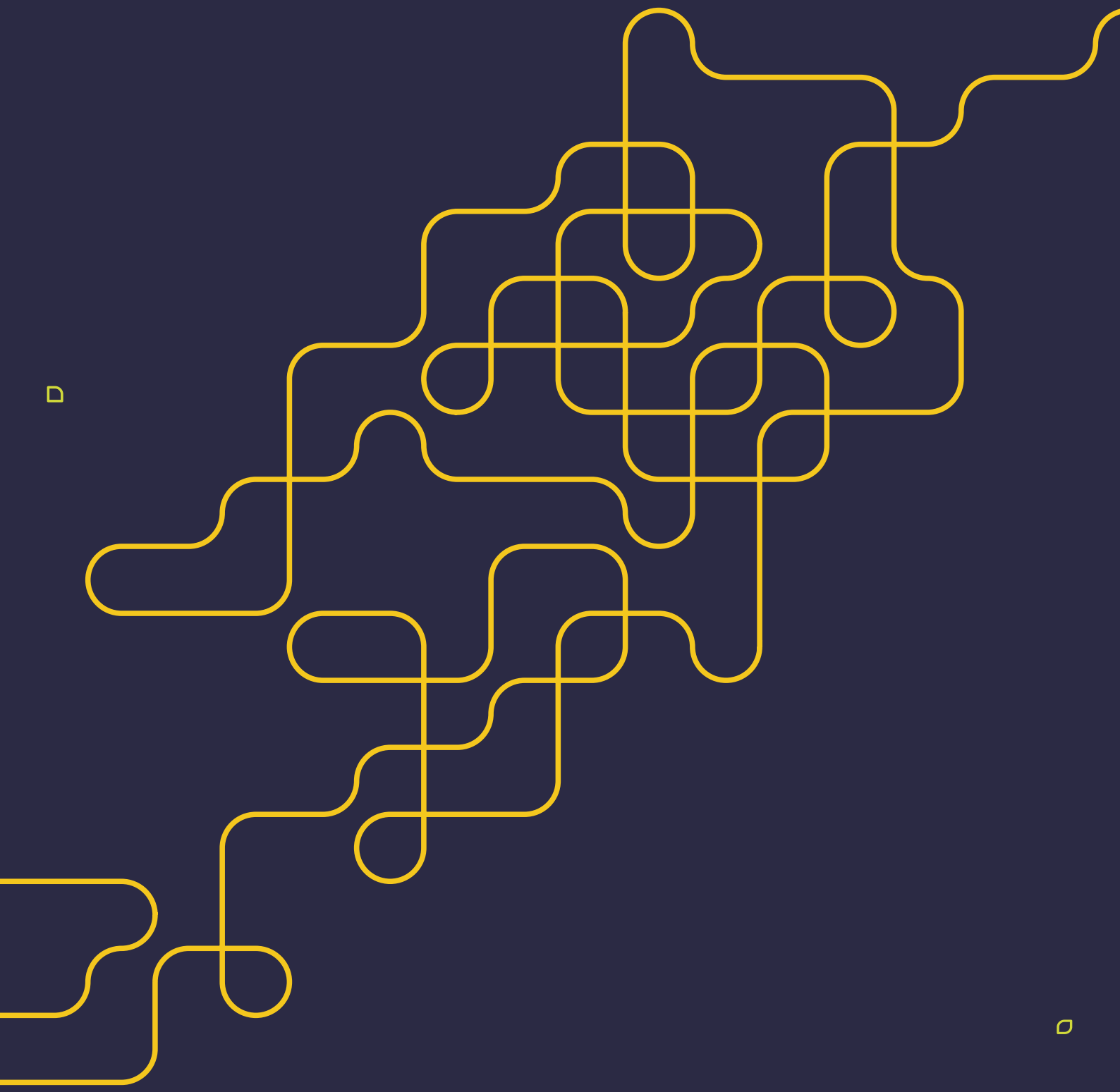
Sugestão de Redação

Art. X: A Política Nacional de Proteção de Dados promoverá a harmonização entre a Lei de Acesso à Informação e a Lei Geral de Proteção de Dados Pessoais, reconhecendo o caráter complementar desses diplomas, vedada a utilização da legislação de proteção de dados como fundamento genérico ou automático para a negativa de pedidos de acesso à informação pública, devendo a decisão ser devidamente motivada e, sempre que possível, precedida da adoção de medidas de anonimização ou de acesso parcial.

Art. X: O Conselho Nacional de Proteção de Dados pode realizar projetos e cooperar com conselhos, comissões ou instâncias responsáveis por políticas de transparência e controle social, com o objetivo de alinhar diretrizes, compartilhar boas práticas e promover soluções integradas entre proteção de dados e transparência pública.

Disposições Finais

Para garantia de incorporação das sugestões e debate social amplo a respeito da política, a proposta é garantir um prazo de dois anos para sua implementação. Além disso, prevê expressamente o financiamento e recursos orçamentários para custeio de suas ações.



DataPrivacyBR

DataPrivacyBR
Research