Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

SUBSÍDIOS PARA ELABORAÇÃO DA POLÍTICA NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE

2025

Conselho Nacional de Proteção de Dados Pessoais e Privacidade

SUBSÍDIOS PARA ELABORAÇÃO DA POLÍTICA NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE

RELATÓRIO COMPILADO

Brasília – DF

Junho de 2025

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA

Presidente do CNPD
Secretária de Direitos Digitais
Lílian Cintra de Melo

Vice-Presidente do CNPD
Victor Epitacio Cravo Teixeira

SECRETARIA DE COMUNICAÇÃO SOCIAL DA PRESIDÊNCIA DA REPÚBLICA

Secretário de Políticas Digitais
João Caldeira Brant Monteiro de Castro

Chefe de Gabinete
Samara Mariana de Castro

CASA CIVIL DA PRESIDÊNCIA DA REPÚBLICA

Secretário-Executivo Adjunto
Pedro Helena Pontual Machado

Secretário Adjunto IV da Secretaria Especial de Articulação e Monitoramento
Rodrigo Rodrigues da Fonseca

MINISTÉRIO DA SAÚDE

Secretária de Informação e Saúde Digital
Ana Estela Haddad

Coordenadora-Geral de Demandas de Órgãos Externos de Informação e Saúde Digital.
Adriana Macedo Marques

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS

Diretor da Privacidade e Segurança da Informação
Leonardo Rodrigo Ferreira

Coordenadora-Geral de Privacidade
Marta Juvina de Medeiros

OUTROS PODERES, ÓRGÃOS OU INSTITUIÇÕES PÚBLICAS

Conselheiro do Senado Federal
Fábio Veras

Conselheiro do Senado Federal
Wederson Advincula Siqueira

Conselheiro da Câmara dos Deputados
Fernando Antonio Santiago Junior

Conselheira da Câmara dos Deputados
Gisela Carvalho de Freitas

Conselheiro do Conselho Nacional de Justiça
Rodrigo Badaró Almeida de Castro

Secretário de Estratégia e Projetos do Conselho Nacional de Justiça
Gabriel da Silveira Matos

Conselheiro do Conselho Nacional do Ministério Público
Moacyr Rey Filho

Conselheiro do Conselho Nacional do Ministério Público
Fernando da Silva Comin

Coordenadora do Comitê Gestor da Internet no Brasil
Renata Vicentini Mielli

Secretário Executivo do Comitê Gestor da Internet no Brasil
Hartmut Richard Glaser

ORGANIZAÇÕES DA SOCIEDADE CIVIL COM ATUAÇÃO COMPROVADA EM PROTEÇÃO DE DADOS PESSOAIS

Bruno Ricardo Bioni
(Data Privacy Brasil de Pesquisa)

Ricardo Alexandre de Oliveira
(ABCOMM, ABINC e ABRAPP)

Isabella Vieira Machado Henriques
(Instituto Alana)

Raquel Lima Saraiva
(IP.rec)

INSTITUIÇÕES CIENTÍFICAS, TECNOLÓGICAS E DE INOVAÇÃO

Gabrielle Bezerra Sales Sarlet
(PUCRS)

Ana Paula Moraes Canto de Lima
(ABCCRIM)

Cláudio Simão de Lucena Neto
(UFPB)

Rodrigo Pironti Aguirre de Castro
(IBDA)

Tiago Lopes de Aguiar
(FAPERO)

Têmis Limberger
(UNISINOS)

CONFEDERAÇÕES SINDICAIS REPRESENTATIVAS DAS CATEGORIAS ECONÔMICAS DO SETOR PRODUTIVO

Cassio Augusto Muniz Borges
(CNI)

Fernando Bueno Fernandes
(Sistema OCB)

Myreilla Aloia Triumpho Pereira da Cruz
(CONSIF)

Marcos Vinícius Barros Ottoni
(CNSaúde)

João Frederico Chagas Maranhão
(CNT)

ENTIDADES REPRESENTATIVAS DO SETOR EMPRESARIAL RELACIONADO À ÁREA DE TRATAMENTO DE DADOS PESSOAIS

Rony Vainzof
(CIESP/FIESP)

Ana Paula Martins Bialer
(ABINEE, ABOOH, Cmara-e.Net, ITI, MBC)

Vitor Morais de Andrade
(ABEMD e outras)

Annette Martinelli de Mattos Pereira (ABECS e Febraban)

ENTIDADES REPRESENTATIVAS DO SETOR LABORAL

Alexandre Zago Boava
(Núcleo de Tecnologia do MTST)

Claudio Eduardo Lobato De Abreu Rocha
(SINAGÊNCIAS)

Débora Sirotheau Siqueira Rodrigues
(CUT)

João Marcos Pereira Vidal
(UGT)

EQUIPE DA SECRETARIA-GERAL

Secretária-Geral da ANPD
Núbia Augusto de Sousa Rocha
Secretária-Geral substituta da ANPD
Michelle Catyana Mota Lira

EQUIPE DE CONSOLIDAÇÃO
Assessora da Secretaria de Direitos Digitais do MJSP
Janaína Gomes Lopes
Assessor da Secretaria de Direitos Digitais do MJSP
Pedro de Barros Correia Amaral

SUMÁRIO

APRESENTAÇÃO

O Conselho Nacional de Proteção de Dados Pessoais e Privacidade – CNPD é um órgão consultivo da Autoridade Nacional de Proteção de Dados – ANPD, composto por membros da sociedade civil e representantes do poder público, designados pelo Presidente da República, nos termos do Decreto n° 11.758, de 30 de outubro de 2023 que alterou o Decreto nº 10.474 de 26 de agosto de 2020.

Consoante o art. 58-B, inciso I, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD), uma das atribuições do CNPD é "propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD". Seu objetivo é fomentar atividades econômicas e tecnológicas que estejam em sintonia com direitos e garantias fundamentais, visando assegurar, no país, um ambiente adequado ao desenvolvimento da sociedade e o fluxo informacional com foco na proteção de dados pessoais.

Assim, no uso das atribuições que conferidas pelos arts. 14, 15, 16 e 17 do Anexo I ao Decreto nº 10.474, de 26 de agosto de 2020 e pela Resolução CNPD nº 2, de 26 de setembro de 2024, e considerando a deliberação adotada na 2ª reunião ordinária do CNPD, foram instituídos, pelas Portarias CNPD nº1 a 6, de 4 de outubro de 2024, os Grupos de Trabalho Temporários - GTTs com duração de 120 dias, e finalidade de fornecer os referidos subsídios, de acordo com as seguintes temáticas:

(i) Educação e capacitação em proteção de dados
(ii) Mecanismos, instâncias e práticas de conformidade de proteção de dados
(iii) Governança de dados (I)
(iv) Governança de dados (II)
(v) Dados pessoais para o desenvolvimento econômico, tecnológico e a inovação; e
(vi) LAI & LGPD: dados abertos como infraestrutura crítica em conformidade com LGPD

As atividades dos GTTs iniciaram-se em outubro de 2024 e se prolongaram até janeiro de 2025. Após inúmeras reuniões virtuais, que somaram aproximadamente 60 reuniões, foram entregues em fevereiro de 2025 os relatórios finais dos GTTs, fruto da redação colaborativa de seus membros. Na 4ª reunião ordinária do CNPD, realizada em 14 de março de 2025, os coordenadores dos GTTs apresentaram os relatórios finais à apreciação do pleno, oportunidade em que foram discutidas as sugestões de subsídios, que receberam comentários e sugestões redacionais.

Nessa oportunidade, também foi deliberado, por maioria de votos, a consolidação dos relatórios finais, considerando os pareceres conclusivos, pela Secretaria de Direitos Digitais do Ministério da Justiça e Segurança Pública, ocupante da posição de presidente do CNPD, trazendo mais concisão à proposta a ser encaminhada à ANPD. Os relatórios finais aprovados pelo Pleno serão encaminhados na íntegra como anexos.

Portanto, este documento compila as conclusões das recomendações de cada GTT. Cada contribuição foi sistematizada em um quadro sinóptico com as categorias princípios, diretrizes, objetivos e instrumentos. Tal classificação é recorrente em políticas nacionais, a exemplo da Política Nacional de Segurança Pública, da Política Nacional de Cibersegurança e da Política Nacional de Inovação. Caberá avaliação da ANPD quanto à sua pertinência, pois buscou-se manter as recomendações na íntegra, exceto quando necessárias adaptações pontuais para coerência textual.

Nesse contexto, os subsídios buscam fortalecer a capacidade institucional da ANPD para coordenar ações intersetoriais, promover a harmonização regulatória entre diferentes órgãos e entidades, e desenvolver estratégias preventivas e educativas que ampliam significativamente seu impacto social.

