Rede Amazonense de Proteção de Dados
Tribunal de Justiça do Estado do Amazonas

PROTEÇÃO DE DADOS NO SETOR PÚBLICO

Experiências de Cooperação Interinstitucional no Amazonas

COORDENAÇÃO
VÂNIA MARQUES MARINHO

Íkono.
PUBLICAÇÕES

Coordenação

VÂNIA MARQUES MARINHO

Rede Amazonense de Proteção de Dados

Tribunal de Justiça do Estado do Amazonas

PROTEÇÃO DE DADOS NO SETOR PÚBLICO

Experiências de Cooperação Interinstitucional no Amazonas

Autores

Elisângela Nogueira Rodrigues
Cley Barbosa Martins
Felipe Augusto Fonseca Vianna
Rudson Fernandes Nunes
Carolina de Souza Lacerda Aires França
Diego Enrique Linares Troncoso
Nycolle Oliveira Souza Santos
Eduardo Nicolas Bitencourt Neves
Luan Silva Seminario
Joabe Cota Riker
Lucilene Florêncio Viana
Gleuson Silva Chaves
Emerson Silva de Souza
Sérgio Augusto Costa da Silva
Igor de Carvalho Leal Campagnolli
Aldo Evangelista
José Victor Oliveira de Oliveira
Arquelau Carvalho do Nascimento Neto
Marcos Laylson Nunes da Silva
Lorena de Oliveira Pereira
Gerbeson Vieira de Souza

Manaus/2025

Primeira coletânea sobre LGPD no setor público com perspectiva amazônica.

Ícono Publicações
Alameda Albânia, 50 – Ponta Negra
CEP: 69.037-063 - Manaus-AM
Telefone: (92) 98174-7379
E-mail: contato@ikono.pro.br

Dados Internacionais de Catalogação na Publicação (CIP)
(eDOC BRASIL, Belo Horizonte/MG)

P967p

Proteção de Dados [livro eletrônico] : experiências de cooperação interinstitucional no Amazonas / organização de Vânia Marques Marinho. – 1. ed. – Manaus, AM: Ícono Publicações, 2025.

Formato: PDF
Requisitos de sistema: Adobe Acrobat Reader
Modo de acesso: World Wide Web
Inclui bibliografia.
ISBN 978-65-5278-357-8
DOI 10.70271/250818.1424

1. Proteção de dados – Aspectos jurídicos. 2. Direito à privacidade – Brasil. 3. Administração pública – Amazonas. I. Marinho, Vânia Marques, 1959-.

CDD 342.085

Elaborado por Maurício Amormino Júnior – CRB6/2422

Rede Amazonense de Proteção de Dados
Tribunal de Justiça do Estado do Amazonas

www.ikono.pro.br | contato@ikono.pro.br

Editor-Chefe: **Franklin Carioca Cruz**
Revisão: **Meiryjane Moura e Fabíola Borges**
Capa e Projeto Gráfico: **Marcelo Maciel dos Reis**

Tribunal de Justiça do Estado do Amazonas

Gestão 2025

Presidência

Desembargador JOMAR RICARDO SAUNDERS FERNANDES

Vice-Presidência

Desembargador AIRTON LUÍS CORRÊA GENTIL

Corregedoria-Geral de Justiça

Desembargador JOSÉ HAMILTON SARAIVA DOS SANTOS

Ouvidoria-Geral de Justiça

Desembargador JORGE MANOEL LOPES LINS

Desembargadores

Desembargador JOÃO DE JESUS ABDALA SIMÕES
Desembargadora MARIA DAS GRAÇAS PESSÔA FIGUEIREDO
Desembargadora SOCORRO GUEDES MOURA
Desembargador DOMINGOS JORGE CHALUB PEREIRA
Desembargador YEDO SIMÕES DE OLIVEIRA
Desembargador FLÁVIO HUMBERTO PASCARELLI LOPES
Desembargador PAULO CESAR CAMINHA E LIMA
Desembargador CLÁUDIO CÉSAR RAMALHEIRA ROESSING
Desembargadora CARLA MARIA SANTOS DOS REIS
Desembargador JORGE MANOEL LOPES LINS
Desembargador LAFAYETTE CARNEIRO VIEIRA JÚNIOR
Desembargadora NÉLIA CAMINHA JORGE
Desembargador JOMAR RICARDO SAUNDERS FERNANDES
Desembargador AIRTON LUÍS CORRÊA GENTIL
Desembargador JOSÉ HAMILTON SARAIVA DOS SANTOS
Desembargador ERNESTO ANSELMO QUEIROZ CHÍXARO
Desembargador DÉLCIO LUÍS SANTOS
Desembargadora VÂNIA MARQUES MARINHO
Desembargador ABRAHAM PEIXOTO CAMPOS FILHO
Desembargadora ONILZA ABREU GERTH
Desembargador CEZAR LUIZ BANDIERA
Desembargadora MIRZA TELMA DE OLIVEIRA CUNHA
Desembargadora LUIZA CRISTINA NASCIMENTO DA COSTA MARQUES
Desembargador HENRIQUE VEIGA LIMA
Desembargadora IDA MARIA COSTA DE ANDRADE
Desembargadora LIA MARIA GUEDES DE FREITAS

COORDENAÇÃO GERAL

Desembargadora Vânia Marques Marinho

Presidente do Comitê Gestor de Proteção de Dados do Tribunal de Justiça do Estado do Amazonas

Paulo Motta De Morais – Secretário do Comitê Gestor de Proteção de Dados do TJAM

Fabíola Nazaré Borges – Assessora do Comitê Gestor de Proteção de Dados do TJAM

REDE AMAZONENSE DE PROTEÇÃO DE DADOS

Presidente:

Igor Campagnoli – Magistrado e Encarregado de Dados do TJAM

Vice-Presidente:

Aldo Evangelista – Advogado e Encarregado de Dados da OAB-AM

Secretário-Executivo:

Josenildo Pereira Soares – Membro do Comitê e Encarregado de Dados do TRE-AM

DEMAIS ÓRGÃOS PARTICIPANTES

Ministério Público do Estado do Amazonas

Cley Barbosa Martins – Encarregada de Dados

Defensoria Pública do Estado do Amazonas

Rudson Fernandes Nunes – Encarregado de Dados

Controladoria-Geral do Estado do Amazonas

Elisângela Nogueira Rodrigues – Encarregada de Dados

Procuradoria-Geral do Estado do Amazonas

Luan Silva Seminario – Encarregado de Dados

Prefeitura Municipal de Manaus

Lucilene Florêncio Viana – Encarregada de Dados

Tribunal Regional do Trabalho da 11ª Região

Carolina de Souza Lacerda Aires França – Encarregada de Dados

Tribunal de Contas do Estado do Amazonas

Saulo Coelho Lima

Universidade Federal do Amazonas

Nycolle Oliveira Souza Santos

Universidade do Estado do Amazonas

Marcus Orleans Arnaud Araújo

Processamento de Dados Amazonas S.A.

Emerson Silva de Souza

Secretaria de Estado de Segurança Pública

Sérgio Augusto Costa da Silva

Polícia Civil do Estado do Amazonas

Caio César da Rocha Medeiros Nunes

Ordem dos Advogados do Brasil - Seccional Amazonas

Aldo Evangelista

Desembargadora *Vânia Marques Marinho*

Presidente do Comitê Gestor de Proteção de Dados
Tribunal de Justiça do Estado do Amazonas

Trajetória Profissional

Doutora em Direito e Justiça pela Universidade Federal de Minas Gerais-UFMG(2023)eMestraemDireitoAmbientalpelaUniversidade do Estado do Amazonas (2004). Possui graduação em Direito (1995) e Geologia (1981) pela Universidade Federal do Amazonas. Ingressou no Ministério Público em 1998, trabalhou nas Comarcas de Tefé e Silves, também na 44.ª Promotoria de Justiça perante a 1.ª Vara da Fazenda Pública Municipal; na 18.ª Promotoria de Justiça de Defesa do Meio Ambiente e na 52.ª Promotoria de Urbanismo. Atuou como promotora da 28.ª Promotoria de Justiça da Infância e Juventude, perante a Vara Especializada da Infância e Juventude da Comarca de Manaus. Desde 2006 atua como professora estatutária da Universidade do Estado do Amazonas, titular dos módulos de Legislação Ambiental e disciplinas relacionadas a Crimes Ambientais. Atualmente é Desembargadora do Tribunal de Justiça do Estado do Amazonas (2021) e exerce também as funções de: (i) Coordenadora Psicossocial Judiciária; (ii) Presidente da Comissão de Gestão de Tecnologia da Informação e Comunicação; e (iii) Presidente do Comitê Gestor de Proteção de Dados do Poder Judiciário do Amazonas.

Liderança em Proteção de Dados

A **Desembargadora Vânia Marinho** é reconhecida como pioneira na implementação de políticas de proteção de dados no Judiciário amazonense. Sua visão estratégica sobre a necessidade de cooperação interinstitucional para enfrentar os desafios da LGPD no contexto amazônico levou à criação da primeira rede estadual de proteção de dados no Brasil, demonstrando que a liderança judicial pode ser catalisadora de transformações significativas no setor público.

Idealizadora da Rede Amazonense

Como idealizadora e coordenadora da Rede Amazonense de Proteção de Dados, conduziu o processo de articulação política e técnica que resultou na formalização do Acordo de Cooperação Técnica nº 53/2024 - TJAM, reunindo quinze instituições do estado em uma iniciativa inovadora. Sua liderança foi fundamental para transformar uma ideia inicial em realidade operacional, estabelecendo um modelo de cooperação que pode ser replicado em outras regiões do país.

Principais Conquistas na Rede

- Criação da primeira rede estadual de cooperação em proteção de dados no Brasil;
- Articulação de 15 instituições públicas em torno de objetivos comuns;
- Estabelecimento de metodologia de reuniões mensais e governança colaborativa;
- Coordenação desta primeira coletânea sobre LGPD com perspectiva amazônica;
- Desenvolvimento de modelo replicável para outros estados brasileiros.

> *"A proteção de dados pessoais não é apenas obrigação legal, mas expressão concreta do respeito à dignidade humana e à cidadania plena. Quando implementada através de cooperação interinstitucional, torna-se um verdadeiro serviço público que beneficia toda a sociedade."*
>
> ***Desembargadora Vânia Marques Marinho***

Visão para o Futuro

Sob sua coordenação, a Rede Amazonense tem como objetivos futuros a expansão para outras instituições, a criação de um centro de referência em proteção de dados para a região Norte, e o compartilhamento da experiência para replicação em outros estados. Sua visão é de que a cooperação institucional pode transformar desafios regionais em oportunidades nacionais de inovação em políticas públicas.

Contato Institucional
Comitê Gestor de Proteção de Dados
Tribunal de Justiça do Estado do Amazonas
E-mail: encarregado@tjam.jus.br | Site: https://www.tjam.jus.br

Ao Tribunal de Justiça do Estado do Amazonas,
instituição que acolheu e apoiou
esta iniciativa pioneira.

À Desembargadora Nélia Caminha Jorge,
que apoiou a criação da Rede,
e ao Desembargador Jomar Ricardo Saunders Fernandes,
que compreendeu sua importância
e deu continuidade ao projeto,
garantindo que esta cooperação interinstitucional
se consolidasse no Amazonas.

Aos servidores públicos do Amazonas
que trabalham incansavelmente
na proteção dos dados pessoais
dos cidadãos amazônidas.

Aos povos indígenas e comunidades tradicionais
da Amazônia, cuja proteção digital
é também proteção cultural
e preservação de identidades.

A todos que acreditam
que a cooperação institucional
é o caminho para um Estado
mais eficiente e respeitoso
com os direitos fundamentais.

Desembargadora Vânia Marinho
Presidente do Comitê Gestor de Proteção de Dados
Tribunal de Justiça do Estado do Amazonas

Agradecimentos

Inicio estes agradecimentos reconhecendo o **Tribunal de Justiça do Estado do Amazonas,** instituição que não apenas acolheu esta iniciativa pioneira, mas a apoiou de forma irrestrita desde sua concepção. Registro especial gratidão à **Desembargadora Nélia Caminha Jorge**, que apoiou a criação da Rede com visão estratégica, e ao **Desembargador Jomar Ricardo Saunders Fernandes**, atual presidente, que compreendeu sua importância e deu continuidade ao projeto com o mesmo comprometimento institucional, garantindo que esta cooperação interinstitucional se consolidasse como modelo de referência no enfrentamento dos desafios da proteção de dados no contexto amazônico, proporcionando todo o suporte necessário para que esta iniciativa se tornasse realidade operacional duradoura.

Manifesto profunda gratidão aos **dirigentes das quinze instituições signatárias** do Acordo de Cooperação Técnica nº 53/2024 - TJAM, que demonstraram visão estratégica e compromisso institucional ao apoiarem esta iniciativa pioneira no cenário nacional. Estas instituições compreenderam desde o primeiro momento que os desafios impostos pela Lei Geral de Proteção de Dados ao setor público amazônico só poderiam ser adequadamente enfrentados através da colaboração institucional e do compartilhamento de experiências e recursos.

Reconheço especialmente o comprometimento das seguintes instituições:

Tribunal de Justiça do Estado do Amazonas, Prefeitura Municipal de Manaus, Tribunal Regional Eleitoral do Amazonas, Tribunal Regional do Trabalho da 11ª Região, Controladoria-Geral do Estado do Amazonas, Ordem dos Advogados do Brasil - Seccional Amazonas, Tribunal de Contas do Estado do Amazonas, Ministério Público do Estado do Amazonas, Processamento de Dados Amazonas S.A., Secretaria de Estado de Segurança Pública do Amazonas, Fundação Universidade do Amazonas, Universidade do Estado do Amazonas, Polícia Civil do Estado do Amazonas, Defensoria Pública do Estado do Amazonas e Procuradoria-Geral do Estado do Amazonas.

Aos **autores desta coletânea**, expresso reconhecimento especial pela generosidade em compartilhar suas experiências e conhecimentos especializados, transformando expertise institucional acumulada ao longo de anos de trabalho em bem público acessível a toda a comunidade interessada na proteção de dados. Cada contribuição representa não apenas

competência técnica refinada, mas compromisso genuíno e duradouro com o avanço da proteção de dados no setor público amazonense e com a construção de uma administração pública mais consciente de suas responsabilidades com a privacidade dos cidadãos.

Aos **representantes que participaram da instalação oficial da Rede** em outubro de 2024 e aos que assumiram cargos de direção em dezembro do mesmo ano, registro o empenho pessoal e institucional extraordinário que transformou uma ideia inicialmente abstrata em realidade operacional concreta e produtiva. Suas dedicações tornaram possível a criação de um modelo de cooperação inovador que pode inspirar outras regiões do país a adotarem iniciativas similares de enfrentamento coletivo dos desafios contemporâneos da proteção de dados.

Agradeço também aos **servidores públicos** que, no exercício de suas funções cotidianas, abraçaram a causa da proteção de dados como elemento fundamental do serviço público de qualidade. Suas contribuições práticas e sugestões valiosas foram essenciais para que a Rede se tornasse uma realidade operacional efetiva.

Como idealizadora desta rede e desta publicação, tenho a convicção profunda de que estamos construindo um legado duradouro para a proteção de dados no Brasil, um modelo que pode se tornar referência nacional e demonstrar que é possível implementar a legislação de proteção de dados com excelência mesmo enfrentando as particularidades e limitações regionais. Do sonho inicial ao Acordo de Cooperação de setembro de 2024, da instalação em outubro à estruturação em dezembro, e agora com o lançamento desta obra em agosto de 2025, cada etapa confirmou nossa convicção de que a cooperação institucional é o caminho mais eficaz e sustentável para enfrentar os desafios complexos e multifacetados da proteção de dados no setor público contemporâneo.

A todos que contribuíram direta ou indiretamente para esta conquista coletiva, manifestando apoio, dedicando tempo, compartilhando conhecimento ou simplesmente acreditando na viabilidade desta iniciativa mesmo nos momentos de maior incerteza, minha mais sincera e duradoura gratidão.

Desembargadora Vânia Marinho
Presidente do Comitê Gestor de Proteção de Dados
Tribunal de Justiça do Estado do Amazonas

Prefácio

A implementação da Lei Geral de Proteção de Dados (LGPD) no setor público brasileiro ganhou contornos únicos na região amazônica, onde comunidades ribeirinhas dispersas, povos indígenas com direitos diferenciados e infraestrutura tecnológica em desenvolvimento criam desafios para proteger dados pessoais que vão muito além das questões técnicas e jurídicas convencionais. Esta coletânea resulta de uma experiência pioneira de cooperação interinstitucional voltada especificamente à LGPD no Brasil: a Rede Amazonense de Proteção de Dados. Formalizada em setembro de 2024 com a adesão de quinze instituições do estado, segundo a qual a efetividade das políticas de proteção de dados pessoais exige um ecossistema articulado e colaborativo, e não ações isoladas.

Em seus primeiros meses de funcionamento, a Rede realizou reuniões mensais, escolheu sua estrutura de direção e demonstrou que a colaboração institucional pode superar limitações individuais no enfrentamento dos desafios complexos da proteção de dados, partindo do reconhecimento de que no contexto amazônico, onde o Tribunal de Justiça compartilha cotidianamente dados sensíveis com o Ministério Público em investigações e processos, com a Defensoria Pública em questões de assistência judiciária, com a Polícia Civil em inquéritos e laudos periciais, e com diversos órgãos municipais e estaduais em execuções fiscais e questões administrativas, não é suficiente que cada instituição promova isoladamente sua adequação à LGPD se os demais elos da cadeia não estiverem alinhados e adequados, uma vez que vulnerabilidades em qualquer ponto comprometem a segurança de todo o sistema.

Desde 2020, quando a LGPD entrou em vigor, o setor público enfrenta obrigações crescentes que se intensificaram com a Emenda Constitucional nº 115/2022, que elevou a proteção de dados a direito fundamental, e com a Resolução CNJ nº 363/2021, que estabeleceu requisitos específicos para o Judiciário e criou marcos obrigatórios para todos os tribunais do país. No Amazonas, com sua geografia desafiadora e diversidade populacional única, esses marcos normativos criaram demandas que nenhuma instituição isolada poderia atender adequadamente, levando o Tribunal de Justiça do Estado a reconhecer que sua posição central no sistema de justiça e sua natural interação com diversos órgãos públicos o colocavam numa posição estratégica não apenas para implementar a LGPD, mas para liderar a criação de um modelo efetivo de proteção sistêmica de dados que transformasse uma

obrigação legal em oportunidade de ofertar um serviço público inovador à sociedade amazonense.

A resposta foi a criação da primeira rede estadual de cooperação em proteção de dados, reunindo desde tribunais e órgãos de controle até universidades e empresas públicas das três esferas de governo em um modelo inovador que permite compartilhar expertise, recursos e soluções, transformando limitações individuais em força coletiva e demonstrando que quando o Estado atua de forma integrada e coordenada, pode oferecer proteção mais eficaz aos dados pessoais dos cidadãos, criando um verdadeiro serviço público de proteção de dados que atende ao interesse coletivo e redesenha a forma como as instituições públicas cumprem suas responsabilidades com a privacidade e dignidade dos amazonenses.

Esta coletânea oferece uma jornada completa pela implementação da LGPD no setor público amazonense, organizada em quatro partes complementares que conduzem o leitor do conhecimento teórico às aplicações práticas mais específicas, começando com os fundamentos e marcos normativos estabelecidos através da magistral análise da Controladoria-Geral do Estado sobre a complexa harmonização entre LGPD e Lei de Acesso à Informação, dilema central para gestores públicos que precisam equilibrar transparência e privacidade em um contexto de cooperação interinstitucional, seguida pela fundamentação jurídica apresentada pelo Ministério Público do Estado sobre a tutela coletiva em proteção de dados, oferecendo instrumental teórico indispensável aos operadores do direito que precisam compreender os mecanismos de defesa coletiva dos direitos dos titulares em um ambiente de compartilhamento sistemático de informações entre órgãos públicos.

A segunda parte revela as perspectivas humanas e sociais da implementação da LGPD através da experiência da Defensoria Pública no atendimento a populações vulneráveis, tema de especial relevância no contexto amazônico onde comunidades tradicionais, povos indígenas e populações ribeirinhas demandam atenção diferenciada e onde a proteção efetiva de seus dados depende da coordenação entre múltiplas instituições que prestam serviços a essas comunidades, complementada pela análise do Tribunal Regional do Trabalho da 11ª Região sobre a proteção de dados de trabalhadores terceirizados, grupo frequentemente negligenciado nas discussões sobre LGPD, mas essencial para a administração pública e cujos dados transitam entre diversos órgãos contratantes, e encerrada pela

contribuição da Universidade Federal do Amazonas que conecta proteção de dados com educação para cidadania digital, demonstrando como a formação de uma consciência coletiva sobre direitos digitais fortalece todo o ecossistema de proteção de dados no estado.

A terceira parte concentra-se na implementação prática e gestão, oferecendo ferramentas concretas para aplicação coordenada da LGPD através das metodologias estruturadas para resposta a incidentes de segurança apresentadas pela Procuradoria-Geral do Estado, tema crítico quando incidentes podem afetar múltiplas instituições que compartilham dados, exigindo protocolos integrados de resposta e comunicação, da experiência municipal completa compartilhada pela Prefeitura de Manaus, incluindo análise SWOT que será valiosa para outros gestores que precisam coordenar suas práticas de proteção de dados com órgãos estaduais e federais, e da visão técnica avançada oferecida pela PRODAM sobre a integração entre LGPD e normas internacionais de segurança da informação, demonstrando como harmonizar diferentes frameworks normativos quando se atua em um ambiente de cooperação interinstitucional que exige padrões técnicos compatíveis.

A quarta e última parte aborda o controle social e especificidades setoriais com perspectivas únicas que incluem a exploração pela Secretaria de Segurança Pública do papel inovador da Ouvidoria no controle social da proteção de dados, apresentando como este instrumento democrático pode atuar de forma coordenada entre diferentes órgãos para fortalecer a fiscalização cidadã das políticas de proteção de dados, a análise do Tribunal de Justiça do Estado sobre as complexas tensões entre publicidade processual e proteção de dados sensíveis, questão central quando processos judiciais envolvem informações que transitam entre diversos órgãos e exigem equilíbrio delicado entre transparência judicial e proteção de dados em um contexto de cooperação interinstitucional, e a reflexão provocativa da Ordem dos Advogados do Brasil - Seccional Amazonas sobre os limites da regulação estatal e a autorregulação profissional, encerrando a obra com uma discussão sobre como diferentes formas de regulação podem conviver harmonicamente em um ecossistema integrado de proteção de dados.

Esta obra destina-se especificamente a gestores públicos, encarregados de dados, servidores, magistrados, promotores, defensores, advogados e estudiosos da LGPD que buscam não apenas conhecimento teórico, mas soluções práticas testadas na realidade amazônica e apresentadas

com linguagem acessível tanto para iniciantes quanto para profissionais experientes que já atuam na área e precisam compreender como implementar a proteção de dados em um contexto de cooperação interinstitucional. Embora cada capítulo possa ser lido independentemente conforme o interesse específico do leitor, a sequência proposta facilita a compreensão progressiva dos desafios e soluções em um ambiente onde a efetividade das políticas de proteção de dados depende da coordenação entre múltiplas instituições, enquanto os casos práticos e metodologias apresentadas são deliberadamente adaptáveis a diferentes contextos institucionais, respeitando as particularidades regionais sem perder a aplicabilidade geral que permite sua replicação em outras realidades do setor público brasileiro que enfrentem desafios similares de integração e cooperação.

A Rede Amazonense já demonstra resultados concretos que incluem a identificação e discussão coletiva de problemas comuns enfrentados pelas instituições participantes, o compartilhamento de boas práticas e experiências exitosas entre órgãos que antes atuavam isoladamente, e o desenvolvimento de uma compreensão mútua sobre desafios específicos que permite apoio recíproco na busca por soluções adequadas à realidade amazonense, conquistas que serão celebradas no I Encontro da Rede, previsto para agosto de 2025, evento que marca o lançamento desta coletânea e consolida o Amazonas como referência regional em proteção sistêmica de dados, demonstrando que é possível transformar uma obrigação legal em instrumento efetivo de melhoria do serviço público. Os próximos passos desta iniciativa pioneira incluem: (i) expansão da Rede para outros órgãos interessados em integrar-se a este modelo de cooperação, (ii) a criação de um centro de referência em proteção de dados para a região Norte que possa orientar iniciativas similares, e (iii) o compartilhamento sistemático da experiência para replicação em outros estados brasileiros que enfrentem desafios similares, especialmente considerando que a implementação crescente de inteligência artificial no setor público, orientada pela Resolução CNJ nº 615/2024, cria novos desafios de proteção de dados que exigirão ainda mais cooperação e coordenação interinstitucional para serem enfrentados adequadamente.

A proteção de dados pessoais representa muito mais que uma simples obrigação legal, constituindo-se como expressão concreta do respeito à dignidade humana e à cidadania plena em uma sociedade cada vez mais digitalizada, e quando implementada através de cooperação interinstitucional coordenada, torna-se um verdadeiro serviço público que

beneficia toda a sociedade amazonense, razão pela qual esta coletânea oferece não apenas conhecimento técnico especializado, mas também inspiração para transformar realidades institucionais através da cooperação e do compartilhamento de experiências exitosas que demonstram como o Estado pode ser mais eficiente e efetivo quando atua de forma integrada. Convido todos os leitores a esta experiência pelos caminhos da proteção de dados no Amazonas, estado que apresenta desafios únicos, bem como oportunidades extraordinárias para inovação em políticas públicas, certos de que encontrarão aqui ferramentas práticas e fundamentação teórica sólida para enfrentar os desafios de implementar a LGPD com excelência através da cooperação interinstitucional, respeitando as particularidades regionais e construindo um setor público verdadeiramente comprometido com os direitos fundamentais dos cidadãos e com a construção de uma administração pública mais transparente, eficiente e respeitosa com a privacidade, que reconhece que a proteção efetiva de dados é uma responsabilidade coletiva que exige a coordenação de todos os atores públicos em benefício da sociedade.

Presidente Do Comitê Gestor de Proteção de Dados

Desembargadora Vânia Marques Marinho

Manaus, agosto de 2025

Sobre os Autores

CONTROLADORIA-GERAL DO ESTADO DO AMAZONAS - CGE-AM

Elisângela Nogueira Rodrigues

Assessora Técnica/ Encarregada de Proteção de Dados

Bacharel em Direito, Pós-graduada em Direito Público com ênfase em Direito Eleitoral e experiência na implementação de políticas de proteção de dados pessoais no setor público

elisangela.nogueira@cge.am.gov.br

José Victor Oliveira de Oliveira

Assessor de Controle Interno / Suplente do Encarregado de Dados

Bacharel em Administração, com experiência em Administração Pública e na implementação de políticas de proteção de dados pessoais no setor público.

jose.oliveira@cge.am.gov.br

DEFENSORIA PÚBLICA DO ESTADO DO AMAZONAS - DPE-AM

Rudson Fernandes Nunes

Diretor adjunto da Diretoria Geral / Encarregado de Proteção de Dados

Formado em Análise de Sistema / Especialista em Gestão de Projeto / Especialista em Segurança Digital, Governança e Gestão de Dados.

rudson_nunes@defensoria.am.def.br

MINISTÉRIO PÚBLICO DO ESTADO DO AMAZONAS - MPAM

Cley Barbosa Martins

Promotora de Justiça de Entrância Final / Encarregada de Proteção de Dados

Coordenadora do Grupo Gestor do SAJ/MP e Encarregada pelo Tratamento de Dados Pessoais no âmbito do Ministério Público do Estado do Amazonas.

cleymartins@mpam.mp.br

Felipe Augusto Fonseca Vianna

Agente Técnico - Jurídico / Membro do Grupo de Trabalho de Apoio ao Comitê Gestor de Proteção de Dados Pessoais do MPAM

Master of Science in Criminal Justice (Summa Cum Laude) pela California Coast University. Especialista em Direito Constitucional pela PUC de São Paulo. Bacharel em Direito pela UFAM. Licenciando em História pela Universidade La Salle. Agente Técnico Jurídico do Ministério Público do Estado do Amazonas.

felipevianna@mpam.mp.br

Arquelau Carvalho do Nascimento Neto

Agente Técnico - Administrativo / Membro do Grupo de Trabalho de Apoio ao Comitê Gestor de Proteção de Dados Pessoais do MPAM

Graduando em Direito pela Universidade Federal do Amazonas. Bacharel em Administração pela Universidade do Estado do Amazonas. Mestre em Administração pela Must University. Agente de Apoio - Administrativo do Ministério Público do Estado do Amazonas.

arquelauneto@mpam.mp.br

ORDEM DOS ADVOGADOS DO BRASIL - SECCIONAL AMAZONAS - OAB-AM

Aldo Evangelista

Advogado / Encarregado da OAB/AM

Educador e Advogado em direitos digitais. Procurador Municipal de Carreira. Mestre em Ciências Forenses pela UNIFESSPA. Doutorando pela UNIVALI – CIESA. Presidente da Comissão de Direitos Digitais, Startups e Inovação da OAB-AM. Encarregado da OAB-AM. Palestrante e músico.

aldoadvocacia7@gmail.com

PREFEITURA MUNICIPAL DE MANAUS - PMM

Joabe Cota Riker

Chefe de Divisão de Integridade e Compliance

Contador; Professor; Bacharel em Economia; Especialista em Gestão de Finanças, Controladoria e Auditoria; e Mestre em Engenharia de Produção pela Universidade Federal do Amazonas (UFAM), com experiência em Controle Interno, Compliance e Proteção de Dados.

joabe.cota@pmm.am.gov.br

Lucilene Florêncio Viana

Controladora-Geral Adjunta / Encarregada de Proteção de Dados

Contadora; Professora; Mestre em Contabilidade e Controladoria pela UFAM; Pós-graduada nas seguintes áreas: Administração Pública, Ciências Contábeis, Auditoria, Direito Tributário, Auditoria e Controle Interno, com experiência em Contabilidade Pública, Controladoria, Auditoria, Tributos e Fiscalização, Integridade, Compliance e Proteção de Dados.

lucilene@pmm.am.gov.br

Gleuson Silva Chaves

Diretor do Departamento de Controladoria

Contador; Pós-graduado nas seguintes áreas: Auditoria e Controladoria pela Faculdade Martha Falcão, com experiência em Contabilidade Pública, Controladoria, Auditoria, Integridade, Compliance e Proteção de Dados.

gleuson.chaves@pmm.am.gov.br

Lorena de Oliveira Pereira

Contadora, Pós-graduanda em MBA em Auditoria e Auditoria pela UEA.

Marcos Laylson Nunes da Silva

Bacharel em Direito, Pós-graduando em Licitações Públicas e Contratos Administrativos, e em Controladoria e Finanças Públicas pelo Gran Centro Universitário.

PROCESSAMENTO DE DADOS AMAZONAS S.A. - PRODAM

Emerson Silva de Souza

Assessor / Encarregado de Proteção de Dados

Bacharel em Ciência da Computação, Espec. Gerenciamento de Projetos, Certificações em EXIN Certified DPO, OneTrust Certified Privacy e participação ativa como Membro Titular do Grupo de Trabalho de Segurança da Informação da ABEP-TIC, Membro Titular do Sub-grupo de Segurança Cibernética do GTD. GOV e Membro Titular da Rede de Encarregados de Proteção de Dados do Amazonas.

emerson.souza@prodam.am.gov.br

PROCURADORIA-GERAL DO ESTADO DO AMAZONAS - PGE-AM

Luan Silva Seminario

Procurador do Estado / Encarregado de Dados

Procurador-Chefe da Procuradoria Jurídica da Secretaria de Estado de Saúde do Amazonas (SES/AM). Mestrando em Direito pela Universidade de Brasília (UnB). Pós-graduado em Direito Tributário e Aduaneiro pela Pontifícia Universidade Católica de Minas Gerais (PUC-MG). Bacharel em Direito pela Universidade Federal do Amazonas (UFAM). Técnico em Informática pela Fundação Nokia de Ensino (FNE).

luan.seminario@pge.am.gov.br

Eduardo Nicolas Bitencourt Neves

Analista de Tecnologia da Informação e Encarregado de Dados Substituto da PGE/AM.
Pósgraduado em Cibersegurança e Governança de Dados pela PUC de Minas Gerais. Bacharelando em Engenharia da Computação pela FUCAPI. Tecnólogo em Segurança da Informação pelo Centro Universitário do Vale do Ipojuca (UNIFAVIP-Wyden). Técnico em Informática pelo Instituto Federal de Educação, Ciência e Tecnologia do Amazonas (IFAM).
eduardo.neves@pge.am.gov.br

SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA - SSP-AM

Sérgio Augusto Costa da Silva

Ouvidor-Geral da SSP-AM/ Encarregado de Proteção de Dados
Graduado em Direito e bacharel em Teologia, especialista em Direito Público e Direito Penal/Processo Penal, pós-graduando no MBA em Gestão Financeira e Contábil no Setor Público.
ouvidoriadeseguranca@ssp.am.gov.br / sergioadvogados@hotmail.com

Gerbeson Vieira de Souza

Assessor de Controla Interno da UCI/SSP-AM.
Pós-graduando em MBA em Gestão Financeira e Contábil pela UEA. Bacharel em Direito pela Uninorte.
gerbesonvieira@gmail.com

TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS - TJAM

Igor de Carvalho Leal Campagnolli

Magistrado / Encarregado de Proteção de Dados
Mestrado na Universidade de São Paulo - USP em Direito do Estado. Especialização em Direito Civil e Processual Civil pelo CIESA.
igor.campagnolli@tjam.jus.br

TRIBUNAL REGIONAL DO TRABALHO DA 11ª REGIÃO - TRT-11

Carolina de Souza Lacerda Aires França

Magistrada / Servidora / Encarregada de Proteção de Dados
Bacharel em Direito e Especialista em Direito Tributário pela Universidade Federal do Amazonas (UFAM).
carolina.franca@trt11.jus.br

Diego Enrique Linares Troncoso

Magistrado / Servidor / Encarregado de Proteção de Dados (Substituto)
Bacharel em Direito pela Universidade de São Paulo (USP) e Especialista em Direito do Trabalho e Direito Processual do Trabalho pela Universidade Presbiteriana Mackenzie (UPM).
diego.troncoso@trt11.jus.br

UNIVERSIDADE FEDERAL DO AMAZONAS - UFAM

Nycolle Oliveira Souza Santos

Administradora / Encarregada de Proteção de Dados
Bacharel em Administração pela Universidade do Estado do Amazonas (UEA), Mestre em Engenharia de Produção pela Universidade Federal do Amazonas (UFAM). Experiência em compras e contratações e em proteção de dados.
nycollesnts@ufam.edu.br

Sumário

Introdução

A **Rede Amazonense de Proteção de Dados** representa um marco na implementação da Lei Geral de Proteção de Dados (LGPD) no Brasil, constituindo-se como a primeira iniciativa de cooperação interinstitucional específica para proteção de dados no setor público brasileiro. Criada em setembro de 2024 através do Acordo de Cooperação Técnica nº 53/2024 - TJAM, a Rede reúne quinze instituições do estado do Amazonas em uma experiência pioneira que demonstra como a colaboração institucional pode transformar desafios individuais em soluções coletivas.

A necessidade de uma abordagem cooperativa surgiu da compreensão de que no contexto amazônico, onde as instituições públicas compartilham cotidianamente dados sensíveis e enfrentam desafios únicos relacionados à diversidade populacional, geografia desafiadora e infraestrutura tecnológica em desenvolvimento, a implementação efetiva da LGPD exige muito mais que adequação individual de cada órgão. A proteção de dados pessoais no Amazonas demanda uma visão sistêmica que reconheça as interdependências operacionais entre as instituições e promova a segurança de toda a cadeia de tratamento de dados pessoais.

O CONTEXTO AMAZÔNICO E SEUS DESAFIOS ÚNICOS

O estado do Amazonas apresenta particularidades que tornam a implementação da LGPD especialmente complexa e, ao mesmo tempo, estratégica para a proteção dos direitos fundamentais dos cidadãos. Com uma área territorial de mais de 1,5 milhão de quilômetros quadrados, o estado abriga comunidades ribeirinhas dispersas, povos indígenas com direitos diferenciados, populações tradicionais com modos de vida específicos e centros urbanos em constante crescimento, criando um mosaico populacional que demanda abordagens diferenciadas para a proteção de dados pessoais.

As instituições públicas amazônicas enfrentam desafios operacionais únicos que incluem limitações de conectividade em áreas remotas, necessidade de coleta de dados através de intermediários como agentes comunitários e lideranças locais, marcos legais sobrepostos especialmente no que se refere aos direitos indígenas, e a necessidade de harmonizar a proteção de dados com outros direitos fundamentais como transparência e acesso à informação. Esses desafios evidenciaram que nenhuma instituição isolada possuía recursos ou expertise suficientes para enfrentar adequadamente todas as complexidades da implementação da LGPD na região.

Missão da Rede Amazonense de Proteção de Dados
Promover a implementação coordenada e efetiva da Lei Geral de Proteção de Dados no setor público amazonense através da cooperação interinstitucional, compartilhamento de conhecimentos e desenvolvimento de soluções coletivas que respeitem as particularidades regionais e garantam a proteção dos direitos fundamentais dos cidadãos.

ESTRUTURA E FUNCIONAMENTO DA REDE

A Rede Amazonense de Proteção de Dados funciona através de uma estrutura colaborativa que privilegia a participação horizontal entre as instituições, promovendo reuniões mensais para discussão de problemas comuns, compartilhamento de boas práticas e alinhamento de estratégias. O modelo de governança adotado permite que cada instituição contribua com sua expertise específica, criando sinergias que beneficiam todo o ecossistema de proteção de dados no estado.

As atividades da Rede incluem a identificação e discussão coletiva de desafios enfrentados pelas instituições participantes, o compartilhamento de experiências exitosas e lições aprendidas, o desenvolvimento de uma compreensão mútua sobre problemas específicos que permite apoio recíproco, e a promoção de eventos e capacitações que fortalecem a cultura de proteção de dados no setor público amazonense.

ESTA COLETÂNEA: PROPÓSITO E ORGANIZAÇÃO

Esta coletânea documenta as experiências, desafios e soluções desenvolvidas pela Rede Amazonense de Proteção de Dados em seus primeiros meses de funcionamento, oferecendo uma visão abrangente e prática da implementação da LGPD no contexto amazônico. A obra está organizada em quatro partes que conduzem o leitor dos fundamentos teóricos até as aplicações mais específicas e especializadas da proteção de dados no setor público.

Parte I - Fundamentos e Marcos Normativos estabelece as bases teóricas e práticas essenciais, abordando a harmonização entre LGPD e Lei de Acesso à Informação e os fundamentos jurídicos da tutela coletiva em

proteção de dados. **Parte II - Perspectivas Humanas e Sociais** revela o olhar humanizado da implementação da LGPD, focando no atendimento a populações vulneráveis e na proteção de trabalhadores terceirizados. **Parte III - Implementação Prática e Gestão** oferece ferramentas concretas para aplicação da LGPD, incluindo metodologias para resposta a incidentes e integração com normas internacionais. **Parte IV - Controle Social e Especificidades Setoriais** aborda questões especializadas como o papel da Ouvidoria e as tensões entre publicidade processual e proteção de dados.

COMO USAR ESTA OBRA

Esta coletânea foi concebida para servir tanto como material de consulta quanto como guia prático para implementação da LGPD no setor público. Embora cada artigo possa ser lido independentemente, recomenda-se a leitura sequencial para uma compreensão progressiva dos desafios e soluções. Os casos práticos e metodologias apresentadas são adaptáveis a diferentes contextos institucionais, respeitando particularidades regionais sem perder a aplicabilidade geral.