Ainda, o estabelecimento da Política Nacional de Proteção de Dados Pessoais e da Privacidade conferirá à autoridade maior legitimidade e respaldo técnico para suas decisões, criando um ambiente propício para o diálogo com *stakeholders* nacionais e internacionais, o que é essencial para posicionar o Brasil como referência em governança de dados na região e fortalecer a confiança dos cidadãos nas instituições responsáveis pela proteção de seus direitos fundamentais.

Espera-se que os subsídios ora sistematizados oriundos da participação social, da expertise técnica e da experiência prática acumulada, ofereçam ferramentas estratégicas para o fortalecimento do sistema brasileiro de proteção de dados pessoais e para o alcance dos objetivos fundamentais estabelecidos pela LGPD.

GTT 1 - Educação e capacitação em proteção de dados pessoais

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 e Tiago Lopes de Aguiar

Considerações

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 GTT 1. 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:

(i) 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; criação de um catálogo de cursos e de programas de capacitação; desenvolvimento de materiais didáticos e de recursos educativos; estabelecimento de parcerias com instituições de ensino e de pesquisa; promoção de eventos e de atividades de divulgação; e certificação de profissionais e de organizações.

(ii) 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; criação de um comitê organizador; realização de outros concursos; distribuição de prêmios; e incentivo à participação da sociedade civil.

(iii) Parceria com o Ministério da Educação

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; incentivo à inclusão da educação em proteção de dados na Base Nacional Comum Curricular - BNCC; desenvolvimento de programas de capacitação para professores em proteção de dados e privacidade; promoção de eventos e debates sobre proteção de dados nas universidades; fortalecimento de parcerias e ações com o Sistema de Garantia de Direitos e com o MEC, Comunidade Escolar e Conselhos da área; criação de um programa de Alfabetização Digital para Proteção de Dados; promoção de *hackathons* e desafios de inovação; e incentivo à participação dos cidadãos na fiscalização do uso de seus dados.

(iv) 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; elaboração de propostas de aprimoramento; articulação com outros atores relevantes; participação e organização de audiências públicas e debates; e divulgação das propostas.

(v) 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, 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; definição de áreas temáticas prioritárias; criação de grupos de trabalho interinstitucionais; realização de eventos e treinamentos; desenvolvimento de campanhas de conscientização; e integração de conteúdos nos canais de comunicação dos órgãos.

(vi) 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; adaptação da linguagem e dos formatos; criação de materiais de conscientização voltados especificamente ao público infantil e juvenil; promoção de campanhas de conscientização; estabelecimento de parcerias; criação de um guia de boas práticas; e elaboração de enunciados que orientem o tratamento de dados pessoais dos grupos vulneráveis.

(vii) Parceria com a Escola Nacional de Administração Pública – 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; criação de cursos online e presenciais; promoção da trilha de aprendizagem "Privacidade e Segurança da Informação; desenvolvimento de cursos específicos; realização de eventos e seminários conjuntos; e incentivo à produção de pesquisas e estudos.

(viii) Parceria com a Ordem dos Advogados do Brasil 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; realização de eventos e seminários sobre proteção de dados para a comunidade jurídica; criação de um programa de certificação em proteção de dados para advogados; inclusão obrigatória de questões sobre proteção de dados no Exame de Ordem; e apoio à criação de comissões de proteção de dados nas seccionais da OAB.

(ix) Encontros profissionais

O sucesso do I Encontro ANPD de Encarregados demonstrou a importância da troca de experiências e do diálogo entre os profissionais responsáveis pela proteção de dados nas organizações, evidenciando também a necessidade de ampliar o alcance da conscientização e da capacitação em proteção de dados para outros públicos-alvo que 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; definição dos temas e formatos; realização de eventos temáticos; promoção da interação entre os participantes; divulgação das boas práticas; e promoção de intercâmbio entre entidades e órgãos públicos com disseminação de boas práticas.

(x) 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; definição de temas e formatos; produção de conteúdo educativo; realização de campanhas de conscientização; e participação em eventos, *podcasts* e *lives*.

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.

QUADRO SINÓPTICO

Princípios

Universalidade, acessibilidade, integração e inovação.

Objetivos

Criar uma rede colaborativa interinstitucional para: integrar a proteção de dados nos currículos escolares e universitários; capacitar servidores públicos e empresas sobre a LGPD e boas práticas; estimular a pesquisa acadêmica sobre privacidade e segurança de dados; ampliar a disseminação de informações ao público por meio de campanhas educativas; promover a conscientização jurídica e regulatória sobre proteção de dados; e criar um ecossistema educacional robusto para a formação de uma cultura de proteção de dados.

Diretrizes

- Parcerias e colaborações institucionais;
- Realização de eventos e atividades interativas;
- Produção e disseminação de conteúdo;
- Integração curricular e capacitação profissional;
- Campanhas de conscientização de engajamento público; e
- Desenvolvimento de plataformas e recursos digitais.

Instrumentos

- Desenvolver parcerias com o MEC para promoção da cultura de proteção de dados pessoais;
- Aproximar-se, produzir e revisar conteúdo da ENAP para capacitação de servidores públicos;
- Realizar evento em comemoração ao aniversário da LGPD;
- Realizar webinários sobre compartilhamento de dados no poder público para servidores públicos, tratamento de dados pessoais de crianças e adolescentes e segurança da informação para agentes de tratamento de pequeno porte, em parceria com o Sebrae;
- Produzir e divulgar material sobre o Regulamento de Direito dos Titulares e o 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; e
- Produzir e divulgar conteúdos sobre *cookies*.

GTT 2 - Mecanismos, instâncias e práticas de conformidade de proteção de dados

Membros

Vitor Morais de Andrade (coordenador), Cláudio Eduardo Lobato de Abreu Rocha, Tiago Lopes de Aguiar; Annette Martinelli de Mattos Pereira e Ana Paula Moraes Canto de Lima.

Considerações

A conformidade com a legislação de proteção de dados pessoais vai além do mero cumprimento formal de requisitos legais, demandando uma abordagem holística que envolve mudanças culturais, implementação de processos robustos e adoção de práticas que efetivamente protejam os dados pessoais e os direitos fundamentais dos titulares.

Neste contexto, o reconhecimento de mecanismos, instâncias e práticas de conformidade torna-se elemento central para o sucesso da Política Nacional de Proteção de Dados Pessoais e da Privacidade.

Tais elementos são essenciais não apenas para garantir o cumprimento legal, mas principalmente para criar um ambiente de confiança e responsabilidade no tratamento de dados pessoais, estimulando a adoção de boas práticas de conformidade e promovendo o desenvolvimento econômico e tecnológico e a inovação de forma ética e sustentável. A experiência internacional e as práticas já adotadas por organizações brasileiras demonstram que a conformidade efetiva requer uma combinação de diferentes elementos, conforme abaixo listados:

(i) Mecanismos de governança e prestação de contas;

(ii) Instâncias adequadas para supervisão e implementação de programas de privacidade;

(iii) Materiais informativos e Guias de Boas Práticas;

(iv) Práticas que traduzam os princípios legais em ações concretas e mensuráveis;

(v) Ferramentas e processos que permitam demonstrar a conformidade. A definição desses elementos na Política Nacional é fundamental por diversas razões:

(vi) Promover segurança jurídica ao estabelecer parâmetros claros para avaliação da conformidade;

(vii) Facilitar a adoção de boas práticas por organizações de diferentes portes e setores;

(viii) Incentivar a autorregulação e o desenvolvimento de padrões setoriais;

(ix) Permitir uma fiscalização mais eficiente e focada em resultados concretos; e

(x) Contribuir para a construção de uma cultura de proteção de dados pessoais no país.

Portanto, ao propor, na seção 2 deste Relatório, os subsídios para as diretrizes na elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade, o Grupo de Trabalho pautou-se pelos elementos acima, apresentando 8 (oito) temáticas a serem levadas em consideração na elaboração da PNDP, no que tange ao reconhecimento de mecanismos, instâncias e práticas de conformidade adequadas, especialmente no que tange ao seu reconhecimento positivo como boas práticas, as quais estão abaixo sintetizadas:

1. Incentivo à adoção e à orientação de mecanismos, instâncias e práticas de conformidade, especialmente por meio de mecanismos já previstos na LGPD e sinergia com outras normas já existentes. Além disso, a PNDP pode fomentar o equilíbrio entre as atividades de orientação e regulamentação pela ANPD, a fim de evitar a criação de ônus excessivos ou de obstáculos indevidos ao tratamento de dados pessoais.

2. Estímulo ao diálogo da ANPD com a sociedade em todas as suas esferas de atuação, promovendo a participação social por meio de consultas, audiências públicas e outros mecanismos. Estímulo, também, à atuação responsiva da ANPD, especialmente, no que tange à atividade fiscalizatória, promovendo sempre o diálogo entre a Autoridade e os titulares e agentes de tratamento.

3. Fomento à adoção de boas práticas de governança de dados pessoais de forma ampla, e não apenas como previsto no art. 50, da LGPD, bem como incentivo à criação selos e certificações de conformidade.

4. Incentivo à promoção de ações educacionais, pela ANPD e outros órgãos, voltadas não só aos titulares, como também aos agentes de tratamento.

5. Estímulo e incentivo a adoção de mecanismos amigáveis de resolução de disputas e litígios, seja por meio da mediação como meio de solução de controvérsias entre particulares e a autocomposição de conflitos no âmbito da administração pública.

6. Estímulo à promoção de diretrizes claras para incentivar a implementação de programas de compliance em organizações públicas e privadas, por meio do fomento à Cultura Organizacional de Privacidade, bem como de orientações específicas para Pequenas e Médias Empresas e estímulo à formação de Parcerias Público-Privadas para desenvolvimento de recursos que auxiliem na implementação eficaz de programas de *compliance* em proteção de dados pessoais.

7. Incentivo ao reconhecimento de Padrões de Auditoria, Implementação de Sistemas de Monitoramento Contínuo e programas de capacitação e certificação para profissionais responsáveis por auditorias internas, além do incentivo à realização de auditorias internas pelas próprias organizações. Essas práticas não obrigatórias podem ser reconhecidas como boas práticas pela PNPD.

8. Incentivo ao desenvolvimento e manutenção, pela ANPD, de planos formais de resposta à incidentes de segurança, bem como a definição de prazos claros e procedimentos padronizados para notificação de incidentes à Autoridade e aos titulares afetados, além do reconhecimento de boas práticas não obrigatórias das organizações, como a designação pelas de equipes ou indivíduos responsáveis pela gestão de incidentes de segurança e a realização de testes e simulações.

9. Direcionamento à priorização, pela ANPD, da viabilização dos mecanismos de transferência internacional de dados pessoais, conforme previsto na LGPD.

Dessa forma, nota-se que as diretrizes propostas pelo Grupo de Trabalho, que podem ser adotadas na Política Nacional de Proteção de Dados Pessoais e da Privacidade, estão voltadas, precipuamente, à uma atuação responsiva da ANPD, à ampla participação e engajamento social, à orientação sobre práticas de conformidade já previstas na LGPD e ao incentivo ao reconhecimento como boas práticas de outros mecanismos e práticas de conformidade, de forma equilibrada e positiva para os titulares e os agentes de tratamento.

A Política Nacional de Proteção de Dados Pessoais e da Privacidade desempenhará um papel essencial na construção de um ambiente regulatório sólido, equilibrado e eficaz para o tratamento de dados pessoais no Brasil. Ao estabelecer diretrizes e incentivar a adoção de boas práticas, a Política fortalecerá a segurança jurídica e impulsionará a conformidade com a LGPD, garantindo, também, um cenário de maior maturidade sobre o tema em organizações públicas e privadas e, por consequência, maior confiança da sociedade no uso responsável de informações pessoais.

O incentivo à implementação de mecanismos de compliance, a valorização do diálogo entre a ANPD e a sociedade, o incentivo à capacitação e a criação de incentivos regulatórios são pilares fundamentais para consolidar uma cultura nacional de proteção de dados pessoais que beneficie tanto os titulares quanto os agentes de tratamento. Além disso, a fim de concretizar seus objetivos, é essencial que, após sua elaboração, a Política seja continuamente aprimorada para acompanhar os avanços tecnológicos e as demandas sociais, assegurando, assim, que o Brasil se mantenha alinhado às melhores práticas globais.

Dessa forma, a Política Nacional não apenas fortalecerá a proteção dos dados pessoais, mas também impulsionará a competitividade global do país ao promover a privacidade como um valor central para o desenvolvimento econômico, tecnológico e inovação.

QUADRO SINÓPTICO

Princípios

Segurança; prevenção; responsabilização e prestação de contas.

Objetivo

Promover a conformidade com a LGPD e, ao mesmo tempo, incentivar o desenvolvimento econômico e tecnológico e a inovação.

Diretrizes

- Promover segurança jurídica por meio de parâmetros claros para avaliação da conformidade;
- Facilitar a adoção de boas práticas por organizações de diferentes portes e setores;
- Incentivar a autorregulação e o desenvolvimento de padrões setoriais;
- Permitir uma fiscalização mais eficiente, focada em resultados concreto; e
- Contribuir para a construção de uma cultura de proteção de dados pessoais no país.

Instrumentos

- Mecanismos de governança e prestação de contas;
- Instâncias adequadas para supervisão e implementação de programas de privacidade;
- Materiais informativos e Guias de Boas Práticas;
- Práticas que traduzam os princípios legais em ações concretas e mensuráveis; e
- Ferramentas e processos que permitam demonstrar a conformidade.

Outras recomendações

- Incentivar a adoção de mecanismos de conformidade já previstos na LGPD, garantindo um equilíbrio entre orientação e regulamentação pela ANPD;
- Estimular o diálogo da ANPD com a sociedade por meio de consultas públicas, audiências e mecanismos participativos;
- Fomentar boas práticas de governança, não apenas como previsto no art. 50 da LGPD, mas de forma ampla e facilitada, e incentivando certificações de conformidade;
- Promover ações educacionais para titulares de dados e agentes de tratamento;
- Incentivar a adoção de mecanismos amigáveis de resolução de disputas e litígios, como mediação e autocomposição de conflitos na administração pública;
- Estimular o reconhecimento da implementação de programas de compliance em organizações públicas e privadas, incluindo diretrizes específicas para Pequenas e Médias Empresas (PMEs) e incentivo a Parcerias Público-Privadas (PPPs);
- Incentivar que os padrões e metodologias nacionais e internacionais, assim como padrões e metodologias próprios adotados pelos agentes de tratamento para auditorias não obrigatórias em proteção de dados pessoais possam ser reconhecidos como boas práticas;
- Desenvolver e manter planos formais de resposta a incidentes de segurança, definindo prazos e procedimentos claros para a notificação; e
- Priorizar a viabilização de mecanismos de transferência internacional de dados pessoais conforme previsto na LGPD;

GTT 3 – Governança de dados no âmbito corporativo e privado

Membros

Myreilla Aloia Triumpho Pereira da Cruz (coordenadora), Cassio Augusto Muniz Borges, Claudio Eduardo L. de Abreu Rocha, Fernando Antonio Santiago Junior, João Frederico Chagas Maranhão, João Marcos Pereira Vidal e Marcos Vinícius Barros Ottoni.

Considerações

A Governança de Dados Pessoais é fundamental para organizações que almejam maior competitividade, rentabilidade e principalidade nos clientes e titulares, garantindo conformidade, segurança, eficiência e menor custo. Um ambiente de negócios confiável, o qual promove a inovação e o respeito à privacidade e segurança de dados pessoais, sem dúvida é respaldado por um programa de Governança de Dados Pessoais bem estruturado pautado em dados pessoais confiáveis, precisos e seguros.

Para atender as demandas de mercado e rigorosas regulações sobre privacidade e proteção de dados pessoais é essencial o compromisso contínuo com a governança. Dito isto, talvez seja pertinente a ANPD refletir sobre a necessidade de detalhar o tema Governança de Dados Pessoais em documento público específico.

Isto posto, como conclusão dos estudos realizados e considerando como temas prioritários, entendemos que a Política no que tange a Governança de Dados Pessoais, deve abordar essencialmente:

(i) Entendimento sobre o escopo e abrangência da Governança de Dados Pessoais;

(ii) Implantação de Política de Governança de Dados Pessoais e de Plano de Governança de Dados Pessoais nas empresas com foco na transversalidade, ou seja, no envolvimento de diversas áreas, como a Tecnologia da Informação, Jurídico, Compliance, Segurança da Informação, Riscos, CDO e todas as áreas que tratam dados pessoais;

(iii) Implantação de diretrizes e boas práticas para a Governança de Dados Pessoais abrangendo os temas constantes do item 4.7 do presente Relatório Final;

(iv) Implantação de métricas e indicadores para medir o desempenho e os resultados das ações de Governança de Dados Pessoais;

(v) A estrutura organizacional no que tange a atribuições, responsabilidades e processos;

(vi) O mapeamento e Gestão do Ciclo de Vida dos Dados Pessoais pelas empresas;

(vii) As organizações devem avaliar se os padrões e frameworks, alguns citados no item 4.6 do Relatório Final, podem auxiliar na implantação e monitoramento de uma Política de Governança de Dados Pessoais.

Conclui-se, portanto, que a definição e a implementação de práticas robustas de Governança de Dados Pessoais são essenciais para assegurar o tratamento adequado e a proteção dos dados pessoais, conforme exigido pela LGPD.

A Governança de Dados Pessoais deve ser vista como uma iniciativa transversal e estratégica, em que se espera que as organizações adotem abordagens proativas e sistemáticas para garantir a conformidade, a transparência e a confiança dos titulares de dados, promovendo um ambiente de respeito à privacidade.