Gestores públicos encontrarão aqui ferramentas práticas para implementação, encarregados de dados descobrirão soluções testadas na prática, servidores públicos compreenderão melhor suas responsabilidades, e estudiosos da LGPD terão acesso a uma perspectiva única sobre proteção de dados no contexto amazônico. Mais que um manual técnico, esta obra representa um testemunho coletivo de transformação institucional e um convite para que outras regiões adotem modelos similares de cooperação.

A experiência da Rede Amazonense de Proteção de Dados demonstra que quando o Estado atua de forma integrada e coordenada, é possível não apenas cumprir as exigências legais da LGPD, mas também oferecer um serviço público mais eficiente e respeitoso com os direitos fundamentais dos cidadãos. Esta coletânea é o primeiro fruto dessa experiência cooperativa e um passo importante na construção de uma cultura de proteção de dados no setor público brasileiro.

LGPD versus LAI: A Busca do Equilíbrio entre o Direito à Privacidade e a Prevalência do Interesse Público de Acesso à Informação

Controladoria-Geral do Estado do Amazonas

Análise da complexa harmonização entre a Lei Geral de Proteção de Dados e a Lei de Acesso à Informação no contexto da administração pública amazonense.

José Victor Oliveira de Oliveira

Bacharel em Administração pela UFAM
Assessor da Subcontroladoria-Geral de Transparência e Ouvidoria
Suplente de Encarregado de Dados da Controladoria-Geral do Estado do Amazonas

Elisângela Nogueira Rodrigues

Bacharel em Direito pela UFAM
Especialista em Direito Público
Assessora Técnica da Subcontroladoria-Geral de Transparência e Ouvidoria Encarregada de Dados da Controladoria-Geral do Estado do Amazonas

Resumo

O presente artigo propõe-se a examinar os desafios jurídicos e operacionais enfrentados pelos órgãos do Poder Executivo do Estado do Amazonas na conciliação entre dois direitos fundamentais em potencial tensão: o direito à proteção de dados pessoais, assegurado pela Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), e o direito de acesso à informação, previsto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação – LAI). A pesquisa adota uma abordagem qualitativa, com ênfase na análise bibliográfica e documental, além da observação empírica de práticas administrativas implementadas no âmbito estadual.

Com foco na atuação da Controladoria-Geral do Estado do Amazonas (CGE), o estudo analisa os fundamentos jurídicos, os instrumentos técnicos e os procedimentos institucionais voltados à promoção simultânea da transparência pública e da proteção da privacidade dos titulares de dados. São abordadas, ainda, boas práticas de governança, estudos de caso, mecanismos de gestão de dados pessoais e propostas de aprimoramento normativo e organizacional. O objetivo é contribuir para o fortalecimento da cultura de acesso à informação compatível com os princípios da proteção de dados, no contexto da Administração Pública estadual.

Palavras-chave: LGPD. LAI. Governança de Dados. Administração Pública.

1. Introdução

A crescente digitalização dos serviços públicos e a maior demanda da sociedade por transparência têm colocado em evidência o necessário equilíbrio entre o direito fundamental à privacidade e o acesso à informação. No Brasil, esse equilíbrio é formalizado por meio da convivência entre duas legislações fundamentais: a Lei nº 12.527/2011, conhecida como Lei de Acesso à Informação (LAI), e a Lei nº 13.709/2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD). Ambas têm por base os princípios constitucionais e se aplicam diretamente à administração pública, incluindo o Executivo Estadual.

No âmbito do Estado do Amazonas, a Controladoria-Geral do Estado (CGE) atua como órgão central na governança da informação pública, sendo responsável pela implementação de políticas de acesso à informação e de proteção de dados. O desafio enfrentado pela CGE-AM reflete uma realidade mais ampla: *como garantir a publicidade dos atos administrativos sem comprometer a proteção de dados pessoais dos cidadãos?*

Este artigo propõe uma análise técnica e normativa desse cenário, com uma abordagem qualitativa, com ênfase na análise bibliográfica e documental, além da observação empírica de práticas administrativas implementadas no âmbito estadual na busca de instrumentalizar a harmonização normativa e operacional e fortalecer a cultura de integridade, governança e legalidade na administração pública.

2. Marco Jurídico: A Convivência entre LGPD e LAI

A coexistência normativa entre a Lei de Acesso à Informação (LAI) e a Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil representa um avanço no fortalecimento da democracia e dos direitos fundamentais, exigindo da administração pública a adoção de práticas técnicas e jurídicas que assegurem simultaneamente a transparência e a privacidade. Ambas as legislações possuem respaldo constitucional: a LAI está ancorada no princípio da publicidade e do controle social da Administração Pública (art. 5º, inciso XXXIII; art. 37, caput; e art. 216, §2º da Constituição da República Federativa do Brasil), enquanto a LGPD concretiza o direito à privacidade e à proteção de dados pessoais como garantias fundamentais (art. 5º, inciso X, e art. 1º da LGPD).

A LAI estabelece o dever dos órgãos públicos de garantir amplo acesso a informações de interesse coletivo ou geral, ressalvadas as hipóteses legais de sigilo, como aquelas que possam comprometer a segurança do Estado ou a intimidade do cidadão. Já a LGPD introduz o conceito de tratamento adequado de dados pessoais,

exigindo base legal, finalidade específica, necessidade e segurança da informação, inclusive no setor público, conforme seus arts. 7º e 23 a 30.

É nesse cenário que se verifica uma aparente tensão entre os dispositivos legais: enquanto a LAI favorece o acesso, a LGPD impõe restrições à divulgação de dados que identifiquem direta ou indiretamente a pessoa natural. No entanto, a leitura dessas normas deve ser harmônica e integrada, conforme já orientado pela Autoridade Nacional de Proteção de Dados (ANPD), pela Controladoria-Geral da União (CGU) e por decisões do Supremo Tribunal Federal (STF).

A harmonização dessas normas no setor público exige análise contextualizada, considerando a finalidade do tratamento, o interesse público envolvido e a adoção de técnicas como anonimização, classificação de informações sensíveis e aplicação de princípios como o da minimização de dados. O desafio está em consolidar uma cultura institucional que compreenda essas legislações como complementares e não excludentes, orientando-se por boas práticas de governança e conformidade regulatória.

3. Fundamentos Constitucionais e Princípios da Administração Pública

O cotejo entre a LGPD e a LAI requer um exame acurado dos fundamentos constitucionais que embasam tanto o direito à privacidade quanto o direito ao acesso à informação. Esses direitos são consagrados na CRFB/88 como cláusulas pétreas e devem ser interpretados à luz dos princípios que regem a Administração Pública, em especial os elencados no caput do art. 37: *legalidade, impessoalidade, moralidade, publicidade e eficiência*.

O *direito à informação*, previsto no art. 5º, inciso XXXIII, assegura a todos o acesso a informações dos órgãos públicos, salvo aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado. Paralelamente, o inciso X do mesmo artigo garante a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, assegurando o direito à indenização em caso de violação. O inciso LXXII, por sua vez, estabelece o *habeas data* como instrumento jurídico para assegurar o conhecimento e a retificação de informações pessoais em registros públicos.

Esses dispositivos formam a base constitucional de um modelo de governança pública da informação que equilibra o acesso à informação como regra geral e a proteção de dados como limitação legítima. Não há hierarquia entre esses direitos; o que se impõe, portanto, é a técnica da ponderação de princípios, conforme proposta pelo jurista alemão, Robert Alexy, em sua obra "*Teoria dos Direitos Fundamentais*", por meio do qual se avalia a finalidade do tratamento, dos riscos envolvidos, e do interesse público envolvido na divulgação ou sigilo da informação, resultando na precedência de um princípio sobre o outro.

No setor público, a aplicação desses fundamentos deve ser guiada, de forma premente, também pelos princípios da **supremacia do interesse público**, da **razoabilidade** e da **proporcionalidade**, sendo essencial que qualquer restrição ao acesso à informação ou qualquer tratamento de dados pessoais tenha **justificativa jurídica adequada (base legal)**, vinculada à finalidade institucional e à necessidade concreta da ação administrativa.

A atuação da Controladoria-Geral do Estado do Amazonas, nesse sentido, visa observar prioritariamente esses fundamentos como diretrizes obrigatórias, adotando políticas e processos que garantam tanto a efetividade da LAI quanto o cumprimento dos deveres impostos pela LGPD. A compatibilização normativa, portanto, não é apenas desejável — é constitucionalmente exigida.

4. Aplicabilidade no Setor Público: Interseções e Conflitos Práticos

A aplicação simultânea da **Lei de Acesso à Informação (LAI) e da Lei Geral de Proteção de Dados Pessoais (LGPD)** no setor público demanda a superação de desafios operacionais, normativos e interpretativos. Embora ambas estejam alicerçadas em direitos fundamentais, suas finalidades distintas — ***transparência e privacidade*** — muitas vezes se encontram em rota de colisão na prática administrativa.

No âmbito do **Executivo Estadual,** situações recorrentes revelam esse embate: solicitações de informações que envolvem **dados pessoais identificáveis,** como nomes, salários, históricos funcionais, prontuários médicos, entre outros. De um lado, a LAI impõe ao poder público o dever de garantir o acesso à informação como regra, conforme o art. 7º da referida lei. De outro, a LGPD determina que qualquer tratamento de dados pessoais seja embasado por fundamento legal, finalidade específica e respeito à autodeterminação informativa do titular.

Conforme estabelece o **art. 31 da LGPD**, os dados pessoais, sob guarda da administração pública, devem ter acesso restrito a agentes públicos autorizados, salvo se houver previsão legal ou consentimento do titular. O mesmo dispositivo reconhece que o acesso pode ser viabilizado **mediante anonimização e/ou pseudoanonimização** ou por exigência de interesse público relevante, desde que observado o *princípio da proporcionalidade*.

Na prática, é necessário aplicar metodologias de **análise de risco informacional,** a partir de critérios como:

- **Finalidade do pedido:** o objetivo está relacionado ao controle social ou mera curiosidade?

- **Natureza do dado:** é pessoal, sensível ou anonimizado?
- **Risco de exposição indevida**: pode gerar dano à imagem, honra ou segurança da pessoa?
- **Alternativas viáveis:** é possível fornecer a informação de forma generalizada ou anonimizando/pseudonimizando?

Essas questões exigem, por parte dos órgãos públicos, a existência de fluxos internos bem definidos, com **matrizes de decisão, papéis claramente atribuídos** (como o do Encarregado de Dados) e **sistemas capazes de classificar e proteger adequadamente as informações.**

Outro ponto de atenção diz respeito à **publicidade ativa,** prevista na LAI. Muitos entes públicos ainda publicam dados pessoais ostensivamente em portais de transparência, sem análise de risco ou base legal apropriada. A LGPD impõe um reexame dessas práticas, exigindo avaliação de proporcionalidade e, quando necessário, medidas corretivas, como a retirada de conteúdo ou a pseudonimização de dados.

Portanto, a aplicação integrada da LAI e LGPD, no setor público, deve adotar uma abordagem **baseada em riscos, princípios e boas práticas administrativas**, assegurando a legalidade e a legitimidade da informação pública disponibilizada.

5. A Experiência da Controladoria-Geral do Estado do Amazonas

A **Controladoria-Geral do Estado do Amazonas** tem desempenhado papel estratégico na harmonização entre a **Lei Geral de Proteção de Dados Pessoais (LGPD) e a Lei de Acesso à Informação (LAI)** no âmbito do Poder Executivo Estadual. Como órgão central do sistema de controle interno, a CGE atua diretamente na regulamentação, orientação e supervisão de práticas relacionadas à governança da informação, integridade pública e proteção de dados pessoais.

5.1 Estrutura Normativa e Organizacional

A atuação da CGE está respaldada na **Lei Complementar Estadual nº 224/2021**, que estabelece suas competências dentro da estrutura do sistema de Controle Interno do Estado do Amazonas, e no **Decreto nº 40.824/2019**, que define seu regimento interno. Com base nesses instrumentos, a Controladoria conta com a **Subcontroladoria-Geral de Transparência e Ouvidoria (SGTO),** que reúne as unidades responsáveis por acesso à informação e atendimento ao cidadão.

Em conformidade com a LGPD, foi nomeada uma **Encarregada pelo Tratamento de Dados Pessoais**, responsável por garantir a conformidade institucional com a Lei nº 13.709/2018, atuando como canal de comunicação entre

a CGE, os titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD). Além disso, a instituição possui a designação formal de uma **Autoridade de Monitoramento da LAI, conforme** exigido pelo Decreto Estadual nº 48.999/2024 e de uma servidora para exercício das funções de Ouvidoria, conforme determina a Lei Federal n° 13.460/2017.

5.2 Políticas e Instrumentos de Governança

Entre os principais instrumentos desenvolvidos pela CGE destacam-se:

- **Sítio Eletrônico da CGE** (https://www.cge.am.gov.br/lgpd/), onde na aba "Institucional", acessa-se o *link* LGPD que reúne informações institucionais, contatos da Encarregada de Dados, orientações e materiais de apoio para os demais órgãos do Poder Executivo Estadual;
- **Instrução Normativa nº 01/2024,** que orienta a forma de tratamento de informações em processos administrativos eletrônicos, estabelecendo critérios objetivos visando a garantir a proteção dos dados pessoais tratados em ambiente digital;
- **Manual do Usuário LGPD no SIGED,** que instrui os servidores sobre a correta classificação de documentos digitais no **Sistema de Gestão Eletrônica de Documentos** (SIGED), classificando os dados entre *públicos, pessoais e sensíveis.*

5.3 Capacitação e Difusão de Boas Práticas

A CGE também tem investido em **capacitação interna e articulação interinstitucional**. Um exemplo disso foi o **I Encontro Estadual de Controle Interno,** realizado em 2023, que reuniu servidores e gestores de diversos órgãos para debater o fortalecimento da LGPD no Estado. Durante o evento, foram discutidas experiências práticas e anunciada a criação de um **grupo de trabalho transversal** para apoiar a implementação da LGPD de forma colaborativa entre secretarias e entidades da administração indireta.

Além disso, a CGE mantém parcerias com outras controladorias estaduais e órgãos de controle externo para **construção de referenciais técnicos comuns,** fomentando a padronização de processos e a interoperabilidade entre os sistemas estaduais.

5.4 Desafios Atuais e Próximos Passos

Embora os avanços sejam significativos, a CGE reconhece a existência de desafios, tais como:

- a necessidade de ampliar a cultura de proteção de dados nos demais órgãos estaduais;

- o fortalecimento das ferramentas de anonimização/pseudoanonimização e controle de acesso aos sistemas;
- a consolidação de indicadores de conformidade para monitorar a eficácia das políticas implementadas.

A experiência da CGE demonstra que o *equilíbrio entre privacidade e transparência no setor público* não depende apenas da existência de normas, mas da ***capacidade institucional de interpretá-las, operacionalizá-las e fiscalizá-las*** de maneira integrada e sustentável.

6. Estudos de Caso: Conflitos entre Transparência e Privacidade

A aplicação simultânea da **LGPD** e da **LAI** no setor público tem gerado situações práticas que exigem interpretação sistemática e decisões criteriosas, especialmente quando envolvem dados pessoais sensíveis ou com potencial possibilidade de identificação de seus titulares. A seguir, são apresentados três estudos de caso com base em situações tipicamente enfrentadas por órgãos do Executivo Estadual, incluindo a **CGE**, ilustrativos das problemáticas e estratégias adotadas.

6.1 Publicação de Remuneração Individualizada de Servidores

Um dos casos mais emblemáticos diz respeito à **publicação de salários individualizados de servidores públicos** nos portais de transparência. A LAI (art. 7º, §3º) determina que informações relacionadas à remuneração de agentes públicos são de interesse coletivo e, portanto, devem ser divulgadas. No entanto, a LGPD impõe a necessidade de avaliação da ***finalidade, adequação e necessidade*** do tratamento desses dados.

A CGE optou por manter a divulgação dos salários brutos, com base no entendimento de que se trata de dado funcional relacionado ao cargo público e não à esfera privada do servidor. A divulgação é feita em formato aberto e com informações funcionais, sem expor dados bancários, CPF ou outros identificadores pessoais. Essa decisão segue jurisprudência do STF no RE 652.777/DF (Tema 284 de Repercussão Geral), que consolidou o entendimento de que **a transparência prevalece sobre a privacidade em matéria de gastos públicos com pessoal.**

6.2 Acesso a Processos Disciplinares

Outro caso recorrente envolve **pedidos de acesso a procedimentos disciplinares administrativos** ainda em curso. A LAI impõe a transparência como regra, mas a LGPD determina que a divulgação de dados pessoais deve respeitar o devido processo legal e não pode gerar dano indevido ao titular.

A CGE, nesses casos, adota como prática **a restrição de acesso enquanto o**

processo está em tramitação, com base nos *princípios da legalidade* e da *presunção de inocência*. Apenas após a conclusão do processo e havendo sanção administrativa é que os dados podem ser parcialmente divulgados, respeitando o princípio da minimização e, sempre que possível, com anonimização/pseudoanonimização de dados de terceiros envolvidos.

6.3 Pedidos de Informações Médicas ou Psicológicas

Pedidos envolvendo **atestados médicos, laudos ou informações sobre afastamentos por motivo de saúde** representam um dos maiores riscos de violação à LGPD, por envolverem dados sensíveis. Mesmo quando apresentados por terceiros (ex: outros servidores ou membros do controle social), a divulgação é vedada salvo com consentimento do titular ou ordem judicial.

A CGE, balizada por pareceres técnicos da CGU e pela própria LGPD, nega o fornecimento de tais dados com base no art. 11 da LGPD, que classifica dados de saúde como sensíveis e de acesso restrito. A resposta padrão informa sobre o motivo da negativa com base no art. 31, §1º da LAI, preservando o direito do titular e a responsabilidade objetiva do ente público.

Esses casos ilustram a necessidade de **capacitação contínua, protocolos padronizados e análise jurídica integrada** no trato da informação pública. A boa gestão dessas situações fortalece a confiança institucional e evita responsabilizações administrativas, cíveis e éticas dos agentes públicos envolvidos.

7. Instrumentos Técnicos para a Harmonização Normativa

A harmonização entre a **Lei Geral de Proteção de Dados Pessoais (LGPD)** e a **Lei de Acesso à Informação (LAI)** no setor público não se dá apenas por interpretação jurídica, mas pela adoção de **instrumentos técnicos e operacionais** que possibilitem a compatibilização entre privacidade e transparência de forma sistemática, documentada e rastreável. No contexto do Executivo Estadual, e especialmente na experiência da CGE, algumas ferramentas e metodologias vêm sendo utilizadas ou recomendadas como boas práticas.

7.1 Classificação da Informação

A base da governança da informação está na **classificação adequada dos dados tratados** pela administração pública. Os documentos e registros devem ser classificados em, no mínimo:

- **informações públicas (ostensivas):** disponíveis para qualquer interessado, nos termos da LAI;
- **informações pessoais identificáveis**: protegidas nos termos da LGPD, com acesso restrito;

- **informações sensíveis:** conforme art. 5º, II da LGPD, exigem maior nível de segurança e controle de acesso; e,
- **informações sigilosas:** conforme a LAI (art. 23 a 31), com restrição legal ou fundamentação expressa.

Ferramentas como o **SIGED** (Sistema de Gestão Eletrônica de Documentos) integram essa lógica por meio de campos obrigatórios de classificação documental, o que permite rastreabilidade e prevenção de acessos indevidos.

7.2 Anonimização e Pseudonimização

As técnicas de **anonimização** (remoção de elementos que permitam a identificação do titular) e **pseudonimização** (substituição por identificadores indiretos) são meios eficazes para permitir a divulgação de informações públicas sem infringir a LGPD. São particularmente úteis em:

- divulgação de bases de dados estatísticas;
- publicação de decisões administrativas;
- compartilhamento de dados com órgãos de controle externo.

O uso de anonimização deve estar documentado, preferencialmente com evidências técnicas e respaldo jurídico, tratamento esse quem vem sendo adotado pela CGE e orientado como boas práticas aos demais órgãos e entidades da Administração Pública, a exemplo do que costa do Ofício-Circular n° 025/2023-GCG/CGE, e reiterado por meio elo Ofício-Circular n° 011/2025-CGC/CGE.

7.3 Matriz de Risco de Informação

Outra ferramenta recomendada é a **matriz de risco de divulgação de informações,** que avalia:

- tipo de dado (público, pessoal, sensível);
- finalidade do tratamento ou do pedido de acesso;
- potencial de dano à pessoa titular;
- interesse público legítimo.

Essa matriz pode ser utilizada para embasar decisões da autoridade de monitoramento da LAI e do encarregado de dados, garantindo consistência e defesa em eventuais auditorias ou questionamentos.

7.4 Fluxogramas e Protocolos Padronizados

A criação de **procedimentos operacionais padronizados (POPs)** com **fluxos de decisão** é essencial para garantir uniformidade e segurança jurídica nas respostas a pedidos de informação. Esses fluxos devem conter:

- Etapas de análise preliminar;

- Participação do encarregado de dados;
- Registro da decisão e da fundamentação legal;
- Indicação de medidas de mitigação (ex: anonimização ou negativa justificada).

Esses instrumentos aumentam a maturidade da governança de dados e reduzem o risco de decisões equivocadas ou incoerentes entre diferentes órgãos do mesmo ente federativo.

Esses mecanismos reforçam a capacidade do Estado de agir de forma preventiva, responsiva e transparente, fortalecendo tanto a **confiança institucional** quanto a **eficácia na proteção dos direitos fundamentais** dos cidadãos.

8. Propostas para Fortalecimento Institucional

A adequada implementação e conciliação entre a **Lei Geral de Proteção de Dados Pessoais (LGPD)** e a **Lei de Acesso à Informação (LAI)** no âmbito do Executivo Estadual requer mais do que cumprimento normativo: *exige a consolidação de uma* ***estrutura institucional robusta,*** *com cultura organizacional alinhada, instrumentos técnicos consolidados e diretrizes estratégicas articuladas*. A seguir, apresentam-se propostas voltadas ao fortalecimento da **governança pública da informação**, com ênfase na atuação da CGE, como órgão central.

8.1 Criação de Comitês Multissetoriais de Proteção de Dados e Transparência

A criação de **Comitês Permanentes de Governança da Informação**, compostos por representantes das áreas de ouvidoria, transparência, jurídico, tecnologia da informação e controle interno, permitiria:

- discussão de casos complexos que envolvam conflitos entre transparência e privacidade;
- deliberação sobre critérios para classificação e divulgação de informações;
- padronização de respostas a pedidos sensíveis ou controversos;
- apoio ao encarregado de dados e à autoridade de monitoramento da LAI.

Esses comitês podem ser instituídos por meio de decreto estadual ou de portarias internas, com representação mínima e reuniões periódicas documentadas.

8.2 Elaboração de um Plano Estadual de Governança de Dados Pessoais

Inspirado no Plano Nacional de Governo Digital e nas diretrizes da ANPD, propõe-se a formulação de um ***Plano Estadual de Governança de Dados Pessoais***, com objetivos de:

- mapear fluxos de dados pessoais entre os órgãos estaduais;
- estabelecer metas de conformidade com a LGPD;
- integrar a proteção de dados com as políticas de transformação digital;
- estimular o uso ético de dados por meio da análise preditiva, com respeito à privacidade.

Esse plano deve ser público, com metas e prazos definidos, e revisado anualmente.

8.3 Ampliação da Capacitação e Sensibilização de Servidores

A LGPD e a LAI exigem atuação técnica e consciente dos servidores públicos. Para isso, propõe-se:

- inclusão obrigatória de módulos de LGPD e LAI nos programas de capacitação da Escola de Governo;
- realização de oficinas práticas por órgãos setoriais;
- criação de trilhas formativas específicas para perfis-chave (encarregado, gestor de TI, pregoeiro, analista jurídico).

Capacitação recorrente reduz o erro operacional e fortalece a responsabilização positiva dos servidores.

8.4 Criação de Indicadores de Conformidade e Maturidade

Pode-se adotar um **modelo de avaliação periódica** de maturidade institucional em proteção de dados e transparência, com base em critérios como:

- existência de normativos internos;
- nomeação de encarregados e autoridades de monitoramento;
- volume e tipo de respostas a pedidos via LAI;
- incidentes reportados envolvendo dados pessoais.

Esses indicadores devem integrar relatórios anuais de controle interno e fomentar a melhoria contínua.

8.5 Integração entre LGPD, LAI e Lei do Governo Digital

Por fim, é fundamental alinhar as práticas de proteção de dados à **Lei nº 14.129/2021 (Lei do Governo Digital)**, que prevê a interoperabilidade e uso intensivo de dados para a prestação de serviços públicos. O desafio está em garantir que esse uso seja:

- finalístico e legítimo;
- seguro, com base em princípios da LGPD;
- transparente e controlado por mecanismos de accountability.

Essas propostas visam fortalecer o modelo institucional de governança da informação, promovendo a compatibilidade entre eficiência administrativa, segurança jurídica e proteção aos direitos fundamentais.

9. Considerações Finais

A convivência normativa entre a Lei Geral de Proteção de Dados Pessoais (LGPD) e a Lei de Acesso à Informação (LAI) exige, por parte do setor público, uma atuação fundamentada em princípios constitucionais, interpretação técnica e práticas administrativas coerentes. No contexto do **Executivo Estadual do Amazonas**, especialmente sob a coordenação da **Controladoria-Geral do Estado (CGE)**, tem-se buscado institucionalizar esse equilíbrio por meio de normativos internos, políticas de capacitação, instrumentos digitais e articulação intersetorial.

A análise desenvolvida neste artigo demonstra que não se trata de uma escolha entre privacidade ou transparência, mas da adoção de mecanismos que permitam a materialização simultânea de ambos os direitos fundamentais, de forma legítima, proporcional e transparente. As situações práticas ilustradas evidenciam que a aplicação conjunta dessas legislações impõe desafios, mas também oportunidades de aprimoramento da administração pública.

A experiência da CGE revela avanços importantes, como a formalização de encarregados de dados, a regulamentação do uso do SIGED para classificação informacional e a produção de manuais orientativos. No entanto, permanece o desafio de consolidar uma cultura institucional de proteção de dados e de transparência qualificada, que alcance todos os níveis da estrutura estadual e envolva não apenas gestores, mas também servidores operacionais e áreas de apoio.

A LGPD e a LAI não são normas concorrentes, mas complementares. A primeira assegura que o uso de dados se dê com ética, segurança e respeito aos direitos dos titulares; a segunda garante que o Estado preste contas de sua atuação de forma ativa, proativa e acessível ao cidadão. Quando aplicadas de forma harmônica, ambas contribuem para o fortalecimento da governança pública, da integridade institucional e da confiança social.

Diante disso, é imprescindível que o Estado do Amazonas continue investindo em:

- governança da informação baseada em risco e finalidade;
- padronização de fluxos e decisões sobre pedidos de acesso;
- desenvolvimento de soluções tecnológicas seguras e interoperáveis;
- acompanhamento regulatório e articulação com a ANPD e outros órgãos de controle.

Esse caminho fortalece a conformidade normativa, mas, acima de tudo,

reafirma o compromisso da administração pública estadual com uma atuação ética, legal e voltada à promoção do interesse público e à proteção da dignidade da pessoa humana.

Referências

ALEXY, Robert. *Teoria dos direitos fundamentais*. Tradução de Virgílio Afonso da Silva. São Paulo: Malheiros, 2008.

AMAZONAS. Controladoria-Geral do Estado do Amazonas. *Acesso à informação*. Manaus: CGE-AM, 2025. Disponível em: https://www.cge.am.gov.br/acesso-a-informacao/. Acesso em: 25 abr. 2025.

AMAZONAS. Controladoria-Geral do Estado do Amazonas. *Governo do Amazonas discute fortalecimento da LGPD em Encontro Estadual de Controle Interno*. Manaus: CGE-AM, 2023. Disponível em: https://www.cge.am.gov.br/governo-do-amazonas-discute-fortalecimento-da-lgpd-em-encontro-estadual-de-controle-interno/. Acesso em: 25 abr. 2025.

AMAZONAS. Controladoria-Geral do Estado do Amazonas. *Instrução Normativa n. 01, de 25 de novembro de 2024*. Estabelece diretrizes para classificação de informações no SIGED. Disponível em: https://www.cge.am.gov.br/wp-content/uploads/2025/02/25.11.24_INSTRUCAO-NORMATIVA-01-2024-Assinatura-CGE.pdf. Acesso em: 25 abr. 2025.

AMAZONAS. Controladoria-Geral do Estado do Amazonas. *Manual do usuário LGPD no SIGED*. Manaus: CGE-AM, 2024. Disponível em: https://www.cge.am.gov.br/wp-content/uploads/2024/11/Manual-do-Usuario-LGPD-no-SIGED-Versao-Final.pdf. Acesso em: 25 abr. 2025.

AMAZONAS. Controladoria-Geral do Estado do Amazonas. *Sítio eletrônico da CGE*. Manaus: CGE-AM, 2025. Disponível em: https://www.cge.am.gov.br/. Acesso em: 25 abr. 2025.

BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil de 1988*. Diário Oficial da União: seção 1, Brasília, DF, 5 out. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 25 abr. 2025.

BRASIL. Lei n. 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º da Constituição Federal. *Diário Oficial da União: seção 1*, Brasília, DF, 18 nov. 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 25 abr. 2025.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei n. 12.965, de 23 de abril de 2014 (Lei Geral de Proteção de Dados Pessoais – LGPD). *Diário Oficial da União: seção 1*, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 25 abr. 2025.

BRASIL. Lei n. 14.129, de 29 de março de 2021. Dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública. *Diário Oficial da União: seção 1*, Brasília, DF, 30 mar. 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14129.htm. Acesso em: 25 abr. 2025.

BRASIL. Supremo Tribunal Federal. *Recurso Extraordinário n. 652777/DF*. Rel. Min. Cármen Lúcia. Brasília, DF, jul. 2011. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=6204410. Acesso em: 25 abr. 2025.

2

Legitimidade do Ministério Público na Tutela Coletiva da Proteção de Dados Pessoais

Ministério Público do Estado do Amazonas

Fundamentação jurídica da atuação do Ministério Público na defesa coletiva dos direitos relacionados à proteção de dados pessoais.

Arquelau Carvalho do Nascimento Neto

Graduando em Direito pela Universidade Federal do Amazonas. Bacharel em Administração pela Universidade do Estado do Amazonas. Mestre em Administração pela Must University. Servidor do Ministério Público do Estado do Amazonas.

Cley Barbosa Martins

Promotora de Justiça de Entrância Final do Ministério Público do Estado do Amazonas. Coordenadora do Grupo Gestor do SAJ/MP e Encarregada pelo Tratamento de Dados Pessoais no âmbito do Ministério Público do Estado do Amazonas.

Felipe Augusto Fonseca Vianna

Master of Science in Criminal Justice (Summa Cum Laude) pela California Coast University. Especialista em Direito Constitucional pela Pontifícia Universidade Católica de São Paulo. Bacharel em Direito pela Universidade Federal do Amazonas. Licenciando em História pela Universidade La Salle. Agente Técnico Jurídico do Ministério Público do Estado do Amazonas.

Resumo

Este artigo investiga a legitimidade do Ministério Público na atuação coletiva voltada à proteção de dados pessoais no Brasil. A partir da análise da Lei Geral de Proteção de Dados (LGPD), do Código de Defesa do Consumidor e da Lei da Ação Civil Pública, bem como de doutrina e jurisprudência recentes, demonstra-se que o Parquet detém competência legal e constitucional para instaurar inquéritos civis, firmar termos de ajustamento de conduta e ajuizar ações civis públicas em aspectos relacionados a proteção de dados pessoais. Com base no estudo, conclui-se que sua atuação é essencial para a efetividade dos direitos difusos, coletivos e individuais homogêneos em matéria de privacidade informacional, devendo ser aprimorada por meio de capacitação técnica, articulação institucional e estruturação de núcleos especializados.

Palavras-chave: Proteção de Dados Pessoais. Ministério Público. Direito Fundamental. Tutela Coletiva.

1. Introdução

A era digital intensificou a coleta, o processamento e o compartilhamento de dados pessoais em larga escala, tornando a proteção dessas informações um dos principais desafios jurídicos contemporâneos. Nesse contexto, o direito à privacidade, à autodeterminação informativa e à segurança no uso de dados pessoais passou a ocupar posição central no rol dos direitos fundamentais, exigindo mecanismos institucionais eficazes para sua salvaguarda.

A promulgação da Lei n.º 13.709/2018 — Lei Geral de Proteção de Dados Pessoais (LGPD) — representou um marco normativo relevante, ao estabelecer princípios, direitos e deveres que regulam o tratamento de dados, bem como prever mecanismos de responsabilização e fiscalização, proteção esta constitucionalizada por meio da Emenda nº. 115/2022, a qual incluiu o inciso LXXIX ao art. 5º, estabelecendo que é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. Contudo, para que tais garantias sejam efetivamente observadas, é essencial a atuação de órgãos com legitimidade e capacidade técnica para promover sua defesa em juízo e fora dele.

Nesse cenário, a tutela coletiva surge como instrumento jurídico essencial para a proteção de interesses transindividuais afetados por violações sistêmicas à proteção de dados. O Ministério Público, conforme previsão constitucional (art. 129, II, da CF) e legal (Leis nº. 7.347/1985 e 8.078/1990), desempenha papel de destaque na defesa desses direitos, com legitimidade para instaurar inquéritos civis, firmar termos de ajustamento de conduta e ajuizar ações civis públicas.

Desse modo, este artigo tem por objetivo analisar a legitimidade do Ministério Público na tutela coletiva da proteção de dados pessoais, à luz do ordenamento jurídico brasileiro. Busca-se demonstrar que o *Parquet* atua como agente fundamental na consolidação de uma cultura de proteção de dados, sendo responsável tanto pela repressão a condutas ilícitas quanto pela promoção de políticas públicas preventivas e estruturantes.

Para compreender o papel do Ministério Público nessa seara, é necessário, inicialmente, examinar o arcabouço normativo que estrutura a proteção de dados pessoais no Brasil, a fim de contextualizar os instrumentos jurídicos disponíveis e os sujeitos titulares de direitos.

2. A Proteção de Dados Pessoais no Brasil

A proteção de dados pessoais no ordenamento pátrio encontra-se, atualmente, consolidada pela LGPD, inspirada no Regulamento Geral de Proteção de Dados da

União Europeia (GDPR). Nesse sentido, a Lei n.º 13.709/2018 representa um marco regulatório no ordenamento jurídico brasileiro que harmoniza interesses privados e públicos, impondo limites ao tratamento de dados pessoais e criando garantias para os titulares. O art. 2º, III e V, da LGPD, assim estabelece:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I - o respeito à privacidade;
> II - a autodeterminação informativa;
> [...] *omissis* [...]
> IV - a inviolabilidade da intimidade, da honra e da imagem;

Obviamente, tais fundamentos legais da proteção de dados pessoais buscam pálio normativo na própria Constituição da República, principalmente quando ela garante que são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas (art. 5º, X, da CRFB), bem como ser inviolável o sigilo de dados (art. 5º, XII, da CRFB) e, finalmente, que é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais (art. 5º, LXXIX, da CRFB, incluído pela EC 115/2022). Diga-se que, antes mesmo da LGDP vir à lume, o E. STF já entendia pela proteção dos dados pessoais como direito fundamental, decorrente do art. 5º, *caput*, X e XII:

> Tais informações, relacionadas à identificação – efetiva ou potencial – de pessoa natural, configuram dados pessoais e integram, nessa medida, o âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII). Sua manipulação e tratamento, desse modo, hão de observar, sob pena de lesão a esses direitos, os limites delineados pela proteção constitucional. (ADI 6.387 MC-Ref/DF, Rel. Min. Rosa Weber, decisão monocrática, j. 24/04/2020)

O respeito à privacidade, inclusive, é o objetivo maior da LGDP, assim previsto em seu art. 1º: "Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural."

Neste aspecto, ganha relevo o direito à privacidade. No clássico artigo "*The Right to Privacy*", escrito a quatro mãos pelos juízes da Suprema Corte dos Estados Unidos Samuel D. Warren e Louis D. Brandeis, o **direito à privacidade** tem como objeto "a privacidade da vida privada." (WARREN; BRANDEIS, 1890). O escopo da proteção são os assuntos pessoais, em relação aos quais não se vislumbra interesse público

legítimo na sua revelação, e que o indivíduo prefere manter privados. Não obstante as diversas modificações no que se entende por privacidade frente às mudanças sociais, políticas e econômicas ocorridas ao longo dos séculos, permanece como denominador comum da privacidade e da autodeterminação o entendimento de que a privacidade somente pode ceder diante de justificativa consistente e legítima. Nos dizeres dos juízes:

> O desenho da lei deve ser proteger aquelas pessoas com cujos assuntos a comunidade não tem nenhuma preocupação legítima, de serem arrastadas para uma publicidade indesejável e indesejada e proteger todas as pessoas, seja qual for sua posição ou status, de ter assuntos que elas podem preferir manter privados tornados públicos contra sua vontade. É a invasão injustificada da privacidade individual que é repreendida e deve ser, na medida do possível, prevenida. (Warren e Brandeis, 1890, p. 214-215, tradução livre)

Tais aspectos históricos tornaram-se importantes marcos para a evolução do tema de proteção de dados pessoais. Foi por isso que LGPD tratou de definir dado pessoal como "informação relacionada a pessoa natural identificada ou identificável" (art. 5º, I) e estabeleceu princípios como finalidade, adequação, necessidade e transparência (art. 6º) para subsidiar o intérprete na tomada de decisões relativas ao tratamento de dados pessoais. Além disso, a legislação previu direitos aos titulares — acesso, correção, anonimização, bloqueio e eliminação de dados desnecessários (art. 18) —, e atribuiu à Autoridade Nacional de Proteção de Dados (ANPD) a fiscalização e aplicação de sanções (art. 52), essas últimas em casos, por exemplo, de responsabilização de empresas ou órgãos públicos em função de vazamento de dados, reconhecendo-se prejuízos morais coletivos em casos de incidentes de segurança.

Nesse sentido, consumidores e demais titulares contam com mecanismos de proteção previstos no Código de Defesa do Consumidor (CDC), que complementa a LGPD no plano sancionatório e reparatório (art. 6º, VI, CDC).

Também se destaca a importância dos relatórios de impacto à proteção de dados (RIPD), previstos no art. 38 da LGPD, como instrumento de prevenção de riscos aos direitos dos titulares. Outro ponto relevante é a interação entre a LGPD e normas setoriais específicas, como a Lei do Cadastro Positivo (Lei n.º 12.414/2011) e a Lei de Acesso à Informação (Lei n.º 12.527/2011).

Dessa forma, a atuação do Ministério Público deve considerar tanto a legislação geral quanto as disposições setoriais, o que reforça a necessidade de atuação multidisciplinar e integrada.

3. A Tutela Coletiva no Ordenamento Jurídico Brasileiro

A tutela coletiva é uma das mais relevantes inovações do direito processual contemporâneo, especialmente por sua capacidade de lidar com lesões a direitos transindividuais, que transcendem a esfera individual dos sujeitos. Essa forma de proteção jurídica visa a assegurar a efetividade de direitos que, por sua natureza coletiva, não podem ser adequadamente tutelados por meio das vias tradicionais do processo individual.

No ordenamento jurídico brasileiro, os direitos tuteláveis coletivamente são classificados doutrinariamente em três categorias distintas: direitos difusos, direitos coletivos *stricto sensu* e direitos individuais homogêneos. A definição legal desses conceitos se encontra no art. 81, parágrafo único, do Código de Defesa do Consumidor (Lei n.º 8.078/1990), que serve como base interpretativa para todas as ações coletivas, ainda que não envolvam diretamente relações de consumo.

Os direitos difusos são aqueles de titularidade indeterminada, indivisíveis, e que se originam de uma situação de fato comum, como é o caso da proteção ao meio ambiente ou à privacidade de usuários de uma plataforma digital.