Em síntese, a Governança de Dados Pessoais não é apenas um requisito regulatório, mas um diferencial competitivo estratégico no mercado atual. Sua implementação efetiva requer comprometimento das organizações em estabelecer políticas claras, processos bem definidos e práticas alinhadas às questões regulatórias e frameworks disponíveis.

Ao tratar os dados pessoais com segurança, precisão, transparência e responsabilidade, os agentes de tratamento, além de estarem em conformidade com a legislação, fortalecem a confiança dos titulares e promovem a inovação em um ambiente de negócios cada vez mais desafiador. Assim, a Governança de Dados Pessoais deve ser compreendida como um pilar essencial para a sustentabilidade, a competitividade e a proteção dos direitos fundamentais à privacidade no cenário em constante evolução.

QUADRO SINÓPTICO

Princípios

Governança de Dados Pessoais estruturada é indispensável para fomentar atividades econômicas e tecnológicas que estejam em sintonia com direitos e garantias fundamentais, visando assegurar, no país, um ambiente adequado ao desenvolvimento da sociedade e o fluxo informacional com foco na proteção de dados pessoais.

Objetivos

Estabelecer que a Governança de Dados Pessoais, nitidamente, é medida essencial e necessidade estratégica para maior competitividade e assertividade das organizações, além de proporcionar principalidade dos titulares de dados pessoais, conformidade regulatória e segurança em um ambiente cada vez mais digital.

Diretrizes

- Definição de Governança de Dados
- Benefícios na Governança de Dados:

Melhor Qualidade dos Dados Pessoais; Interoperabilidade; Maior eficiência; Redução de Custo; Segurança e Privacidade; e Redução de riscos regulatórios, financeiros e reputacionais.

- Estrutura de Governança de Dados

Estrutura Organizacional: Encarregado, Gestor de Dados Pessoais, Detentor de Dados Pessoais; Comitê de Governança de Dados Pessoais e Fóruns de Aprovação em diferentes alçadas de acordo com a criticidade do cenário em discussão; e Equipe de Segurança da Informação.

- Ciclo de Vida dos Dados

Fase de Coleta; Tratamento; Validação; Armazenamento; Modalidades de Acesso e Compartilhamento de Dados Pessoais; Reutilização e Análise Estatística; e Arquivamento Eletrônico.

- Diretrizes e Boas Práticas

Planejamento Estratégico; Definição de Propósito; Mapeamento do Ciclo de Vida dos Dados Pessoais; Políticas Claras e Acessíveis; Códigos de Conduta; Regras de Segurança e Backup; Monitoramento Contínuo e Avaliação; Capacitação Contínua; e Avaliação de padrões e *frameworks.*

Instrumentos e Recomendações

- Implantação de Política de Governança de Dados Pessoais;
- Implantação de Plano de Governança de Dados Pessoais nas empresas com foco na transversalidade envolvendo áreas como Tecnologia e Segurança da Informação, Jurídico, Compliance, Riscos, CDO e todas as áreas que tratam dados pessoais;
- Implantação de diretrizes e boas práticas para a Governança de Dados Pessoais;
- Implantação de métricas e indicadores para acompanhamento do desempenho e resultados das ações de Governança de Dados Pessoais;
- Implantação de estrutura organizacional no que tange a participantes, atribuições, responsabilidades e processos; e
- Implantação do mapeamento e Gestão do Ciclo de Vida dos Dados Pessoais.

GTT 4 - Governança de dados no setor público

Membros

Ana Paula Bialer (Coordenadora), Adriana Macedo Marques, Ana Estela Haddad, Bruno Ricardo Bioni, Renata Vicentini Mielli, Rony Vainzof e Samara Mariana de Castro.

Considerações

O trabalho desenvolvido pelo GTT-4 ao longo de todo período analisado revelou um cenário diversificado quanto à governança de dados no setor público. Embora existam avanços significativos em algumas áreas, as diferenças de maturidade entre os níveis federal, estadual e municipal demonstram a necessidade de estratégias mais inclusivas e adaptadas às realidades locais bastante distintas.

Com efeito, ainda que se perceba um movimento em direção à orientação centralizada sobre o assunto na esfera federal, verifica-se uma atuação fragmentada e sem articulação institucional dos entes federativos. Não obstante existam bons exemplos de ações isoladas, não há um regramento unificado que trata das competências, atribuições e regras mínimas de atuação, muito embora o Ministério da Gestão e Inovação tem uma produção volumosa de materiais relevantes.

As entrevistas realizadas foram fundamentais para compreender as particularidades de cada nível e identificar desafios estruturais, boas práticas e soluções inovadoras que vêm sendo implementadas. Embora houvesse intenção de entrevistar representantes de todos os níveis do Poder Executivo, as limitações de tempo e a busca por maior profundidade nas análises levaram à realização de entrevistas a partir da seleção de representantes estratégicos. Ainda assim, o GT-4 conseguiu capturar informações relevantes e detalhadas, podendo ser completadas futuramente com a inclusão de novos cenários e perspectivas.

A partir das análises e discussões, apresentam-se as recomendações para elaboração da Política Nacional de Proteção de Dados Pessoais e Privacidade, bem como recomendações para a atuação da ANPD no fortalecimento da governança de dados no setor público.

A partir da análise realizada e as necessidades específicas do setor público brasileiro, para fins da Política Nacional de Proteção de Dados Pessoais e da Privacidade, em matéria de governança de dados pessoais, listamos abaixo uma coletânea de objetivos, princípios e diretrizes que sugerimos sejam incorporadas na política, ainda que em parte aplicáveis tanto para setor público como setor privado.

(i) Objetivos

Para fins da Política Nacional de Proteção de Dados Pessoais e da Privacidade, em matéria de governança de dados, entende-se que devem ser considerados os seguintes objetivos:

Objetivo geral: assegurar o direito fundamental à proteção dos dados pessoais, inclusive nos meios digitais.

Objetivos específicos (relacionados à governança de dados): (i) contribuir para um governo orientado por dados que assegure a privacidade, proteção de dados pessoais e o compartilhamento adequado de dados pessoais; (ii) incentivar a educação em proteção de dados pessoais, fomentando o letramento digital e a inclusão digital, de modo a contribuir para a promoção da equidade e autodeterminação informativa; (iii) fomentar a cultura em proteção de dados pessoais, promovendo a sensibilização e conscientização para tratamento adequado destes dados pelo setor público; e (iv) fortalecer a participação e o controle social no tratamento de dados; e. promover a transparência e a prestação de contas no tratamento de dados pessoais por organizações públicas e privadas.

(ii) Princípios e diretrizes norteadores da política no que tange o poder público

1. Diretrizes para Governança de Dados Pessoais: Estabelecimento de diretrizes para que organizações tenham políticas internas de governança de dados pessoais, incluindo definição de atribuições de competências individuais dentro da organização, considerando referências como a Portaria SGD/MGI nº 852/2023;

2. Uso apropriado, ético e responsável dos dados, considerando preceitos como a não discriminação; a inclusão social e digital; a promoção da confiança pública e a integridade da informação.

3. Infraestrutura e arquitetura de dados: Garantia de infraestrutura e arquitetura de dados adequados ao volume e à natureza dos dados tratados;

4. Qualidade e Integridade dos Dados Pessoais: Recomenda-se a adoção de medidas contínuas para assegurar a qualidade e integridade dos dados pessoais tratados pelo Poder Público, prevenindo e evitando erros e redundâncias que possam comprometer a confiabilidade das informações.

5. Interoperabilidade dos dados pessoais: é recomendável a promoção da interoperabilidade dos dados pessoais tratados pelo Poder Público, criando condições para a padronização e o compartilhamento seguro e eficiente entre diferentes órgãos e entidades, em conformidade com normas de proteção de dados e segurança da informação.

6. Canais de Interface para Titulares: Sugere-se que os órgãos públicos estabeleçam canais acessíveis, claros e eficientes para que os titulares de dados possam exercer seus direitos, como acesso, retificação, exclusão e portabilidade de informações.

7. Capacitação e Sensibilização contínua: recomenda-se a adoção de programas contínuos de capacitação para servidores e gestores públicos, com foco em segurança da informação, proteção de dados pessoais e governança de dados.

8. Fomento a cooperação entre Entes Públicos: O fomento de iniciativas a atuação integrada entre órgãos e entidades do poder público, de diferentes níveis, federal, estadual e municipal, para troca de experiências em implementação de política e práticas de governança, conforme Lei nº 14.129, de 29 de março de 2021.

9. Medidas Técnicas e Administrativas: Para garantir uma proteção robusta dos dados pessoais tratados pelo setor público, recomenda-se a implementação de medidas técnicas e administrativas eficazes que considerem o volume e a natureza dos dados tratados.

10. Política de Governança de Dados: orientação quanto a adoção de política de governança de dados contendo, desde regras para a coleta ao descarte de dados, regras para manutenção e atualização constantes dos catálogos de dados e metadados, assim como critérios definidos para reuso de dados, buscando eficiência nos recursos públicos.

(iii) Recomendações de mandamentos e obrigações

1. Criação de um Fórum Intergovernamental: recomenda-se a criação de um fórum intergovernamental possivelmente coordenado pela ANPD, que possa funcionar como espaço para troca de experiências e materiais entre as instituições e fixação de boas práticas envolvendo os entes federais, estaduais e municipais. Uma possibilidade seria o secretariado pela Secretaria de Governo Digital (SGD), que já possui um vasto repertório de material relevante e poderia se aproveitar do Fórum como um *locus* de escoamento de inúmeros materiais de referência e de treinamento. O Fórum teria, em princípio, o objetivo de facilitar a troca de experiências e materiais entre as instituições, proporcionar capacitação contínua aos participantes.

2. Desenvolvimento de ferramentas de Autoavaliação e Monitoramento: Para que os órgãos públicos possam avaliar sua conformidade com as normas de proteção de dados e aprimorar suas políticas, recomenda-se a criação de ferramentas acessíveis de autoavaliação e monitoramento. Essas ferramentas devem permitir: (i) a verificação do cumprimento das diretrizes da LGPD e outras normativas aplicáveis; (ii) a identificação de riscos e áreas que necessitam de melhorias; e (iii) o acompanhamento contínuo da implementação das políticas de proteção de dados, buscando-se algum grau de harmonização nesta implantação. Sugere-se que essas

ferramentas sejam desenvolvidas em formato digital, com interface intuitiva e de fácil usabilidade, garantindo que todos os órgãos e entidades possam utilizá-las de forma eficiente.

3. Cooperação Estratégica: Para aprimorar a implementação de políticas de proteção de dados nos diferentes níveis da Administração Pública, recomenda-se o incentivo ao estabelecimento de coordenações estratégicas, como por exemplo entre as Controladorias Gerais dos Estados e Municípios. Essas colaborações podem contribuir para o desenvolvimento de guias e orientações conjuntas sobre a aplicação da LGPD, além de possibilitar um monitoramento mais eficiente do cumprimento das normas pelos órgãos estaduais e municipais.

(iv) Recomendações para a Autoridade Nacional de Proteção de Dados

Muito embora o objetivo inicial do Grupo de Trabalho tenha sido a elaboração de subsídios para a elaboração da Política Nacional de Privacidade e Proteção de Dados Pessoais, ao longo do processo de nossos estudos e especialmente das entrevistas realizadas para prover um diagnóstico, identificamos algumas recomendações que nos pareceram não seriam cabíveis em termos da Política propriamente dita mas que poderiam ser levadas a conhecimento da ANPD, para que a Autoridade as considere no âmbito de suas atividades.

Nesse sentido, abaixo elencamos algumas destas considerações e recomendações:

1. Capacitação contínua e cooperação interinstitucional: Sugere-se que a ANPD colabore com a Escola Nacional de Administração Pública (ENAP) e outras instituições como SGD/MGI e RNP/MCTI para oferecer cursos sobre proteção de dados pessoais. Além disso, seria importante organizar reuniões periódicas para discutir atualizações nas regulamentações e promover a troca de experiências e boas práticas.

2. Desenvolvimento de cartilhas orientativas: Recomenda-se que a ANPD crie um *toolkit* e cartilhas orientativas para apoiar a administração pública, fornecendo orientação sobre fluxos de segurança da informação e proteção de dados pessoais.

3. Fortalecimento e clareza da função do Encarregado de Dados Pessoais no setor público: Recomenda-se que a ANPD crie diretrizes claras para as funções e responsabilidades dos Encarregados de Dados Pessoais no setor público, endereçando sugestões de estruturas internas a serem adotadas. Além disso, sugere-se a criação de um canal institucional de suporte aos Encarregados, facilitando a troca de experiências e a resolução de dúvidas.

4. Ações Colaborativas: Sugere-se a promoção de colaborações com a sociedade civil, setor privado, terceiro setor e academia, criando um ambiente inclusivo e participativo para fortalecer a proteção de dados pessoais.

Dada a transversalidade do objeto regulado da LGPD, que é espelhado pela amplitude do escopo deste GTT - governança de dados, a governança de dados no setor público é um elemento central para a proteção de dados pessoais e a conformidade com a LGPD. O trabalho desenvolvido pelo GTT-4 permitiu mapear os principais desafios e oportunidades na estruturação de uma Política Nacional de Governança de Dados no Setor Público, enfatizando a importância de uma abordagem coordenada entre os entes federativos.

A implementação das recomendações apresentadas contribuirá para o fortalecimento da governança de dados, garantindo maior segurança jurídica, eficiência na gestão de informações e proteção dos direitos dos titulares. A articulação entre órgãos públicos, a capacitação contínua de servidores e o desenvolvimento de diretrizes claras são passos essenciais para consolidar um ecossistema de governança de dados eficaz e alinhado aos princípios da LGPD.

QUADRO SINÓPTICO

Princípios

Uso apropriado, ético e responsável dos dados, considerando preceitos como a não discriminação; a inclusão social e digital; a promoção da confiança pública e a integridade da informação.

Objetivos

Objetivo geral: assegurar o direito fundamental à proteção dos dados pessoais, inclusive nos meios digitais.

Objetivos específicos: (i) incentivar a educação em proteção de dados pessoais, fomentando o letramento digital e a inclusão digital, de modo a contribuir para a promoção da equidade e autodeterminação informativa; (ii) fomentar a cultura em proteção de dados pessoais, promovendo a sensibilização e conscientização para tratamento adequado; e (iii) fortalecer a participação e o controle social no tratamento de dados; e promover a transparência e a prestação de contas no tratamento de dados pessoais por organizações públicas e privadas.

Diretrizes

- Diretrizes para governança de dados pessoais;
- Uso apropriado, ético e responsável dos dados;
- Infraestrutura e arquitetura de dados;
- Qualidade e integridade dos dados pessoais;
- Interoperabilidade dos dados pessoais;
- Canais de interface para titulares;
- Capacitação e sensibilização contínua;
- Fomento a cooperação entre Entes Públicos; e
- Medidas técnicas e administrativas.

Instrumentos

- Cooperação estratégica e criação de um Fórum Intergovernamental;
- A verificação do cumprimento e desenvolvimento de ferramentas de autoavaliação e monitoramento;
- A identificação de riscos e áreas que necessitam de melhorias; e
- O acompanhamento contínuo da implementação das políticas de proteção de dados, buscando-se algum grau de harmonização nesta implantação.

Outras recomendações

- Capacitação contínua e cooperação interinstitucional;
- Desenvolvimento de cartilhas orientativas;
- Fortalecimento do Encarregado de Dados Pessoais; e
- Ações colaborativas.

GTT 5 - Dados pessoais para o desenvolvimento econômico, tecnológico a inovação

Membros

Rony Vainzof (coordenador), Alexandre Zago Boava, Myreilla Aloia Triumpho Pereira da Cruz, Vitor Morais de Andrade, Fábio Veras, Débora Sirotheau Siqueira Rodrigues e Cassio Augusto Muniz Borges.

Considerações

Diante de todo o trabalho exposto e consignado neste Relatório Final e respectivos anexos, o GTT-5 do CNPD fornece os seguintes subsídios, na temática de dados pessoais para o desenvolvimento econômico, tecnológico e a inovação, para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade:

1. O desenvolvimento econômico, tecnológico e a inovação é também pautado no tratamento e circulação dos dados pessoais, conforme demonstrado nos Estudos de Caso e constante nas mais variadas estratégias, planos e políticas de Estado. Porém, o tratamento de dados pessoais não pode ser feito sem observar a legislação, especialmente a LGPD, de forma a garantir os direitos dos titulares. Assim, é preciso ampliar a percepção da proteção de dados pessoais como condição e indutor para o desenvolvimento econômico, tecnológico e a inovação, nos termos do art. 2º, inc. V, da LGPD;

2. A Política Nacional de Proteção de Dados deve refletir o equilíbrio dos dois principais objetivos da LGPD: (i) proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural; e (ii) permitir geração de valor e ser base do desenvolvimento econômico a partir do tratamento e circulação dos dados pessoais, desde que sejam realizados de forma lícita;

3. A LGPD é instrumento para a inovação e não deve ser vista ou interpretada como entrave para o desenvolvimento econômico e tecnológico. Associado a isto os dados devem ser tratados de forma a beneficiar todos os titulares de dados;

4. Estimular a prática do *Privacy by Design* nos setores público e privado, pois, ao integrar a proteção de dados pessoais desde a concepção de produtos, serviços e processos, a abordagem equilibra inovação, desenvolvimento econômico e proteção de dados e privacidade, contribuindo com:

a) O fomento à confiança do indivíduo: os agentes de tratamento ganham credibilidade e aumentam a fidelização, o que impulsiona o consumo e fortalece a reputação no mercado e dos serviços públicos;

b) Redução de riscos e custos relacionados a multas, indenizações e incidentes;

c) Impulso à inovação e à eficiência: quando a privacidade é implementada desde o início, além de os agentes de tratamento terem visibilidade total acerca de novos produtos e serviços que envolvam dados pessoais, não será necessário fazer mudanças estruturais ou funcionais neles, posteriormente, para atender às regulamentações, como a LGPD. Essas alterações posteriores podem ser custosas, tanto financeiramente quanto em termos de tempo. O *PbD* também torna processos mais ágeis, transparentes e explicáveis e ao evitar a coleta excessiva de dados, os agentes de tratamento economizam custos de armazenamento, processamento e descarte. Por fim, estimula a criação de soluções tecnológicas avançadas, como anonimização, criptografia e design ético, que atendem às demandas do mercado e às exigências regulatórias; e

d) Competitividade global: empresas se alinham a padrões internacionais, ganhando vantagem competitiva em mercados globais.