Já os direitos coletivos *stricto sensu* são também indivisíveis, mas pertencem a um grupo, categoria ou classe determinada de pessoas, unidas por uma relação jurídica comum. Entende Kazuo Watanabe que a diferença entre direitos difusos e os coletivos pauta-se na determinabilidade, "seja através da relação jurídica-base que as une entre si (membros de uma associação de classe ou ainda acionistas de uma mesma sociedade), seja por meio do vínculo jurídico que as liga à parte contrária (contribuintes de um mesmo tributo, contratantes de um segurador com um mesmo tipo de seguro, estudantes de uma mesma escola etc.)" (1991, p. 625).

Nesse diapasão, Didier Jr. e Zaneti Jr. (2023, p. 114) "para fins de tutela jurisdicional, o que importa é a possibilidade de identificar um grupo, categoria ou classe, vez que a tutela se revela indivisível, e a ação coletiva não está "à disposição" dos indivíduos que serão beneficiados".

Por fim, os direitos individuais homogêneos são aqueles que, embora individuais, possuem origem comum, permitindo uma abordagem coletiva quanto à sua tutela, sobretudo quando a lesão é massiva e padronizada.

Quanto à legitimidade ativa, o art. 5º da Lei da Ação Civil Pública elenca os legitimados para a propositura de ações coletivas. São eles:

(a) **Ministério Público:** como defensor do interesse público e dos direitos fundamentais, possui legitimidade universal e ampla para tutela de qualquer dos direitos coletivos;

(b) **Defensoria Pública:** conforme o art. 134 da Constituição Federal e a Lei Complementar 80/1994, pode propor ações civis públicas em defesa de grupos vulneráveis, bem como em contextos de desigualdade informacional;

(c) **União, Estados, Municípios e Distrito Federal:** detêm legitimidade quando os interesses públicos sob sua responsabilidade estiverem sendo afetados;

(d) **Autarquias, empresas públicas, fundações e sociedades de economia mista:** possuem legitimidade restrita às suas áreas de atuação; e

(e) **Associações civis:** desde que estejam legalmente constituídas há pelo menos um ano e incluam, entre seus objetivos institucionais, a proteção dos interesses a serem tutelados.

No âmbito da defesa do consumidor, o CDC estabelece, em seu art. 82, a legitimidade de entidades civis para defender interesses difusos e coletivos, e, em seu art. 81, define o juízo competente e o rito processual especial. Dessa forma, mesmo não sendo expressa na LGPD, a aplicação subsidiária do CDC assegura a utilização do rito sumário para reclamações coletivas relacionadas à proteção de dados.

Outro mecanismo de tutela coletiva relevante é o incidente de resolução de demandas repetitivas (IRDR), previsto no Código de Processo Civil Brasileiro, que permite uniformizar decisões acerca de temas recorrentes de proteção de dados.

4. Tutela Coletiva: Legitimidade do Ministério Público

A atuação do Ministério Público na tutela coletiva dos direitos fundamentais é uma das mais marcantes expressões do seu papel institucional no Estado Democrático de Direito. A Constituição Federal de 1988, ao conferir ao Ministério Público autonomia funcional e administrativa (art. 127, §1º), fortaleceu sua posição como fiscal da lei e defensor da ordem jurídica e dos interesses sociais e individuais indisponíveis.

Em matéria de tutela coletiva, a legitimidade do Ministério Público está expressamente prevista em diversos diplomas legais. Como se vê, o art. 129, III, da Constituição estabelece como função institucional do órgão "promover o inquérito civil e a ação civil pública, para a proteção do patrimônio público e social, do meio ambiente e de outros interesses difusos e coletivos". A Lei da Ação Civil Pública (Lei n.º 7.347/1985), por sua vez, em seu art. 5º, inciso I,

reafirma essa legitimidade, autorizando expressamente o Ministério Público a propor ação civil pública para a defesa de direitos transindividuais, inclusive no que se refere à proteção de dados pessoais.

Entretanto, a legitimidade do Ministério Público, não se limita a uma previsão normativa. Ela decorre de sua missão constitucional de defesa dos direitos fundamentais, os quais, na contemporaneidade, incluem de forma inequívoca o direito à proteção de dados. A promulgação da Lei Geral de Proteção de Dados (LGPD – Lei n.º 13.709/2018), e posteriormente a elevação do direito à proteção de dados ao patamar de direito fundamental com a Emenda Constitucional n.º 115/2022, reforçam ainda mais o papel institucional do Ministério Público nesse campo.

Tal atuação em prol da tutela coletiva se torna ainda mais claro quando se pensa em nos – infelizmente – frequentes vazamentos de dados pessoais coletados por órgãos de crédito de consumidores, ou quando são coletados de forma indevida e/ou ilícita dados pessoais de idosos, menores, incapazes, pessoas em situação de vulnerabilidade ou outros grupos sobre os quais recaia especial guarida do *Parquet*.

Importante destacar que o Ministério Público, ao atuar em defesa da proteção de dados, pode adotar uma gama variada de instrumentos extrajudiciais e judiciais. No campo extrajudicial, destaca-se o inquérito civil público, que permite a investigação de condutas potencialmente lesivas, viabilizando a celebração de termos de ajustamento de conduta (TACs). No plano judicial, a ação civil pública é o principal mecanismo para buscar a responsabilização e a reparação coletiva.

Por outro lado, o Ministério Público também pode atuar em cooperação com órgãos reguladores, como a Autoridade Nacional de Proteção de Dados (ANPD), cuja atuação é essencialmente administrativa, mas que pode se articular com o *parquet* para viabilizar a responsabilização judicial dos agentes de tratamento de dados. Tal articulação institucional tem sido apontada como fundamental para o fortalecimento do sistema de *enforcement* da LGPD.

Por essa razão, a legitimidade do Ministério Público para a tutela coletiva da proteção de dados pessoais é ampla, expressamente prevista em lei e reforçada por sua missão constitucional. A atuação do *parquet* representa não apenas uma possibilidade jurídica, mas uma necessidade institucional diante da complexidade e da gravidade dos danos que podem decorrer da violação sistemática e em larga escala desses direitos fundamentais.

5. Considerações Finais

Este artigo buscou discutir a respeito da missão constitucional do Ministério Público brasileiro em sua legitimidade para capitanear tutela coletiva em função da proteção de dados pessoais. A análise revela que o Ministério Público possui

legitimidade incontestável para atuar na tutela coletiva da proteção de dados pessoais, com respaldo constitucional, legal e jurisprudencial. A LGPD, em cooperação com o CDC e a Lei da Ação Civil Pública, oferece robusto arcabouço para a defesa de direitos transindividuais, permitindo ao *parquet* promover ações civis públicas, inquéritos civis e firmar termos de ajustamento de conduta.

Entretanto, desafios persistem, como a necessidade de maior capacitação técnica dos membros e unidades especializadas, o aprimoramento da atuação conjunta com a ANPD e a uniformização de jurisprudência. Futuras pesquisas poderão avaliar os impactos efetivos das ações coletivas na cultura de privacidade e na redução de incidentes de tratamento de dados.

Referências

DIDIER JR., Fredie. ZANETI Jr., Hermes. *Curso de Direito Processual Civil*: Processo Coletivo. 17 ed. Salvador: JusPodivm, 2023.

WARREN, Samuel D.; BRANDEIS, Luis D. *The Right to Privacy*. Harvard Law Review, Cambridge, v. IV, n. 5, december 15, p. 193-220, 1890.

WATANABE, Kazuo. *Acesso à Justiça e Processo Coletivo*: Estudos e pareceres. São Paulo: Revista dos Tribunais, 2019.

3

A Defensoria Pública do Amazonas como Controladora de Dados: Responsabilidades e Desafios no Tratamento de Dados de Populações Vulneráveis

Defensoria Pública do Estado do Amazonas

Experiência da Defensoria Pública no atendimento a populações vulneráveis com enfoque especial em comunidades tradicionais e povos indígenas.

Rudson Fernandes Nunes

Diretor adjunto da Diretoria Geral / Encarregado de Proteção de Dados
Formado em Análise de Sistema / Especialista em Gestão de Projeto / Especialista em Segurança Digital, Governança e Gestão de Dados.

Resumo

O artigo oferece uma análise técnica e humanizada sobre o impacto da Lei Geral de Proteção de Dados Pessoais (LGPD – Lei n. 13.709/2018) na atuação da Defensoria Pública do Estado do Amazonas (DPE-AM). Mais do que uma mera adequação legal, o texto ressalta que este novo marco representa uma "reinvenção das práticas institucionais" para uma entidade cujo público-alvo é majoritariamente composto por cidadãos em situação de alta vulnerabilidade, que enfrentam riscos elevados de exposição, discriminação e revitimização no tratamento de seus dados. As responsabilidades da DPE-AM vão além das disposições gerais da LGPD. O contexto amazônico e o perfil dos assistidos impõem responsabilidades adicionais. A DPE-AM, ao desenvolver um modelo próprio de proteção de dados que respeita tanto os princípios legais quanto as particularidades regionais, tem o potencial de estabelecer referências importantes não apenas para outras Defensorias, mas para todo o sistema de justiça brasileiro. Trata-se de um chamado à criatividade, flexibilidade e sensibilidade cultural, características que a Defensoria já aplica em outras frentes de sua atuação.

Palavras-chave: Proteção de Dados Pessoais. Defensoria Pública. Populações Vulneráveis.

1. Introdução

A Lei Geral de Proteção de Dados Pessoais (LGPD – Lei n. 13.709/2018) transformou profundamente a forma como empresas públicas e privadas tratam dados pessoais. No Amazonas, esse impacto é ainda maior. Além da exigência legal, o território apresenta desafios únicos: sua vasta extensão, realidades socioeconômicas complexas, a forte presença de comunidades tradicionais e a persistente exclusão digital. Para a Defensoria Pública do Estado do Amazonas – DPE-AM, o novo marco legal representa não apenas um desafio administrativo, mas um chamado ético-político à revisão e reinvenção das práticas de tratamento de dados pessoais, pois o público-alvo da assistência jurídica gratuita é justamente composto, em sua maioria, por cidadãos que correm riscos elevados de exposição, discriminação e revitimização.

Neste artigo, propomos uma reflexão sobre o papel da Defensoria Pública do Amazonas como controladora de dados pessoais de populações vulneráveis. Nossa abordagem prioriza um olhar humanizado, focado na experiência real daqueles que vivem à margem dos direitos sociais e, ainda mais, das políticas de informação. Queremos dar destaque ao aspecto vivencial do tratamento de dados, evitando o formalismo excessivo e discussões puramente tecnicistas, mas sempre mantendo a fidelidade aos parâmetros legais e doutrinários.

2. A Defensoria Pública do Estado do Amazonas, a LGPD e as Populações Vulneráveis

2.1 Estrutura da DPE-AM

A Defensoria Pública do Estado do Amazonas foi criada pela Lei Complementar Estadual nº 01, de 30 de março de 1990, e reorganizada pela Lei Complementar Estadual nº 01, de 30 de março de 2004. Atualmente, a instituição conta com aproximadamente 155 (cento e cinquenta e cinco) defensores públicos, distribuídos entre a capital e interior, além de cerca de 467 (quatrocentos e sessenta e sete servidores, 245 (duzentos e quarenta e cinco) residentes e 530 (quinhentos e trinta) estagiários.

A estrutura da DPE-AM compreende órgãos de administração superior, órgãos de atuação (Defensorias Públicas de 1ª e 2ª Instâncias) e órgãos auxiliares, como Núcleos Especializados.

Entre os Núcleos Especializados, destacam-se aqueles que atendem populações em situação de especial vulnerabilidade:

- Núcleo de Defesa dos Direitos Humanos e Coletivos (NDDHC)

- Núcleo de Atendimento Prisional (NAP)
- Núcleo de Defesa da Mulher (NUDEM)
- Núcleo de Defesa da Criança e do Adolescente (NUDECA)
- Núcleo de Atendimento às Comunidades Tradicionais
- Núcleo de Defesa do Consumidor (NUDECON)
- Núcleo de Defesa da Pessoa Idosa e da Pessoa com Deficiência
- Núcleo de Defesa da Saúde (NUDESA)

A atuação da DPE-AM estende-se por diversas áreas do direito, incluindo família, cível, criminal, fazenda pública, execução penal, infância e juventude, além de ações coletivas e atendimento extrajudicial. Em 2024, segundo a DPE/AM (2024) foram realizados de 817.288 atos, que incluem as diversas atividades desempenhadas pela instituição, como atendimentos, petições, ações judiciais e o acionamento de órgãos competentes.

2.2 Os primeiros passos da LGPD na DPE-AM: uma trajetória em construção

A jornada de adequação da Defensoria Pública do Estado do Amazonas à Lei Geral de Proteção de Dados começou ainda em 2019, quando a administração superior do Órgão, atenta às mudanças legislativas que se avizinhavam, passou a investir na aquisição de conhecimento técnico por meio da contratação de cursos especializados sobre a Lei Geral de Proteção de Dados. Naquele momento, poucos órgãos públicos na região Norte demonstravam preocupação com a temática, o que evidenciava certo pioneirismo institucional, ainda que motivado pela necessidade de conformidade legal.

O marco formal desse processo ocorreu em setembro de 2020, com a publicação das Portarias nº 591/2020-GDPG/DPE/AM e nº 593/2020-GDPG/DPE/AM na edição 1.303 do Diário Oficial da DPE/AM. Por meio desses instrumentos, foram instituídos, respectivamente, o primeiro Comitê Gestor de Proteção de Dados e a designação do Encarregado de Dados.

Entre 2020 e os dias atuais, a DPE-AM colocou em prática uma série de ações estruturantes que criaram alicerces para a proteção de dados na instituição. Esse trabalho demonstra o real compromisso da Defensoria com a segurança das informações dos assistidos. Seguindo esse caminho, a Defensoria continua aperfeiçoando seus métodos e práticas dia após dia, adaptando-se às novas exigências legais num processo natural de crescimento que fortalece, a cada passo, todo seu sistema de proteção de dados pessoais.

A relevância desse compromisso é destacada na literatura sobre inovação na

gestão pública, que aponta a segurança da informação como prioridade gerencial. Conforme afirma Fiel et al. (2023, p. 173): A segurança da informação tem que ser alvo da atenção do gestor público, que deve considerar a utilização de softwares, hardwares apropriados e investimentos constante em pessoas, treinamento e incorporar na cultura da instituição mantras de segurança da informação.

Entre as iniciativas podemos citar a elaboração da Política de Proteção de Dados Pessoais, criação de página específica sobre LGPD no sítio eletrônico institucional, a realização de mapeamentos sistemáticos dos fluxos de dados e a produção de pareceres técnicos sobre situações específicas enfrentadas no cotidiano defensorial.

No campo da formação continuada, a instituição incorporou a temática da proteção de dados nos diversos níveis de sua estrutura humana: defensores públicos recém-empossados passaram a receber treinamento específico durante os cursos de formação; novos servidores, também participam de palestras de proteção de dados durante as integrações funcionais; assim como, estagiários e residentes foram incluídos nesse processo educativo – uma abordagem abrangente que reconhece que a cultura de proteção de dados precisa permear todos os níveis organizacionais.

Nos aspectos contratuais e de governança, houve revisão dos instrumentos vigentes para inclusão de cláusulas específicas sobre proteção de dados, implementação da rotina de encaminhamento à Assessoria de Proteção de Dados os processos para formação de novos contratos, acordos e elaboração de Relatórios de Impacto à Proteção de Dados Pessoais (RIPD), além da disponibilização de canal direto de comunicação com o Encarregado através do site institucional, facilitando o exercício de direitos pelos titulares.

Atualmente, a estrutura dedicada à proteção de dados pessoais na DPE-AM é representada pela Assessoria de Proteção de Dados Pessoais - APDP, que opera com uma configuração composta pelo Encarregado, seu substituto e uma estagiária. Uma equipe que além das funções comunicativas, também exercem funções técnicas que constam como boas práticas em proteção de dados.

A equipe da Assessoria de Proteção de Dados Pessoais, embora eficiente, encontra desafios proporcionais à complexidade e abrangência das demandas institucionais. Em reconhecimento à importância estratégica desta área, um novo Comitê Gestor foi instituído pela Portaria nº 383/2025-GDPG/DPE/AM, publicada na edição nº 2368 do diário oficial em 28 de fevereiro de 2025, renovando o compromisso institucional e ampliando a representatividade das diversas áreas da Defensoria.

Apesar desses avanços, a cada novo mapeamento de dados realizado pela APDP revela camadas adicionais de complexidade. Os desafios se multiplicam quando o tratamento envolve dados de pessoas em situação de vulnerabilidade – justamente o público-alvo da instituição. As entrevistas com defensores e servidores

que atuam na linha de frente evidenciam que a proteção de dados, no contexto amazônico e de extrema vulnerabilidade social, exige muito mais que adaptações procedimentais: demanda uma verdadeira reinvenção das práticas institucionais e um olhar culturalmente sensível às realidades locais.

2.3 Realidade Sociojurídica Amazônica

O Estado do Amazonas possui uma das mais baixas densidades demográficas do Brasil, vasto território cortado por rios, floresta e comunidades afastadas dos centros urbanos. Poucos domicílios no estado possuem acesso regular à internet, uma taxa que despenca em regiões rurais e aldeias indígenas. Isso significa barreiras imensas não apenas no acesso aos direitos, mas também na compreensão e exercício dos novos direitos informacionais previstos em lei.

A DPE/AM, ao realizar sua missão constitucional de garantir assistência jurídica à população hipossuficiente, atua diretamente nessas rotas incertas, seja com atuações itinerantes, seja por meio dos núcleos especializados ou polos do interior. Na trajetória desse trabalho, coleta informações imprescindíveis, de dados básicos como nome, origem e renda, até registros especialmente sensíveis, como a história familiar, situação de saúde, etnia, identidade de gênero, entre outros.

2.4 Limitações Orçamentárias e de Infraestrutura

Além das questões geográficas e culturais, a implementação efetiva da LGPD na DPE-AM enfrenta outros desafios significativos; eles tocam na própria base material da instituição: o orçamento e a infraestrutura. A Defensoria opera com um duodécimo fixado em 1,6% da Receita Líquida Tributária do Estado. Segundo a DPE/AM (2025), esse percentual não sofre reajuste desde 2021.

Essa estagnação orçamentária, em um cenário de inflação e aumento das demandas, impacta diretamente a capacidade de investimento. Torna-se um obstáculo concreto para a aquisição de tecnologia de ponta, a contratação e retenção de pessoal especializado em segurança da informação e proteção de dados, e a realização de mudanças estruturais necessárias para a plena conformidade com a LGPD. A carência de recursos, em particular, impede a aplicação dos fundamentos de segurança da informação e a implementação dos controles técnicos e administrativos essenciais para proteger os dados dos assistidos.

2.5 Enquadramento Normativo: Controladora de Dados e Responsabilidade Social

A Defensoria Pública do Estado do Amazonas, como órgão público dotado de autonomia funcional, administrativa e orçamentária, enquadra-se como controladora de dados nos termos do artigo 5º, VI, da LGPD, sendo responsável pelas decisões referentes ao tratamento de dados pessoais que realiza no exercício de suas atribuições legais e constitucionais.

Este enquadramento como controladora implica em responsabilidades específicas estabelecidas pela LGPD, incluindo:

- Observância dos princípios estabelecidos no artigo 6º (finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas);
- Garantia dos direitos dos titulares previstos no artigo 18 (confirmação da existência de tratamento, acesso aos dados, correção, anonimização, portabilidade, eliminação, informação sobre compartilhamento etc.);
- Implementação de medidas de segurança técnicas e administrativas (artigo 46), conforme preconizam as boas práticas e normas internacionais de segurança da informação. De acordo com Hintzbergen et al. (2018, p. 20), os princípios mais importantes em todos os programas de segurança são a confidencialidade, integridade e disponibilidade.
- Elaboração de relatório de impacto à proteção de dados pessoais quando solicitado pela ANPD (artigo 38);
- Indicação de encarregado pelo tratamento de dados pessoais (artigo 41);
- Comunicação à ANPD e aos titulares em caso de incidente de segurança relevante (artigo 48);
- Manutenção de registros das operações de tratamento realizadas (artigo 37).

Importante ressaltar que, em determinadas situações, a DPE-AM pode atuar também como operadora de dados, quando realiza tratamento em nome de outro controlador, como nos casos de convênios com outros órgãos públicos ou quando atua em programas interinstitucionais.

No contexto da atuação da DPE-AM, as principais bases legais aplicáveis são:

- Cumprimento de obrigação legal ou regulatória (art. 7º, II): A coleta e o tratamento de dados necessários para o cumprimento da missão constitucional da Defensoria (art. 134 da CF/88) e de suas atribuições legais (LC 80/94 e LC Estadual 01/2004) enquadram-se nesta hipótese. Exemplos incluem dados coletados para verificação da hipossuficiência econômica e para a prestação da assistência jurídica.
- Execução de políticas públicas (art. 7º, III): Como órgão público responsável pela implementação da política pública de acesso à justiça, a DPE-AM pode tratar dados pessoais necessários para esta finalidade. Exemplos incluem dados coletados em projetos de educação em direitos, mutirões de atendimento e programas de resolução extrajudicial de conflitos.

- Exercício regular de direitos em processo (art. 7º, VI): O tratamento de dados necessários para o exercício da defesa dos assistidos em processos judiciais e administrativos enquadra-se nesta hipótese. Exemplos incluem dados coletados para elaboração de petições, produção de provas e acompanhamento processual.
- Tutela da saúde (art. 7º, VIII): Em casos envolvendo direito à saúde, como ações para fornecimento de medicamentos ou tratamentos médicos, esta base legal pode ser aplicável, especialmente quando o assistido não está em condições de fornecer consentimento.
- Proteção da vida ou da incolumidade física (art. 7º, VII): Em situações emergenciais, como casos de violência doméstica ou ameaças à vida, esta base legal autoriza o tratamento de dados necessários para a proteção do titular.
- Consentimento (art. 7º, I): Embora não seja a base legal predominante para a atuação da Defensoria, o consentimento pode ser necessário em situações específicas, como uso de imagem ou depoimento de assistidos para fins institucionais.

Para dados pessoais sensíveis (art. 5º, II), que são frequentemente tratados pela DPE-AM em casos envolvendo saúde, origem racial ou étnica, orientação sexual, entre outros, aplicam-se as hipóteses mais restritas do artigo 11, com destaque para:

- Cumprimento de obrigação legal ou regulatória (art. 11, II, "a");
- Tutela da saúde (art. 11, II, "f");
- Proteção da vida ou da incolumidade física (art. 11, II, "e");
- Exercício regular de direitos em processo (art. 11, II, "d").

A identificação da base legal adequada para cada operação de tratamento é fundamental para determinar as obrigações específicas da DPE-AM, os direitos exercíveis pelos titulares e as medidas de segurança aplicáveis.

A DPE-AM, além das responsabilidades gerais estabelecidas pela LGPD para todos os controladores, enfrenta responsabilidades específicas decorrentes do contexto amazônico e do perfil de seus assistidos:

Adaptação cultural da proteção de dados: Responsabilidade de adaptar procedimentos e comunicações sobre proteção de dados às diversas realidades culturais dos assistidos, incluindo povos indígenas, comunidades tradicionais e populações ribeirinhas.

Acessibilidade comunicacional: Dever de garantir que informações sobre tratamento de dados sejam compreensíveis para pessoas com diferentes níveis de

escolaridade, incluindo analfabetos ou indivíduos com baixo letramento.

Proteção de conhecimentos tradicionais: Responsabilidade especial quanto ao tratamento de dados que possam envolver conhecimentos tradicionais associados à biodiversidade, práticas culturais ou territorialidades específicas de povos e comunidades tradicionais.

Garantia de não discriminação algorítmica: Dever de assegurar que eventuais sistemas automatizados utilizados pela instituição não reproduzam ou ampliem discriminações históricas contra grupos vulneráveis da região amazônica.

Proteção contra exploração de dados: Responsabilidade de proteger dados de populações vulneráveis contra uso indevido por terceiros.

Adequação a realidades de baixa conectividade: Dever de desenvolver procedimentos alternativos para exercício de direitos dos titulares em regiões sem acesso à internet ou com conectividade limitada.

Estas responsabilidades específicas exigem da DPE-AM uma abordagem contextualizada da LGPD, que considere as particularidades regionais e as vulnerabilidades específicas de seus assistidos, indo além do mero cumprimento formal da legislação.

2.6 Natureza dos Dados e Riscos Enfrentados

Os dados coletados diariamente pela Defensoria vão muito além de simples registros cadastrais. Envolvem relatos de violência doméstica, detalhamento de vulnerabilidades sociais, histórico de saúde mental, pertencimento étnico e informações sobre migração, refúgio e territorialidade, entre outros. O risco de exposição desses dados é múltiplo: trata-se não só de evitar constrangimentos, mas de proteger a própria integridade do titular e de coletivos – como ocorre com dados sobre territórios indígenas ameaçados por invasores ou interesses econômicos.

Não à toa, a doutrina alerta para o "dilema identitário" na proteção de dados de grupos vulneráveis: para eles, um vazamento pode representar mais do que uma ofensa à privacidade. Pode resultar em perseguição, discriminação ou recrudescimento da exclusão social (Doneda, 2019, p. 77).

3. Os Fluxos de Dados na Defensoria: entre a Teoria e o Cotidiano

3.1 Mapeamento dos Principais Fluxos de Dados

Toda implementação efetiva da LGPD requer a compreensão detalhada dos fluxos informacionais existentes na empresa ou instituição. A partir de análise documental e entrevistas com gestores e servidores da Defensoria, identificamos os seguintes fluxos críticos de tratamento de dados pessoais:

- Triagem e avaliação de hipossuficiência: Processo inicial de atendimento que envolve a coleta de dados socioeconômicos para verificação da elegibilidade do assistido. Inclui informações sobre renda, composição familiar, patrimônio, despesas mensais e documentos comprobatórios.
- Atendimento jurídico inicial: Registro da demanda jurídica do assistido, incluindo narrativa dos fatos, documentos pessoais básicos e informações preliminares sobre a questão jurídica apresentada.
- Atendimento especializado por núcleos temáticos: Coleta de dados específicos conforme a área de atuação (família, criminal, direitos humanos etc.), frequentemente incluindo dados sensíveis como informações de saúde, orientação sexual, origem racial ou étnica.
- Atendimento multidisciplinar: Registro de avaliações psicossociais, laudos técnicos e relatórios elaborados por equipes de psicologia, serviço social e outras especialidades que apoiam a atuação jurídica.
- Elaboração e acompanhamento processual: Sistematização dos dados coletados para elaboração de peças processuais, produção de provas e acompanhamento de processos judiciais e administrativos.
- Atendimento itinerante: Coleta e tratamento de dados durante deslocamentos a comunidades remotas, frequentemente realizada em condições logísticas desafiadoras e com limitações tecnológicas.
- Educação em direitos: Registro de participantes em atividades educativas, palestras e oficinas realizadas pela Defensoria em comunidades, escolas e outros espaços.
- Gestão de convênios e parcerias: Compartilhamento de dados com outros órgãos públicos e organizações parceiras para viabilizar atendimentos integrados ou encaminhamentos.
- Comunicação institucional: Utilização de dados e imagens de assistidos em materiais de divulgação, relatórios de atividades e campanhas institucionais.

- Gestão de recursos humanos: Tratamento de dados pessoais de defensores e servidores para fins administrativos.

Cada um destes fluxos apresenta riscos específicos e demanda medidas apropriadas de proteção, considerando a natureza dos dados tratados, o volume de titulares afetados e as particularidades do contexto amazônico.

3.2 Desafios Específicos nos Fluxos Informacionais

A análise dos fluxos informacionais da DPE-AM revela características específicas do contexto institucional que orientam a evolução contínua da implementação da LGPD:

- Documentação incompleta ou informal: Muitos assistidos, especialmente de comunidades tradicionais, não possuem documentação completa ou formalizada, dificultando procedimentos padrão de identificação e verificação de identidade.
- Barreiras linguísticas: A diversidade linguística do Amazonas, com dezenas de línguas indígenas, cria desafios para a obtenção de consentimento informado e para a comunicação clara sobre direitos dos titulares.
- Conectividade intermitente: Algumas unidades da Defensoria, especialmente no interior do estado, enfrentam problemas de conectividade que dificultam a sincronização de dados e a implementação de medidas de segurança em tempo real.
- Necessidade de documentação audiovisual: Em comunidades com tradição oral ou baixo letramento, o registro audiovisual frequentemente substitui documentação escrita, gerando desafios específicos para armazenamento e proteção.
- Limitações de infraestrutura física: Algumas unidades funcionam em espaços adaptados, exigindo maiores cuidados para garantir a confidencialidade dos atendimentos ou a segurança do armazenamento de documentos.
- Predominância do transporte fluvial: Grande parte do estado é acessível apenas por via fluvial, com deslocamentos que podem durar dias ou semanas. Isso cria desafios para manutenção de equipamentos eletrônicos e resposta rápida a incidentes de segurança.
- Isolamento sazonal de comunidades: Durante os períodos de seca dos rios (julho a novembro), muitas comunidades ficam ainda mais isoladas, dificultando o acesso de equipes técnicas para manutenção de sistemas ou treinamento de pessoal.

- Infraestrutura elétrica instável: Parte dos municípios amazonenses enfrentam problemas recorrentes de fornecimento de energia elétrica, com oscilações e interrupções frequentes que comprometem a operação de sistemas eletrônicos e aumentam riscos de perda de dados.

Estes desafios exigem soluções criativas e adaptadas ao contexto amazônico, que conciliem a necessidade de proteção de dados com as realidades operacionais da DPE-AM e as características específicas de seus assistidos.

3.3 Dados Sensíveis e Grupos Especialmente Vulneráveis

A DPE-AM lida rotineiramente com dados sensíveis de grupos em situação de especial vulnerabilidade, o que demanda atenção redobrada quanto à proteção de dados. Destacam-se:

- Povos indígenas: O tratamento de dados de povos indígenas envolve questões complexas relacionadas a direitos coletivos, conhecimentos tradicionais e autodeterminação. Informações sobre práticas culturais, territorialidades e organização social podem ser extremamente sensíveis, especialmente em contextos de conflitos fundiários ou ameaças à integridade territorial.
- Vítimas de violência doméstica: Os Núcleos de Defesa da Mulher e da Criança e do Adolescente tratam dados extremamente sensíveis relacionados a violência física, sexual e psicológica. A proteção inadequada desses dados pode resultar em revitimização ou mesmo riscos à segurança física das vítimas.
- Pessoas privadas de liberdade: O Núcleo de Atendimento Prisional lida com dados de pessoas em situação de extrema vulnerabilidade institucional, cujo vazamento pode resultar em estigmatização permanente ou mesmo riscos à integridade física dentro do sistema prisional.
- Pessoas com transtornos mentais: Casos envolvendo saúde mental frequentemente incluem laudos psiquiátricos, históricos de internação e outras informações extremamente sensíveis, cuja exposição indevida pode resultar em discriminação e prejuízos à reintegração social.
- Crianças e adolescentes em situação de risco: O NUDECA trata dados de menores em situação de vulnerabilidade, incluindo vítimas de abuso, exploração sexual, trabalho infantil e outras violações graves, exigindo proteção reforçada conforme o artigo 14 da LGPD.
- Migrantes e refugiados: Dados sobre status migratório, razões de refúgio e condições de vulnerabilidade de migrantes internacionais requerem proteção especial, considerando riscos de xenofobia e potenciais impactos em processos de regularização migratória.

- Comunidades em conflitos socioambientais: Dados coletados em ações coletivas envolvendo conflitos socioambientais podem expor lideranças comunitárias a riscos concretos, considerando o histórico de violência em questões ambientais na Amazônia.

Para estes grupos, a adequação da DPE-AM à LGPD deve ir além do cumprimento formal da lei, incorporando uma abordagem baseada em direitos humanos que reconheça as vulnerabilidades específicas e os riscos diferenciados associados ao tratamento de seus dados pessoais.

4. Caminhos para uma Proteção de Dados Humanizada

4.1 Políticas de Capacitação e Educação Digital

O respeito à LGPD só é possível com capacitação continuada não apenas para servidores e defensores, mas também para assistidos e redes de apoio. Materiais educativos precisam ser disponibilizados em múltiplos formatos — texto, áudio, vídeo, ilustrativos — respeitando costumes, línguas maternas e realidades locais. Incentivar o letramento digital é investir no exercício da cidadania informacional.

4.2 Protocolos Específicos Para Grupos Vulneráveis

Considerando as vulnerabilidades específicas dos assistidos da DPE-AM, medidas diferenciadas para proteção de seus dados estão sendo delineadas, buscando contemplar, entre outros aspectos:

- Protocolos específicos para povos indígenas: Desenvolvimento de protocolos que respeitem processos próprios de tomada de decisão, incorporem consulta prévia quando aplicável e reconheçam direitos coletivos sobre determinados tipos de dados.
- Medidas reforçadas para vítimas de violência: Implementação de controles de acesso mais rigorosos, pseudonimização sistemática e compartimentalização de informações para dados de vítimas de violência doméstica, sexual ou institucional.
- Proteção especial para dados de crianças e adolescentes: Adoção de medidas adicionais de segurança para dados de menores em situação de vulnerabilidade, incluindo anonimização em relatórios, restrição de compartilhamento e revisão periódica da necessidade de retenção.
- Salvaguardas para comunidades em conflitos territoriais: Implementação de protocolos especiais para tratamento de dados relacionados a comunidades envolvidas em conflitos fundiários ou socioambientais, considerando riscos específicos de perseguição ou retaliação.

- Proteção de conhecimentos tradicionais associados: Estabelecimento de salvaguardas específicas para dados que possam envolver conhecimentos tradicionais associados à biodiversidade ou práticas culturais, respeitando protocolos comunitários existentes.
- Gestão diferenciada de consentimento: Implementação de formas culturalmente apropriadas de obtenção e registro de consentimento, que possam incluir gravações de áudio em línguas nativas, testemunhas comunitárias ou outras adaptações necessárias.
- Avaliações de impacto participativas: Realização de avaliações de impacto à proteção de dados com participação ativa dos grupos potencialmente afetados, incorporando suas percepções sobre riscos e medidas mitigadoras.
- Canais de denúncia acessíveis e seguros: Criação de canais diversificados para denúncia de incidentes relacionados a dados pessoais, incluindo opções não digitais e possibilidade de denúncias anônimas ou por intermediários confiáveis.
- Revisão periódica de impactos não previstos: Estabelecimento de mecanismos para identificação e correção de impactos negativos não previstos das práticas de proteção de dados sobre grupos vulneráveis específicos.

Estas medidas reconhecem que a proteção de dados de grupos vulneráveis não pode seguir abordagens padronizadas, exigindo adaptações que considerem vulnerabilidades específicas, contextos culturais diversos e riscos diferenciados.

Conclusão

A análise desenvolvida ao longo deste artigo permite identificar que as adequações à LGPD na Defensoria Pública do Estado do Amazonas representam simultaneamente um desafio significativo e uma oportunidade estratégica para fortalecimento institucional e aprimoramento da proteção dos direitos dos assistidos.

Como controladora de dados pessoais, a DPE-AM possui responsabilidades legais abrangentes, que se tornam ainda mais complexas considerando o perfil de seus assistidos – majoritariamente pessoas em situação de vulnerabilidade socioeconômica – e as particularidades geográficas, culturais e estruturais do estado do Amazonas.

Os principais desafios identificados incluem limitações orçamentárias e de infraestrutura, barreiras geográficas e logísticas, diversidade linguística e cultural, baixos índices de letramento digital e necessidades específicas de proteção para dados sensíveis de grupos especialmente vulneráveis.

Apesar destes desafios, muitas iniciativas já foram realizadas e outras estão em curso na DPE-AM. As estratégias propostas – governança adaptada ao contexto amazônico, soluções tecnológicas apropriadas, capacitação culturalmente sensível e medidas específicas para grupos vulneráveis – oferecem caminhos viáveis para uma implementação abrangente da LGPD.

As adequações à LGPD na Defensoria Pública do Estado do Amazonas não devem ser vistas apenas como uma obrigação legal a ser cumprida, mas como uma oportunidade para repensar práticas institucionais, fortalecer a confiança dos assistidos e aprimorar a proteção de seus direitos fundamentais.

O desafio de adequar-se à LGPD no contexto amazônico exige criatividade, flexibilidade e sensibilidade cultural, características que a DPE-AM já demonstra em outras áreas de sua atuação. Ao desenvolver um modelo próprio de proteção de dados, que respeite simultaneamente os princípios legais e as particularidades regionais, a instituição pode estabelecer referências importantes não apenas para outras Defensorias, mas para todo o sistema de justiça brasileiro.

Referências

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais*. Diário Oficial da União: seção 1, Brasília, DF, v. 160, n. 157, p. 1-7, 15 ago. 2018.

DEFENSORIA PÚBLICA DO ESTADO DO AMAZONAS. *Defensoria do Amazonas fecha 2024 com mais de 817 mil atos realizados e 10 novas unidades inauguradas*. 2024. Disponível em: https://defensoria.am.def.br/2024/12/31/defensoria-do-amazonas-fecha-2024-com-mais-de-817-mil-atos-realizados-e-10-novas-unidades-inauguradas/#:~:text=A%20Defensoria%20P%C3%BAblica%20do%20Estado,Em%202023%2C%20foram%20801.145%20atos. Acesso em: 23 maio 2025.

DEFENSORIA PÚBLICA DO ESTADO DO AMAZONAS. *Defensoria Pública do Amazonas mais que triplica atendimentos no interior do Estado em quatro anos*. 2025. Disponível em: https://defensoria.am.def.br/2025/05/07/defensoria-publica-do-amazonas-mais-que-triplica-atendimentos-no-interior-do-estado-em-quatro-anos/. Acesso em: 23 maio 2025.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*: fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Revista dos Tribunais, 2019.

FIEL, Alécio et al. Inovação na Gestão Pública: cultura, liderança, normas, métodos, tecnologia e aplicação. 1. ed. São Paulo: Savier Editora, 2023.

HINTZBERGEN, Jule et al. *Fundamentos de segurança da informação*: com base na ISO 27001 e na ISO 27002. Rio de Janeiro: Brasport, 2018.

Administração Pública e Trabalhadores Terceirizados – A necessária proteção de dados

Tribunal Regional do Trabalho da 11ª Região

Análise das responsabilidades e desafios na proteção de dados de trabalhadores terceirizados no contexto da administração pública.

Carolina de Souza Lacerda Aires França

Juíza do Trabalho Titular da 9ª Vara do Trabalho de Manaus. Vice-diretora da Escola Judicial do TRT 11-EJUD11 (biênios 2018-2020 e 2020-2022). Juíza Auxiliar da Presidência do TRT11 (biênio 2022-2024). Bacharel em Direito e Especialista em Direito Tributário pela Universidade Federal do Amazonas (UFAM).

Diego Enrique Linares Troncoso

Juiz do Trabalho do Tribunal Regional do Trabalho da 11ª Região (Amazonas e Roraima). Bacharel em Direito pela Universidade de São Paulo (USP) e Especialista em Direito do Trabalho e Direito Processual do Trabalho pela Universidade Presbiteriana Mackenzie (UPM).