5. Dentro da prática do *Privacy by Design*, estimular:

a) A incorporação a priori dos princípios e garantias da LGPD desde as etapas iniciais do desenvolvimento do produto digital, passando pelo seu desenho, implementação e testes;

b) Uma abordagem multinível para verificar a conformidade com os princípios da LGPD em diferentes estágios do desenvolvimento, de acordo com o nível de risco das atividades de tratamento;

c) Funcionalidades que permitam aos usuários exercerem seus direitos, criando interfaces e fluxos que promovam a transparência sobre o uso e tratamento de dados pessoais;

d) O desenvolvimento de glossário centralizado ou a ser distribuído nas aplicações que fortaleça a compreensão da política de privacidade e proteção de dados adaptado ao contexto de sistemas de software, e desenvolver checklists e quadros de apoio para cada princípio da LGPD;

e) Medidas técnicas e administrativas para garantir a segurança e prevenção de incidentes, adotando práticas de minimização de dados, coletando apenas o necessário para as finalidades específicas e legítimas; e

f) Tecnologias de Anonimização e Pseudonimização devem ser estimuladas, quando possível, reduzindo os riscos associados ao tratamento de dados pessoais, especialmente para o treinamento de IA.

6. Estimular práticas de proteção de dados por meio de incentivos regulatórios e econômicos, beneficiando tanto o setor público quanto o privado, como nos seguintes exemplos:

a) Linhas de crédito específicas, oferecidas por bancos públicos ou privados, para pequenas e médias empresas investirem em adequação à proteção de dados;

b) Subsídios ou descontos tributários vinculados à certificação em proteção de dados;

c) Acesso a linhas de crédito ou subsídios para projetos de inovação relacionados à proteção de dados;

d) Prioridade em licitações e contratos públicos; e

e) Divulgar ranking público destacando empresas e organizações com as melhores práticas de governança em proteção de dados.

7. Estabelecer diretrizes para que empresas entendam a privacidade como diferencial competitivo, estimulando soluções tecnológicas éticas e centradas no usuário;

8. Implementar o conceito de *Fair Design Patterns*, que promove a experiência mais ética e respeitosa, priorizando a autonomia do usuário, a transparência na coleta e no uso de dados, e a facilidade de acesso a configurações de privacidade. É a antítese dos padrões obscuros de design;

9. Incentivar o uso de técnicas de *Legal Design* e *Visual Law* para estimular o desenvolvimento de políticas de privacidade claras, acessíveis e compreensíveis aos titulares dos dados. A linguagem deve ser simples, objetiva e livre de jargões técnicos ou termos jurídicos complexos, assegurando uma comunicação eficaz. Além disso, o design da informação deve priorizar a organização visual e hierarquia clara, utilizando recursos gráficos e estruturais que facilitem a navegação, a assimilação e a interação, promovendo uma experiência inclusiva e transparente;

10. Ressaltar a importância de o controlador fornecer, sempre que solicitado, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial, bem como acerca do direito que os titulares têm de solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade;

11. Promover a transparência e explicabilidade sobre o uso de dados pessoais em sistemas de IA fornecendo informações claras aos titulares sobre como seus dados são utilizados;

12. Promover padrões para governança e interoperabilidade de dados, permitindo o uso compartilhado em setores estratégicos sem comprometer a segurança e a privacidade;

13. Promover espaços de dados pessoais como ecossistemas integrados, regidos por políticas claras, para fomentar a economia de dados. A Administração

Pública deve ampliar a política de dados abertos em conjunto com a inciativa privada para dados que são produzidos em espaços públicos, compartilhando proativamente informações relevantes, acessíveis e reutilizáveis com todas as partes interessadas. Isso facilita inovações e colaborações entre governo, setor privado e sociedade, além de permitir transações complexas com regras claras sobre o uso de dados.

Recomenda-se a criação de um Comitê Multissetorial, envolvendo governo, sociedade civil, academia, setor produtivo e representação de trabalhadores, para orientar políticas públicas de dados abertos. Os dados pessoais compartilhados nos espaços de dados devem ser tratados em consonância com a LGPD;

14. A ANPD deve estar ao lado dos demais Órgãos Setoriais, Legislativo, Executivo e Judiciário, por meio de cooperação interinstitucional, para que políticas de Estado já nasçam, desde a sua concepção, seguindo o princípio do *Privacy by Design*;

15. A ANPD, de acordo com as suas competências, deve desempenhar o papel na conexão e equilíbrio entre Direito e inovação, pois não se antagonizam. Pelo contrário, devem caminhar juntos;

16. Estimular o fortalecimento e maior autonomia institucional da ANPD, como forma de proteção a direitos e gerar maior segurança jurídica;

17. Fortalecer a cooperação com o setor privado e a sociedade civil, por meio de instrumentos como os Acordos de Cooperação Técnica e o fórum de comunicação permanente previsto na LGPD;

18. Reconhecer a importância da Análise de Impacto Regulatório como ferramenta para avaliar as intervenções regulatórias e minimizar os impactos negativos sobre os agentes econômicos e a sociedade;

19. Aprimoramento do processo de monitoramento regulatório (Avaliação de Resultado Regulatório e Monitoramento do Ambiente Regulado);

20. Apoiar iniciativas acadêmicas, empresariais e populares em Pesquisa & Desenvolvimento relacionadas à proteção de dados e privacidade, fortalecendo a base tecnológica do país;

21. Criar zonas regulatórias experimentais (*sandboxes* regulatórios) para empresas de qualquer natureza testarem soluções tecnológicas, de forma controlada e monitorada pela ANPD;

22. Decisões de adequação e o reconhecimento de cláusulas-contratuais equivalentes orientadas pela ANPD são fundamentais para tornar mais seguro ao titular de dados o fluxo internacional de seus dados pessoais;

23. Os princípios da finalidade, adequação e necessidade, previstos na LGPD, devem ser interpretados de maneira que permitam usos futuros compatíveis com o propósito original, garantindo segurança jurídica e inovação, especialmente no uso de dados para treinamento da Inteligência Artificial;

24. Não há hierarquia entre as bases legais autorizativas para o tratamento de dados pessoais previstas na LGPD. Em termos do desenvolvimento econômico, tecnológico e a inovação, uma das principais discussões envolve a utilização adequada e lícita, principalmente, das bases legais do consentimento e do legítimo interesse. O fenômeno da fadiga do consentimento precisa ser endereçado com transparência ativa ("consentimento informado"), avaliação dos mais variados níveis de hipossuficiência ("livre") e novas formas, como o *legal design* e *visual law*, para a manifestação do titular ("inequívoco"), como previsto na própria LGPD.

Já o interesse legítimo permite que as organizações tratem dados quando têm um interesse genuíno e válido, desde que este não prejudique os direitos e liberdades dos indivíduos. Esta base legal deve ser acompanhada por fortes obrigações de responsabilização e avaliação de risco, garantindo a proteção dos indivíduos. Ainda, ela é contextual e requer uma avaliação caso a caso, além de o indivíduo ter o direito de se opor ao tratamento de seus dados sob o interesse legítimo, em caso de descumprimento da legislação;

25. As ponderações acerca da base legal adequada devem ser ainda mais criteriosas em se tratando do tratamento de dados de crianças e adolescentes, especialmente para atender o consentimento qualificado, conforme artigo 14 da LGPD e nos termos da Res. 245/24, do CONANDA;

26. Prevenção ao cibercrime e a fraudes envolvendo dados pessoais:

a) Fomentar frentes que objetivem a redução de ilícitos relacionados a dados pessoais, em conexão e cooperação com políticas de segurança pública;

b) Promover campanhas educativas para a população, destacando os riscos de fraudes cibernéticas e como proteger seus dados pessoais em transações online;

c) Criar canais acessíveis para que cidadãos possam reportar fraudes e obter orientação sobre como proteger seus dados em caso de incidentes, permitindo a coleta e análise de dados de incidentes e auxiliando na identificação de padrões e ameaças;

d) Estabelecer parcerias entre instituições públicas e privadas para a troca de informações e o desenvolvimento de estratégias conjuntas de prevenção a fraudes, sempre observando os limites legais de compartilhamento de dados;

e) Implementação de ferramentas para monitorar e identificar atividades suspeitas em tempo real;

f) Implementação de soluções e sistemas para garantir maior segurança nos processos de autenticação e identificação de identidade;

g) Implementação de protocolos que propiciem rastreamento e recuperação rápida de perdas;

h) Medidas de cibersegurança integrada entre todas as áreas envolvidas no processo;

i) Incentivo à inovação e pesquisa fomentando o desenvolvimento de soluções para prevenção à fraude baseadas em inteligência artificial e biometria comportamental, aumentando a segurança no tratamento de dados, protegendo os titulares e contribuindo para o desenvolvimento de um ambiente digital confiável e competitivo, com total conformidade à LGPD; e

j) Realização de testes e simulações de incidentes.