Resumo

O artigo aborda a necessidade de proteção de dados pessoais dos trabalhadores terceirizados no âmbito da Administração Pública, especialmente após a entrada em vigor da Lei Geral de Proteção de Dados Pessoais (LGPD). Embora a terceirização seja permitida para atividades acessórias, a Administração Pública, ao receber e tratar dados desses trabalhadores, torna-se controladora dessas informações, assumindo deveres legais de proteção, transparência e segurança. O texto enfatiza que os dados pessoais frequentemente compartilhados — como CPF, endereço, biometria e até informações de saúde — são sensíveis e, quando tratados sem critérios legais e medidas de proteção adequadas, expõem os trabalhadores a riscos de violação da privacidade e constrangimentos no ambiente de trabalho. A LGPD impõe que o tratamento de dados siga princípios como finalidade, necessidade e proporcionalidade, o que muitas vezes não é observado nos contratos administrativos. Além das obrigações legais, os autores ressaltam que a proteção de dados deve ser compreendida como expressão da dignidade da pessoa humana, princípio constitucional que deve orientar todas as ações do Poder Público. O trabalhador terceirizado, por estar em posição de vulnerabilidade contratual, institucional e informacional, requer especial atenção do Estado quanto à sua proteção informacional. O artigo ainda destaca os desafios específicos enfrentados no Estado do Amazonas, como deficiências tecnológicas, ausência de políticas de governança de dados e baixa capacitação dos agentes públicos, especialmente em regiões do interior. Propõem-se soluções como a capacitação dos gestores, formalização de cláusulas específicas sobre dados nos contratos administrativos, criação de órgãos internos especializados e o fortalecimento de redes interinstitucionais como a Rede Amazonense de Proteção de Dados. Conclui-se que o respeito à privacidade e à proteção de dados dos trabalhadores terceirizados deve ser tratado com o mesmo rigor conferido aos servidores efetivos, não apenas como obrigação legal, mas como um dever ético e constitucional.

Palavras-chave: Proteção de Dados Pessoais. Trabalhadores Terceirizados. Administração Pública.

1. Introdução

Apesar de o Supremo Tribunal Federal (STF), ao julgar a ADPF 324 e o RE 958.252, com repercussão geral (Tema 725), ter reconhecido a constitucionalidade da terceirização irrestrita na iniciativa privada, inclusive para atividades-fim, quando se trata de terceirização pela Administração Pública, esta deve sempre obedecer ao regime jurídico-administrativo e aos princípios do concurso público (art. 37, II, da Constituição Federal), já que o Tribunal de Contas da União adota como entendimento predominante que a terceirização no setor público só é admissível para atividades acessórias, instrumentais ou de apoio, como vigilância, limpeza, recepção e suporte técnico.

Mesmo assim, ela é amplamente utilizada pelo Estado para garantir a continuidade dos serviços públicos e a contenção de despesas com pessoal, mas enfrenta com frequência problemas contratuais, como atrasos de salários e não pagamentos de direitos trabalhistas pelas empresas terceirizadas, levando à grande judicialização pelos trabalhadores que buscam a responsabilização subsidiária do ente público. Por isso, a adequada fiscalização dos contratos de terceirização é essencial para garantir legalidade, eficiência e proteção dos direitos dos trabalhadores envolvidos.

Além disso, após a entrada em vigor da Lei 13.709/2018 – Lei Geral de Proteção de Dados – e da introdução na Constituição da República Federativa do Brasil da proteção de dados como direito fundamental (art. 5º, LXXIX, na redação da Emenda Constitucional n. 115, de 10.2.2022), a Administração Pública também passou a enfrentar desafios relacionados à proteção de dados pessoais dos trabalhadores terceirizados.

É que a contratação de empresas prestadoras de serviços exige, com frequência, o compartilhamento de dados pessoais — por vezes sensíveis — com o ente público, o que amplia os riscos de exposição, tratamento inadequado e violação de direitos fundamentais. Embora os trabalhadores terceirizados não integrem diretamente o quadro de pessoal da Administração Pública, o tratamento de seus dados pelo Poder Público impõe deveres objetivos de proteção, transparência e segurança, conforme os princípios constitucionais da legalidade, moralidade e eficiência.

Neste contexto, o presente artigo propõe-se a analisar a atuação da Administração Pública como controladora de dados pessoais no âmbito da terceirização de serviços, examinando os limites normativos impostos pela LGPD e pelas normas de direito administrativo, bem como as medidas que devem ser adotadas para garantir a proteção dos direitos dos trabalhadores terceirizados.

2. Trabalhadores Terceirizados como Titulares de Dados – Uma Questão de Dignidade

A proteção de dados no Brasil tem como sua norma principal a Lei Geral de Proteção de Dados Pessoais - Lei nº 13.709, de 14.8.2018, mais conhecida como LGPD, que estabelece um marco legal essencial para a proteção da privacidade e dos direitos fundamentais no tratamento de dados pessoais no Brasil. Antes dela, a Lei nº 12.965/2014 – Marco Civil da Internet - garantiu a proteção de dados pessoais no ambiente digital e reforçou o dever de consentimento informado e de segurança de dados.

Já a Constituição da República Federativa do Brasil garante a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas (Art. 5º, X), assegura o sigilo das comunicações (Art. 5º, XII) e, após a promulgação da Emenda Constitucional nº 115/2022, a proteção de dados foi alçada a direito fundamental. Ademais, foi criada a Autoridade Nacional de Proteção de Dados (ANPD) pela Lei nº 13.853/2019, como órgão responsável por zelar, regulamentar e fiscalizar a aplicação da LGPD que, no exercício do seu mister, publica guias, notas técnicas, resoluções e atua na educação e fiscalização, inclusive no setor público.

Todo esse arcabouço normativo é aplicado ao Poder Público e aos seus trabalhadores terceirizados contratados por empresas prestadoras de serviço à Administração Pública, que são titulares de dados e, como tais, merecem proteção legal.

De acordo com o art. 17 da LGPD, os titulares de dados, como também são os trabalhadores terceirizados, têm assegurados direitos fundamentais, como o acesso à informação sobre o tratamento de seus dados, a correção de dados incompletos, a eliminação de dados excessivos ou desnecessários, bem como a portabilidade e a oposição ao tratamento em determinadas hipóteses, cabendo ao órgão público, na qualidade de controlador de dados, assegurar a observância da legislação mesmo quando o tratamento for realizado, em parte, pela empresa contratada (operadora).

Na prática, no entanto, muitos contratos administrativos não preveem cláusulas específicas sobre a proteção de dados pessoais dos trabalhadores da contratada, tampouco medidas claras de segurança da informação, controle de acesso ou gestão de riscos. Outra situação crítica que se observa na prática é o uso indevido de dados sensíveis, como informações de saúde (atestados médicos, laudos ocupacionais) ou dados biométricos (controle de ponto eletrônico). Conforme dispõe o art. 11 da LGPD, esses dados só podem ser tratados em situações excepcionais, mediante previsão legal ou consentimento expresso e informado. O compartilhamento desses dados com a Administração, sem o devido enquadramento legal ou contratual,

configura violação direta à norma e pode comprometer a dignidade e a privacidade do trabalhador.

É necessário, ainda, observar que o mero consentimento do trabalhador terceirizado não afasta a responsabilidade do controlador público, uma vez que o tratamento realizado por entes estatais deve estar sempre fundamentado em bases legais objetivas e compatíveis com os princípios da finalidade, necessidade e transparência (art. 6º da LGPD). Assim, a terceirização de serviços não exime o Estado de responder pela proteção de dados dos profissionais que, ainda que indiretamente, atuam em sua estrutura.

Como se observa, os trabalhadores terceirizados da Administração Pública são um grupo de pessoas em posição de grande vulnerabilidade em vários aspectos: estão sujeitos à vulnerabilidade contratual, pois mantêm vínculo com empresas privadas prestadoras de serviço, frequentemente de menor porte e com estrutura frágil de governança e proteção de dados; há a vulnerabilidade institucional, já que, embora atuem dentro do ambiente da Administração Pública, não se beneficiam das garantias típicas dos servidores efetivos, como estabilidade, controle interno e representação sindical fortalecida. Por fim, verifica-se uma clara vulnerabilidade informacional, pois os dados desses trabalhadores circulam entre diferentes agentes (contratante, contratada, gestores públicos, setores administrativos), nem sempre com transparência ou respeito às finalidades específicas. Não raro, tais trabalhadores não estão cientes dessa situação.

Esse cenário acaba se agravando no dia-a-dia, quando há a exigência, por parte da Administração Pública, de documentos como antecedentes criminais, exames médicos, fichas de frequência com dados biométricos, histórico funcional e até informações de natureza familiar ou previdenciária, que são requisitados sem a devida fundamentação legal específica ou sem critérios claros de proporcionalidade e necessidade, contrariando os princípios da LGPD e colocando em risco a dignidade do trabalhador, dado o caráter de dados sensíveis de boa parte deles.

Resta claro, assim, que os trabalhadores terceirizados da Administração Pública ocupam uma posição jurídica e social que os torna mais suscetíveis a violações de privacidade e tratamento indevido de seus dados, o que exige uma abordagem protetiva mais enfática. Neste caso, é imprescindível que a proteção de dados pessoais seja compreendida como uma expressão concreta da dignidade da pessoa humana, princípio fundante da Constituição Federal de 1988 (art. 1º, III).

Nesse contexto de ampla vulnerabilidade desses trabalhadores, a dignidade da pessoa humana não pode ser reduzida a um conceito retórico, mas sim orientar, de forma concreta, as práticas de contratação, gestão e fiscalização dos contratos administrativos de prestação de serviços, de modo que o trabalhador terceirizado não

seja tratado como um recurso descartável, mas como um sujeito de direitos, inclusive o direito à autodeterminação informativa, que é a capacidade de controlar quais de seus dados são coletados, para quais finalidades, por quem e por quanto tempo.

Além disso, o uso indevido ou excessivo de dados pode gerar impactos concretos na vida dessas pessoas, desde constrangimentos e discriminações no ambiente de trabalho até dificuldades de reinserção no mercado, caso haja exposição pública ou vazamento de informações sensíveis. Em casos extremos, já se registraram situações de trabalhadores terceirizados demitidos ou discriminados com base em informações mal interpretadas ou indevidamente compartilhadas no âmbito da Administração Pública.

Reconhecer a titularidade de dados dos trabalhadores terceirizados não é apenas uma questão de mera conformidade à LGPD, mas uma exigência constitucional de respeito à dignidade, à privacidade e à igualdade material dessas pessoas. A omissão da Administração Pública, nesse caso, pode aprofundar desigualdades, fragilizar direitos sociais e gerar responsabilizações civis, administrativas e até penais.

Portanto, é dever da Administração não apenas respeitar os direitos previstos na LGPD, mas também adotar medidas positivas para proteger ativamente a dignidade dos terceirizados, o que inclui cláusulas contratuais específicas sobre proteção de dados, treinamento dos gestores públicos, transparência nos fluxos de dados e escuta ativa dos trabalhadores no processo de definição das práticas de tratamento.

Somente com a efetiva internalização do valor da dignidade humana nos contratos públicos e na gestão de pessoas será possível construir uma Administração mais ética, inclusiva e comprometida com os fundamentos do Estado Democrático de Direito.

3. A Administração Pública na Condição de Controladora de Dados – Deveres Inerentes

Nos termos do artigo 5º, inciso VI, da Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018), o controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais.

Desta forma, a Administração Pública, ao contratar empresas terceirizadas para a prestação de serviços, assume a condição de controladora de dados, ao lado das empresas prestadoras de serviço, uma vez que terá de tomar decisões relativas aos dados pessoais dos trabalhadores terceirizados colocados à sua disposição.

Considerando-se o fato de se caracterizarem como serviço público delegado pelo Estado, os serviços notariais e de registro exercidos em caráter privado são equiparados às pessoas jurídicas de direito público em relação ao tratamento de

dados (artigo 23, § 4º, da LGPD). Por sua vez, no que concerne ao tratamento de dados, as empresas públicas e as sociedades de economia mista que atuam em regime de concorrência terão o mesmo tratamento conferido às pessoas jurídicas de direito privado (artigo 24 da LGPD).

Da leitura da norma do artigo 23 da LGPD, extrai-se que o tratamento de dados pelas pessoas jurídicas de direito público possui uma finalidade específica, qual seja, o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais atinentes ao setor público.

Assim, tendo em vista o princípio da finalidade e sob a ótica da dignidade do trabalhador terceirizado, alguns deveres aplicáveis à Administração Pública na condição de controladora de dados pessoais de trabalhadores terceirizados são extraídos da LGPD.

Um dos principais deveres da Administração Pública nessa condição é garantir a **transparência no tratamento dos dados pessoais dos trabalhadores**. Isso implica assegurar que tais indivíduos possam, por meio de canais adequados, ter ciência sobre o tratamento de seus dados, os fundamentos legais que o sustentam e os direitos que lhes assistem enquanto titulares.

Seria o caso, por exemplo, de órgão público que contrata uma empresa de limpeza terceirizada para atuar em prédios administrativos. Para permitir o acesso dos funcionários ao sistema de controle de ponto e crachás de identificação, o ente público coleta dados pessoais como nome, CPF e foto dos terceirizados. Mesmo que a coleta seja operacionalizada pela empresa, a finalidade é definida pelo ente público, que assume o papel de controlador e, portanto, deve garantir que esses trabalhadores sejam informados sobre o tratamento e possam exercer seus direitos.

Além disso, a Administração Pública deve adotar **medidas preventivas e de segurança da informação**, visando mitigar riscos relacionados à integridade, confidencialidade e disponibilidade dos dados. Isso inclui a responsabilidade de orientar e fiscalizar servidores e empresas prestadoras de serviços, que atuam como operadoras de dados, nos termos do artigo 5º, inciso VII, da LGPD. Essa relação deve ser formalizada por meio de cláusulas contratuais específicas, exigindo-se da empresa de prestação de serviços a adoção de boas práticas de governança em privacidade, bem como o cumprimento de padrões mínimos de segurança.

Neste sentido, em uma contratação de empresa de vigilância, por exemplo, o edital e o contrato administrativo devem conter cláusulas exigindo que a empresa contratada adote criptografia para armazenar e-mails funcionais, controle de acesso a documentos com dados pessoais e forneça treinamentos básicos de proteção de dados aos trabalhadores. A ausência dessas exigências poderá gerar responsabilização do ente público em caso de incidente.

Outro dever imposto pela LGPD é a **prestação de contas (*accountability*)**, conforme previsto no artigo 6º, inciso X. A Administração Pública deve ser capaz de demonstrar que adota medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados, especialmente no contexto da terceirização, em que o risco de vazamento ou tratamento inadequado de informações é ampliado, seja pelo elevado número de trabalhadores colocados à disposição do ente público ou pela falta de estrutura adequada das empresas prestadoras de serviços em coletar e armazenar os dados pessoais dos seus trabalhadores.

Assim, se a Autoridade Nacional de Proteção de Dados (ANPD) solicitar evidências de conformidade, o ente público deverá apresentar, por exemplo, cópia de contratos administrativos com cláusulas de proteção de dados nos contratos com as empresas terceirizadas, relatórios de auditoria interna, registro de incidentes e políticas de segurança da informação aplicáveis a terceiros.

De igual forma, a nomeação de um **Encarregado pelo Tratamento de Dados Pessoais (DPO)** é também uma exigência da LGPD aos entes públicos (art. 41, §1º), sendo este o canal de comunicação entre os titulares de dados, a Autoridade Nacional de Proteção de Dados (ANPD) e o próprio controlador. O Encarregado deve estar acessível para atender a eventuais solicitações de trabalhadores terceirizados cujos dados estejam sendo tratados pela Administração Pública.

Se, por exemplo, um auxiliar de serviços gerais terceirizado desejar saber quais dados seus estão sendo tratados pelo órgão contratante, a solicitação deverá ser recebida e respondida pelo Encarregado da Administração Pública, por se tratar de dado sob sua guarda.

De igual forma, deve-se destacar que o **dever de proteger dados pessoais** deve ser incorporado desde a concepção de qualquer processo ou política pública que envolva a terceirização de serviços, em conformidade com os princípios do ***privacy by design* e *privacy by default***, previstos implicitamente nos artigos 46 e 50 da LGPD.

O princípio do *privacy by design* é aquele segundo o qual a privacidade e a proteção de dados devem ser incorporadas desde o início do desenvolvimento de qualquer projeto, sistema, processo ou serviço, e não adicionadas apenas depois, como um ajuste. A ideia é que a proteção de dados esteja integrada "*por padrão*" ao design do sistema, sendo parte essencial e não opcional.

Neste sentido, se um órgão público desenvolve um sistema eletrônico de ponto para trabalhadores terceirizados, deverá prever, no momento da concepção, medidas de segurança à privacidade, tais como a coleta mínima de dados (apenas nome e número funcional, por exemplo); criptografia de dados sensíveis; perfis de acesso distintos (para evitar que todos os gestores vejam todos os dados); e registro de *logs* de acesso e alterações.

Por sua vez, o princípio do *privacy by default* significa que os níveis mais altos de proteção de dados devem ser aplicados automaticamente, sem que o titular precise agir para garantir sua privacidade. Portanto, os sistemas devem ser configurados por padrão para minimizar a coleta, o uso e o compartilhamento de dados.

Assim, por exemplo, se um sistema de acesso utilizado por terceirizados permitir o registro facial, a configuração padrão deve ser a não ativação da biometria, a menos que haja fundamento legal claro e real necessidade.

Por fim, a Administração Pública deverá observar o **dever de compartilhamento responsável de dados (artigo 26)**. A Administração Pública pode compartilhar dados com outros órgãos ou com entes privados, mas esse compartilhamento deve ter finalidade pública e compatível com o tratamento original; não pode ter finalidade comercial; e deve ser informado ao titular, salvo nos casos de sigilo ou previsão legal.

Isso é particularmente importante quando os dados de um trabalhador terceirizado são repassados a outro órgão ou empresa pública, por exemplo, para fins de auditoria ou segurança patrimonial.

2. Desafios ao Tratamento de Dados de Trabalhadores de Empresas Terceirizadas pela Administração Pública no Estado do Amazonas

A aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) no setor público enfrenta desafios significativos em todo o país, mas, no Estado do Amazonas, essas dificuldades são acentuadas por fatores geográficos, estruturais e socioeconômicos específicos, dado que se trata do maior maior Estado da Federação, com profunda desigualdade regional, com concentração de desenvolvimento na capital e vulnerabilidade multidimensional no interior, especialmente entre comunidades ribeirinhas e indígenas.

De modo geral, o tratamento adequado de dados pessoais no âmbito da Administração Pública no Estado exige não apenas a conformidade com as bases legais estabelecidas pela LGPD, mas também a superação de obstáculos relacionados à infraestrutura tecnológica, à capacitação dos agentes públicos e à ausência de consolidação de políticas internas de governança de dados.

Um desses principais obstáculos é a desigualdade na estrutura tecnológica dos órgãos públicos, especialmente na esfera municipal e no interior do Amazonas. Por exemplo, prefeituras e secretarias municipais do Estado não dispõem de sistemas informatizados seguros para o armazenamento e processamento de dados, recorrendo

ainda a documentos físicos ou sistemas terceirizados sem controle adequado.

Sem dúvidas, esse cenário fragiliza a proteção dos dados dos cidadãos que se relacionam de alguma forma com órgãos públicos, gerando riscos de extravio, vazamento ou tratamento inadequado de informações sensíveis, como prontuários médicos, dados escolares ou registros funcionais.

Como já amplamente mencionado, a relação entre a Administração Pública e empresas terceirizadas envolve o compartilhamento e tratamento de diversos dados pessoais, tanto dos representantes legais quanto dos trabalhadores envolvidos na execução.

Nesse caso, na grande maioria dos órgãos públicos locais, envolvendo o Poder Judiciário no Estado do Amazonas, os desafios são particularmente relevantes diante da necessidade de proteger dados pessoais de trabalhadores terceirizados que atuam, muitas vezes, em áreas sensíveis desses, como segurança, limpeza, apoio técnico e atendimento ao público.

Com a entrada em vigor da LGPD, um dos principais problemas enfrentados refere-se à ausência ou insuficiência de cláusulas contratuais que tratem especificamente da proteção de dados pessoais nos contratos administrativos com essas empresas.

Exemplificativamente, embora os tribunais locais, como o Tribunal Regional do Trabalho da 11ª Região (TRT11), tenham adotado normativos internos e iniciativas de adequação à LGPD, muitos contratos anteriores à vigência plena da lei não previam obrigações claras das contratadas quanto à segurança da informação, controle de acesso e guarda de dados pessoais dos empregados.

Além disso, dados dos trabalhadores terceirizados — como nome completo, CPF, endereço, dados bancários, biometria e, em alguns casos, informações de saúde ou antecedentes criminais — são exigidos para cadastro, emissão de crachás, controle de acesso, registro de ponto e pagamentos, sendo frequentemente compartilhados entre a contratada e o tribunal sem clareza sobre os mecanismos de proteção e limites de uso.

Outra dificuldade enfrentada reside na fragilidade da governança de dados por parte das empresas contratadas, especialmente quando se trata de prestadoras de pequeno porte, muitas vezes sem estrutura mínima de conformidade com a LGPD.

O Judiciário, como ente contratante e controlador dos dados, acaba assumindo riscos adicionais ao permitir o tratamento de dados por operadores que não seguem padrões adequados de segurança da informação, contrariando o art. 46 da LGPD.

Para a superação dos obstáculos acima elencados, algumas soluções são propostas.

Inicialmente, destaca-se a necessidade de conscientização de administradores públicos sobre a relevância da adequada proteção de dados segundo as diretrizes da LGPD, os direitos dos titulares de dados e a possibilidade de responsabilização do gestor público. Percebe-se que a LGPD, apesar de publicada em 2018, ainda não se encontra integralmente difundida no setor público estadual ou municipal, cujos gestores muitas vezes sequer conhecem o seu teor.

Desta forma, seria oportuno o oferecimento de congressos, palestras, cursos e treinamentos com o objetivo de capacitar servidores públicos em temas próprios da proteção pessoal de dados.

Outra solução a ser apontada é a assinatura de convênios e cooperações técnicas entre diversos órgãos públicos, a fim de fornecerem apoio e cooperação mútuos, auxiliando sobretudo os órgãos que possuem maiores dificuldades técnicas ou estruturais na implementação das diretrizes da LGPD.

Neste sentido, destaque-se o papel da Rede Amazonense de Proteção de Dados Pessoais, que reúne diversos órgãos do segmento público para discutir, compartilhar boas práticas e fomentar a cooperação entre as instituições visando à melhor implementação da LGPD no Estado do Amazonas. A Rede é integrada por várias instituições públicas do Estado do Amazonas, tais como o Tribunal Regional do Trabalho da 11ª Região; o Tribunal de Justiça do Amazonas (TJAM); o Ministério Público Estadual (MPE); a Defensoria Pública Estadual (DPE); a Controladoria-Geral do Estado (CGE); a Empresa de Processamento de Dados do Amazonas (Prodam); a Universidade do Estado do Amazonas (UEA); a Universidade Federal do Amazonas (UFAM); a Prefeitura de Manaus (PMM); o Tribunal Regional Eleitoral do Amazonas (TRE-AM); o Tribunal de Contas do Estado (TCE-AM); a Ordem dos Advogados do Brasil - Seccional Amazonas (OAB-AM); a Secretaria de Segurança Pública (SSP) e a Procuradoria-Geral do Estado (PGE).

Além disso, sugere-se a criação de órgãos ou departamentos específicos, com corpo de servidores próprios, vinculado ao Encarregado de Proteção de Dados, com o objetivo de promover o adequado tratamento dos dados de servidores e trabalhadores e municiar a Administração Pública de informações e pareceres sobre a aplicação da LGPD, quando solicitado.

De igual forma, não se pode ignorar a necessidade de investimentos públicos em estrutura tecnológica e informatizada para que se realize o adequado tratamento dos dados pessoais, sobretudo nos municípios do interior que, conforme já mencionado, muitas vezes sequer possuem acesso estável à internet. O trabalhador, enquanto titular de dados pessoais, buscará o setor público para que solucione problemas relacionados à sua privacidade e proteção de dados. Para tanto, a Administração Pública deverá estar devidamente equipada para a solução destes conflitos.

Assim, diante das já mencionadas vulnerabilidades estruturais existentes no Estado do Amazonas, a aplicação da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD) exige atenção redobrada quanto à segurança jurídica e à proteção dos titulares de dados, notadamente daqueles relativos aos trabalhadores terceirizados colocados à disposição da Administração Pública.

Conclusão

A terceirização de atividades acessórias, instrumentais ou de apoio, como vigilância, limpeza, recepção e suporte técnico pela Administração Pública é uma realidade, que traz alguns desafios.

Dentre eles, destaca-se a necessidade de conferir proteção aos dados pessoais dos trabalhadores terceirizados. A contratação de empresas prestadoras de serviços exige, com frequência, o compartilhamento de dados pessoais — por vezes sensíveis — com o ente público, o que amplia os riscos de exposição, tratamento inadequado e violação de direitos fundamentais.

O tratamento de dados desses trabalhadores pelo Poder Público impõe deveres objetivos de proteção, transparência e segurança, conforme os princípios constitucionais da legalidade, moralidade e eficiência.

No entanto, mais do que isso, o correto tratamento dos dados desses trabalhadores é uma questão de dignidade.

Sabe-se que os trabalhadores terceirizados ocupam uma posição jurídica e social que os torna mais suscetíveis a violações de privacidade e tratamento indevido de seus dados. Neste caso, é imprescindível que a proteção de dados pessoais seja compreendida como uma expressão concreta da dignidade da pessoa humana, princípio fundante da Constituição Federal de 1988 (art. 1º, III).

A dignidade da pessoa humana (e destes trabalhadores) não pode ser reduzida a um conceito retórico, mas sim orientar, de forma concreta, as práticas de contratação, gestão e fiscalização dos contratos administrativos de prestação de serviços, de modo que o trabalhador terceirizado não seja tratado como um recurso descartável, mas como um sujeito de direitos e titular dos seus dados pessoais.

Sob esta ótica, alguns deveres surgem para a Administração Pública para que promova o correto tratamento de dados, tais como a transparência, a adoção de medidas preventivas e de segurança de informação, a prestação de contas, a nomeação de um Encarregado de Proteção de Dados, o dever de proteção de dados pessoais por meio dos princípios de *privacy by design* e *privacy by default* e o compartilhamento responsável de dados.

As dificuldades para a concretização da dignidade desses trabalhadores em matéria de proteção de dados, sobretudo no Estado do Amazonas, são variadas. Fatores geográficos, estruturais e socioeconômicos específicos constituem obstáculos à devida proteção de dados. Para tanto, algumas soluções são propostas - conscientização e educação de gestores públicos, assinatura de convênios e cooperações técnicas entre órgãos públicos, criação de departamentos e órgãos específicos vinculados a um Encarregado de Proteção de Dados e investimentos públicos em estrutura tecnológica e informatizada adequada.

De toda forma, é necessário conscientizar-se que a proteção dos dados pessoais dos trabalhadores terceirizados deve ser compreendida não apenas como uma obrigação legal imposta pela Lei Geral de Proteção de Dados (LGPD), mas como uma expressão concreta do respeito à dignidade da pessoa humana. Ao assegurar que as informações sensíveis desses profissionais sejam tratadas com responsabilidade, transparência e segurança, as organizações contribuem para a valorização do trabalho e o reconhecimento da individualidade desses sujeitos, muitas vezes invisibilizados na estrutura organizacional.

É imperativo, portanto, que a privacidade dos trabalhadores terceirizados seja tratada com a mesma seriedade conferida aos demais agentes públicos, reafirmando que a dignidade humana não pode ser terceirizada.

Referências

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais: elementos da formação da autoridade nacional*. Rio de Janeiro: Forense, 2021.

MACHADO, Diego; CASTRO, Fabrício da Mota Alves. *LGPD para o setor público*. Brasília: Escola Nacional de Administração Pública – ENAP, 2021.

PINTO, Felipe Palhares. *Lei Geral de Proteção de Dados Comentada*: artigo por artigo. São Paulo: Revista dos Tribunais, 2020.

SARLET, Ingo Wolfgang. *Dignidade da pessoa humana e direitos fundamentais na Constituição Federal de 1988*. 20. ed. São Paulo: Atlas, 2022.

A Experiência da UFAM na Implementação da LGPD: Consolidando uma Cultura de Proteção de Dados

Universidade Federal do Amazonas

Perspectiva educacional e formativa da proteção de dados, conectando LGPD com cidadania digital e formação universitária.

Nycolle Oliveira Souza Santos

Administradora / Encarregada de Proteção de Dados

Formada em Administração, Mestre em Engenharia de Produção, com experiência em planejamento de compras e contratações e em proteção de dados.

Resumo

Este artigo analisa a experiência da Universidade Federal do Amazonas (UFAM) na implementação da Lei Geral de Proteção de Dados Pessoais (LGPD), destacando seu papel na consolidação de uma cultura institucional de proteção de dados. Diante do cenário de transformação digital e crescente tratamento de informações pessoais no setor público, a UFAM adotou uma abordagem estratégica, normativa e educativa. Desde a nomeação de seu primeiro Encarregado pelo Tratamento de Dados Pessoais (DPO), em 2021, a universidade estruturou ações integradas com o Comitê de Governança Digital e a Coordenação de Segurança da Informação do CTIC, alinhadas ao Plano de Privacidade e Segurança da Informação do Governo Federal. A atuação do Escritório de Proteção de Dados Pessoais da Ufam (DPO) inclui ações educativas, como campanhas de conscientização, respostas a incidentes com abordagem formativa e apoio técnico contínuo às unidades. Fundamentado em um estudo de caso institucional, o artigo reforça que, mais do que atender a exigências legais, a UFAM tem se posicionado como agente formador da cidadania digital e da ética informacional. A experiência serve de referência para outras universidades públicas que buscam articular governança, formação e responsabilidade no tratamento de dados pessoais.

Palavras-chave: LGPD; universidade pública; proteção de dados; cidadania digital; governança da informação.

1. Introdução

A sociedade contemporânea vive uma profunda transformação digital marcada pelo uso intensivo de dados pessoais. Com a consolidação de plataformas digitais, serviços *online* e sistemas de informação integrados, tornou-se imperativo refletir sobre a ética, a segurança e a transparência no tratamento de dados. Nesse contexto, a Lei Geral de Proteção de Dados Pessoais (LGPD), sancionada em 2018 e em vigor desde setembro de 2020, representa um importante marco regulatório, aplicável tanto ao setor privado quanto ao setor público. No setor público, em especial, a adaptação à LGPD envolve uma complexa articulação entre os princípios da administração pública e os direitos fundamentais dos cidadãos. Entre os desafios estão a conscientização dos servidores, a adequação tecnológica dos sistemas e a adoção de uma cultura institucional voltada à proteção de dados.

Nesse novo cenário informacional, a implementação da LGPD exige não apenas adequações jurídicas e técnicas, mas sobretudo uma revisão crítica sobre os modelos de organização social que emergem da economia baseada em dados. Como alerta Zuboff (2020), "a informação privada tornou-se a matéria-prima de uma nova lógica de acumulação", que pode comprometer direitos fundamentais quando não regulada e compreendida criticamente. Nessa perspectiva, o papel das universidades públicas torna-se central, não apenas para cumprir exigências legais, mas para liderar o debate sobre os limites éticos da coleta e do uso de dados pessoais. Ao promover conhecimento, reflexão e práticas institucionais responsáveis, a universidade contribui para a formação de uma cultura de resistência ao uso abusivo da informação e de valorização da privacidade como dimensão essencial da cidadania.

As universidades públicas, como espaços de produção e disseminação do conhecimento, possuem papel central na formação de uma sociedade mais consciente sobre o uso de informações pessoais. A Universidade Federal do Amazonas (UFAM), uma das principais instituições de ensino superior da região Norte do Brasil, buscou colocar em prática a adequação à LGPD. Desde a nomeação do seu primeiro Encarregado pelo Tratamento de Dados Pessoais (*Data Protection Officer*/DPO), em janeiro de 2021, conforme processo SEI nº 23105.000879/2021-50, a UFAM tem implementado uma série de ações estruturantes, pedagógicas e administrativas para incorporar os princípios da proteção de dados à sua rotina institucional.

O objetivo deste artigo é analisar o papel da UFAM na consolidação de uma cultura de proteção de dados, abordando os marcos da sua atuação institucional, os desafios enfrentados e os avanços obtidos. Como metodologia, utiliza-se um estudo de caso qualitativo, com base na análise documental de normativas

internas, no Guia da ANPD sobre o setor público (2023) e na experiência prática da equipe responsável pela adequação à LGPD na universidade. A estrutura do artigo está organizada em três partes além da introdução: na seção 2, apresenta-se o referencial teórico sobre a LGPD, a governança da informação e o papel das universidades na cidadania digital; na seção 3, discute-se a experiência concreta da UFAM; e, por fim, são apresentadas as considerações finais com recomendações para outras instituições públicas de ensino superior.

2. Referencial Teórico

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), inspirada no Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR), estabelece um conjunto de princípios, direitos e deveres aplicáveis ao tratamento de dados pessoais no Brasil. Seu objetivo é garantir a proteção da liberdade, da privacidade e do livre desenvolvimento da personalidade da pessoa natural (art. 1º, LGPD). A LGPD se aplica também ao setor público, que, conforme aponta a Autoridade Nacional de Proteção de Dados (ANPD), deve realizar o tratamento de dados sempre com base legal, respeitando os princípios da finalidade, necessidade, adequação e transparência.

Entre os conceitos fundamentais da LGPD estão os de dado pessoal e dado sensível. Dados pessoais são aqueles relacionados à pessoa natural identificada ou identificável, enquanto dados sensíveis incluem informações sobre origem racial ou étnica, convicção religiosa, opinião política, dados genéticos, biométricos e de saúde, entre outros (art. 5º, I e II). O tratamento desses dados exige não apenas bases legais adequadas, mas também maior responsabilidade institucional. O controlador e o operador são os principais agentes de tratamento de dados definidos na LGPD. O controlador, segundo Doneda (2020), é quem toma as decisões sobre o tratamento de dados, assumindo posição central na governança informacional. Já o operador executa o tratamento sob as ordens do controlador.

Destaca-se ainda a figura do Encarregado pelo Tratamento de Dados Pessoais, ou DPO (*Data Protection Officer*), que atua como canal de comunicação entre o controlador, os titulares de dados e a ANPD, sendo peça-chave na implementação da cultura de proteção de dados. A governança da informação é um conceito transversal às exigências da LGPD. Para Bioni (2021), a governança se expressa pela capacidade da instituição em organizar fluxos de dados de forma ética, transparente e segura, integrando políticas internas, capacitação, infraestrutura tecnológica e ações pedagógicas. Nesse contexto, a LGPD impõe ao setor público um dever institucional de estruturação de práticas que assegurem a proteção de dados pessoais, não apenas como obrigação jurídica, mas como valor público. Nas

universidades públicas, esse dever assume uma dimensão ampliada.

Além de prestadoras de serviços educacionais, elas são centros de produção e circulação de conhecimento, onde o uso de dados ocorre de forma contínua — seja em pesquisas, atividades acadêmicas, sistemas administrativos, ou mesmo em eventos e redes sociais institucionais. Segundo Miriam Wimmer (2021), o ambiente universitário é estratégico para a consolidação da cidadania digital, pois forma sujeitos capazes de compreender os impactos éticos e sociais do uso de seus dados. A formação de uma cultura de proteção de dados, portanto, envolve não apenas normas e procedimentos, mas também processos de sensibilização coletiva, educação digital e a internalização dos princípios da LGPD na rotina institucional. De acordo com Westin (1967), o direito à privacidade está diretamente relacionado à autodeterminação informativa, ou seja, à capacidade dos indivíduos de controlarem suas informações pessoais.

Promover esse controle é uma responsabilidade compartilhada entre o Estado, as instituições e os próprios titulares dos dados. Nesse cenário, a atuação das universidades públicas como protagonistas na difusão da cultura de dados se mostra não apenas necessária, mas urgente. A LGPD oferece o arcabouço legal; a universidade, os meios pedagógicos e institucionais para que essa legislação se traduza em práticas cotidianas de respeito, responsabilidade e inclusão digital.

O papel das universidades na formação de uma nova cultura na sociedade vai além da transmissão de conteúdos acadêmicos: trata-se de um compromisso com a transformação social. A universidade deve ser vista como uma instituição social de importância estratégica, cuja função vai além da simples transmissão do conhecimento, assumindo o compromisso de gerar novos saberes e colaborar para a formação de uma sociedade mais equitativa e democrática (SANTOS, 2005).

Nesse sentido, as universidades públicas assumem uma função central na consolidação de valores coletivos, como a ética, a cidadania e os direitos fundamentais — incluindo a proteção de dados pessoais. Ao promover ações educativas, fomentar o debate crítico e estruturar políticas institucionais comprometidas com esses princípios, a universidade contribui diretamente para a construção de uma cultura voltada à responsabilidade digital e à defesa da dignidade humana em um mundo cada vez mais informatizado.

3. A Experiência da UFAM

A Universidade Federal do Amazonas (UFAM) tem buscado consolidar a implementação da Lei Geral de Proteção de Dados Pessoais (LGPD) dentro de suas unidades acadêmicas e administrativas. Desde a nomeação oficial de seu primeiro Encarregado pelo Tratamento de Dados Pessoais (DPO), em janeiro de 2021, a

instituição passou a estruturar um conjunto de medidas normativas, educativas e corretivas que envolvem vários setores da administração universitária.

Um dos primeiros passos foi a capacitação especializada do então encarregado, por meio de curso oferecido pela *IT Partners*, abordando temas como a norma ISO/IEC 27001 e os fundamentos do Regulamento Geral sobre a Proteção de Dados (GDPR). Essa formação foi determinante para viabilizar o trabalho intersetorial com pró-reitorias, centros administrativos e unidades acadêmicas, promovendo uma cultura institucional voltada à proteção de dados.

Atualmente, o Escritório de Proteção de Dados é composto pela encarregada titular e por seu substituto, ambos designados por portaria. A estrutura do DPO está vinculada diretamente à Chefia de Gabinete da Reitoria, o que demonstra o comprometimento da alta gestão da UFAM com a pauta da proteção de dados pessoais. Essa vinculação estratégica garante maior visibilidade às ações do DPO e reforça o papel institucional do tema no âmbito universitário. Além disso, a inserção da equipe do DPO no Comitê de Governança Digital (CGD/UFAM) — órgão colegiado de caráter estratégico e deliberativo — consolida o alinhamento entre as políticas de tratamento de dados e os objetivos de governança da universidade. Ao reconhecer a importância da privacidade e da segurança da informação como valores organizacionais, a UFAM fortalece a formação de uma cultura institucional de responsabilidade, ética informacional e cidadania digital.

Cabe ressaltar, ainda, que atuação do DPO também é fortemente integrada à Coordenação de Segurança da Informação do Centro de Tecnologia da Informação e Comunicação (CTIC), com a qual compartilha responsabilidades na implementação do Plano de Privacidade e Segurança da Informação (PPSI), conforme previsto pelo Governo Federal. Nesse modelo, a UFAM cumpre as metas do índice de privacidade (Ipriv), sob responsabilidade do Escritório de Proteção de Dados, e do índice de segurança (Iseg), sob a responsabilidade do CTIC.

Entre as atribuições essenciais do Escritório de Proteção de Dados (DPO) destaca-se sua função orientativa, conforme previsto no art. 41, §2º, inciso III da LGPD e regulamentado pela ANPD. Cabe ao DPO orientar servidores e contratados da instituição quanto às práticas adequadas de tratamento de dados pessoais, prestando assistência técnica contínua e especializada. Essa atuação consultiva abrange desde esclarecimentos sobre medidas de segurança e conformidade até o suporte na elaboração de documentos e políticas internas, promovendo uma cultura organizacional alinhada à proteção de dados e à governança institucional.

Nesse contexto, como parte de sua atuação orientativa, destaca-se a campanha de conscientização "Semana da Segurança da Informação e Privacidade", realizada de 25 a 30 de novembro de 2024, por iniciativa do CTIC, com o apoio do

Escritório de Proteção de Dados (DPO) e da Assessoria de Comunicação. A iniciativa englobou cartilhas digitais, pôsteres e conteúdos audiovisuais divulgados nos canais institucionais, com foco na disseminação de boas práticas de proteção de dados e segurança da informação. A experiência demonstra o que Wimmer (2021) define como "a função pedagógica da universidade na formação da cidadania digital", ao integrar conhecimento técnico, engajamento social e cultura organizacional.