27. Promover a implementação de políticas robustas para o fortalecimento e expansão de data centers em território nacional, priorizando investimentos em infraestrutura de alta eficiência energética, segurança de dados e integração com redes globais. Essas políticas devem fomentar iniciativas públicas de investimento e parcerias público-privadas nos termos do que fortalece a soberania digital e o interesse popular;

28. Promoção do letramento e da conscientização: garantir disseminação de conhecimento na sociedade acerca do uso de dados pessoais, seus benefícios, riscos e aspectos legais;

29. Investimento em educação e capacitação, conscientizando agentes de tratamento e titulares sobre a importância do tratamento adequado de dados pessoais, com transparência e respeito aos direitos dos titulares e demais regramentos estabelecidos pela LGPD, incentivando as práticas legitimas de tratamento de dados pessoais;

30. Desenvolver iniciativas que eduquem os titulares de dados sobre o valor de suas informações pessoais, seus direitos previstos na legislação e as formas de exercê-los;

31. Incentivar a criação de centros de excelência em IA de interesse público e desenvolver programas de capacitação em IA e proteção de dados para profissionais, empreendedores e população em geral são passos importantes para fomentar um ecossistema de inovação que priorize a privacidade e os direitos dos titulares de dados.

32. Promoção do letramento e da conscientização: garantir a disseminação de conhecimento sobre proteção de dados junto a crianças e adolescentes por meio

de atuação combinada com outros órgãos da administração como o Ministério da Educação e Ministério dos Direitos Humanos e Cidadania e por meio de parcerias com Estados e Municípios;

33. Proteção de dados na educação: a proteção de dados e a privacidade e os direitos de crianças e adolescentes devem ser priorizados como base em iniciativas tecnológicas no âmbito educacional, devendo as plataformas de *Edtech* garantir conformidade com padrões de privacidade e segurança em relação aos dados estudantis;

34. Incorporar a avaliação de impacto sobre as crianças e adolescentes aos governos em todos os níveis e o mais cedo possível no desenvolvimento de leis e políticas, e também serem realizadas pelas companhias no sentido de garantir a sua sustentabilidade empresarial em relação aos direitos de crianças e adolescentes;

35. A construção de uma política nacional integrada, alinhada às melhores práticas globais, é essencial para proteger os direitos dos trabalhadores e fomentar relações laborais mais justas e equilibradas;

36. Promover programas de capacitação para empregadores, gestores e trabalhadores sobre o tratamento responsável de dados pessoais no ambiente laboral;

37. Desenvolver materiais de conscientização voltados aos trabalhadores, destacando seus direitos como titulares de dados e os limites legais do uso de suas informações;

38. Incentivar as negociações coletivas para estabelecimento de normas mais específicas para o tratamento de dados pessoais de trabalhadores no contexto laboral, como forma de equilibrar a relação entre empregadores e empregados, estabelecendo salvaguardas claras para proteção dos direitos e liberdades dos trabalhadores, gerando maior segurança jurídica.

QUADRO SINÓPTICO

Princípios

O desenvolvimento econômico, tecnológico e a inovação; a proteção dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural; proteção de crianças e adolescentes; e fomento relações laborais mais justas e equilibradas.

Objetivos

- Ressaltar a importância de o controlador fornecer, sempre que solicitado, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada;
- Promover a transparência e explicabilidade sobre o uso de dados pessoais em sistemas de IA; padrões para governança e interoperabilidade de dados; e espaços de dados pessoais como ecossistemas integrados;
- Estimular cooperação interinstitucional, com o setor privado e a sociedade civil e fortalecimento institucional da ANPD.

Diretrizes

- Estimular a prática do *Privacy by Design* nos setores público e privado;
- Implementar o conceito de *Fair Design Patterns*, que promove a experiência mais ética e respeitosa;
- Os princípios da finalidade, adequação e necessidade, previstos na LGPD, devem ser interpretados de maneira que permitam usos futuros compatíveis com o propósito, especialmente na Inteligência Artificial; e
- Prevenção ao cibercrime e a fraudes envolvendo dados pessoais.

Instrumentos

- Estimular práticas de proteção de dados por meio de incentivos regulatórios e econômicos;
- Reconhecer a importância da Análise de Impacto Regulatório, da Avaliação de Resultado Regulatório e do Monitoramento do Ambiente Regulado;
- Apoiar iniciativas de Pesquisa & Desenvolvimento;
- Criar zonas regulatórias experimentais (*sandboxes* regulatórios);
- Decisões de adequação e o reconhecimento de cláusulas-contratuais equivalentes orientadas pela ANPD são fundamentais para tornar mais seguro ao titular de dados o fluxo internacional de seus dados pessoais;
- Promoção do letramento e da capacitação de proteção de dados, inclusive na educação;
- Investimento em educação e capacitação;
- Incentivar a criação de centros de excelência em IA de interesse público e desenvolver programas de capacitação;
- Incorporar a avaliação de impacto sobre as crianças e adolescentes aos governos em todos os níveis e o mais cedo possível no desenvolvimento de leis e políticas;
- Incentivar as negociações coletivas para estabelecimento de normas mais específicas para o tratamento de dados pessoais de trabalhadores no contexto laboral.

GTT 6 - LAI & LGPD: dados abertos como infraestrutura crítica em conformidade com LGPD

Membros

Bruno Bioni (coordenador) Isabela Henriques, Ana Paula Bialer, Têmis Limberger, Annette Pereira, Raquel Saraiva, e Gabrielle Sarlet.[1]

Considerações

O GTT-6 do Conselho Nacional de Proteção de Dados buscou consolidar relatos, normas, entendimentos jurisprudenciais e doutrinários sobre a interseção da proteção de dados pessoais e transparência pública. Nossa contribuição é para trazer subsídios à Política Nacional de Proteção de Dados para garantir que esses direitos fundamentais não sejam considerados conflitantes, mas sim complementares.

Para isso, apresentamos abaixo uma série de recomendações para serem levadas a plenário, de modo a contribuir para a promoção da cultura de proteção de dados no Brasil.

• Em seus fundamentos, conter menção à garantia do acesso à informação e ao exercício da cidadania, de forma a evidenciar sua relevância e reforçar a lógica de harmonização entre transparência e proteção de dados pessoais. A Política deve se somar e reforçar ao arcabouço normativo já existente que leve em consideração acordos e compromissos internacionais referentes à garantia da transparência pública;

• Estabelecer um sistema de cooperação entre ANPD e outros órgãos, não se restringindo a interações apenas na esfera federativa, sendo importante o contato com entidades no âmbito estadual e municipal. Atendo-se à temática da transparência, é imprescindível que haja trocas entre as instituições para suas decisões, publicações, enunciados, entre outros documentos, permaneçam harmônicas e complementares. O engajamento conjunto das entidades é essencial para barrar excessos nos processos de solicitação de informações, por exemplo, a exigência de uma motivação do solicitante a fim de cumprir com o princípio da finalidade;

[1] As recomendações apresentadas foram resultado de um processo participativo que contou com reuniões online com apresentação de especialistas sobre o tema, contribuições escritas e orais encaminhadas em chamada aberta instaurada pelo GTT6 e um evento online para debate sobre o tema da interseção entre transparência e proteção de dados. Participaram destes diversos tipos de contribuição as organizações: AB2L, Alana, ANPD, CGU, Descodifica, DPE/SP, Fiquem Sabendo, ICO, Observatório do Código Florestal, Open Knowledge Brasil, SEDIGI/MJSP, Transparência Brasil e Information Commissioner Office do Reino Unido (ICO-UK).

• Exigir e estimular a implementação de programas de capacitação de servidores públicos com relação às normas de proteção de dados pessoais, reforçando os posicionamentos estabelecidos pela CGU, bem como demais entendimentos estabelecidos em conjunto com a ANPD, tratando-se de transparência envolvendo dados pessoais.