No plano operacional, a atuação do Escritório de Proteção de Dados (DPO) se destaca especialmente na resposta a incidentes envolvendo dados pessoais. Quando ocorrem situações desse tipo, o DPO coordena todas as etapas necessárias, como a notificação da unidade envolvida, a comunicação ao titular dos dados, a remoção do conteúdo indevido, a apuração interna do caso e a promoção de ações educativas junto aos servidores responsáveis. Esse modelo de resposta formativa, além de cumprir os princípios da responsabilização e prestação de contas (*accountability*), está alinhado com a noção de autodeterminação informativa de Westin (1967), segundo a qual os indivíduos devem controlar o uso de seus próprios dados.

Além de suas funções corretivas, o Escritório atua como um núcleo permanente de orientação técnica e jurídica. Entre suas ações contínuas estão a emissão de pareceres sobre adequação de sistemas e documentos, treinamentos para servidores e a elaboração de cartilhas e manuais institucionais. O contato direto com os titulares de dados também é assegurado por meio de e-mail institucional e pelo sistema Fala.BR, em parceria com a Ouvidoria da UFAM.

Essa estrutura demonstra a capacidade da UFAM de integrar governança e cultura institucional com os preceitos da LGPD. Como aponta Bioni (2021), a proteção de dados no setor público demanda não apenas estruturas formais, mas um processo contínuo de transformação cultural e de sensibilização das organizações para os direitos fundamentais dos cidadãos. Ao promover formação, prevenir riscos e garantir respostas responsáveis, a UFAM cumpre seu papel como espaço formador e promotor de uma ética pública digital.

Considerações Finais

A promulgação da LGPD e sua aplicação no setor público têm exigido uma profunda transformação na cultura institucional brasileira, especialmente em instituições como as universidades públicas. A experiência da UFAM evidencia que, mesmo diante de limitações estruturais e desafios culturais, é possível implementar uma política de proteção de dados alinhada aos princípios legais e à missão educativa da universidade.

Ao adotar medidas administrativas e educativas, estabelecer canais institucionais de comunicação, capacitar seu DPO e envolver a comunidade

universitária em ações de sensibilização, a UFAM não apenas atende a uma obrigação normativa, mas reafirma seu compromisso com a formação de cidadãos críticos e conscientes na era digital.

Essa experiência pode servir de referência para outras instituições de ensino superior que buscam se adequar à LGPD, demonstrando que a construção de uma cultura de proteção de dados passa por políticas internas consolidadas, pela valorização do papel estratégico e pedagógico do DPO e pela criação de espaços permanentes de diálogo, educação e governança em privacidade.

Mais do que uma exigência legal, a proteção de dados deve ser compreendida como um direito fundamental e um elemento estruturante da cidadania digital. As universidades, enquanto espaços de produção de conhecimento, debate público e formação ética, têm o dever, e ainda, a oportunidade, de liderar essa transformação cultural, contribuindo para uma sociedade mais informada, segura e comprometida com os valores da privacidade e da dignidade humana.

Referências

ANPD – Autoridade Nacional de Proteção de Dados. *Guia Orientativo*: Tratamento de dados pessoais pelo Poder Público. Versão 2.0. Brasília, 2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes. Acesso em: 15 maio 2025.

BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e os limites do consentimento. 2. ed. São Paulo: Thomson Reuters Brasil, 2021. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais. Diário Oficial da União, Brasília, DF, 15 ago. 2018.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Dispõe sobre a proteção de dados pessoais. Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*: elementos da formação da nova cultura de dados no Brasil. 2. ed. Rio de Janeiro: Forense, 2020.

MENEZES, Rafael da Silva. *Ofício nº 001.DP/2021/DDAPLIC/UFAM*. Processo SEI nº 23105.000879/2021-50. Manaus: Universidade Federal do Amazonas, 2021.

SANTOS, Boaventura de Sousa. *A universidade no século XXI*: para uma reforma democrática e emancipatória da universidade. 3. ed. São Paulo: Cortez, 2005.

UFAM – UNIVERSIDADE FEDERAL DO AMAZONAS. Política institucional de proteção de dados pessoais. Manaus: UFAM, 2021.

WIMMER, Miriam. *Regulação e proteção de dados pessoais*: fundamentos para uma cultura de privacidade no Brasil. In: MACHADO, Diego (org.). LGPD: desafios e perspectivas. São Paulo: Revista dos Tribunais, 2021.

WESTIN, Alan. *Privacy and freedom*. New York: Atheneum, 1967.

ZUBOFF, Shoshana. *A era do capitalismo de vigilância*: a luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca, 2020.

6

Resposta a Incidentes de Segurança de Dados Pessoais: Perspectivas para a Administração Pública

Procuradoria-Geral do Estado do Amazonas

Metodologias estruturadas para resposta a incidentes de segurança com foco na cooperação interinstitucional.

Luan Silva Seminario

Procurador do Estado e Encarregado de Dados. Procurador-Chefe da Procuradoria Jurídica da Secretaria de Estado de Saúde do Amazonas (SES/AM). Mestrando em Direito pela Universidade de Brasília (UnB). Pós-graduado em Direito Tributário e Aduaneiro pela Pontifícia Universidade Católica de Minas Gerais (PUC-MG). Bacharel em Direito pela Universidade Federal do Amazonas (UFAM). Técnico em Informática pela Fundação Nokia de Ensino (FNE).

Eduardo Nicolas Bitencourt Neves

Analista de Tecnologia da Informação e Encarregado de Dados Substituto. Pós-graduado em Cibersegurança e Governança de Dados pela Pontifícia Universidade Católica de Minas Gerais (PUC-MG). Bacharelando em Engenharia da Computação pela FUCAPI. Tecnólogo em Segurança da Informação pelo Centro Universitário do Vale do Ipojuca (UNIFAVIP-Wyden). Técnico em Informática pelo Instituto Federal de Educação, Ciência e Tecnologia do Amazonas (IFAM).

Resumo

O presente artigo analisa a aplicação da Lei n.º 13.709/18 (Lei Geral de Proteção de Dados Pessoais – LGPD) no setor público, com ênfase na elaboração e execução de planos de resposta a incidentes de segurança envolvendo dados pessoais. A pesquisa aborda a importância da governança e dos controles internos de privacidade, a correlação entre segurança da informação e proteção de dados, a conceituação jurídica de incidentes à luz da LGPD, os riscos decorrentes de vazamentos e os elementos essenciais de um plano de resposta eficaz. Para tanto fundamenta-se na legislação brasileira de regência, em diretrizes da Agência Nacional de Proteção de Dados (ANPD), no Regulamento Geral para Proteção de Dados (GDPR) e em boas práticas internacionais para, ao final, propor a identificação de medidas de conformidade normativa e de proteção dos direitos dos titulares no contexto da Administração Pública.

Palavras-chave: LGPD; Dados Pessoais; Administração Pública.

1. Introdução

A intensificação do processo de transformação digital no âmbito da Administração Pública, associada ao exponencial aumento do volume de dados pessoais sob a guarda do Estado, tem imposto complexos desafios em matéria de privacidade e segurança da informação.

A recorrência de vazamentos e incidentes envolvendo dados pessoais evidencia a necessidade de estruturas de governança sólidas e mecanismos eficazes de prevenção, detecção e resposta a incidentes, especialmente no setor público.

Nesse contexto, sabe-se que a Lei n.º 13.709/18 instituiu um novo marco normativo essencial à proteção dos direitos fundamentais à liberdade e à privacidade, impondo deveres específicos aos agentes de tratamento – inclusive os entes estatais – quanto à implementação de medidas de segurança da informação e à adoção de planos formais de resposta a incidentes de vazamento de dados pessoais.

A pesquisa proposta neste ensaio parte do objetivo geral de análise dos elementos estruturantes de um plano de resposta a incidentes de segurança envolvendo dados pessoais, a partir da perspectiva exigida pela LGPD, e com enfoque para sua aplicação na Administração Pública. Para tanto, será analisada, em um primeiro momento, a importância da governança corporativa e dos mecanismos de controle interno de privacidade no setor público – enquanto instrumentos de prevenção e gestão de incidentes com dados pessoais – em consonância com os comandos da LGPD e referenciais técnicos internacionais.

Ademais, será examinada a relação entre a segurança da informação e a proteção de dados pessoais, a fim de demonstrar como medidas de segurança – física, organizacional e lógica – contribuem para mitigação de riscos e para a conformidade legal em caso de incidentes. De igual modo, pela definição do estado da arte do conceito de incidentes de segurança de dados pessoais na LGPD, serão identificadas as obrigações que recaem sobre os agentes de tratamento frente à autoridade regulatória.

O ensaio identificará e classificará os riscos associados aos incidentes de segurança a fim de ilustrar suas repercussões concretas no contexto da Administração pública, bem como descreverá os componentes essenciais de um plano de resposta a tais incidentes – com ênfase nas etapas de detecção, contenção, comunicação, remediação e aprendizado – para, ao final, apresentar medidas práticas de prevenção e resposta a tais ocorrências, destacando iniciativas administrativas adotadas em entidades nacionais e internacionais, com vistas à consolidação de uma estrutura organizacional orientada à proteção de dados no setor público.

2. Governança Corporativa e Controles Internos de Privacidade no Setor Público

A instituição de um programa de governança em privacidade é medida essencial para que os entes públicos assegurem a conformidade com LGPD e estejam devidamente preparados para prevenir, conter e responder a incidentes de segurança envolvendo dados pessoais. Nos termos do 50 da LGPD, tem-se que recai sobre os controladores de dados da Administração Pública o dever de adotar regras de boas práticas e de governança interna, abrangendo, entre outros elementos, mecanismos de supervisão contínua, gestão e mitigação de riscos, além de planos específicos de resposta e remediação de incidentes (Brasil, 2018).

A norma legal, portanto, estimula a integração da proteção de dados às estruturas de governança organizacional, mediante políticas, procedimentos e controles voltados à tutela sistemática e abrangente dos dados pessoais sob custódia do Estado.

Neste particular, a governança em privacidade deve harmonizar-se com os sistemas já instituídos de governança pública e controle interno, de modo a compor um arranjo institucional coerente e funcional. Para tanto, órgãos e entidades da administração direta e indireta devem incorporar, em suas estruturas de integridade e compliance, instrumentos como políticas de proteção de dados, códigos de conduta específicos, comitês multidisciplinares de privacidade, fluxos de auditoria e protocolos de resposta a incidentes.

Destaca-se, nesse arranjo, a figura do Encarregado pelo Tratamento de Dados Pessoais – ou *Data Protection Officer (DPO)* –, cuja designação é obrigatória no setor público, conforme dispõe nos termos do art. 23, III, da LGPD (Brasil, 2018), a quem cabe atuar de forma transversal na estrutura organizacional, com conhecimentos preferencialmente das áreas de segurança da informação, tecnologia, jurídica e de gestão de riscos, mormente porque será este quem realizará a triagem técnica e análise crítica das notificações de incidentes para, ao final, deliberar sobre a necessidade de comunicação ao ente regulador, aos titulares afetados e aos órgãos de controle externo (Brasil, 2022).

Com efeito, sabe-se que a consolidação de uma governança de privacidade eficaz no setor público também demanda, como elemento indissociável, a implementação de controles internos robustos voltados à proteção dos dados pessoais sob custódia estatal.

Tais controles devem abranger tanto medidas técnicas – a exemplo de gestão de acessos, criptografia, *backup* de informações e monitoramento de redes – quanto mecanismos administrativos – como políticas institucionais de classificação

da informação, termos formais de confidencialidade e programas contínuos de capacitação dos servidores –, todos voltados à conformidade com o princípio da segurança para privacidade (*security for privacy*).

Nos termos do art. 46 da LGPD (Brasil, 2018), incumbe aos agentes de tratamento a adoção de "medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados e contra situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito".

A escolha e implementação dessas salvaguardas devem ser proporcionais à natureza e à sensibilidade dos dados tratados, bem como ao grau de risco envolvido. Assim, órgãos públicos que processem dados sensíveis – como informações de saúde, biometria ou de natureza fiscal – devem adotar camadas adicionais de segurança, observando os requisitos específicos da legislação setorial e as diretrizes técnicas expedidas pela ANPD.

Paralelamente, a governança de privacidade deve ser concebida de forma integrada aos demais marcos normativos que regulam o tratamento de informações no setor público, em especial a Lei n.º 12.527/11 (Lei de Acesso à Informação – LAI), de modo a evitar conflitos entre o dever de transparência e a obrigação de resguardar a privacidade dos titulares, mormente uma vez que a LAI impõe ao Poder Público obrigações de transparência ativa, passiva e reativa, inclusive em relação a informações que, em certos casos, podem conter dados pessoais (Brasil, 2011).

Desta maneira, cabe aos entes da Administração definir parâmetros objetivos que sejam capazes de compatibilizar a publicidade administrativa com a proteção de dados pessoais, sendo certo que uma governança hígida deve vir acompanhada de orientações claras para os servidores e gestores públicos quanto ao tratamento de pedidos de acesso à informação que envolvam dados pessoais, como medida de prevenção de incidentes de segurança, bem como deve alinhar-se às políticas institucionais de segurança da informação, a exemplo da Política de Segurança da Informação e Comunicações (POSIC) adotada por cada ente público, assegurando que a proteção de dados pessoais seja internalizada como valor transversal e estruturante da cultura organizacional.

Em síntese, a governança corporativa e os controles internos de privacidade, quando devidamente implementados na Administração Pública, configuram a linha inicial de contenção e prevenção contra incidentes de segurança envolvendo dados pessoais, na medida em que servem para instituir um regime de conformidade normativa e de maturidade organizacional por meio dos quais os diversos níveis hierárquicos passam a compreender com clareza suas atribuições frente ao regime instituído pela LGPD.

Não bastasse, este mecanismo fortalece o alicerce institucional de resposta célere e coordenada em casos de incidentes, notadamente porque possibilita a definição *ante factum* de planos de contigência, fluxos internos de comunicaçõa e critérios objetivos de tomada de decisão, em harmonia à noção de gestão (*management*) ou prestação de contas (*accountability*).

3. Segurança da Informação e Proteção ee Dados Pessoais

A figura da segurança da informação e da proteção de dados pessoais são disciplinas juridicamente e tecnicamente interdependentes, muito embora possuam escopos distintos e complementarmente articulados.

A primeira – segurança da informação – tem por objeto a salvaguarda de ativos informacionais de maneira ampla, assegurando os atributos de confidencialidade, integridade e disponibilidade – a denominada tríade CID – (Yee; Zolkipli, 2021), por meio da adoção de políticas, controles e tecnologias voltadas à prevenção de acessos não autorizados, perda de dados e falhas operacionais.

Por sua vez, a segunda – proteção de dados pessoais – concentra-se na observância dos direitos fundamentais dos titulares e na legalidade do tratamento de dados pessoais segundo princípios estruturantes como finalidade, adequação, necessidade, transparência, segurança, prevenção, não discriminação e responsabilização, conforme delineado no art. 6º da LGPD:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI - transparência: garantia, aos titulares, de informações claras, precisas

> e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas. (Brasil, 2018)

Nesse contexto, é possível inferir, portanto, que a segurança da informação constitui pilar indispensável à efetividade da proteção de dados, visto que a ausência de salvaguardas técnicas e administrativas compromete inevitavelmente a integridade de todo o regime de privacidade, principalmente se considerarmos que incidentes de segurança – como acessos indevidos ou usos abusivos – podem culminar na violação direta dos direitos dos titulares.

Conforme se infere do dispositivo transcrito acima, a LGPD consagrou de maneira expressa os deveres objetivos e contínuos dos agentes de tratamento com relação à segurança e a prevenção de dados pessoais, circunstância que, aliada à determinação do art. 46 da LGPD (Brasil, 2018), coloca a gestão da segurança da informação em posição central de conformidade do ente público ao regime de privacidade da norma de regência, na medida em que compreende os aspectos operacionais basilares à efetivação das medidas exigidas pela norma, tais como o controle de acessos, proteção de redes, detecção e resposta a *softwares* maliciosos, registro e análise de *logs* ou o registro de acesso em bases de dados públicas.

Assim, tem-se que proteção de dados pessoais possui escopo normativo mais amplo do que a segurança da informação, em que pese com ela mantenha relação de interdependência. Ora, sem a adoção de medidas efetivas de segurança, não se pode falar em proteção substancial dos dados, ou, dito de outro modo, revelar-se-ia inócua a intenção do legislador em estabelecer um regime de requisitos jurídicos relacionados ao tratamento de dados pessoais se não forem implementadas as devidas medidas administrativas capazes de impedir falhas técnicas de acesso indevido ou vazamento de informações pessoais.

Portanto, a segurança da informação configura condição necessária – ainda que não suficiente – à efetividade do regime de proteção de dados. Tal premissa também

se verifica no Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR), que serviu de base e modelo à LGPD, segundo o qual a violação de dados pessoais configura um incidente de segurança da informação que compromete dados pessoais, resultando em sua destruição, perda, alteração, divulgação não autorizada ou acesso indevido (União Europeia, 2016). A partir dessa concepção normativa, observa-se que o ponto de inflexão que aciona os deveres legais em matéria de proteção de dados é, em regra, a quebra nos controles de segurança.

Por outro lado, a perspectiva regulatória da proteção de dados pessoais confere à segurança da informação tradicional uma nova dimensão, qual seja, a que se centra nos riscos aos titulares e nos impactos jurídicos da exposição indevida de seus dados.

Nem todo incidente de segurança nos sistemas de tecnologia da informação ensejará, por si só, consequências no âmbito da LGPD. Isso porque, situações como o caso de interrupção de um serviço digital ou de comprometimento de credenciais administrativas, pode ser grave do ponto de vista operacional, mas, na ausência de violação de dados pessoais, não enseja necessariamente a incidência dos deveres previstos na legislação de proteção de dados (Blum; Vainzof; Moraes, 2021).

Contudo, uma vez confirmada a exposição de dados pessoais, especialmente dados sensíveis, passa-se a exigir avaliação jurídica específica dos potenciais danos à privacidade, à integridade moral e à segurança individual dos titulares, sendo este o contexto que demanda a atuação coordenada entre as equipes técnicas de segurança da informação e o encarregado pelo tratamento de dados (DPO) no âmbito dos órgãos públicos, de modo a assegurar uma resposta institucional que concilie, de forma simultânea, os requisitos técnicos – contenção, erradicação e recuperação – e os deveres legais previstos na LGPD – tais como o de comunicação à ANPD, suporte aos titulares e mitigação de danos individuais.

Portanto, da relação entre segurança da informação e proteção de dados pessoais, infere-se que a primeira é responsável por fornecer os instrumentos operacionais e tecnológicos de prevenção, detecção e contenção de ameaças, ao passo que a segunda define o conteúdo jurídico a ser tutelado – os dados pessoais – e os direitos fundamentais a ele vinculado.

No contexto da Administração Pública, essa integração se expressa por meio de práticas como capacitações conjuntas em privacidade e segurança, avaliações de impacto à proteção de dados que contemplam requisitos técnicos de segurança, e pela internalização do princípio da privacidade desde a concepção e por padrão (*data protection by design* e *data protection by default*), o qual determina a incorporação de medidas de segurança já na fase de concepção de sistemas informatizados ou de políticas públicas que possam envolver o tratamento de dados pessoais (Blum; Vainzof; Moraes, 2021).

4. Incidentes de Segurança na Lei N.º 13.709/18 (LGPD)

A LGPD não consagra definição expressa para os termos "incidente de segurança" ou "violação de dados pessoais". Não obstante, a norma dispõe sobre as obrigações decorrentes de tais eventos, circunstância que permite a extração dos contornos normativos e operacionais de ambos os conceitos, *ex vi lege*:

> Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.
> § 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:
> I - a descrição da natureza dos dados pessoais afetados;
> II - as informações sobre os titulares envolvidos;
> III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
> IV - os riscos relacionados ao incidente;
> V - os motivos da demora, no caso de a comunicação não ter sido imediata; e
> VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.
> § 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:
> I - ampla divulgação do fato em meios de comunicação; e
> II - medidas para reverter ou mitigar os efeitos do incidente.
> § 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.
> Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares. (Brasil, 2018)

Nos termos do mencionado art. 48 da LGPD, a obrigatoriedade de comunicação à ANPD e, quando cabível, aos titulares dos dados, está condicionada à existência de risco ou dano relevante aos direitos dos titulares. Assim, nem todo incidente, por si só, enseja dever de notificação, dado que somente aqueles com potencial de impacto significativo sobre a esfera jurídica dos titulares – notadamente em termos de privacidade, segurança, reputação ou integridade pessoal – serão alvo de tutela específica no contexto da LGPD.

Importa destacar que o conceito abrange tanto situações decorrentes de ação dolosa – como ataques cibernéticos externos, vazamentos deliberados por agentes internos ou fraudes intencionais – quanto eventos acidentais, resultantes de falhas humanas, deficiências técnicas ou vulnerabilidades não corrigidas. Em ambos os casos, a característica essencial é a quebra das salvaguardas de segurança que deveriam assegurar o tratamento adequado dos dados, expondo-os a acessos indevidos ou usos incompatíveis com a finalidade autorizada.

A título de exemplos representativos, tem-se: as invasões a sistemas públicos que armazenam bases cadastrais sensíveis; extravio ou furto de dispositivos contendo bancos de dados desprotegidos; publicação não autorizada de dados pessoais em portais institucionais; ou o envio indevido de informações sigilosas a destinatários equivocados.

O art. 48 da LGPD recebeu regulamentação minudente por parte do ente regulador por meio da Resolução CD/ANPD n.º 15/24 que aprovou o Regulamento de Comunicação de Incidentes de Segurança (RCIS), segundo a qual o controlador deve comunicar à ANPD a ocorrência de incidente de segurança de dados pessoais no prazo de até três dias úteis contados do momento em que tiver conhecimento da ocorrência (Brasil, 2024).

O mesmo prazo se aplica, quando cabível, à comunicação aos titulares afetados, revelando, na prática, um alinhamento substancial com a regra de 72 horas do art. 33 do GDPR (União Europeia, 2016), ainda que com adaptações terminológicas e procedimentais ao contexto regulatório brasileiro, veja-se:

> 1. No caso de uma violação de dados pessoais, o responsável pelo tratamento deve, sem demora injustificada e, sempre que possível, no prazo máximo de 72 horas após ter tomado conhecimento da mesma, notificar a violação de dados pessoais à autoridade de controlo competente nos termos do artigo 55.º , a menos que seja pouco provável que a violação de dados pessoais resulte num risco para os direitos e liberdades das pessoas singulares. Se a notificação à autoridade de controlo não for efetuada no prazo de 72 horas, deve ser acompanhada dos motivos do atraso.
> 2. O processador deverá notificar o controlador sem demora injustificada após tomar conhecimento de uma violação de dados pessoais.
> 3. A notificação referida no parágrafo 1 deve, pelo menos: (a) descrever a natureza da violação de dados pessoais, incluindo, sempre que possível, as categorias e o número aproximado de titulares de dados envolvidos e as categorias e o número aproximado de registros de dados pessoais envolvidos; (b) comunicar o nome e os dados de contacto do responsável pela proteção de dados ou de outro ponto de contacto onde possam ser obtidas mais informações; (c) descrever as prováveis consequências da violação de dados pessoais; (d) descrever as medidas tomadas ou

> propostas pelo controlador para lidar com a violação de dados pessoais, incluindo, quando apropriado, medidas para mitigar seus possíveis efeitos adversos.
> 4. Quando, e na medida em que, não for possível fornecer as informações ao mesmo tempo, as informações poderão ser fornecidas em fases, sem atrasos indevidos.
> 5. O controlador deverá documentar quaisquer violações de dados pessoais, incluindo os fatos relacionados à violação de dados pessoais, seus efeitos e as medidas corretivas tomadas. Essa documentação deverá permitir que a autoridade de supervisão verifique o cumprimento deste artigo. (União Europeia, 2016)

A partir dessas premissas, pode-se inferir que o incidente reportável – ou, portanto, o incidente de segurança relevante para a LGPD – é aquele que envolva, de forma efetiva ou provável, a violação de deveres de confidencialidade, integridade ou disponibilidade de dados pessoais, aliado ao fator prejudicial aos respectivos titulares.

Portanto, não constituirão incidentes para fins exigidos para a LGPD, por exemplo, falhas técnicas internas ou indisponibilidades temporárias de sistemas que não impliquem em comprometimento de dados pessoais, ao passo que certamente atrairão a incidência das normas de proteção de dados as situações de vazamento – aqui entendido como coleta, acesso, divulgação ou repasse indevido – de dados pessoais a terceiros não autorizados.

Neste último caso, a notificação à ANPD e aos titulares afetados revela-se imprescindível, mormente porque tal ocorrência pode ensejar consequências graves, tais como fraudes, práticas de engenharia social, golpes financeiros e comercialização ilícita de dados, afetando diretamente a privacidade, a segurança e a integridade dos titulares envolvidos.

Oportuno destacar, ainda, que a LGPD impõe aos agentes de tratamento o dever de manter registros formais dos incidentes de segurança ocorridos, documentando de forma adequada as circunstâncias do evento, as medidas de resposta adotadas e a análise de risco correspondente. O RCIS, por sua vez, reforça esse dever documental ao estabelecer, em seu art. 16, a obrigatoriedade de preservação dos registros por, no mínimo, cinco anos – sendo que tal exigência se aplica inclusive aos incidentes que, após avaliação técnica, não tenham ensejado uma comunicação à ANPD.

Com efeito, a manutenção desse histórico não apenas concretiza o princípio da responsabilização e prestação de contas (*accountability*), como também serve como evidência da diligência institucional em caso de auditorias ou fiscalizações futuras. Ademais, o exame sistemático desses registros permite a identificação de padrões de vulnerabilidade recorrentes e o aperfeiçoamento contínuo das medidas

de segurança e governança de privacidade.

No contexto da Administração Pública, alguns incidentes emblemáticos ilustram a magnitude dos riscos associados ao tratamento de dados pessoais. Em novembro de 2020, o Superior Tribunal de Justiça (STJ) sofreu um ataque de *ransomware* que comprometeu integralmente o acesso aos seus sistemas processuais eletrônicos, resultando na paralisação das sessões e na indisponibilidade dos dados judiciais, representando um episódio que evidenciou os riscos à continuidade da prestação jurisdicional (Brasil, 2020).

Em dezembro de 2021, o Ministério da Saúde foi alvo de invasão por agentes vinculados ao grupo "*Lapsus$*", que comprometeram a plataforma ConecteSUS, afetando a emissão de certificados de vacinação contra a COVID-19 e gerando o risco de exposição massiva de dados sensíveis da população. Ainda em 2020, identificou-se a extração indevida de uma base contendo dados de aproximadamente 243 milhões de pessoas – número que, paradoxalmente, supera a população brasileira –, obtida por meio da exploração de vulnerabilidades em sistemas governamentais, revelando a extensão potencial de um incidente envolvendo estruturas públicas (Brasil, 2021).

Tais ocorrências reforçam a razão pela qual a LGPD, em convergência com os marcos internacionais, enfatiza a necessidade de estratégias robustas de prevenção, detecção e resposta a incidentes. Considerando que os órgãos públicos detêm bases expressivas de dados pessoais, a ocorrência de uma única falha de segurança pode repercutir em escala nacional, afetando não apenas os direitos fundamentais dos indivíduos diretamente envolvidos, mas também a credibilidade institucional e a confiança da sociedade nas estruturas estatais.

Neste particular, sabe-se que um incidente de vazamento de dados pessoais pode ensejar uma cadeia de riscos interconectados e de múltiplas dimensões, a exemplo: (*i*) risco operacional: compromete a continuidade dos serviços essenciais, como evidenciado nos ataques ao STJ (2020) e ao Ministério da Saúde (2021); (*ii*) risco financeiro: manifesta-se em despesas extraordinárias com resposta técnica, reforço de segurança e, em casos mais graves, indenizações judiciais por violação de dados, ainda que órgãos públicos não estejam sujeitos a sanções pecuniárias pela ANPD; (*iii*) risco reputacional: os danos à imagem do ente público e à confiança institucional são intensificados pela obrigatoriedade legal de fornecimento de dados pessoais à Administração, de modo que incidentes como o megavazamento de dados de saúde em 2021 e a interrupção do ConecteSUS em 2021 abalam a credibilidade dos serviços públicos digitais, desestimulando sua utilização pela sociedade; (*iv*) risco regulatório: decorre da atuação da ANPD e de órgãos de controle, os quais podem instaurar procedimentos administrativos e impor medidas corretivas,

mesmo quando não se aplicam multas pecuniárias; (*v*) risco jurídico: refere-se ao ajuizamento de ações judiciais individuais ou coletivas por titulares de dados, com base na violação de direitos da personalidade, além da responsabilização funcional de agentes públicos por omissão ou negligência grave; e, por fim, (*vi*) risco político: gestores públicos podem ter sua imagem abalada, com consequências políticas e administrativas.

Destarte, conforme assinalado, tais riscos não operam de forma isolada, sendo certo que um único incidente pode desencadear simultaneamente todos esses impactos, a exemplo: imagine-se um vazamento de dados cadastrais e biométricos de eleitores por parte de um órgão público federal, neste caso a administração poderá enfrentar a necessidade de mitigar o dano operacional (resposta emergencial e reconfiguração de sistemas), suportará custos significativos (contratação de perícia, reforço de segurança), sofrerá desgaste público e político (reputação institucional e confiança no processo eleitoral), será submetida à apuração pela ANPD e demais órgãos de controle (risco regulatório), e, por fim, poderá ser acionada judicialmente por titulares afetados ou por partidos políticos (risco jurídico).

5. Medidas de Conformidade Frente a um Incidente de Segurança de Dados no Setor Público

O Plano de Resposta a Incidentes de Segurança de Dados Pessoais consiste em um instrumento normativo-organizacional que estabelece, de forma estruturada e previamente definida, os procedimentos operacionais a serem adotados diante da ocorrência de eventos que comprometam a segurança de dados sob a guarda da instituição.

Trata-se de documento formal, usualmente vinculado ao Programa de Governança em Privacidade e Segurança da Informação, que define, com clareza, os fluxos de atuação, os agentes responsáveis, os critérios de classificação e os protocolos de resposta aplicáveis às diversas hipóteses de incidentes de segurança envolvendo dados pessoais.

A elaboração do plano deve observar, cumulativamente, os requisitos legais previstos da LGPD – especialmente aqueles constantes do art. 48 relativos à notificação de incidentes com potencial de risco ou dano relevante aos titulares – e as boas práticas consagradas em normativos técnicos internacionais, como a NIST SP 800-61 e ISO/IEC 27035.

Neste particular, a partir das orientações e premissas contidas nas normas de regência e considerando as boas práticas adotadas por organismos internacionais em situações similares, tem-se como razoável considerar que um plano de resposta bem delineado deverá, em maior ou menor medida, contemplar os seguintes componentes:

a) ***Política de Resposta a Incidentes:***

Trata-se do documento formal de compromisso do ente com a gestão de incidentes de segurança, que delimita o escopo de aplicação (sistemas, unidades e categorias de dados abrangidos), estabelece definições técnicas e jurídicas pertinentes (conceito de incidente, níveis de severidade, tipologia de dados afetados) e explicita a articulação com outros instrumentos institucionais, como o Plano de Continuidade de Negócios e o Plano de Comunicação de Crises.

b) ***Equipe de Resposta a Incidentes:***

Requisito que deve ser expressamente identificado no plano, com definição clara das atribuições funcionais de seus integrantes.

No âmbito da Administração Pública, a equipe deve obrigatoriamente envolver o Encarregado pelo Tratamento de Dados Pessoais (DPO), além de representantes das áreas de tecnologia da informação, segurança da informação, assessoria jurídica, comunicação e, quando cabível, das áreas finalísticas diretamente impactadas.

Assim, caberá ao plano de gestão de incidentes de segurança de dados atribuir responsabilidades específicas – por exemplo, identificação e contenção técnica do incidente, condução da análise de impacto, elaboração de notificações à ANPD e aos titulares, validação de comunicações externas e articulação com órgãos de controle.

c) ***Classificação de incidentes:***

O plano também deve prever critérios objetivos para a classificação da gravidade dos incidentes, levando em consideração fatores como a natureza e a sensibilidade dos dados afetados, o volume de registros comprometidos, o número de titulares impactados, a criticidade dos serviços eventualmente afetados e os riscos potenciais à integridade e privacidade.

A classificação poderá adotar escalas de severidade (baixa, moderada, alta, crítica), com base em modelos técnicos como o da ENISA, que sugere a ponderação de elementos como: categoria dos dados, possibilidade de identificação dos titulares, tipo de violação (confidencialidade, integridade, disponibilidade) e grau de impacto.

d) ***Fluxo de resposta:***

O plano de resposta deve prever, de forma encadeada, as etapas que compõem o fluxo de resposta institucional, desde a detecção inicial até o encerramento formal do ciclo, sendo oportuno a inclusão das seguintes fases:

- *Detecção e análise*: etapa em que a ocorrência do incidente é identificada e submetida a análise preliminar. Envolve a utilização de mecanismos técnicos

de monitoramento e detecção (tais como logs, alertas de antivírus, sistemas de detecção de intrusão) e a triagem inicial por parte da equipe responsável, a fim de distinguir eventos reais de falsos positivos. Confirmado o incidente, deve-se iniciar a coleta de evidências, identificar os sistemas e dados envolvidos e avaliar, ainda que preliminarmente, a extensão e a criticidade da violação;

- *Contenção*: etapa em que são adotadas medidas emergenciais com vistas a impedir a progressão dos danos (a exemplo: isolamento de dispositivos comprometidos, a desativação temporária de sistemas, a aplicação de atualizações de segurança e a alteração imediata de credenciais expostas;

- *Erradicação*: superada a etapa anterior, a atenção se volta à eliminação da causa raiz do incidente. Essa etapa pode compreender a remoção completa de códigos maliciosos, a revogação de acessos indevidamente concedidos ou a revisão de falhas processuais que tenham contribuído para a ocorrência. Embora interdependente da fase anterior, a erradicação visa restaurar a segurança do ambiente de forma estrutural, eliminando vulnerabilidades que poderiam ensejar recorrência de incidentes;

- *Recuperação*: etapa em que se inicia o processo de restauração dos sistemas e serviços impactados, incluindo-se a restauração de backup, a reativação gradual de servidores, a execução de testes de integridade e a validação da normalização do ambiente. Durante esta etapa, deve ser mantido monitoramento reforçado a fim de identificar eventuais resquícios da ameaça ou reincidência do evento;

- *Comunicação e notificação*: trata-se de fase independente que pode – e deve – ocorrer de maneira paralela às etapas anteriores. O plano deve estabelecer os protocolos de comunicação interna e externa, a fim de viabilizar a notificação à ANPD e até três dias úteis por meio de formulário padronizado, bem como a comunicação dos titulares de dados nos casos em que o incidente gerar risco ou dano grave e, finalmente, nos casos de incidentes de maior repercussão social, o plano deve prever medidas de comunicação institucional com o público em geral, inclusive com a elaboração de notas oficiais, designação de porta-voz para o gerenciamento de crise reputacional;

O fluxo de atuação em resposta a incidentes de segurança de dados pode ser visualizado da seguinte maneira, veja-se:

(Fonte: elaborado pelo autor)

Finalmente, por oportuno, destaca-se que em âmbito federal a estruturação de um plano de resposta a incidentes deve, obrigatoriamente, considerar a articulação com instâncias especializadas de apoio técnico e coordenação institucional. Destaca-se, nesse sentido, o papel do Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov), vinculado ao Gabinete de Segurança Institucional da Presidência da República (GSI/PR), que atua como núcleo de referência na gestão de incidentes cibernéticos de alto impacto envolvendo órgãos da esfera federal.

6. Conclusão

O uso de dados pessoais pelo Poder Público impulsionado pela digitalização de serviços, pela interoperabilidade de bases e pelo uso de tecnologias da informação na formulação e execução de políticas públicas, impôs aos entes estatais o dever de estruturar mecanismos efetivos de prevenção e resposta a incidentes de segurança.

A promulgação LGPD consolidou esse dever abstrato em norma cogente, elevando a proteção de dados à condição de obrigação legal, exigível de todos os agentes de tratamento, públicos ou privados. Nesse cenário, a elaboração e implementação de planos de resposta a incidentes, integrados à governança institucional, deixaram de ser uma recomendação técnica e passaram a configurar exigência normativa vinculante.

Ao longo deste estudo, demonstrou-se que a governança de privacidade, quando ancorada em estruturas corporativas sólidas e controles internos robustos, fornece a base necessária para o cumprimento sistemático da LGPD na Administração Pública.

Atribuição de responsabilidades, como a designação formal do Encarregado pelo Tratamento de Dados Pessoais (DPO), a definição de políticas internas e a incorporação de rotinas de compliance com foco em proteção de dados, são medidas que evidenciam o comprometimento institucional com a legalidade e a *accountability*.

Nesse arranjo, a segurança da informação não é acessória, mas eixo estruturante: sua fragilização compromete a totalidade do sistema protetivo. A definição jurídica de incidente de segurança como qualquer evento que envolva violação de dados com potencial dano a titulares impõe às instituições resposta tempestiva, transparente e tecnicamente adequada – conforme, aliás, exige o art. 48 da LGPD e as diretrizes da Resolução CD/ANPD n.º 15/24.

Examinaram-se, ainda, os principais riscos decorrentes de incidentes de vazamento de dados pessoais na esfera pública, com destaque para os impactos operacionais, financeiros, reputacionais, regulatórios, jurídicos e políticos, ocasião em que se evidenciou a presença concreta de tais riscos na experiência recente do setor público brasileiro, circunstância que revela a necessidade de planos de resposta abrangentes, articulando dimensões técnicas, normativas e comunicacionais, com protocolos de detecção, contenção, erradicação e recuperação devidamente formalizados.

No plano operacional devem ser delineadas medidas de resposta imediata – como isolamento de sistemas, escalonamento interno da informação, preservação de evidências e comunicação transparente – e de prevenção continuada, que compreendem capacitações regulares, aprimoramento de controles de acesso, uso de criptografia, auditorias de segurança e simulações periódicas de incidentes.

Finalmente, impõe-se ponderar que a atuação da Administração Pública quanto ao cumprimento da LGPD deve almejar, de maneira contínua, construir um vetor de fortalecimento da relação entre o Estado e o cidadão, pois, toda vez que um indivíduo fornece dados pessoais a um órgão público, deposita neles uma confiança

legítima de que tais informações serão tratadas com zelo, finalidade específica e proteção adequada. Neste particular, o plano para resposta a incidentes de segurança surge como o instrumento capaz de materializar este dever institucional, na medida em que sinaliza que, mesmo diante de falhas ou ataques, o Poder Público estará preparado para agir.

Conclui-se, portanto, que, em um cenário em que os dados pessoais equivalem a ativos estratégicos da sociedade, sua proteção pelo Estado é expressão direta do dever constitucional de assegurar os direitos fundamentais e garantir a integridade das políticas pública, cabendo a este prevenir e responder a incidentes de segurança de dados por meio de um processo essencialmente evolutivo: não há estágio final de conformidade, mas sim um compromisso institucional permanente com a melhoria contínua.

REFERÊNCIAS

BLUM, Renato Opice; VAINZOF, Rony; MORAES, Henrique Fabretti. *Data Protection Officer (Encarregado)*: Teoria e Prática de acordo com a LGPD e GDPR. São Paulo: Thomson Reuters, 2. ed. rev., atual. e ampl., 2021.

BRASIL. Autoridade Nacional de Proteção de Dados. *Resolução CD/ANPD nº 15, de 24 de abril de 2024*. Regulamento de Comunicação de Incidentes de Segurança (RCIS). Brasília, DF: Autoridade Nacional de Proteção de Dados, 2024. Disponível: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/resolucao-cd-anpd-no-15-de-24-de-abril-de-2024.pdf. Acesso em: 23 mai. 2025.

BRASIL. Presidência da República. *Lei nº 12.527, de 18 de novembro de 2011*. Lei de Acesso à Informação (LAI). Brasília, DF: Presidência da República, 2011. Disponível: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 23 mai. 2025.

BRASIL. Presidência da República. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 20 mai. 2025.

BRASIL. Polícia Federal. *Atuação da PF no ataque hacker ao Ministério da Saúde. Brasília, DF*: Polícia Federal. Disponível: https://www.gov.br/pf/pt-br/assuntos/noticias/2021/12/atuacao-da-pf-no-ataque-hacker-ao-ministerio-da-saude. Acesso em: 23 mai. 2025.

BRASIL. Serviço Federal de Processamento de Dados. *Violação de dados pessoais*: o que fazer antes, durante e depois de um incidente? Disponível: https://www.serpro.gov.br/menu/noticias/noticias-2022/o-que-fazer-em-caso-de-violacao-de-dados-pessoais. Acesso em: 20 mai. 2025.

BRASIL. Superior Tribunal de Justiça. *Em razão de ataque cibernético, STJ funcionará em regime de plantão até o dia 9*. Brasília, DF: Superior Tribunal de Justiça. Disponível: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/04112020-Em-razao-de-ataque-cibernetico–STJ-funcionara-em-regime-de-plantao-ate-o-dia-9.aspx. Acesso em: 23 mai. 2025.

UNIÃO EUROPEIA. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016*: relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral

sobre a Proteção de Dados – GDPR). Jornal Oficial da União Europeia. Disponível: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679. Acesso em: 23 mai. 2025.

YEE, Chai Kar; ZOLKIPLI, Mohamad Fadli. *Review on Confidentiality, Integrity and Availability in Information Security. Journal of ICT in Education (JICTIE)*, vol. 8, issue n.º 2, p. 34-42, 2021. Disponível: https://doi.org/10.37134/jictie.vol8.2.4.2021. Acesso em: 20 mai. 2025.

7

Desafios e Soluções na Implementação da Lei Geral de Proteção de Dados (LGPD) no Setor Público: o caso da Prefeitura de Manaus

Prefeitura Municipal de Manaus

Estudo de caso municipal completo com análise SWOT e metodologias práticas para implementação da LGPD.

Joabe Cota Riker

Professor de Ensino Superior, Contador, Bacharel em Economia, Mestre em Engenharia de Produção pela UFAM.

Lucilene Florêncio Viana

Professora de Ensino Superior, Contadora, Mestra em Contabilidade e Controladoria pela UFAM.

Gleuson Silva Chaves

Contador, Pós-graduado em Auditoria e Controladoria pela Faculdade Martha Falcão.

Lorena de Oliveira Pereira

Contadora, Pós-graduanda em MBA em Auditoria e Auditoria pela UEA.

Marcos Laylson Nunes da Silva

Bacharel em Direito, Pós-graduando em Licitações Públicas e Contratos Administrativos, e em Controladoria e Finanças Públicas pelo Gran Centro Universitário.

Resumo

A Lei nº 13.709/2018, Lei Geral de Proteção de Dados (LGPD), busca garantir a privacidade e liberdade dos indivíduos ao regulamentar o tratamento de dados pessoais e sensíveis, incluindo o setor público. Diante das vulnerabilidades observadas em órgãos governamentais, esta pesquisa analisou os desafios da implementação da LGPD na Prefeitura de Manaus, identificando vulnerabilidades e oportunidades de melhoria. O estudo adotou uma abordagem normativa-jurídica exploratória, com revisão bibliográfica e análise de leis, além de um estudo de caso na Controladoria-Geral do Município (CGM). A Prefeitura demonstrou forças, como diretrizes claras e experiência em dados sensíveis, mas enfrenta fraquezas, como sistemas legados e recursos limitados. Oportunidades incluem a modernização dos sistemas e o fortalecimento da confiança pública, enquanto as ameaças englobam sanções e danos à reputação. A implementação da LGPD exigiu reestruturação de processos e capacitação contínua, revelando-se um desafio multifacetado. O estudo concluiu que, apesar das dificuldades, houve avanços na governança de dados, destacando a importância da sinergia entre LGPD, governança e compliance para otimizar serviços e garantir a segurança da população. A continuidade dos investimentos em treinamento e integridade é fundamental para consolidar as melhorias obtidas.

Palavras-chave: Lei Geral de Proteção de Dados, Dados Sensíveis, Governança Pública.

1. Introdução

A Lei Geral de Proteção de Dados (LGPD), instituída pela Lei nº 13.709 em 14 de agosto de 2018, regulamentada no município de Manaus por meio do Decreto nº 5.621, de junho de 2023, alterado pelo Decreto nº 6.124, de 29 de abril de 2025, tem como propósito garantir a privacidade, a liberdade e o desenvolvimento pessoal dos indivíduos. A legislação estabelece diretrizes de governança e boas práticas, permitindo aos responsáveis pelo tratamento de dados definir regras de organização, segurança, procedimentos para reclamações e petições, normas técnicas e mecanismos de controle e mitigação de riscos. A partir da promulgação deste dispositivo, houve uma corrida para a adaptação do setor público às suas exigências (Machado, Oliveira Filho & Queiroz, 2023).

A LGPD regulamenta o tratamento de informações pessoais, inclusive dados sensíveis em ambientes digitais, com o objetivo de resguardar os direitos fundamentais de privacidade e liberdade dos indivíduos. Segundo a legislação, dados sensíveis incluem informações sobre origem racial ou étnica, crenças religiosas, posicionamento político, vínculo com sindicatos ou entidades religiosas, filosóficas ou políticas, além de dados relacionados à saúde, vida sexual, genética ou biometria, sempre que estejam associados a uma pessoa física (Brasil, 2018).

Para garantir a segurança dos dados, foi implementada uma estrutura de governança digital federal, abrangendo toda a administração pública, centralizando informações (Brasil, 2017). Uma auditoria do TCU sobre a governança digital da Administração Pública Federal apontou que, apesar do cumprimento adequado dos procedimentos formais, ainda há fragilidades na gestão de riscos, sobretudo na transformação digital (Brasil, 2021). Uma dessas vulnerabilidades é a não cobertura completa da complexidade desse ambiente, que resulta em lacunas na definição de responsabilidades, afetando tanto o setor público quanto o privado (Brasil, 2011).

As normas regulatórias priorizam a proteção de dados sensíveis, que podem ser expostos inadvertidamente em bancos de dados públicos. Por isso, é essencial que as informações tratadas sejam estritamente relevantes às necessidades dos cidadãos (Brasil, 2018). Nesse sentido, tendo em vista a vulnerabilidade enfrentada por diversos órgãos públicos, com dificuldades semelhantes entre si em todas as esferas de governo, surge a seguinte questão de pesquisa: **quais ferramentas podem ser utilizadas para superar os desafios enfrentados na adaptação à LGPD, na Prefeitura de Manaus?**

O objetivo geral é identificar vulnerabilidades relacionadas ao processo de implantação da LGPD na Prefeitura de Manaus.

Para tal, os objetivos específicos incluem:

a) Avaliar a eficácia da proteção de dados sensíveis, considerando as particularidades locais;
b) Explorar oportunidades para a aplicação eficiente dos dispositivos legais no

tratamento de dados sensíveis da população de Manaus; e

c) Sugerir medidas corretivas ao processo de implementação, se necessário for, para garantir a conformidade administrativa e o respeito ao *compliance*.

A justificativa da pesquisa se dá pela relevância do tema, uma vez que há a obrigatoriedade entre os entes públicos em promover a transparência e o acesso à informação de forma democrática. Porém, devido aos avanços tecnológicos, há um aumento significativo nos vazamentos de dados sensíveis, evidenciando fragilidades nos sistemas internos de órgãos governamentais (Brasil, 2011). Uma análise de dados disponibilizados virtualmente por diversas prefeituras no país, revelou falhas nos sistemas de gestão, e isso levou o Brasil, em 2022, a liderar casos de vazamento de dados em todo o mundo (Campos, 2022). Assim, tornou urgente as ações de melhoria na administração dos bancos de dados da Administração Pública como um todo.

2. Referencial Teórico

2.1 Contexto Histórico da Lei 13.709, de 14 de agosto de 2018

Para entender o motivo dos entes adaptarem-se aos aspectos gerais de um normativo legal, faz-se importante apresentar as necessidades da sua promulgação. Nesse sentido, a Lei nº 13.709, de 14 de agosto de 2018, popularmente conhecida como Lei Geral de Proteção de Dados (LGPD), surgiu com o propósito de garantir a segurança dos dados pessoais, enfatizando a proteção da liberdade, privacidade e do desenvolvimento individual das pessoas naturais. Isto é, proteção, liberdade, privacidade e personalidade. Pilares citados no primeiro artigo da lei (Brasil, 2018).

No ano de 2022, o movimento em torno do tema inspirou formuladores a inserir, através da Emenda Constitucional nº 115, os preceitos da LGPD à Carta Magna. A adição consta no inciso LXXIX, do artigo 5º, assegurando a proteção de dados como direito e garantia fundamental da pessoa humana, inclusive nas plataformas digitais (Brasil, 1988). A inclusão do inciso reforçou a importância da regulamentação e reflete a preocupação com a segurança no trato das informações pessoais, sobretudo no meio digital.

Importante mencionar, dentro desse resgate histórico, que antes mesmo da emenda de 2022, no ano de 2020, o Supremo Tribunal Federal (STF), por meio de Ação Direta de Inconstitucionalidade nº 6387, afirmou que o direito à proteção de dados e a liberdade de decidir sobre seu uso, são direitos fundamentais autônomos, derivados da garantia de privacidade (art. 5º, X), do princípio da dignidade humana (art. 1º, III) e do *habeas data* (art. 5º, LXXII) (Brasil, 2020). Dessa forma, a emenda oficializou um valor intrínseco, já defendido na jurisprudência como constitucional.

O especialista *Opice Blum* aponta que a LGPD foi inspirada em uma legislação europeia, chamada *General Data Protection Regulation* (GDPR), aprovada naquele

continente no ano de 2016. Entre as principais características da norma está o consentimento prévio do titular para a coleta e tratamento dos dados, sendo responsabilidade da entidade provar que a permissão foi dada e que o titular tem plena ciência sobre isso (Opice Blum, 2018). A norma brasileira prevê ainda uma categoria especial, chamada: "dados pessoais sensíveis". Ela inclui informações como origem racial, opiniões, convicções religiosas, saúde, genética e biometria (Brasil, 2018).

O professor *Marcelo Romão Marineli* explica que a LGPD se aplica a qualquer tratamento de dados realizado por pessoas físicas ou jurídicas, públicas ou privadas cobrindo todas as operações realizadas no Brasil, relacionado aos dados de indivíduos que estão no país ou coletados no território nacional (art. 3º) (Marineli, 2019). E o professor *Danilo Doneda* reforça a importância da LGPD como um marco regulador no Brasil, destacando que a lei é essencial para reorganizar como os dados pessoais são tratados, garantindo privacidade e direitos individuais (Doneda, 2020).

A verdade é que, historicamente a coleta de dados pessoais sempre existiu, seja para registro em compras de bens como imóveis ou veículos, ou para qualquer outro tipo de contrato que exija identificação. A grande questão nesse cenário que motivou a criação da LGPD, foi a maneira como esses dados passaram a ser manipulados e explorados comercialmente. Em 2019, por exemplo, o jornal *The Economist* citou essa problemática ao afirmar que os dados pessoais se tornaram "o novo petróleo", sendo agora o recurso mais valioso do mundo. Daí decorre a necessidade de os entes, redobrarem esforços ao cumprimento desta matéria.

2.2 Modernização da Gestão de Dados Sensíveis

A adaptação à Lei Geral de Proteção de Dados (LGPD), não é uma tarefa simples. Isso é tão verdade que, após promulgada, o processo para que os entes efetivamente respondessem pelo artifício legal passou por dois períodos, compostos por: um prazo curto para a criação da Autoridade Nacional de Proteção de Dados (ANPD) e um prazo mais longo, de 24 meses, para a implementação completa do restante das regras (Brasil, 2019). Na cidade de Manaus, por exemplo, a regulamentação se deu pelo Decreto nº 5.621, publicado somente em junho de 2023. À época, a coleta de dados sensíveis, como as que ocorrem em emissões de guias de serviços *online*, em geral não continha a garantia de que era realizado com segurança, sobretudo nos órgãos municipais, o que necessitou de ajustes.

Nisso, o entendimento geral derivativo da norma deixou evidente a indispensável necessidade da adaptação, pelos entes públicos, às exigências da governança dos dados, incluídos mecanismos de planejamento e controle para a efetiva execução dos pontos descritos na legislação. O objetivo é permitir uma gestão mais eficiente nessa temática, garantindo a segurança das informações da

população. Nesse sentido, o Decreto Federal n.º 9.203 de 2017 define governança como um conjunto de mecanismos estratégicos para avaliar, direcionar e monitorar a administração pública, assegurando serviços de qualidade e políticas eficazes para a sociedade.

A governança de dados fortalece a gestão, a capacidade no atendimento às demandas sociais, de forma célere, e sem perder a eficiência. Afinal, o cerne do serviço público é o promover o bem-estar social por meio da execução de políticas públicas, e claro, dentro desse escopo, cabe a LGPD. Essa, inclusive, é uma forma moderna de se pensar o tratamento dos dados, uma vez que o *compliance* vem se tornando um mecanismo crucial para fomentar programas de governança, elevando a transparência e confiabilidade dos serviços públicos (Balbino & Silva, 2024).

2.3 A Nova Política Integrada com a Tecnologia e Parcerias Estratégicas

O aprimoramento dessa nova política, a da governança, depende da qualificação dos servidores, o que se faz com o intuito de gerar competências inerentes ao fortalecimento da LGPD, em se tratando especificamente dessa matéria. Na medida em que a legislação é aplicada a todos os entes, em todas as esferas de governo, de forma célere e transparente, conforme decisão do Supremo Tribunal Federal no Recurso Extraordinário com Agravo 1.445.879, o qual incluiu até mesmo as Universidades Públicas, criou-se instantaneamente e intuitivamente uma rede de proteção de dados, que mesmo de forma individualizada, trabalha para a melhoria contínua dos serviços prestados à população.

A partir desse entendimento, parcerias estratégicas foram sendo formadas, e programas de capacitação contínua foram sendo estabelecidos pelos órgãos e entidades da administração pública com o intuito de otimizar o tratamento de dados pessoais e sensíveis da população. Esse papel entre os entes é fundamental para gerar um entendimento unificado do que reza a legislação, bem como para estabelecer padrões únicos sobre a preparação e implementação das ações em decorrência da Lei, sobretudo no campo digital, cada vez mais conectado e integrado às políticas governamentais. Nesse contexto, o Decreto Federal nº 9.991/2019, reforça a necessidade de qualificação constante dos agentes públicos.

Importante frisar que a capacitação continuada dos servidores públicos emerge como pilar estratégico para a governança de dados na administração pública brasileira. Diante do cenário complexo imposto pela LGPD e sua interação com a Lei de Acesso à Informação (LAI), é imperativo que a União, Estados e Municípios invistam em programas de qualificação que transcendam o adestramento pontual, alinhando-se a uma nova política integrada de tecnologia e parcerias estratégicas.

Matos (2023) afirma que tais iniciativas devem visar a internalização de uma cultura de proteção de dados e a otimização de processos, empoderando os agentes públicos a navegarem pela dissonância regulatória e a atuarem como facilitadores

da transparência e garantidores da privacidade. O que se percebe, conforme evidenciado por Lemos e Farias (2022), é que a sintonia entre capital humano e inovação tecnológica, através de colaborações interinstitucionais e parcerias com a academia e o setor privado, não só mitiga os riscos de sanções administrativas e judiciais, como também catalisa a eficiência operacional e a confiança da sociedade na gestão pública de dados.

2.4 Programas de Integridade Enquanto Disseminadores da Cultura de Governança, Fomento ao Compliance e à Proteção de Dados Sensíveis

O *compliance* é um instrumento fundamental para aprimorar a governança pública, fortalecer a proteção de dados e promover transparência na administração municipal. De acordo com a Lei nº 12.846/2013 (Lei Anticorrupção), a adoção de práticas éticas e mecanismos de controle interno são essenciais para prevenir irregularidades e garantir conformidade legal (Silva, 2020).

Além de estabelecer diretrizes para a integridade institucional, o *compliance* contribui para a segurança da informação e a qualidade dos serviços prestados, conforme determinado pelo artigo 55-A da LGPD (Pereira, 2021). A regulamentação mais específica sobre proteção de dados é necessária, como destacado no julgamento do Agravo em Recurso Especial Nº 2.130.619 - SP, que reforça a responsabilidade das instituições na garantia de indenizações em casos de vazamento de informações sensíveis (Mendes, 2022).

Dessa forma, verifica-se o quão imprescindível tornou-se, que órgãos públicos integrem programas de integridade e *compliance* às suas estruturas, fomentando uma cultura organizacional baseada na conformidade e no combate à corrupção. A implementação eficaz depende da cooperação interinstitucional e da criação de incentivos adequados, permitindo um aprimoramento contínuo dos processos administrativos e a proteção dos direitos da população (Carvalho, 2023).

3. Procedimentos Metodológicos

O estudo abrange o município de Manaus, escolhido por sua relevância econômica e interesse público na região Norte do Brasil, e os seus resultados compõem uma Matriz de Análise SWOT. A metodologia da pesquisa adota uma abordagem normativa-jurídica de natureza exploratória, focada em uma revisão bibliográfica de trabalhos correlatos, que abordam o tratamento de dados sensíveis no setor público. Além disso inclui a avaliação de leis, julgamentos e normas, buscando compreender o papel do *compliance* aliado à segurança da informação e à proteção jurídica (Lamy, 2011). A investigação é qualitativa e examina o processo de adaptação da Prefeitura de Manaus ao normativo Geral da Proteção de Dados.

As fontes utilizadas são primárias, como a LGPD, LAI e decretos federais, estaduais e municipais, como o próprio Decreto nº 6.124, de 29 de abril de 2025, e secundárias, derivadas da interpretação de autores sobre essas normas. Os métodos de análise de conteúdo combinam indução, sintetizando padrões a partir de casos repetidos, e dedução, extraindo conclusões a partir de princípios estabelecidos (Bardin, 2011). A pesquisa também se caracteriza como documental, na medida em que examina registros físicos e digitais, coletados na Controladoria-Geral do Município (CGM), Órgão que serviu de Unidade de Observação *in loco* do estudo, além de usar como técnica a análise jurisprudencial de decisões judiciais sobre segurança da informação e vazamento de dados (Queiroz, 2019).

4. Estudo de Caso

Desde 1890, após a Proclamação da República, Manaus passou a ser governada por um chefe do Poder Executivo, inicialmente chamado de Comissário. O título de Prefeito foi instituído em 1926 com a promulgação da Constituição Estadual, sendo atualmente ocupado por David Abisai Pereira de Almeida. A sede histórica da Prefeitura de Manaus é o Paço da Liberdade, um edifício em estilo neoclássico, construído em 1874, que abrigou governos provinciais e republicanos. Em 1917, tornou-se sede administrativa da Prefeitura após a transferência do Governo do Estado para o Palácio Rio Negro. Restaurado e reinaugurado em 2013, hoje abriga o Centro de Memória da Cidade e o Museu Paço da Liberdade, preservando sua arquitetura original.

Atualmente, a Prefeitura funciona em um prédio público na Avenida Brasil, nº 2.971, Bairro Compensa I, onde está localizada a Controladoria-Geral do Município (CGM), Órgão Central do Sistema de Controle Interno do Poder Executivo Municipal, ponto focal para a obtenção de dados desta pesquisa, que atua como responsável pela adaptação da Prefeitura de Manaus à LGPD. Além desta Unidade, o espaço abriga diversas outras Secretarias e Subsecretarias, que atuam no planejamento e gestão dos recursos públicos sob a guarda do município. No total, espalhadas pela cidade, a Prefeitura de Manaus conta com 50 órgãos da administração direta e indireta.

5. Resultados e Discussões

A Lei Geral de Proteção de Dados (LGPD) ainda é um desafio real para muitas prefeituras na atualidade, considerando o lapso temporal desta pesquisa, com a coleta de dados realizada no ano de 2025. Ou seja, levando em conta os vários anos que já se passaram após a publicação da Lei, em 2018. Observa-se que, passar por um processo de adaptação e de mudança de cultura na administração pública leva tempo, depende de inúmeras variáveis e precisa ser pensado, analisado e

estruturado através de planejamento e ações estratégicas.

Na Prefeitura de Manaus, por exemplo, essas ações buscam garantir a privacidade dos cidadãos e a eficiência dos serviços públicos prestados. A LGPD encontra-se em constante evolução no município como um todo, e já passou por diversas etapas, onde cada fase é acompanhada pela Controladoria-Geral do Município (CGM). Para ilustrar os desafios e oportunidades nesse processo na Prefeitura, optou-se por construir uma Matriz de Análise SWOT, e gerar recomendações a partir dos pontos encontrados:

Quadro 1 – Matriz de análise SWOT (FOFA) – LGPD – Prefeitura de Manaus

Forças (Strengths - S)	**Oportunidades (Opportunities - O)**
- Existência de diretrizes e soluções claras (Políticas, Capacitação, Tecnologias, DPO); - Reconhecimento da necessidade de um esforço contínuo para aprimorar políticas, capacitar servidores e investir em tecnologia; - Experiência em lidar com dados sensíveis (saúde, educação, assistência social).	- Possibilidade de fortalecer a confiança da população na administração pública; - Modernização dos sistemas e processos internos, gerando mais eficiência; - Colaboração com outros órgãos públicos e instituições para compartilhamento de boas práticas.
Fraquezas (Weaknesses - W)	**Ameaças (Threats - T)**
- Recursos orçamentários limitados para investimento em tecnologia e segurança da informação; - Sistemas legados que podem não ser facilmente adaptáveis às novas exigências de privacidade; - Falta de conhecimento técnico dos servidores sobre proteção de dados.	- Sanções e multas por descumprimento da LGPD; - Dano à imagem e reputação da Prefeitura em caso de vazamento de dados; - Resistência interna à mudança de processos e culturas; - Aumento da complexidade na gestão de dados.

Fonte: Controladoria-Geral do Município (CGM), Prefeitura de Manaus.

De acordo com os dados coletados na Prefeitura de Manaus, a Lei Geral de Proteção de Dados (LGPD) vem sendo implantada no município com o auxílio de uma empresa de consultoria especializada no tema, contratada para otimizar o processo em todas as Unidades Gestoras do Poder Executivo. Levando em consideração essa informação, têm-se que:

As "forças" existentes, como as diretrizes e soluções claras e a experiência com dados sensíveis, representam um excelente ponto de partida. A nomeação do Encarregado de Dados (DPO) foi um ponto crucial e relevante, que possibilitou suporte ao desenvolvimento de políticas específicas para os dados de maior volume e sensibilidade. No futuro, essas políticas servirão de base para um planejamento estratégico de tecnologia, visando soluções escaláveis e integráveis que reforcem a conformidade e a eficiência.

Quanto às "fraquezas", como recursos orçamentários limitados e sistemas legados, a criatividade para contornar esses problemas é fundamental. Para mitigar a limitação de recursos, a Prefeitura busca parcerias com outros entes para projetos de extensão

em segurança da informação e para explorar soluções de código aberto de baixo custo. Em relação aos sistemas legados, o foco deve ser a segregação dos dados pessoais, minimizando riscos enquanto se planeja a migração futura. A capacitação, por sua vez, pode ser impulsionada com treinamentos internos e o uso de plataformas gratuitas de ensino à distância.

As "oportunidades" inerentes à LGPD, que vão além de custos, podem ser maximizadas. A Prefeitura pode investir em uma comunicação mais ativa internamente, e aumentar o nível de transparência nessa temática, fazendo com que a população se aproxime das ações de LGPD, o que demonstra o compromisso da Prefeitura com a proteção dos dados, e fortalece a confiança da população na gestão pública. A modernização dos sistemas deve ser perseguida também, pois tende a gerar maior agilidade e menos retrabalho, otimizando o serviço público como um todo, o que proporciona maior valor agregado à temática.

Finalmente, para minimizar as "ameaças", como sanções e danos à reputação, ações estratégicas são essenciais, tais como a realização de Avaliações de Impacto à Proteção de Dados (DPIA) nos processos mais críticos, permitirá identificar e mitigar riscos iminentes de sanções. E, a construção de uma cultura de privacidade sólida e contínua, de maneira eficaz e eficiente, validada e certificada por organismos de renome nacional e internacional, pois isso melhora a defesa contra a resistência interna, garantindo a conformidade constante, evitando danos à reputação e multas.

O que se percebe é que a implementação da LGPD em um órgão público municipal, como a Prefeitura de Manaus por exemplo, exige uma abordagem pragmática e fases bem definidas, conciliando a proteção de dados com a realidade dos recursos disponíveis. A chave é a priorização e o esforço contínuo. A adequação à LGPD na Prefeitura de Manaus configurou-se como um desafio multifacetado, a qual demandou uma reestruturação profunda de processos e de mudança na cultura organizacional.

A principal complexidade residiu na necessidade de conciliar a proteção dos dados dos cidadãos à eficiência na prestação de serviços públicos, um equilíbrio que, segundo Cavalcanti *et al*. (2022), é fundamental para a governança de dados. Tanto é fato que, um dos principais obstáculos identificados durante o processo de adequação à LGPD foi o ajuste dos processos internos, que exigiu a revisão e adaptação das rotinas de coleta, armazenamento e uso de dados pessoais.

Complementarmente, a capacitação dos servidores também emergiu como um ponto crítico, sendo que à época, o corpo de servidores possuía limitado conhecimento técnico sobre proteção de dados, portanto, se fez necessário ajustamento através de contínuos treinamentos, cursos, oficinas e capacitações. É nesse sentido que Sarmento (2023), ressalta a urgência de programas de treinamento contínuos para garantir que os funcionários compreendam suas responsabilidades e os princípios da privacidade.

Um outro ponto observado na Prefeitura de Manaus, em relação à LGPD, foi

o enfrentamento a desafios estruturais e operacionais que exigiram planejamento estratégico e investimentos direcionados. Houve a necessidade de contratação de consultoria especializada, porém os recursos financeiros limitados dificultam a modernização tecnológica, e isso acaba refletindo na possibilidade de melhorias no processo de implementação, como medidas de segurança da informação mais robustas, criptografia de dados, e sistemas de gerenciamento e controle centralizados, essenciais para garantir a privacidade dos cidadãos.

Com a publicação da Lei, a Prefeitura de Manaus precisou adaptar-se a todo um processo composto por diversas etapas, até que conseguisse equilibrar a proteção dos dados dos cidadãos com a eficiência dos serviços públicos, garantindo a conformidade com a LGPD, e a partir desse nível, continua trabalhando para atender às necessidades legais da Autoridade Nacional de Proteção de Dados (ANPD), dentro das suas possibilidades gerais.

6. Considerações Finais

Este estudo realizou uma análise com foco na implementação da Lei Geral de Proteção de Dados (LGPD), na Prefeitura de Manaus. O objetivo se propôs a avaliar a eficácia da proteção de dados, considerando as particularidades locais do município. Foram identificadas mudanças nos procedimentos de gestão, que proporcionaram o aprimoramento no processo de tratamento dos dados, coibindo falhas pontuais na administração pública municipal.

A pesquisa foi capaz de explorar as oportunidades para a aplicação eficiente dos dispositivos legais no tratamento de dados sensíveis da população manauara, onde reconheceu-se a necessidade premente de capacitação contínua dos servidores, para que acompanhem as inovações normativas e tecnológicas, garantindo assim, a proteção adequada dos dados. Nesse ínterim, foram sugeridas medidas corretivas ao processo de implementação, visando garantir a conformidade administrativa e o respeito às diretrizes do *compliance*.

Neste ponto, o exame demonstrou a relevância de programas de integridade e *compliance* na administração pública, evidenciando seu papel crucial na correção de falhas e no aprimoramento da gestão de riscos, fomentando a melhoria dos processos. Concluiu-se que, a implementação eficaz da LGPD e o fortalecimento da governança em sinergia com o *compliance*, são premissas essenciais para otimizar os serviços públicos e assegurar a segurança da população diante dos avanços tecnológicos.

Referências

BALBINO, M. R.; SILVA, A. C. R. *O Compliance como instrumento de gestão na administração pública brasileira*: desafios e perspectivas. Revista de Direito Administrativo, Rio de Janeiro, v. 278, n. 3, p. 1-20, jul./set. 2024.

BARDIN, L. *Análise de conteúdo*. Lisboa: Edições 70, 2011.

BRASIL. *Ação Direta de Inconstitucionalidade nº 6387*. Supremo Tribunal Federal, Brasília, DF, 2020. Disponível em: www.stf.jus.br/arquivo/cms/noticianoticiastf/anexo/adi6387mc.pdf. Acesso em: 25 de maio de 2025.

BRASIL. *Decreto nº 9.203, de 22 de novembro de 2017*. Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. Diário Oficial da União, Brasília, DF, 23 nov. 2017.

BRASIL. *Decreto Federal nº 9.991, de 28 de agosto de 2019*. Dispõe sobre a política de desenvolvimento de pessoas da administração pública federal direta, autárquica e fundacional. Diário Oficial da União, Brasília, DF, 29 ago. 2019.

BRASIL. *Emenda Constitucional nº 115, de 10 de fevereiro de 2022*. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais. Diário Oficial da União, Brasília, DF, 11 fev. 2022.

BRASIL. *Lei nº 12.527, de 18 de novembro de 2011*. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Diário Oficial da União, Brasília, DF, 18 nov. 2011.

BRASIL. *Lei nº 12.846, de 1º de agosto de 2013*. Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências. Diário Oficial da União, Brasília, DF, 2 ago. 2013.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018.

BRASIL. *Recurso Extraordinário com Agravo 1.445.879*. Supremo Tribunal Federal, Brasília, DF. Disponível em: https://revistalexlab.org/index.php/lexlab/article/download/12/11/37. Acesso em: 25 de maio de 2025.

BRASIL. Tribunal de Contas da União. *Relatório de Auditoria Operacional sobre Governança Digital na Administração Pública Federal*. Brasília, DF: TCU, 2021.

CAMPOS, P. B*rasil lidera casos de vazamento de dados no mundo em 2022*. Tecmundo, 2022. Disponível em: https://www.tecmundo.com.br/seguranca/233215-brasil-teve-2-8-bilhoes-dados-expostos-2021.htm. Acesso em: 25 de maio de 2025.

CARVALHO, A. C. *Programas de integridade e a governança pública*: desafios e perspectivas. Revista de Direito Público, [S. l.], v. 50, n. 1, p. 1-15, jan./abr. 2023.

CAVALCANTI, A. F. et al. *Governança de dados na administração pública*: o equilíbrio entre a proteção e a eficiência. Revista da Controladoria-Geral da União, Brasília, DF, v. 14, n. 21, p. 1-18, jul./dez. 2022.

DONEDA, D. *Da privacidade à proteção de dados pessoais*. São Paulo: Saraiva Educação, 2020.

LAMY, M. *O método da pesquisa jurídica*: abordagem teórica. Revista de Direito Público, Rio de Janeiro, v. 15, n. 1, p. 11-28, jan./abr. 2011.

LEMOS, J.; FARIAS, F. *O impacto da inovação tecnológica na gestão pública*: a sintonia entre capital humano e novas ferramentas. Revista de Administração Pública, Rio de Janeiro, v. 56, n. 4, p. 556-570, jul./ago. 2022.

MACHADO, L. C. P.; OLIVEIRA FILHO, J. B.; QUEIROZ, S. A. G. O. *A adaptação do setor público à LGPD: desafios e perspectivas*. Revista do Serviço Público, Brasília, DF, v. 74, n. 1, p. 1-25, jan./mar. 2023.

MANAUS. *Decreto nº 5.621, de 30 de junho de 2023*. Dispõe sobre a privacidade e proteção de dados no âmbito da Administração Pública Municipal. Manaus, AM: Prefeitura de Manaus, 2023.

MANAUS. *Decreto nº 6.124, de 29 de abril de 2025*. Dispõe sobre as diretrizes para a aplicação da Lei Federal nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais – LGPD, a instituição do Sistema de Privacidade e Proteção de Dados, o Comitê de Privacidade e Proteção de Dados no âmbito da Administração Pública Municipal e dá outras providências. Manaus, AM: Prefeitura de Manaus, 2025.

MARINELI, M. *LGPD: Lei Geral de Proteção de Dados*. São Paulo: Saraiva Educação, 2019.

MATOS, C. P. B. *Capacitação continuada de servidores públicos e a cultura de proteção de dados*: um estudo sobre a LGPD. Revista de Administração Pública, Rio de Janeiro, v. 57, n. 3, p. 300-315, maio/jun. 2023.

MENDES, G. F. *Agravo em Recurso Especial Nº 2.130.619 - SP*. Superior Tribunal de Justiça, Brasília, DF, 2022. Disponível em: https://scon.stj.jus.br/SCON/pesquisar.jsp?b=ACOR&livre=%28ARESP.

8

Integração LGPD, ISO 27001 e ISO 27701: Uma Abordagem Holística

Processamento de Dados Amazonas S.A.

Visão técnica avançada sobre integração de diferentes frameworks normativos na prática da administração pública.

Emerson Silva de Souza

Assessor / Encarregado de Proteção de Dados

Bacharel em Ciência da Computação, Espec. Gerenciamento de Projetos, Certificações em EXIN Certified DPO, OneTrust Certified Privacy e participação ativa como Membro Titular do Grupo de Trabalho de Segurança da Informação da ABEP-TIC, Membro Titular do Sub-grupo de Segurança Cibernética do GTD.GOV e Membro Titular da Rede de Encarregados de Proteção de Dados do Amazonas.

Resumo

Este artigo analisa os benefícios da integração entre a Lei Geral de Proteção de Dados (LGPD) e as normas internacionais ISO/IEC 27001 e ISO/IEC 27701 a partir de uma abordagem holística. A pesquisa, de natureza qualitativa e exploratória, fundamenta-se em revisão bibliográfica e documental, e discute como essa integração pode contribuir para a redução de riscos, o aumento da confiança dos clientes e a melhoria da reputação organizacional. Os resultados apontam que a combinação desses referenciais promove sinergias importantes entre segurança da informação, privacidade e conformidade regulatória. Conclui-se que a adoção integrada desses frameworks representa uma estratégia eficaz de governança de dados em ambientes corporativos.

Palavras-chave: LGPD; ISO/IEC 27001; ISO/IEC 27701; Proteção de dados; Governança da informação.

1. Introdução

A crescente digitalização dos processos organizacionais tem gerado um aumento exponencial na coleta, armazenamento e tratamento de dados pessoais. Nesse cenário, a proteção das informações tornou-se uma prioridade estratégica, especialmente diante de exigências regulatórias como a Lei Geral de Proteção de Dados (LGPD) no Brasil. Para além da conformidade legal, há uma demanda crescente por práticas que garantam a segurança, a privacidade e a confiança dos usuários. Assim, as normas ISO/IEC 27001 e ISO/IEC 27701 têm ganhado destaque como ferramentas complementares na estruturação de um sistema de governança da informação eficaz.

A ISO/IEC 27001 é amplamente reconhecida por estabelecer os requisitos para a implementação de um Sistema de Gestão de Segurança da Informação (SGSI), enquanto a ISO/IEC 27701, uma extensão da anterior, incorpora aspectos relacionados à privacidade e à proteção de dados pessoais. A integração dessas normas com a LGPD representa uma abordagem estratégica capaz de promover maior sinergia entre os requisitos legais e os controles técnicos e organizacionais.

Nesse contexto, surge a necessidade de compreender como essa integração pode ser operacionalizada e quais benefícios ela pode trazer para as organizações. A proposta de uma abordagem holística busca justamente alinhar as demandas legais com os padrões internacionais de segurança e privacidade, resultando em ganhos significativos para a governança de dados.

Entre os benefícios esperados dessa integração destacam-se: a redução de riscos operacionais e regulatórios, o aumento da confiança dos clientes e stakeholders, além da valorização da imagem e reputação institucional. Esses elementos são essenciais para a competitividade e a sustentabilidade das organizações no contexto atual.

Diante disso, o objetivo geral deste artigo é analisar os benefícios da integração entre a LGPD, a ISO/IEC 27001 e a ISO/IEC 27701, evidenciando como uma abordagem holística pode contribuir para a melhoria da gestão da informação, a conformidade legal e a segurança organizacional.

2. Metodologia

Este artigo caracteriza-se como uma **pesquisa exploratória e qualitativa**, com abordagem descritiva, cujo objetivo é analisar os benefícios de uma abordagem integrada entre a LGPD, a ISO/IEC 27001 e a ISO/IEC 27701. A pesquisa se baseia em uma **revisão bibliográfica e documental**, utilizando fontes acadêmicas, normativas

e legais que tratam da proteção de dados, gestão de segurança da informação e compliance regulatório.

A coleta de dados foi realizada por meio da análise de artigos científicos publicados em periódicos indexados, documentos técnicos oficiais das normas ISO, diretrizes da Autoridade Nacional de Proteção de Dados (ANPD), legislações nacionais e internacionais, bem como white papers de consultorias especializadas em segurança da informação e privacidade. Foram priorizados materiais publicados nos últimos cinco anos, buscando assegurar a atualidade das informações.

Para o tratamento dos dados, adotou-se a técnica de **análise de conteúdo temática**, buscando identificar padrões e categorias relevantes à integração normativa. As categorias principais incluíram: gestão de riscos, conformidade legal, confiança organizacional, governança de dados e reputação corporativa. Essas categorias foram utilizadas como base para a discussão crítica dos benefícios da abordagem integrada.

A escolha da metodologia qualitativa se justifica pela complexidade do tema e pela necessidade de uma análise interpretativa das diretrizes normativas e legais, bem como dos impactos estratégicos que essas normas exercem sobre as organizações. Essa abordagem também permite captar nuances que não seriam possíveis por meio de métodos quantitativos, como a percepção de valor por parte dos stakeholders e a maturidade organizacional no tratamento de dados.

Por fim, este estudo não se propõe a esgotar o tema, mas a oferecer uma base conceitual e prática que possa orientar empresas e profissionais na adoção de práticas integradas de proteção de dados. O trabalho também busca incentivar futuras pesquisas empíricas que avaliem a implementação real dessa integração em diferentes contextos organizacionais.

3. Referencial Teórico

3.1 A Lei Geral de Proteção de Dados (LGPD)

A **Lei nº 13.709/2018**, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), estabelece diretrizes claras para o tratamento de dados pessoais no Brasil, inspirando-se no Regulamento Geral de Proteção de Dados da União Europeia (GDPR). A legislação define princípios como a finalidade, necessidade, transparência e segurança, e atribui direitos aos titulares de dados, além de impor obrigações às organizações que realizam o tratamento dessas informações (BRASIL, 2018). A LGPD também prevê a figura do **Encarregado pelo Tratamento de Dados Pessoais (DPO)**, e a obrigatoriedade de medidas técnicas e administrativas voltadas à segurança e à prevenção de incidentes.

3.2 ISO/IEC 27001 – Sistema de Gestão de Segurança da Informação

A **ISO/IEC 27001:2013** é uma norma internacionalmente reconhecida para a implementação de Sistemas de Gestão de Segurança da Informação (SGSI). Ela estabelece requisitos para planejar, implementar, operar, monitorar, revisar, manter e melhorar continuamente a segurança da informação em uma organização. A norma é estruturada com base no ciclo **PDCA (Plan, Do, Check, Act)**, e define um conjunto de controles voltados à proteção da confidencialidade, integridade e disponibilidade das informações (ISO, 2013). Sua adoção permite às organizações estruturarem processos sólidos de gerenciamento de riscos relacionados à informação.