• Estabelecer procedimentos para a participação pública antes de decisões que impliquem restrição da transparência com relação à bases de dados públicas que contenham dados pessoais. Além de reforçar que para decisões que signifique o fechamento de bases de dados não é aceitável argumentos genéricos, assim como o ônus argumentativo recai sobre a parte que defende a restrição do acesso;

• Fortalecer o princípio da transparência já previsto na LGPD fim de garantir clareza sobre as medidas tomadas na implementação da lei, bem como fornecer espaço para participação popular no processo;

• Reforçar a exceção prevista no art. 31, §3º, da LAI, em especial os incisos IV e V, de modo que a divulgação de dados pessoais é eximida de consentimento quando para a defesa de direitos e para a proteção do interesse público. A exemplo, tem-se a necessidade de acesso a dados pessoais de funcionários públicos, como seus salários, ou ainda de indivíduos que prestam serviços públicos;

• Apontar metodologias e ferramentas que possibilitem fazer melhores análises do caso concreto, como relatório de impacto, teste de interesse público da informação ao lado do teste tripartite do legítimo interesse - enquanto uma das bases legais possível para a abertura de dados, entre outros. Estas ferramentas são essenciais para avaliar a pensar e adaptar o tratamento pretendido a fim de não prejudicar a transparência devido à presença de dados pessoais, bem como implementar medidas de mitigação de risco que legitimem a abertura de dados. Neste sentido, os documentos precisam considerar também o impacto de uma determinada medida sobre a transparência pública;

• Exigir a transparência ativa na condução das atividades tanto da ANPD, quanto do CNPD, desde reuniões aos processos administrativos de fiscalização, sempre em conformidade com as regras aplicáveis aos processos administrativos;

• A realização de audiências públicas e o esgotamento de outros mecanismos de transparência e participação social para a elaboração das diretrizes da política nacional de privacidade e proteção de dados;

QUADRO SINÓPTICO

Princípios

Acesso a informações de órgãos públicos; princípios que regem a administração pública, especialmente o da publicidade; regras de publicidade em relação à gestão da documentação governamental e as providências para franquear sua consulta a quantos dela necessitem.

Objetivos

- Desenvolver diretrizes sobre o tema LAI & LGPD;
- Consolidar relatos, normas, entendimentos jurisprudenciais e doutrinários sobre a interseção da proteção de dados pessoais e transparência pública.

Diretrizes

- A garantia do acesso à informação e ao exercício da cidadania, de forma a evidenciar sua relevância e reforçar a lógica de harmonização entre transparência e proteção de dados pessoais;
- Estabelecer um sistema de cooperação entre ANPD e outros órgãos, não se restringindo a interações apenas na esfera federativa;
- Estabelecer procedimentos para a participação pública antes de decisões que impliquem restrição da transparência;
- Fortalecer o princípio da transparência, já previsto na LGPD, a fim de garantir clareza sobre as medidas tomadas na implementação da lei;
- Reforçar a exceção prevista no art. 31§3º, da LAI, em especial os incisos IV e V, de modo que a divulgação de dados pessoais é eximida de consentimento quando para a defesa de direitos e para a proteção do interesse público; e
- Exigir a transparência ativa na condução das atividades da ANPD.

Instrumentos

- Alinhamento da Política ao arcabouço normativo existente e compromissos internacionais;
- Cooperação entre a ANPD e outros órgãos para harmonizar decisões, publicações e enunciados;
- Proibição de argumentos genéricos para restrição de bases de dados públicas, impondo o ônus argumentativo à parte que defende a restrição;
- Reforço à exceção ao consentimento para a divulgação de dados pessoais prevista no art. 31, §3º, da LAI.
- Implementação de programas de capacitação para servidores públicos sobre normas de proteção de dados.
- Elaboração de guias orientativos para aplicação eficaz da LGPD e da LAI.
- Reforço dos posicionamentos da CGU e ANPD sobre transparência e proteção de dados.
- Uso de ferramentas como relatório de impacto e teste de interesse público para avaliar a abertura de dados.
- Implementação de medidas de mitigação de risco para evitar abusos ou violações de direitos.
- Publicidade e justificativa obrigatória para pedidos de sigilo em processos administrativos.
- Acesso a informações públicas sem necessidade de fornecer dados pessoais.

ANEXO

GTT 1 - Educação e capacitação em proteção de dados pessoais

relatorio-final-gt1-do-cnpd.pdf

GTT 2 - Mecanismos, instâncias e práticas de conformidade de proteção de dados

relatorio-final-gt2-do-cnpd.pdf

GTT 3 - Governança de dados no âmbito corporativo e privado

relatorio-final-gt3-do-cnpd.pdf

GTT 4 - Governança de dados no setor público

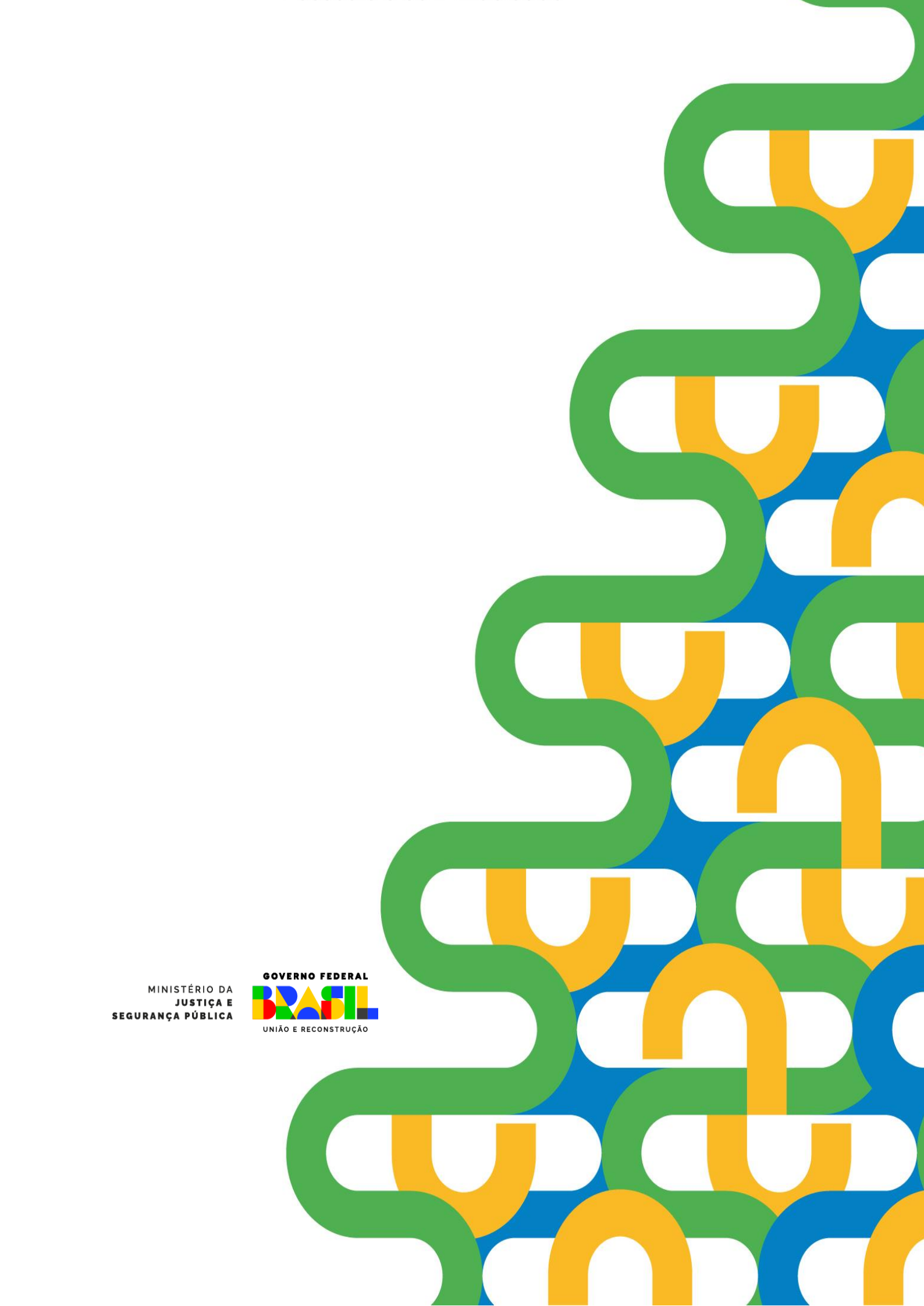
relatorio-final-gt4-do-cnpd.pdf

GTT 5 - Dados pessoais para o desenvolvimento econômico, tecnológico a inovação

relatorio-final-gt5-do-cnpd.pdf

GTT 6 - LAI & LGPD: dados abertos como infraestrutura crítica em conformidade com LGPD

relatorio-final-gt6-do-cnpd.pdf



MINISTÉRIO DA
JUSTIÇA E
SEGURANÇA PÚBLICA

GOVERNO FEDERAL
BRASIL
UNIÃO E RECONSTRUÇÃO