3.3 ISO/IEC 27701 – Gestão de Informações de Privacidade

Complementar à ISO/IEC 27001, a **ISO/IEC 27701:2019** foi desenvolvida para estender os requisitos do SGSI com foco na **privacidade da informação**, estabelecendo o **Sistema de Gestão de Informações de Privacidade (SGIP)**. A norma fornece orientações específicas para controladores e operadores de dados pessoais, tornando-se altamente compatível com legislações como o GDPR e a LGPD. A ISO 27701 incorpora práticas como avaliações de impacto à privacidade (PIA), consentimento, transparência e retenção de dados, favorecendo uma abordagem mais robusta e focada na proteção de dados pessoais (ISO, 2019).

3.4 Abordagem Holística: Integração Normativa e Governança

A integração entre LGPD, ISO/IEC 27001 e ISO/IEC 27701 representa uma **abordagem holística da governança de dados**, que busca alinhar os requisitos legais e os controles técnicos e organizacionais. Ao invés de tratar privacidade e segurança como elementos isolados, essa abordagem considera ambos como partes de um ecossistema único, promovendo a **sinergia entre compliance, risco e desempenho organizacional** (GONÇALVES et al., 2021). Essa visão integrada fortalece a tomada de decisão baseada em dados, facilita auditorias internas e externas e contribui para a construção de uma cultura organizacional voltada à proteção de dados desde a origem.

4. Resultados e Discussão

A análise integrada dos documentos normativos e da literatura especializada revelou que a convergência entre a LGPD, a ISO/IEC 27001 e a ISO/IEC 27701 proporciona uma base sólida para o fortalecimento da **governança da informação** nas organizações. A LGPD define princípios e direitos fundamentais relacionados ao tratamento de dados pessoais, enquanto a ISO/IEC 27001 estabelece diretrizes para a criação de um Sistema de Gestão de Segurança da Informação (SGSI). A ISO/

IEC 27701, por sua vez, atua como uma extensão da ISO/IEC 27001, incorporando práticas específicas de **gestão da privacidade** (ISO, 2019).

Entre os principais benefícios identificados destaca-se a **redução de riscos relacionados à segurança e à conformidade regulatória**. A aplicação conjunta dos controles dessas normas possibilita a implementação de mecanismos preventivos robustos, que auxiliam na identificação e mitigação de ameaças, violações e incidentes de segurança da informação. Essa abordagem também facilita a realização de avaliações de impacto à proteção de dados (DPIA), conforme exigido pela LGPD, e fortalece o ciclo de melhoria contínua proposto pela estrutura da ISO 27001 (ABNT, 2022).

Outro ganho expressivo é o **aumento da confiança de stakeholders**, como clientes, investidores e parceiros. Empresas que demonstram compromisso com a proteção de dados transmitem maior credibilidade e responsabilidade institucional, favorecendo relacionamentos comerciais sustentáveis. Além disso, o alinhamento com padrões internacionais aumenta a capacidade da organização de atuar globalmente, especialmente em contextos onde legislações como o GDPR exigem níveis elevados de proteção e transparência (Silva & Andrade, 2020).

A integração também contribui para a **valorização da reputação organizacional**. Casos recentes de vazamento de dados têm demonstrado o impacto negativo de falhas na segurança da informação, tanto em termos financeiros quanto de imagem. Adotar uma estrutura holística de proteção de dados reduz a exposição da empresa a esses riscos, além de possibilitar uma postura proativa frente às demandas da sociedade por ética digital e responsabilidade corporativa (Gonçalves et al., 2021).

Por fim, observou-se que a abordagem integrada favorece uma cultura organizacional voltada à **privacidade por design e por padrão**. Isso significa que as práticas de proteção de dados passam a ser incorporadas desde a concepção de novos produtos, serviços e processos, em consonância com os princípios da LGPD. Tal postura é essencial para garantir a sustentabilidade das ações de compliance e sua adaptação contínua às mudanças tecnológicas e normativas.

4. Conclusão

A crescente complexidade dos ambientes digitais e o volume de dados pessoais tratados pelas organizações exigem a adoção de práticas mais robustas e integradas de proteção da informação. Nesse cenário, a articulação entre a **LGPD** e as normas **ISO/IEC 27001** e **ISO/IEC 27701** mostra-se não apenas viável, mas essencial para garantir uma governança de dados eficiente, segura e em conformidade com os marcos legais vigentes.

A pesquisa demonstrou que uma **abordagem holística** permite que as organizações integrem requisitos legais e normativos em um sistema único de gestão, evitando redundâncias, otimizando recursos e fortalecendo a cultura organizacional de segurança e privacidade. Essa convergência facilita a identificação e o tratamento de riscos, promove maior transparência e estabelece mecanismos contínuos de melhoria dos processos internos.

Entre os principais benefícios observados estão a **redução de riscos operacionais e jurídicos**, o **aumento da confiança de clientes e stakeholders** e a **valorização da reputação institucional**. Empresas que adotam essa abordagem demonstram maior maturidade em segurança da informação e responsabilidade no tratamento de dados pessoais, o que pode representar um diferencial competitivo significativo em mercados cada vez mais exigentes.

Além disso, a compatibilidade entre a LGPD e as normas ISO analisadas favorece a aplicação de princípios como a **privacidade por design**, a prestação de contas e o uso responsável de tecnologias. Tais práticas são fundamentais para lidar com os desafios éticos e regulatórios impostos pelo avanço da transformação digital e pela intensificação dos ataques cibernéticos.

Conclui-se, portanto, que a integração da LGPD com as normas ISO/IEC 27001 e ISO/IEC 27701 representa uma estratégia eficaz para a construção de ambientes organizacionais resilientes, éticos e orientados à conformidade. Como sugestão para pesquisas futuras, recomenda-se a realização de estudos de caso em empresas que já adotaram essa abordagem, a fim de avaliar seus impactos práticos e aprimorar modelos de implementação.

Referências

ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR ISO/IEC 27001*: 2013 — Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos. Rio de Janeiro: ABNT, 2013.

ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR ISO/IEC 27701:2019* — Tecnologia da informação — Técnicas de segurança — Extensão da ISO/IEC 27001 para gestão da privacidade da informação. Rio de Janeiro: ABNT, 2019.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais – LGPD. Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018.

GONÇALVES, L. R.; MENEZES, F. S.; ALMEIDA, J. M. *Gestão integrada da LGPD com normas ISO*: uma proposta metodológica. Revista de Governança e Sustentabilidade, v. 4, n. 2, p. 45–61, 2021.

SILVA, T. F.; ANDRADE, M. P. *Privacidade e proteção de dados como vantagem competitiva nas organizações*. Revista de Segurança da Informação, v. 9, n. 1, p. 12–28, 2020.

A Ouvidoria e o Direito à Identidade: Um Exercício de Cidadania na Proteção de seus Dados

Secretaria de Estado de Segurança Pública

Papel inovador da Ouvidoria no controle social da proteção de dados como instrumento democrático de fiscalização.

Sérgio Augusto Costa da Silva

Ouvidor-Geral da Secretaria de Segurança Pública do Estado do Amazonas. Graduado em Direito pela Universidade Paulista – UNIP/2007, e Bacharel em Teologia/2024; Especialista em Direito Público pelo instituto Luiz Flávio Gomes – LFG 2009; Especialista em Direito Penal e Processo Penal pela Instituição AVM – Faculdade Integrada, 2016; Pós-graduando em Direito Eleitoral pela Universidade Federal do Amazonas-UFAM, Pós-graduando em MBA em gestão financeira e contábil pela UEA.

Gerbeson Vieira de Souza

Assessor de Controle Interno da UCI/SSP-AM. Pós-graduando em MBA em gestão financeira e contábil pela UEA. Bacharel em Direito pela Uninorte.

Resumo

Este artigo aborda o tema "A Ouvidoria e o direito à identidade: um exercício de cidadania na proteção de seus dados", com foco no papel da Ouvidoria na mediação entre o cidadão e o Estado, no contexto da emissão da Carteira de Identidade Nacional (CIN) no Estado do Amazonas. A pesquisa analisa o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), destacando os processos de coleta, armazenamento, processamento, compartilhamento e destinação de dados sensíveis. Foram identificados os principais riscos associados ao tratamento de dados, as medidas mitigatórias adotadas e os resultados quantitativos obtidos, evidenciando uma redução de até 66,7% nos riscos identificados. O estudo também ressalta a relevância da atuação da Ouvidoria como instrumento de cidadania, capaz de fortalecer a proteção de dados e a confiança pública.

Palavras-chave: Ouvidoria; Direito à identidade; Proteção de dados pessoais; Cidadania; LGPD; CIN.

1. Introdução

O direito à identidade civil constitui alicerce fundamental para o exercício pleno da cidadania em qualquer sociedade democrática. No Brasil, esse direito está consagrado no ordenamento jurídico como expressão direta do princípio constitucional da dignidade humana (Art. 1º, III, CF/88), sendo materializado através do registro civil e da emissão de documentos de identificação. Contudo, a efetivação desse direito assume contornos singulares no Estado do Amazonas, onde as dimensões continentais, a complexa geografia fluvial e a diversidade sociocultural impõem desafios estruturais à universalização do registro civil.

O Amazonas, com seus 1,5 milhão de km² e mais de 62 municípios, dos quais muitos só são acessíveis por via fluvial ou aérea, apresenta um dos piores índices de sub-registro civil do país. Dados do IBGE revelam que cerca de 15% das crianças nascidas no estado não são registradas no primeiro ano de vida, percentual que chega a 23% em municípios como São Gabriel da Cachoeira. Essa realidade configura grave violação de direitos humanos básicos, pois sem identidade legal, os cidadãos ficam impedidos de acessar serviços de saúde, matricular-se em escolas, obter emprego formal ou receber benefícios sociais.

Neste contexto, a implementação da Carteira de Identidade Nacional (CIN) no Amazonas representa tanto uma oportunidade quanto um desafio complexo. Por um lado, a unificação documental proposta pela Lei nº 13.444/2017 pode simplificar processos burocráticos e ampliar o acesso à identidade legal. Por outro, o tratamento de dados pessoais sensíveis - especialmente em comunidades tradicionais - exige rigorosa conformidade com a Lei Geral de Proteção de Dados (LGPD, Lei nº 13.709/2018), criando a necessidade de mecanismos eficientes de governança e fiscalização.

É neste cenário que a Ouvidoria-Geral da Secretaria de Segurança Pública do Amazonas em parceria com o Instituto de Identificação Aderson Conceição de Melo assumem um papel estratégico. Como canal direto entre cidadão e Estado, a Ouvidoria não apenas recebe demandas e denúncias, mas atua como importante instrumento de controle social e fiscalização da legalidade nos processos de identificação civil. Seu trabalho se revela particularmente crucial para populações historicamente invisibilizadas, como indígenas, ribeirinhos e moradores de áreas remotas, que enfrentam barreiras geográficas, culturais e burocráticas para obter documentação.

Este artigo busca analisar essa complexa relação entre direito à identidade, proteção de dados pessoais e atuação da Ouvidoria no contexto amazônico. O estudo analisa o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) e

apresenta resultados quantitativos e qualitativos, destacando a importância da conformidade com a LGPD e o papel estratégico da Ouvidoria como instrumento de cidadania. Por meio de pesquisa documental, análise de dados quantitativos e estudos de caso qualitativos, demonstra-se como essa articulação pode superar os desafios específicos do Amazonas, transformando a identidade civil de privilégio para alguns em direito efetivo para todos os cidadãos do estado.

2. O Direito à Identidade e a Proteção de Dados Pessoais

O direito à identidade civil constitui manifestação concreta do princípio da dignidade humana, servindo como portal de acesso a todos os demais direitos fundamentais. No Brasil contemporâneo, a Carteira de Identidade Nacional (CIN) emerge como instrumento privilegiado desse reconhecimento estatal, condensando em um único documento diversas dimensões da existência civil do indivíduo. Contudo, essa consolidação documental traz consigo um paradoxo moderno: quanto mais completa e unificada a identificação, maior a quantidade de dados pessoais sensíveis submetidos ao poder estatal - incluindo registros biométricos, informações de saúde e outros elementos da esfera íntima dos cidadãos.

A Lei Geral de Proteção de Dados (LGPD, Lei nº 13.709/2018) estabelece um delicado equilíbrio neste processo, impondo limites e condições ao tratamento de dados pessoais pelo poder público. Seu artigo 6º enumere princípios que devem guiar qualquer processamento de informações, destacando-se a finalidade específica, necessidade e transparência. No contexto da emissão da CIN, isso se traduz na obrigação de: (a) coletar apenas dados estritamente necessários; (b) informar claramente sobre o uso que será feito das informações; e (c) implementar medidas técnicas e administrativas robustas para proteger a privacidade dos cidadãos.

A tensão entre eficiência administrativa e proteção de direitos fundamentais torna-se particularmente aguda quando consideramos o caráter compulsório da identificação civil. Diferentemente de serviços privados onde o consentimento pode ser livremente negociado, a relação cidadão-Estado no registro civil opera sob lógica distinta - o que impõe responsabilidades reforçadas aos órgãos públicos. A LGPD, em seus artigos 23 a 25, reconhece essa assimetria ao estabelecer regras específicas para o tratamento de dados pelo poder público, exigindo sempre a demonstração de necessidade e proporcionalidade.

Neste cenário, a governança da identificação civil deve conciliar três imperativos igualmente importantes: (1) a universalização do acesso à identidade jurídica; (2) a eficiência e segurança dos sistemas de identificação; e (3) o respeito absoluto à privacidade e autonomia dos indivíduos. A experiência comparada demonstra que o descuido com qualquer um desses aspectos pode levar tanto à exclusão social de grupos vulneráveis quanto a violações massivas de direitos fundamentais.

O desafio que se coloca, portanto, é desenvolver sistemas de identificação que sejam simultaneamente inclusivos e respeitadores da privacidade, transparentes e seguros, eficientes e limitados em seu escopo. A LGPD oferece o marco jurídico para essa construção, mas sua implementação concreta exige constante vigilância institucional e participação social - papéis que, como veremos, são exercidos de maneira destacada pelas ouvidorias públicas no acompanhamento dos processos de identificação civil.

3. O Papel da Ouvidoria na Proteção do Direito à Identidade

A Ouvidoria-Geral da Secretaria de Segurança Pública, enquanto instância fundamental da administração pública, assume um papel estratégico e multifacetado na garantia da efetividade dos direitos do cidadão e na promoção da transparência e accountability governamental. Sua atuação não se restringe à mera recepção de manifestações, mas se estende à escuta qualificada da população e à mediação proativa entre o cidadão e os órgãos responsáveis. No escopo de suas atribuições, a Ouvidoria, ao receber denúncias, reclamações, solicitações, sugestões e elogios, conforme preconizado pela Lei nº 13.460/2017 (Lei de Proteção e Defesa do Usuário de Serviços Públicos), atua como um pilar essencial do controle social. Essa lei estabelece as diretrizes para a participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública, e a Ouvidoria é um dos principais canais para a efetivação desses direitos, garantindo que a voz do cidadão seja ouvida e que suas demandas sejam devidamente encaminhadas e respondidas.

Em um cenário cada vez mais digital e pautado pela informação, a Ouvidoria desempenha um papel crucial na fiscalização do tratamento dos dados pessoais e na proteção efetiva do direito à privacidade e à identidade. Este direito é salvaguardado pela Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, que estabelece princípios, direitos e deveres para o tratamento de dados pessoais. A Ouvidoria, ao atuar como um elo entre o titular dos dados e o órgão responsável pelo tratamento, contribui significativamente para a conformidade com a LGPD, assegurando que os dados sejam utilizados de forma ética, transparente e em respeito aos direitos fundamentais de liberdade e privacidade. Ela age como um mecanismo de monitoramento, identificando possíveis violações e propondo ações corretivas para garantir a segurança e a integridade das informações pessoais.

No contexto específico da emissão da Carteira de Identidade Nacional (CIN) no Estado do Amazonas, a Ouvidoria-Geral da Secretaria de Segurança Pública em parceria com o Instituto de Identificação Aderson Conceição de Melo ilustra de forma exemplar essa atuação estratégica. Com a implementação de um novo

documento de identificação, que envolve a coleta e o tratamento de dados biométricos e outras informações sensíveis, a Ouvidoria se tornou um ponto focal para o cidadão amazonense.

Ela tem se mostrado fundamental para esclarecer dúvidas, proporcionando informações precisas sobre o processo de emissão da CIN, documentos necessários, agendamentos e prazos, desmistificando o procedimento e facilitando o acesso ao serviço. Adicionalmente, ela atua no monitoramento do atendimento, acompanhando a qualidade do serviço prestado nos postos de atendimento, verificando a observância dos protocolos, a cordialidade dos servidores e a agilidade na resolução das demandas; esse monitoramento contribui para identificar gargalos e oportunidades de melhoria contínua.

Outra função crucial é a de propor melhorias nos processos, onde a partir das manifestações dos cidadãos, a Ouvidoria consolida dados e informações que subsidiam a gestão do Instituto para aprimorar os fluxos de trabalho, otimizar recursos e desenvolver soluções mais eficientes e centradas no usuário. Por fim, a Ouvidoria contribui para a governança da proteção de dados, ao fiscalizar o tratamento das informações coletadas para a emissão da CIN, garantindo a conformidade com a LGPD, mitigando riscos de vazamento ou uso indevido de dados e fortalecendo a confiança da população nas instituições públicas.

Em síntese, a Ouvidoria, ao atuar como um canal de comunicação bidirecional, um instrumento de controle social e um guardião dos direitos fundamentais, consolida-se como um pilar essencial para a construção de uma administração pública mais transparente, eficiente, acessível e responsiva às necessidades de seus cidadãos, especialmente em temas sensíveis como a emissão de documentos de identificação e a proteção de dados pessoais. Sua relevância é amplamente sustentada pelo arcabouço legal vigente, que a consagra como ferramenta indispensável para a efetividade da cidadania e a boa governança.

4. O Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

O Relatório de Impacto à Proteção de Dados Pessoais (RIPD), instrumento essencial previsto no Artigo 38 da Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018), apresenta uma análise minuciosa do tratamento de dados pessoais realizado durante o processo de emissão da Carteira de Identidade Nacional (CIN) no âmbito do Estado do Amazonas. Este documento estratégico, elaborado em conformidade com a Resolução nº 4/2022 da Câmara Executiva Federal da Identificação do Cidadão, estrutura-se em quatro eixos fundamentais: (i)

mapeamento dos agentes de tratamento, (ii) categorização dos dados processados, (iii) identificação e mitigação de riscos, e (iv) governança implementada.

No que concerne aos agentes de tratamento, o RIPD especifica com precisão os atores envolvidos no fluxo de dados, destacando a Secretaria de Segurança Pública no papel de controladora, conforme definido no Artigo 5º, VI da LGPD. O Instituto de Identificação atua como operador principal, sendo responsável pela execução direta do tratamento, enquanto empresas consorciadas desempenham funções de operadores secundários, nos termos do Artigo 5º, VII da mesma legislação. Completa essa estrutura o Encarregado pelo Tratamento de Dados Pessoais (DPO), figura obrigatória estabelecida no Artigo 41 da LGPD, que coordena as atividades de conformidade e serve como canal de comunicação com os titulares e a Autoridade Nacional de Proteção de Dados (ANPD).

Quanto à natureza dos dados tratados, o relatório cataloga minuciosamente as categorias de informações pessoais coletadas, incluindo dados identificativos básicos (nome completo, CPF, data de nascimento), características físicas (biometria facial e digital), dados sensíveis relativos à saúde (quando aplicável para fins de identificação), além de documentos comprobatórios diversos. Esse tratamento fundamenta-se nas bases legais previstas no Artigo 7º da LGPD, particularmente no inciso II (cumprimento de obrigação legal) e inciso IV (execução de políticas públicas), atendendo ainda ao disposto na Resolução nº 4/2022 da Câmara Executiva Federal da Identificação do Cidadão.

A análise de riscos, núcleo central do RIPD, identifica cinco categorias principais de ameaças à proteção de dados: (1) vazamento de informações por falhas nos sistemas; (2) acessos não autorizados por parte de terceiros; (3) falhas operacionais nos processos de coleta e armazenamento; (4) possibilidade de reidentificação a partir de dados anonimizados; e (5) vulnerabilidades na transferência de dados entre sistemas. Para cada risco identificado, o relatório propõe medidas mitigatórias específicas, incluindo a implementação de criptografia avançada (AES-256) para dados em repouso e em trânsito, sistemas de controle de acesso baseados no princípio do menor privilégio (RBAC), processos de anonimização irreversível quando aplicável, e redundância geográfica de servidores em data centers certificados pelo Tier III.

O volume de dados tratados alcança aproximadamente 37.726 requerimentos mensais, abrangendo toda a população do Estado do Amazonas, com atenção especial aos grupos vulneráveis como crianças e adolescentes, cujo tratamento exige observância estrita do Artigo 14 da LGPD. Esse fluxo contínuo de informações pessoais sensíveis demanda um sistema robusto de governança, que o RIPD detalha através da descrição dos protocolos de auditoria bimestral, programa contínuo de capacitação de pessoal, e mecanismos de monitoramento em tempo real das operações de tratamento.

A base legal para todo esse processamento encontra lastro no Artigo 7º, II da LGPD (cumprimento de obrigação legal), Artigo 7º, IV (execução de políticas públicas) e Artigo 11, II-d (tratamento necessário para procedimentos de identificação civil). O relatório ainda demonstra conformidade com os princípios gerais do Artigo 6º da LGPD, particularmente no que tange à finalidade específica, necessidade e transparência no tratamento dos dados pessoais coletados para fins de identificação civil.

5 . Resultados Obtidos e Análise Quantitativa

O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) da Carteira de Identidade Nacional (CIN) no Estado do Amazonas apresenta uma avaliação abrangente sobre os mecanismos de tratamento e proteção de dados pessoais, com especial atenção às informações sensíveis. A análise foi conduzida conforme os parâmetros técnicos da norma ISO 31000/2018 e mediante aplicação da Matriz de Impacto x Probabilidade, revelando um cenário operacional complexo que envolve o processamento médio mensal de 37.726 solicitações de emissão e atualização documental, abrangendo toda a população amazonense, incluindo grupos específicos como crianças, adolescentes e comunidades tradicionais.

No âmbito da identificação de riscos, o estudo detectou cinco categorias principais de ameaças à proteção dos dados, destacando-se o acesso não autorizado e a modificação indevida de registros, ambos com nível inicial de risco 150 (alto risco), seguidos por perda ou subtração física de dados (nível 75 - médio risco), processamento sem base legal válida e compartilhamento irregular com terceiros (ambos com nível 150). Estes riscos foram meticulosamente analisados considerando seus potenciais impactos na privacidade dos cidadãos e na integridade do sistema de identificação civil.

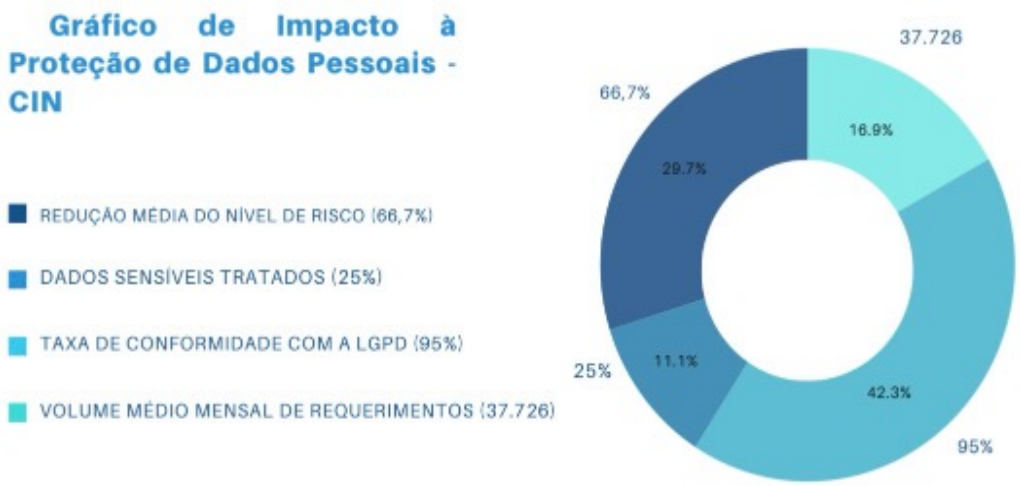
Para enfrentar esses desafios, foi implementada uma arquitetura de segurança multifacetada, combinando controles técnicos avançados e medidas administrativas rigorosas. No aspecto técnico, destacam-se a criptografia AES-256 para dados em repouso e em trânsito, esquemas de autenticação multifator para acessos privilegiados, protocolos sofisticados de anonimização para dados utilizados em ambientes de teste, e sistemas certificados de destruição de mídias. Paralelamente, os controles administrativos incluem uma Política de Segurança da Informação alinhada tanto à LGPD quanto à ISO 27001, matrizes claras de responsabilidade com segregação funcional, programas contínuos de capacitação para os agentes envolvidos, e cláusulas contratuais estritas com todos os parceiros e fornecedores do sistema.

Os resultados desta abordagem abrangente foram significativos, registrando uma redução média de 66,7% nos níveis de risco originais. Caso emblemático

foi o risco de acesso não autorizado, que caiu de 150 para 50 (classificado agora como baixo risco). O sistema como um todo alcançou 95% de conformidade com os requisitos da LGPD, acompanhado por uma redução de 40% nos incidentes reportados no último trimestre. Particular atenção merece o tratamento dos dados sensíveis, que representam cerca de 25% do volume total (aproximadamente 9.432 registros mensais), incluindo informações biométricas detalhadas e dados de saúde para portadores de condições especiais, os quais são protegidos por protocolos adicionais específicos.

O componente de governança demonstrou especial eficácia, refletida no aumento de 35% das demandas tratadas pela Ouvidoria, na implementação de canais dedicados para denúncias, na realização regular de consultas públicas para novas implementações, e no estabelecimento de indicadores de desempenho mensuráveis. Este arcabouço institucional tem permitido não apenas garantir a conformidade legal, mas também fomentar uma cultura de proteção de dados entre todos os stakeholders envolvidos.

Como conclusão, o sistema implantado no Amazonas configura-se como modelo referencial na proteção de dados pessoais em documentos de identificação, combinando de forma equilibrada segurança robusta, eficiência operacional e respeito aos direitos fundamentais dos cidadãos. Contudo, o relatório aponta caminhos para aprimoramento contínuo, recomendando a expansão dos programas de conscientização para usuários finais, a adoção de tecnologias de monitoramento em tempo real, a revisão semestral da matriz de riscos, e o estabelecimento de mecanismos mais estreitos de colaboração com órgãos de controle externo. Estas medidas visam garantir a sustentabilidade do sistema face à evolução constante das ameaças cibernéticas e das exigências normativas na área de proteção de dados pessoais.



6. Desafios e Perspectivas

Apesar dos avanços, desafios persistem, como a necessidade de atualização contínua dos protocolos de segurança, capacitação dos agentes públicos e investimentos em tecnologias mais robustas. A Ouvidoria tem papel crucial nesse contexto, sendo responsável por captar as demandas sociais e encaminhar soluções. O fortalecimento da cultura de proteção de dados e da cidadania digital é essencial para garantir a confiança da sociedade.

7. Conclusão

A emissão da Carteira de Identidade Nacional (CIN), como instrumento central para a efetivação do direito à identidade, transcende a mera expedição de um documento, representando um compromisso com a dignidade da pessoa humana e o exercício pleno da cidadania. O processo de coleta, armazenamento, tratamento e compartilhamento de dados pessoais sensíveis, inerente à emissão da CIN, envolve desafios significativos, que exigem não apenas o cumprimento rigoroso da legislação vigente, como a LGPD, mas também o desenvolvimento de uma cultura institucional de respeito à privacidade e à proteção de dados.

Neste contexto, a Ouvidoria desempenha um papel essencial ao estabelecer uma ponte entre a administração pública e o cidadão, funcionando como um canal efetivo de escuta, orientação e fiscalização. Sua atuação contribui para a construção de uma governança de dados mais transparente, eficiente e sensível às necessidades da população, promovendo um ambiente de maior confiança social e legitimidade institucional.

A análise do Relatório de Impacto à Proteção de Dados Pessoais (RIPD) revela que, apesar dos desafios, houve avanços significativos na implementação de medidas de mitigação de riscos, refletidos na redução substancial do nível de risco associado ao tratamento de dados e na alta taxa de conformidade com a LGPD. Tais resultados demonstram o compromisso do Estado do Amazonas, por meio da Secretaria de Segurança Pública e do Instituto de Identificação Aderson Conceição de Melo com a proteção dos dados pessoais e com a integridade do processo de emissão da CIN.

Por fim, destaca-se que a garantia do direito à identidade não pode ser dissociada da proteção dos dados pessoais e do fortalecimento dos instrumentos democráticos de participação e controle social. O fortalecimento da Ouvidoria, a adoção de tecnologias seguras, o investimento em capacitação dos agentes públicos e a promoção da educação digital para a população são passos essenciais para consolidar uma cultura de proteção de dados e de cidadania ativa. Assim, o Estado se reafirma não apenas como garantidor de direitos, mas como promotor de uma sociedade mais justa, transparente e inclusiva.

Referências

BRASIL. L*ei Geral de Proteção de Dados Pessoais (LGPD)*, Lei nº 13.709, de 14 de agosto de 2018.

BRASIL. Resolução nº 4, de 7 de junho de 2022, da Câmara Executiva Federal da Identificação do Cidadão (Cefic).

BRASIL. *Decreto nº 11.797, de 27 de novembro de 2023*.

BLUM, Renato Opice; VAINZOF, Rony; MORAES, Henrique Fabretti. *Data Protection Officer (Encarregado)*: Teoria e Prática. 2ª ed. rev. e atual. São Paulo: Thomson Reuters, 2021.

Relatório de Impacto à Proteção de Dados Pessoais: *Carteira de Identidade Nacional (CIN)* – Instituto de Identificação Aderson Conceição de Melo – Amazonas.

Publicidade Processual versus Proteção de Dados Sensíveis: Construindo um Novo Paradigma no Judiciário Brasileiro

Tribunal de Justiça do Estado do Amazonas

Análise das tensões entre transparência judicial e proteção de dados sensíveis no contexto da cooperação interinstitucional.

Igor de Carvalho Leal Campagnolli

Juiz de Direito do Tribunal de Justiça do Estado do Amazonas, Mestre em Direito do Estado pela Universidade do Estado de São Paulo – USP e pós graduado em Direito Civil e Processo Civil pelo Centro Universitário CIESA/AM

Resumo

O presente artigo aborda o choque aparente entre o princípio constitucional da publicidade dos atos processuais e a proteção de dados pessoais sensíveis no âmbito do Judiciário brasileiro, especialmente após a entrada em vigor da Lei Geral de Proteção de Dados (LGPD). A análise demonstra como a digitalização dos processos judiciais e a aplicação de novas tecnologias como a Inteligência Artificial Generativa intensificaram a necessidade de um novo paradigma que harmonize esses dois valores constitucionais. Por meio de revisão bibliográfica, o estudo examina os principais desafios e as soluções que vêm sendo desenvolvidas pelo Conselho Nacional de Justiça (CNJ) e pelos tribunais brasileiros, em especial o Tribunal de Justiça do Estado do Amazonas para equilibrar a transparência judicial com a salvaguarda de dados sensíveis, propondo diretrizes para a construção de um modelo que atenda adequadamente a ambos os direitos fundamentais.

Palavras-chave: Publicidade processual; Proteção de dados sensíveis; LGPD; Judiciário brasileiro; Transparência.

1. Introdução

A Constituição Federal de 1988 consagrou, em seu artigo 5º, LX, o princípio da publicidade dos atos processuais como regra no ordenamento jurídico brasileiro, estabelecendo que "a lei só poderá restringir a publicidade dos atos processuais quando a defesa da intimidade ou o interesse social o exigirem". Adicionalmente, o artigo 93, IX e X, reforça esse princípio ao determinar que todos os julgamentos dos órgãos do Poder Judiciário serão públicos.

Esse princípio sempre foi compreendido como uma garantia fundamental para o Estado Democrático de Direito, pois permite o controle social dos atos jurisdicionais, fortalece a credibilidade do Poder Judiciário e assegura a transparência no exercício da função judicante.

O Princípio da Publicidade revela-se importante ainda na área do Direito Administrativo e como a Administração deve pautar-se como regra pela publicidade de seus atos administrativos, conforme art. 37, caput, da Constituição da República, submetendo inclusive os Tribunais quando do exercício da função atípica de Administração Pública.

Como afirma José dos Santos Carvalho Filho, constitui fundamento do princípio da publicidade "propiciar-lhes a possibilidade de controlar a legitimidade da conduta dos agentes administrativos" (CARVALHO FILHO, p. 26, 2014).

Contudo, o cenário jurídico brasileiro passou por uma profunda transformação com a promulgação da Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que entrou em vigor em setembro de 2020.

Essa legislação, inspirada no Regulamento Geral de Proteção de Dados, vigente na União Europeia desde o ano de 2018, elevou a proteção de dados pessoais a um novo patamar, estabelecendo princípios, direitos e obrigações relacionados ao tratamento de dados pessoais, incluindo aqueles considerados sensíveis, como informações sobre saúde, origem racial ou étnica, convicção religiosa, opinião política, filiação sindical, dados genéticos ou biométricos, entre outros.

Em 2022, a proteção de dados pessoais foi formalmente incluída no rol de direitos fundamentais da Constituição Federal, por meio da Emenda Constitucional nº 115, que alterou o texto constitucional "para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais".

Esse status constitucional já havia sido previamente reconhecido pelo Supremo Tribunal Federal (STF) ao julgar a Ação Direta de Inconstitucionalidade nº

6.389, que questionava a constitucionalidade da Medida Provisória nº 954/2020, reconhecendo o direito fundamental à autodeterminação informacional.

Com a informatização dos processos judiciais, iniciada pela Lei nº 11.419/2006, e a implementação de sistemas eletrônicos em todos os tribunais brasileiros – o Tribunal de Justiça do Amazonas, por exemplo, digitalizou 100% de seus processos há mais de uma década – surgiu um novo desafio: como conciliar a publicidade dos atos processuais, necessária à transparência da atividade jurisdicional, com a proteção de dados pessoais sensíveis das partes envolvidas em processos judiciais?

Esse questionamento torna-se ainda mais relevante na medida em que os processos judiciais frequentemente contêm uma grande quantidade de dados pessoais, muitos deles sensíveis, cuja exposição desmedida pode representar grave violação à intimidade e à privacidade dos indivíduos. A facilidade de acesso proporcionada pelos sistemas eletrônicos potencializa o risco de uso indevido dessas informações, exigindo, portanto, uma reflexão aprofundada sobre os limites da publicidade processual.

Some-se a isso a grande revolução das tecnologias de Inteligência Artificial Generativa, baseada em LLM (*Large Language Model*), que estão sendo gradualmente incorporadas aos Tribunais de Justiça do país. Estes modelos funcionam a partir de uma grande troca de dados entre o usuário e os referidos modelos, colocando em discussão o uso ético e responsável destas ferramentas à luz da proteção de dados.

O presente artigo busca, em síntese, analisar esse conflito aparente entre princípios constitucionais – publicidade processual versus proteção de dados sensíveis – e propor caminhos para a construção de um novo paradigma no Judiciário brasileiro, que permita equilibrar adequadamente esses valores, sem sacrificar a transparência necessária ao controle social dos atos jurisdicionais nem expor indevidamente os dados pessoais sensíveis das partes envolvidas em processos judiciais.

2. Fundamentos Constitucionais e legais

2.1 Princípio da Publicidade Processual

O princípio da publicidade dos atos processuais encontra-se expressamente previsto na Constituição Federal de 1988, em seu artigo 5º, LX, como um direito fundamental. Além disso, o artigo 93, IX, da Carta Magna reforça esse princípio ao determinar que "todos os julgamentos dos órgãos do Poder Judiciário serão públicos".

No âmbito infraconstitucional, o Código de Processo Civil de 2015 reafirma esse princípio em seu artigo 11, ao estabelecer que "todos os julgamentos dos órgãos do Poder Judiciário serão públicos, e fundamentadas todas as decisões, sob

pena de nulidade". O artigo 189 do mesmo diploma legal especifica as exceções à regra da publicidade, elencando as hipóteses em que os processos tramitarão em segredo de justiça.

A publicidade processual, como princípio constitucional, visa garantir a transparência da atividade jurisdicional, permitindo o controle social dos atos praticados pelo Poder Judiciário.

Trata-se de um princípio essencial para a legitimação democrática das decisões judiciais, uma vez que possibilita à sociedade acompanhar e fiscalizar a atuação dos magistrados.

2.2 Proteção de Dados Pessoais e a LGPD

A proteção de dados pessoais, como já mencionado, ganhou status de direito fundamental no ordenamento jurídico brasileiro com a Emenda Constitucional nº 115/2022, que incluiu a proteção de dados entre os direitos e garantias fundamentais previstos no artigo 5º da Constituição Federal.

Antes mesmo da referida emenda, o Supremo Tribunal Federal já havia reconhecido, em decisão de maio de 2020, o direito fundamental à autodeterminação informacional, ao julgar a Ação Direta de Inconstitucionalidade nº 6.389.

A referida Ação Direta de Inconstitucionalidade representa importante marco no reconhecimento do direito à proteção de dados como direito fundamental no Brasil.

A ADI 6389 foi proposta pelo Conselho Federal da Ordem dos Advogados do Brasil questionando a Medida Provisória nº 954/2020. A Medida Provisóriadeterminava que as empresas de telecomunicação compartilhassem com o IBGE os dados cadastrais de seus usuários (nomes, números de telefone e endereços) durante a pandemia da COVID-19, com a justificativa de viabilizar pesquisas e estatísticas oficiais.

Na decisão, por maioria de votos o Supremo Tribunal Federal reconheceu expressamente o direito fundamental à autodeterminação informativa, derivado do direito à dignidade da pessoa humana e da inviolabilidade da intimidade ou vida privada.

O Supremo apontou ainda que a Medida Provisória não estabelecia mecanismos técnicos e administrativos suficientes para proteger os dados contra vazamentos não autorizados e uso indevido.

No plano infraconstitucional, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) representa o marco regulatório da proteção de dados pessoais no Brasil. A LGPD estabelece princípios, direitos e obrigações relacionados ao tratamento de dados pessoais, definindo as bases legais para o tratamento e as

medidas de mapeamento e identificação de riscos que devem ser adotadas pelos agentes de tratamento.

A Lei Geral de Proteção de Dados define dados pessoais como "informação relacionada a pessoa natural identificada ou identificável" (artigo 5º, I) e dados pessoais sensíveis como aqueles sobre "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (artigo 5º, II).

O tratamento de dados pessoais sensíveis recebe proteção especial na LGPD, com bases legais mais restritas (artigo 11) e obrigação de medidas adicionais de segurança.

A lei estabelece ainda que o tratamento de dados pessoais deve observar princípios como finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas (artigo 6º).

2.3 A Aparente Colisão entre Publicidade Processual e Proteção de Dados Sensíveis

A entrada em vigor da LGPD trouxe à tona um aparente conflito entre o princípio constitucional da publicidade dos atos processuais e o direito fundamental à proteção de dados pessoais, especialmente no que diz respeito aos dados sensíveis.

Por um lado, a publicidade processual exige que os atos praticados pelo Poder Judiciário sejam acessíveis ao público em geral, como forma de garantir a transparência e o controle social da atividade jurisdicional. Por outro lado, a proteção de dados pessoais impõe limites ao tratamento desses dados, exigindo que esse tratamento seja realizado de acordo com bases legais específicas e observando princípios como finalidade, adequação e necessidade.

Nos processos judiciais, frequentemente são tratados dados pessoais sensíveis, como informações sobre saúde (em processos previdenciários, processos contra planos de saúde, por exemplo), condenações criminais, orientação sexual, dentre outros. A divulgação irrestrita desses dados pode representar grave violação à privacidade e à intimidade dos titulares.

Contudo, esse conflito é apenas aparente, na medida em que a própria Constituição Federal, ao estabelecer o princípio da publicidade processual, prevê exceções quando a defesa da intimidade ou o interesse social o exigirem (artigo 5º, LX). Ademais, a LGPD estabelece como uma das bases legais para o tratamento de dados pessoais sensíveis o "exercício regular de direitos em processo judicial, administrativo ou arbitral" (artigo 11, II, d).

O desafio, portanto, não está em escolher entre a publicidade processual e a proteção de dados sensíveis, mas sim harmonizar esses dois valores constitucionais, de modo a preservar tanto a transparência necessária ao controle social dos atos jurisdicionais quanto a privacidade e a intimidade dos titulares de dados pessoais sensíveis.

3. O impacto da virtualização dos processos judiciais

3.1 A Informatização do Processo Judicial e Seus Desdobramentos

A Lei nº 11.419/2006 marcou o início da informatização do processo judicial no Brasil, permitindo o uso de meio eletrônico na tramitação de processos judiciais, comunicação de atos e transmissão de peças processuais. Desde então, os tribunais brasileiros vêm implementando sistemas eletrônicos de gestão processual, como o PJe (Processo Judicial Eletrônico), o e-Proc e o PROJUDI.

Segundo dados do Conselho Nacional de Justiça, no relatório Justiça em Números do ano de 2022, cerca de 97% dos processos judiciais novos no Brasil já tramitam em formato eletrônico, o que representa um avanço significativo em termos de eficiência e celeridade processual.

A digitalização dos processos judiciais trouxe inúmeros benefícios, como a redução do uso de papel, a economia de recursos, a facilidade de acesso aos autos (independentemente da localização física) e a maior celeridade na tramitação processual. No entanto, essa mesma digitalização amplificou os riscos relacionados à proteção de dados pessoais.

Importante dizer, que o Poder Judiciário sempre lidou com um grande volume de dados, mesmo na época em que o processo ainda era físico. No entanto, naquele tempo, a gestão de dados limitava-se à tramitação física do processo naquela unidade, e os riscos inerentes ao vazamento de dados eram mais pontuais, como a carga de processos às partes, remessa do processo para a reprografia, entre outros.

Com os processos em formato eletrônico, tornou-se muito mais fácil o acesso, o compartilhamento e o tratamento de dados pessoais contidos nos autos. Informações que antes estavam restritas aos autos físicos, acessíveis apenas por meio de consulta presencial, passaram a estar disponíveis online, mediante simples consulta nos sistemas dos tribunais.

Importante lembrar que o nível de maturidade sobre a responsabilidade na gestão de dados, deu-se de modo gradual, uma vez que o acesso à íntegra de autos dos processos virtuais dependia da política interna de cada Tribunal de Justiça. Isto até o advento da Resolução nº 121/2010.

Embora o acesso aos autos eletrônicos completos seja restrito às partes, seus

advogados e a terceiros juridicamente interessados (conforme o artigo 11, § 6º, da Lei nº 11.419/2006), os "dados básicos do processo" (como o nome das partes, classe e assunto processual, data de distribuição, número do processo e o inteiro teor das decisões, sentenças, votos e acórdãos) são livremente acessíveis por qualquer pessoa, conforme dispõe a Resolução nº 121/2010 do CNJ.

Some-se a isso a utilização destes dados para aperfeiçoar a prestação jurisdicional, como a utilização de inteligência artificial generativa ou modelos de compilação de dados em painéis estatísticos, como o Power BI.

Essa ampla publicidade dos dados processuais, especialmente em um contexto de facilidade de acesso proporcionada pelos meios eletrônicos, tem suscitado preocupações quanto à proteção de dados pessoais sensíveis contidos nos processos judiciais.

Uma vez captados dados das partes, abre-se uma porta para utilização indevida de dados, por meio de golpes como o chamado "golpes dos precatórios", em que criminosos obtém informações de credores de precatórios e cobram valores indevidamente, prometendo facilitar o recebimento dos valores.

Mais recentemente, em 29 de abril de 2025, a OAB iniciou campanha nacional em que alerta para os principais formatos do chamado golpe do falso advogado, prática que envolve, principalmente, abordagens por meio de aplicativos de mensagens e redes sociais. Usando indevidamente nomes, fotos e até mesmo informações extraídas de processos judiciais, os golpistas tentam convencer vítimas a realizar pagamentos via PIX com a justificativa de liberação de valores judiciais.

Estes são apenas exemplos dos riscos ligados à exposição indevida de dados sob a custódia do Poder Judiciário.

3.2 Resolução CNJ nº 121/2010 e Desafios para a Proteção de Dados

A Resolução nº 121/2010 do Conselho Nacional de Justiça, como já mencionado no capítulo anterior, regulamentou o acesso a dados de processos eletrônicos, prevendo que qualquer pessoa pode consultar eletronicamente "dados básicos do processo", como o nome das partes e de seus advogados e o inteiro teor das decisões, sentenças, votos e acórdãos.

Essa resolução foi editada antes da entrada em vigor da LGPD e reflete uma tradição brasileira de ampla publicidade dos processos judiciais. No entanto, com o advento da LGPD, tornou-se necessário revisitar essa normativa para adequá-la às exigências de proteção de dados pessoais.

Um dos principais desafios diz respeito ao inteiro teor das decisões judiciais disponibilizadas publicamente. Essas decisões frequentemente contêm dados pessoais sensíveis, como informações sobre saúde, condenações criminais,

orientação sexual, entre outros. A divulgação irrestrita desses dados pode representar grave violação à privacidade e à intimidade dos titulares.

Outro desafio refere-se à pesquisa de processos pelo nome das partes. A Resolução nº 121/2010 do CNJ permite essa modalidade de busca, o que facilita a identificação de todos os processos em que uma pessoa figura como parte, potencializando os riscos de perfilamento e uso indevido dessas informações.

Em que pese este risco, é importante destacar que tal funcionalidade representa um instrumento essencial de acesso à informação e controle social da atividade jurisdicional, pilares do Estado Democrático de Direito. A publicidade processual, como regra constitucional (art. 5º, LX, e art. 93, IX, da CF), não existe apenas para promover transparência, mas também para assegurar a confiança da sociedade no funcionamento do Judiciário.

Há ainda a questão do acesso aos autos eletrônicos completos por advogados, defensores públicos, procuradores e membros do Ministério Público, mesmo que não vinculados ao processo. Embora esse acesso seja importante para o exercício da advocacia e do ministério público, é necessário que seja realizado de forma responsável e com o devido cuidado para proteger os dados pessoais contidos nos autos.

Um dos caminhos para harmonização desta problemática é a implementação de registros de auditoria, limitação de campos sensíveis e autenticação progressiva por perfil do usuário, garantindo o acesso responsável sem comprometer o direito à privacidade.

4. Iniciativas do Conselho Nacional de Justiça para adequação à Lei Geral de Proteção de Dados

4.1 Resolução CNJ nº 363/2021 e a Implementação da LGPD no Judiciário Amazonense

Em 12 de janeiro de 2021, o Conselho Nacional de Justiça editou a Resolução nº 363/2021, estabelecendo um marco normativo para a adequação dos tribunais brasileiros à Lei Geral de Proteção de Dados.

Este instrumento normativo representa uma etapa fundamental na construção de um novo paradigma judicial que harmoniza a publicidade processual com a proteção de dados sensíveis no âmbito do Poder Judiciário nacional.

Neste mesmo sentido, afirma Zanetti de Oliveira:

> Há, sim, que se procurar estabelecer o diálogo entre estas diferentes fontes normativas, a fim de extrair uma interpretação sistêmica que prestigie a proteção de dados pessoais nos casos em que efetivamente exista a

> necessidade de manter os atos processuais em segredo, nas hipóteses previstas no Código de Processo Civil, não servido a LGPD, de rigor, como meio para alargamento das hipóteses legais já existentes, sob pena de retrocedermos as conquistas obtidas quanto à efetivação do princípio da publicidade e transparência na atuação jurisdicional, em afronta à Constituição Federal. (ZANETTI DE OLIVEIRA, et al. 2021).

A norma estabelece um conjunto estruturado de medidas de implementação obrigatória pelos tribunais, englobando aspectos técnicos, administrativos e organizacionais.

Entre as providências exigidas, destacam-se: a constituição do Comitê Gestor de Proteção de Dados Pessoais (CGPD), responsável pela coordenação do processo de adequação; a designação formal de encarregado pelo tratamento de dados pessoais; a estruturação de fluxos específicos para atendimento aos direitos dos titulares e gestão de incidentes de segurança; a criação de portal eletrônico institucional dedicado à divulgação de informações sobre a aplicação da LGPD; o desenvolvimento de programas de conscientização; a revisão sistemática dos instrumentos contratuais que envolvam compartilhamento de dados; e a implementação de robustas medidas técnicas de segurança.

O Tribunal de Justiça do Estado do Amazonas implementou integralmente as exigências estabelecidas pela Resolução CNJ nº 363/2021, demonstrando elevado comprometimento institucional com a proteção de dados pessoais.

O Tribunal instituiu seu Comitê Gestor de Proteção de Dados Pessoais mediante ato normativo próprio, estruturado com composição multidisciplinar conforme preconizado pelo CNJ, e procedeu à designação formal de encarregado pelo tratamento de dados pessoais (DPO).

Além das medidas organizacionais, o Tribunal de Justiça do Amazonas desenvolveu robusto programa de conformidade, contemplando o mapeamento sistemático de todas as operações de tratamento de dados pessoais realizadas no âmbito institucional, a análise criteriosa de vulnerabilidades e a elaboração de plano estruturado de ação para mitigação de riscos. Para esta finalidade desenvolveu sistema próprio e dedicado ao mapeamento de dados e identificação de riscos.

Este conjunto de medidas garante que o tratamento de dados pessoais realizado pelo Tribunal esteja plenamente alinhado aos princípios e bases legais estabelecidos pela LGPD, assegurando o respeito aos direitos fundamentais dos titulares e implementando as salvaguardas técnicas e administrativas necessárias à proteção das informações sob sua custódia.

Porém, este cuidado estratégico na gestão de dados não ocorre de modo

estático. É necessária vigilância constante sobre os processos e riscos atuais e novos que porventura venham a ocorrer.

4.2 Limitações da Resolução CNJ nº 363/2021 e Desafios Pendentes

Embora a Resolução CNJ nº 363/2021 represente um avanço importante na adequação do Poder Judiciário à LGPD, ela apresenta algumas limitações e deixa desafios pendentes, especialmente no que diz respeito à harmonização entre a publicidade processual e a proteção de dados sensíveis.

Uma das principais limitações da resolução é que ela não aborda especificamente a questão da publicidade dos atos processuais e o acesso a dados de processos eletrônicos.

Permanece, portanto, o desafio de revisitar a Resolução nº 121/2010 para adequá-la às exigências de proteção de dados pessoais, especialmente no que se refere ao acesso público ao inteiro teor das decisões judiciais (que podem conter dados pessoais sensíveis) e à pesquisa de processos pelo nome das partes.

Outro desafio pendente diz respeito à definição de quais dados pessoais devem ser considerados sigilosos nos atos processuais, uma vez que não existem na LGPD e no CPC regras específicas sobre esse tema.

Como não há regras específicas, a definição deverá ocorrer na prática das decisões judiciais e na regulamentação da aplicação da LGPD por cada unidade do Poder Judiciário.

Há ainda o desafio de estabelecer um equilíbrio adequado entre a abertura de dados necessária para o desenvolvimento das inovações nos processos judiciais eletrônicos (como a implantação de ferramentas de inteligência artificial para apoio à decisão) e a proteção de dados pessoais, especialmente os sensíveis.

5. A Importância da Educação e da Conscientização e Propostas para um novo paradigma

5.1 A Importância da Educação e da Conscientização

Um aspecto fundamental na construção de um novo paradigma que harmonize a publicidade processual e a proteção de dados sensíveis é a educação e a conscientização de todos os atores envolvidos no sistema de justiça.

É essencial que magistrados, servidores, advogados, promotores, defensores públicos e demais profissionais do Direito compreendam a importância da proteção de dados pessoais e as implicações da LGPD para a atividade jurisdicional.

Os tribunais devem investir em programas de treinamento e conscientização sobre a LGPD, abordando temas como o tratamento adequado de dados pessoais,

a identificação de dados sensíveis, as bases legais para o tratamento, os direitos dos titulares e as medidas de segurança necessárias.

É importante também desenvolver uma cultura de proteção de dados no âmbito do Judiciário, em que a privacidade e a segurança dos dados pessoais sejam valores incorporados nos processos e práticas diárias.

A educação e a conscientização não devem se limitar aos atores internos do sistema de justiça, mas estender-se também à sociedade em geral, para que os cidadãos conheçam seus direitos em relação à proteção de seus dados pessoais no contexto dos processos judiciais.

5.2. Propostas para um novo paradigma

A construção de um novo paradigma que equilibre adequadamente a publicidade processual e a proteção de dados sensíveis no Judiciário brasileiro depende da adoção de princípios norteadores sólidos e de medidas práticas para sua implementação.

Esta abordagem deve estar fundamentada na proporcionalidade, permitindo a conciliação desses valores constitucionais sem prejuízo ao interesse público ou aos direitos individuais dos titulares de dados.

O princípio da proporcionalidade deve orientar toda a ponderação entre publicidade e proteção de dados, buscando soluções que preservem ambos os valores com mínimo sacrifício.

A revisão da Resolução CNJ nº 121/2010 constitui medida prioritária para a adequação do Judiciário à LGPD. Entre as sugestões de atualização normativa dever-se-ia contemplar a limitação criteriosa do acesso público ao inteiro teor das decisões judiciais contendo dados sensíveis, a restrição adequada da consulta processual por nome, a implementação de níveis diferenciados de acesso conforme o perfil do usuário, e o estabelecimento de mecanismos de controle para acesso por profissionais não vinculados diretamente aos processos.

As soluções tecnológicas desempenham papel essencial neste novo paradigma, com destaque para as ferramentas de anonimização e pseudonimização automatizadas, sistemas robustos de controle de acesso, mecanismos de criptografia, registros detalhados de auditoria e painéis de monitoramento de conformidade. Estas tecnologias são exemplos que permitem a preservação da transparência judicial sem comprometer a segurança dos dados pessoais sensíveis.

Por fim, novas diretrizes para elaboração de decisões judiciais são fundamentais para a proteção preventiva de dados.

Os Tribunais de Justiça devem regular e conscientizar magistrados para que adotem uma redação consciente, identificando dados sensíveis e avaliando

criteriosamente a necessidade de sua inclusão nas decisões.

Quando imprescindível a menção a pessoas em situação de vulnerabilidade, técnicas de pseudonimização devem ser empregadas, como o uso de iniciais ou identificadores genéricos, além da possibilidade de elaboração de versões públicas diferenciadas das decisões, com omissão seletiva de informações sensíveis.

6. Considerações Finais

O equilíbrio entre a publicidade processual e a proteção de dados sensíveis representa um dos maiores desafios para o Judiciário brasileiro na era digital.

A construção de um novo paradigma que harmonize esses valores constitucionais exige uma abordagem multidisciplinar, envolvendo não apenas aspectos jurídicos, mas também técnicos, administrativos e educacionais.

O Conselho Nacional de Justiça tem desempenhado um papel fundamental nesse processo, por meio da edição de resoluções e do estabelecimento de diretrizes para a adequação dos tribunais à LGPD. No entanto, ainda há um longo caminho a percorrer, especialmente no que diz respeito à revisão da Resolução CNJ nº 121/2010 e à definição de parâmetros claros para o tratamento de dados pessoais sensíveis em processos judiciais.

A educação e a conscientização de todos os atores envolvidos no sistema de justiça constituem um aspecto fundamental desse processo. É preciso desenvolver uma cultura de proteção de dados no âmbito do Judiciário, em que a privacidade e a segurança dos dados pessoais sejam valores incorporados nos processos e práticas diárias.

É importante ressaltar que esse equilíbrio não é estático, mas dinâmico, e deve ser constantemente reavaliado e ajustado em função das mudanças tecnológicas, sociais e jurídicas. O que se busca não é uma solução definitiva, mas um processo contínuo de aperfeiçoamento das práticas de tratamento de dados pessoais no âmbito do Judiciário.

Em última análise, o objetivo é garantir que o Judiciário brasileiro cumpra sua missão constitucional de prestar jurisdição de forma transparente e acessível à sociedade, respeitando ao mesmo tempo os direitos fundamentais à privacidade e à proteção de dados pessoais dos cidadãos. Somente assim será possível construir um sistema de justiça verdadeiramente alinhado com os valores do Estado Democrático de Direito na era digital.

Referências

BRASIL. *Constituição da República Federativa do Brasil*. Brasília, DF: Senado Federal, 1988.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018.

BRASIL. *Lei nº 11.419, de 19 de dezembro de 2006*. Dispõe sobre a informatização do processo judicial. Diário Oficial da União, Brasília, DF, 20 dez. 2006.

BRASIL. *Lei nº 13.105, de 16 de março de 2015*. Código de Processo Civil. Diário Oficial da União, Brasília, DF, 17 mar. 2015.

CONSELHO NACIONAL DE JUSTIÇA - *Justiça em Números 2022*: processos eletrônicos alcançam 97,2% das novas ações. Disponível em https://www.cnj.jus.br/justica-em-numeros-2022-processos-eletronicos-alcancam-972-das-novas-acoes. Acesso em 07 MAI 2025

CONSELHO NACIONAL DE JUSTIÇA. *Resolução nº 121, de 5 de outubro de 2010*. Dispõe sobre a divulgação de dados processuais eletrônicos na rede mundial de computadores, expedição de certidões judiciais e dá outras providências. Diário de Justiça Eletrônico, Brasília, DF, 11 out. 2010.

CONSELHO NACIONAL DE JUSTIÇA. *Resolução nº 363, de 12 de janeiro de 2021*. Estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos tribunais. Diário de Justiça Eletrônico, Brasília, DF, 18 jan. 2021.

FILHO, *José dos Santos Carvalho. Manual de direito administrativo*. 2. ed. São Paulo: Editora Atlas, p. 26.2014

ORDEM DOS ADVOGADOS DO BRASIL – OAB – Disponível em https://www.oab.org.br/noticia/63063/oab-lanca-campanha-nacional-e-plataforma-de-verificacao-contra-golpe-do-falso-advogado. Acesso em 07 MAI 2025.

ZANETTI DE OLIVEIRA, Dânton Hilário; FREITAS, Cinthia Obladen de Almendra. *Proteção de dados pessoais e publicidade processual*: Um contrassenso? Migalhas, 15 abr. 2021. Disponível em: https://www.migalhas.com.br/depeso/343796/protecao-de-dados-pessoais-e-publicidade-processual-um-contrassenso. Acesso em: 7 mai. 2025.

A Relação entre a OAB e a ANPD

Ordem dos Advogados do Brasil - Seccional Amazonas

Reflexão sobre os limites da regulação estatal e autorregulação profissional no contexto da proteção de dados.

Aldo Evangelista

Educador e Advogado em direitos digitais. Procurador Municipal de Carreira. Mestre em Ciências Forenses pela UNIFESSPA. Doutorando pela UNIVALI – CIESA. Presidente da Comissão de Direitos Digitais, Startups e Inovação da OAB-AM. Encarregado da OAB-AM. Palestrante e músico.

Resumo

Este estudo analisa a complexa relação entre a Ordem dos Advogados do Brasil (OAB) e a Autoridade Nacional de Proteção de Dados (ANPD) no contexto da Lei Geral de Proteção de Dados (LGPD). Partindo da premissa de que a OAB é uma entidade sui generis, de serviço público independente, não subordinada a nenhum controle estatal, inclusive ao Tribunal de Contas da União (TCU), portanto a OAB e a advocacia estariam, de fato, sujeitas à fiscalização e sanções da ANPD? A pesquisa aponta que, embora a LGPD se aplique a pessoas jurídicas de direito público e privado, o Supremo Tribunal Federal (STF) reconheceu a autonomia e independência da OAB. A decisão da ADI nº 3.026/DF destaca que a OAB não é uma entidade da administração indireta da União e não está sujeita a controle estatal. Adicionalmente, a inviolabilidade profissional do advogado, assegurada pela Constituição Federal e pelo Estatuto da OAB, protege o escritório, o local de trabalho e os dados tratados no exercício da profissão. A pesquisa aborda a solicitação da seccional da OAB do Amazonas (OAB-AM) à ANPD, que pedia o reconhecimento da não subordinação da OAB e a criação de um grupo de trabalho conjunto para regulamentar a relação entre as instituições. Diante da lacuna e da ausência de direcionamento adequado para o tratamento de dados pessoais no sistema OAB, o estudo sugere que o Conselho Federal da OAB crie internamente sua própria normatização, fiscalização e sanções para a proteção de dados, que seriam aplicadas pelos Tribunais de Ética e Disciplina do sistema.

Palavras-chave: Ordem dos Advogados do Brasil; Autoridade Nacional de Proteção de Dados; LGPD; Inviolabilidade profissional; Entidade *sui generis*.

1. Análise preliminar

O presente texto nasce com o objetivo de realizar uma breve análise da relação da Ordem dos Advogados do Brasil (OAB) e a Autoridade Nacional de Proteção de Dados (ANPD), visto que a OAB é reconhecida, inclusive em vários julgados do Supremo Tribunal Federal (STF) como sendo uma entidade sui generis, de serviço público independente.

Consequentemente, a OAB é autônoma e independente, não estando sujeita e nem subordinada ao controle estatal. "A Ordem é um serviço público independente, categoria ímpar no elenco das personalidades jurídicas existentes no direito brasileiro".

Desta forma, nem ao Tribunal de Contas da União (TCU) a OAB é subordinada e nem recebe nenhum tipo de fiscalização ou orientação do TCU, logo, estaria a OAB subordinada nos termos da LGPD e da Constituição Federal a ANPD?

2 – A LGPD e a ANPD

A Lei 13.709/2018[1], que é a Lei Geral de Proteção de Dados Pessoais (LGPD), conforme sua ementa, determina em seu art. 1º que todas as pessoas jurídicas de direito público ou privado devem se adequar á Lei, quando estiverem tratando de dados pessoais.

No art. 5º da LGPD[2], define o que é dado pessoal, dado pessoal sensível, tratamento de dados, agentes de tratamento de dados, controlador, operador, encarregado e o titular de dados, nestes termos:

> Art. 5º Para os fins desta Lei, considera-se:
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
> V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII - operador: pessoa natural ou jurídica, de direito público ou privado,

1 BRASIL. Lei nº 13.709, de 2018. Lei Geral de Proteção de Dados. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm . Acesso em: 25/05/2025.
2 Idem

> que realiza o tratamento de dados pessoais em nome do controlador;
> VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
> IX - agentes de tratamento: o controlador e o operador;
> X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

Essas definições são necessárias para esclarecer, uma nova dinâmica trazida pela LGPD ao sistema jurídico brasileiro, ficando claro que, quando houver dado pessoal ou dado pessoal sensível, o tratamento desde a sua coleta e em todo ciclo de vida desses dados, o controlador que são as pessoas jurídicas determinadas no art. 1º, possuem o dever de cumprir, ou seja, se adequar a LGPD e as regulações emitidas pela ANPD.

Nessa nova realidade, o titular de dados pessoais, que são todas as pessoas naturais vivas, possuem direitos sobre seus dados pessoais, estabelecidos de forma não taxativa, nos art. 17 e art. 18 da LGPD[3], nestes termos:

> Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.
> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
> I - confirmação da existência de tratamento;
> II - acesso aos dados;
> III - correção de dados incompletos, inexatos ou desatualizados;
> IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
> V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
> VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
> VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
> VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
> IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

3 Idem

As pessoas naturais, citadas no texto da LGPD são os titulares de dados, e relacionando a LGPD com as pessoas naturais do art. 6º do Código Civil, esse determina que a existência da pessoa natural termina com a morte, logo a LGPD aplica-se somente as pessoas naturais, ou seja, as pessoas físicas vivas, é o entendimento estabelecido pela ANPD através da Nota Técnica nº. 03/2023/CGF/ANPD.[4]

São várias determinações no texto da LGPD, para que essa engrenagem criada pelo seu texto funcione, dentre elas, fica claro que na prática uma pessoa jurídica ao se adequar a Lei, precisa definir de início se é pessoa jurídica de direito público ou privado. Essa diferenciação parece ser obvia, mas não é.

Na maior parte do texto da LGPD deixa claro o seu direcionamento para pessoa jurídica de direito privado, tanto que dispõe do Capítulo IV, regulação ao tratamento da administração pública. E aqui, registre-se que em certos momentos, no texto da LGPD chama a pessoa jurídica de direito público, como poder público, ou administração pública ou órgão público.

Na pratica a administração publica direta e indireta, dos entes da federação, ao cumprir a LGPD não pode utilizá-la de forma isolada pois é imperioso harmonizá-la com as normas e princípios das administrações publica, como por exemplo: o art. 37 da Constituição Federal de 1988; o Marco Civil da Internet (MCI) Lei nº 12.965/2014; a Lei de Acesso a Informação (LAI) Lei nº. 12.527/2011; a Lei sobre a proteção e defesa dos usuários dos serviços públicos Lei nº. 13.460/2017; a Lei do Governo Digital Lei nº. 14.129/2021.

Como brevemente demonstrado que são jornadas diferentes, a adequação da LGPD na pessoa jurídica de direito privado em relação a pessoa jurídica de direito público, outro item importante na engrenagem da LGPD, refere-se ao descumprimento da Lei e regulações da ANPD e a ocorrência de incidente de segurança[5], ao qual os controladores podem responder administrativamente pelo processo administrativo sancionador[6], podendo sofrer as sanções do art. 52[7], nestes termos:

---

4 BRASIL. Nota Técnica nº. 03/2023/CGF/ANPD. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/nota-tecnica-no-3-2023-cgf-anpd.pdf. Acesso em: 25/05/2025.

5 Incidente de segurança é qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais. É o que dispõe o inciso XII do art. 3º da Resolução CD/ANPD Nº 15, de 24 de abril de 2024. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024. Acesso em: 25/05/2025.

6 Processo administrativo sancionador destina-se à apuração de infrações à legislação de proteção de dados de competência da ANPD, nos termos do artigo 55-J, IV, da LGPD. É o que dispõe o Art. 37 da Resolução CD/ANPD Nº 01, de 28 de outubro de 2021. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no1-2021 . Acesso em: 25/05/2025.

7 BRASIL. Lei nº 13.709, de 2018. Lei Geral de Proteção de Dados. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm . Acesso em: 25/05/2025.

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
> III - multa diária, observado o limite total a que se refere o inciso II;
> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
> VI - eliminação dos dados pessoais a que se refere a in
> fração;
> X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (Incluído pela Lei nº 13.853, de 2019)
> XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; (Incluído pela Lei nº 13.853, de 2019)
> XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

A Autoridade Nacional de Proteção de Dados (ANPD) possui sua competência estabelecida nos termos do Art. 55–J da LGPD, dentre elas por exemplo deve: zelar pela proteção de dados pessoais; fiscalizar e aplicar sanções; editar regulamentos e procedimentos.

A ANPD possui a competência exclusiva para aplicar as sanções do art. 52 da LGPD, é o que determina o Art. 55-K[8], nestes termos:

> Art. 55-K. A aplicação das sanções previstas nesta Lei compete exclusivamente à ANPD, e suas competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública.
> Parágrafo único. A ANPD articulará sua atuação com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais e será o órgão central de interpretação desta Lei e do estabelecimento de normas e diretrizes para a sua implementação.

8 BRASIL. Lei nº 13.709, de 2018. Lei Geral de Proteção de Dados. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm . Acesso em: 25/05/2025.

Ocorre que, todas essas sanções citadas no art. 52 da LGPD, são aplicáveis a pessoa jurídica de direito privado. As pessoas de direito público, as multas dos incisos II e III do art. 52, não se aplicam aos gestores da administração pública, como determina o Art. 3º da Resolução CD/ANPD Nº 4, de 24 de fevereiro de 2023[9], que Aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas.

O § 5º do Art. 3º da Resolução CD/ANPD Nº 4, de 24 de fevereiro de 2023[10], direciona que o gestor na administração pública responderá por outras Leis, dentre elas a Lei de atos de improbidade administrativa a Lei nº 8.429/1992, nestes termos:

> Art. 3º As infrações sujeitarão o infrator às seguintes sanções administrativas:
> (...)
> § 5º O disposto nos incisos I e IV a IX, do caput deste artigo, poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990, na Lei nº 8.429, de 2 de junho de 1992, e na Lei nº 12.527, de 18 de novembro de 2011.

Nessas breves considerações até aqui descritas para elucidar pontos que são desafiadores na relação da LGPD, ANPD e a OAB. Logo, como a OAB é uma entidade com especificidades, ela como deve proceder nesse diálogo com o direito fundamento da proteção de dados pessoais nos termos do art. 5º, inciso LXXIX da Constituição Federal de 1988[11]; e com a LGPD e a ANPD; e o com a advocacia.

3 - A Ordem dos Advogados do Brasil (OAB)

A Ordem dos Advogados do Brasil (OAB), criada pelo art. 17 do Decreto nº 19.408/1930[12], nestes termos:

> Art. 17. Fica criada a Ordem dos Advogados Brasileiros, órgão de disciplina e seleção da classe dos advogados, que se regerá pelos estatutos que forem votados pelo Instituto da Ordem dos Advogados Brasileiros, com a colaboração dos Institutos dos Estados, e aprovados pelo Governo.

A Constituição Federal de 1988, no seu art. 133, determina que o advogado é indispensável a administração da justiça e com atos invioláveis no exercício da profissão[13], desta forma a OAB se concretiza como representante da sociedade.

---

9 BRASIL. Resolução CD/ANPD Nº 4, de 24 de fevereiro de 2023. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077. Acesso em: 25/05/2025.

10 Idem.

11 BRASIL. Constituição Federal de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm .Acesso em: 25/05/2025.

12 OAB – Ordem dos Advogados do Brasil. Decreto nº. 19.408/1930. Reorganiza a Corte de Apelação. Disponível em: https://www.oab.org.br/historiaoab/inicio.htm#criacaoordem . Acesso em: 25/05/2025.

13 BRASIL. Constituição Federal de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm .Acesso em: 25/05/2025.

O novo Estatuto da OAB, a Lei nº 8.906/1994, ratifica a inviolabilidade no exercício da profissão, no inciso II do art. 7º[14], nestes termos

> Art. 7º São direitos do advogado:
> I - exercer, com liberdade, a profissão em todo o território nacional;
> II – a **inviolabilidade** de seu escritório ou local de trabalho, bem como de seus instrumentos de trabalho, de sua correspondência escrita, **eletrônica**, telefônica e **telemática**, desde que relativas ao exercício da advocacia; (grifo nosso)

Como a ANPD poderá atuar, se são invioláveis os dados pessoais que a advocacia trata no exercício da sua profissão?

Antes de procurar resposta a esta indagação, outra indagação relevante precisa ser analisada anteriormente, que é o fato da OAB ser uma instituição "*sui generis*", reconhecida por diversas Decisões do Supremo Tribunal Federal (STF), reconhecendo que não há dependência e nem esta sujeita ao controle de qualquer ente da administração pública.

A OAB não é uma entidade da administração indireta, logo não é autarquia, e nem entidade genuinamente privada, mas serviço público independente, categoria *sui generis*, submetida ao direito público, na realização das atividades estatais que lhe foram delegadas, e ao direito privado, no desenvolvimento de suas atividades administrativas e de suas finalidades institucionais e de defesa da profissão. Considerada a natureza de serviço público não estatal, mas serviço público de âmbito federal, os processos judiciais em que a OAB seja interessada sujeitam-se à competência da justiça federal (STF, HC 71.314-9), salvo no caso de cobrança das anuidades (STJ, EREsp 462.273).

O STF em especial julgamento da ADI nº 3.026/DF, reconhece as peculiaridades da OAB, nestes termos:

> AÇÃO DIRETA DE INCONSTITUCIONALIDADE. § 1º DO ARTIGO 79 DA LEI N. 8.906 , 2ª PARTE. "SERVIDORES" DA ORDEM DOS ADVOGADOS DO BRASIL. PRECEITO QUE POSSIBILITA A OPÇÃO PELO REGIME CELESTISTA. COMPENSAÇÃO PELA ESCOLHA DO REGIME JURÍDICO NO MOMENTO DA APOSENTADORIA. INDENIZAÇÃO. IMPOSIÇÃO DOS DITAMES INERENTES À ADMINISTRAÇÃO PÚBLICA DIRETA E INDIRETA. CONCURSO PÚBLICO (ART. 37 , II DA CONSTITUIÇÃO DO BRASIL). INEXIGÊNCIA DE CONCURSO PÚBLICO PARA A ADMISSÃO DOS CONTRATADOS PELA OAB. AUTARQUIAS ESPECIAIS E AGÊNCIAS. CARÁTER JURÍDICO DA OAB. ENTIDADE PRESTADORA DE SERVIÇO PÚBLICO INDEPENDENTE. CATEGORIA ÍMPAR

14 BRASIL. Lei nº 8.906/1994. Estatuto da Advocacia e a Ordem dos Advogados do Brasil (OAB). Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8906.htm .Acesso em: 25/05/2025.

> NO ELENCO DAS PERSONALIDADES JURÍDICAS EXISTENTES NO DIREITO BRASILEIRO. AUTONOMIA E INDEPENDÊNCIA DA ENTIDADE. PRINCÍPIO DA MORALIDADE. VIOLAÇÃO DO ARTIGO 37 , CAPUT, DA CONSTITUIÇÃO DO BRASIL . NÃO OCORRÊNCIA. 1. A Lei n. 8.906 , artigo 79 , § 1º , possibilitou aos "servidores" da OAB, cujo regime outrora era estatutário, a opção pelo regime celetista. Compensação pela escolha: indenização a ser paga à época da aposentadoria. 2. Não procede a alegação de que a OAB sujeita-se aos ditames impostos à Administração Pública Direta e Indireta. 3. A OAB não é uma entidade da Administração Indireta da União. A Ordem é um serviço público independente, categoria ímpar no elenco das personalidades jurídicas existentes no direito brasileiro. 4. A OAB não está incluída na categoria na qual se inserem essas que se tem referido como "autarquias especiais" para pretender-se afirmar equivocada independência das hoje chamadas "agências". 5. Por não consubstanciar uma entidade da Administração Indireta, **a OAB não está sujeita a controle da Administração, nem a qualquer das suas partes está vinculada. Essa não-vinculação é formal e materialmente necessária**. 6. A OAB ocupa-se de atividades atinentes aos advogados, que exercem função constitucionalmente privilegiada, na medida em que são indispensáveis à administração da Justiça [artigo 133 da CB/88]. É entidade cuja finalidade é afeita a atribuições, interesses e seleção de advogados. **Não há ordem de relação ou dependência entre a OAB e qualquer órgão público**. 7. **A Ordem dos Advogados do Brasil, cujas características são autonomia e independência, não pode ser tida como congênere dos demais órgãos de fiscalização profissiona**l. A OAB não está voltada exclusivamente a finalidades corporativas. Possui finalidade institucional. 8. Embora decorra de determinação legal, o regime estatutário imposto aos empregados da OAB não é compatível com a entidade, que é autônoma e independente. 9. Improcede o pedido do requerente no sentido de que se dê interpretação conforme o artigo 37 , inciso II , da Constituição do Brasil ao caput do artigo 79 da Lei n. 8.906 , que determina a aplicação do regime trabalhista aos servidores da OAB. 10. Incabível a exigência de concurso público para admissão dos contratados sob o regime trabalhista pela OAB. 11. Princípio da moralidade. Ética da legalidade e moralidade. Confinamento do princípio da moralidade ao âmbito da ética da legalidade, que não pode ser ultrapassada, sob pena de dissolução do próprio sistema. Desvio de poder ou de finalidade. 12. Julgo improcedente o pedido. (grifo nosso)

Nesta citação da ADI nº 3.026/DF, fica claro a não subordinação da OAB a qualquer controle Estatal, ou seja, o entendimento foi ratificado e cumprido pelo Tribunal de Contas da União (TCU), pois nem o TCU fiscaliza a OAB, e reconhece que a OAB é sui generis com finalidade institucional.

Para fins de prestação de contas, a OAB possui seus próprios instrumentos normativos e mecanismos para aplicação de recursos financeiros, *accountability*,

transparência e aprovação das contas. Não se subordinando a nenhum órgão estatal de controle externo e nem ao controle social.

Em resumo, a OAB é considerada uma entidade *sui generis* porque conjuga autonomia e independência em relação ao Estado com uma finalidade institucional que transcende os interesses corporativos, refletindo a importância constitucional do advogado. A jurisprudência do STF consolidou esse entendimento, desvinculando-a da administração pública indireta e assegurando que sua atuação não seja controlada pelo Poder Executivo ou por órgãos como o TCU.

Logo, a indagação permanece se a OAB estaria subordinada a ANPD?

4 – A (Não)Subordinação da OAB a ANPD

Pelos breves argumentos acima descritos fica claro que a OAB não deve se subordinar a ANPD. Este pleito gerou manifestações favoráveis, outros fervorosamente no tribunal da internet contrários, outros indecisos e outros indiferentes.

Este clamor foi causado quando a Ordem dos Advogado do Brasil seção Amazonas (OAB-AM), por meio da Comissão de Direitos Digitais, Startups e Inovação da OAB-AM, Comissão instituída em 2018 e continua com atuação recorrente, protocolou na ANPD o requerimento requerendo diálogo e que seja criado grupo de trabalho com as instituições (OAB-AM e ANPD) para que[15]:

- seja reconhecida a não subordinação da OAB à ANPD;
- a ANPD crie em conjunto com a OAB um manual de instruções e procedimentos técnicos para estabelecer da relação entre a ANPD e OAB;
- a ANPD crie um grupo de trabalho para debater este tema.

Neste sentido, como a instituição OAB não deve se subordinar a ANPD, os escritórios de advocacia podem seguir um caminho parecido, devido a inviolabilidade constitucional da advocacia, esta não estará sujeita a aplicação do texto da LGPD.

Surge uma nova indagação, estaria a advocacia e a instituição OAB, desobrigadas do direito fundamental da Proteção de Dados Pessoais?

A questão da relação entre a Ordem dos Advogados do Brasil (OAB) e a Autoridade Nacional de Proteção de Dados (ANPD) desdobra-se em três cenários futuros, cada um com implicações jurídicas e práticas distintas. A exploração desses caminhos é essencial para a robustez da pesquisa.

15 OAB/AM pede para não ser subordinada à ANPD. Migalhas. Disponível em: https://www.migalhas.com.br/quentes/350010/oab-am-pede-para-nao-ser-subordinada-a-anpd . Acesso em: 25/05/2025.

4.1 Subordinação Total da OAB à ANPD

Neste cenário, prevaleceria o entendimento de que a OAB e a advocacia, por tratar dados pessoais, estariam integralmente sujeitos à fiscalização e às sanções da ANPD, conforme o artigo 1º da LGPD. As consequências seriam as seguintes:

- Impacto na Autonomia Institucional: A subordinação direta à ANPD poderia ser interpretada como um cerceamento da autonomia e independência da OAB , desconsiderando sua natureza sui generis e o entendimento consolidado do Supremo Tribunal Federal (STF) na ADI nº 3.026/DF. Isso poderia gerar um conflito de competências, onde as prerrogativas constitucionais da OAB seriam confrontadas com as competências sancionatórias da ANPD;
- Conflito com o Sigilo Profissional: A fiscalização da ANPD poderia entrar em choque direto com a inviolabilidade do escritório, dos instrumentos de trabalho e das comunicações do advogado. A ANPD, para fiscalizar, precisaria acessar dados que estão sob sigilo profissional, o que levantaria sérios questionamentos éticos e jurídicos sobre a proteção do cliente e a confiança na relação advogado-cliente;
- Aplicação de Sanções Não Compatíveis: As sanções da LGPD, especialmente as multas, foram desenhadas para empresas privadas. Aplicá-las a uma entidade de serviço público como a OAB, que não tem finalidade lucrativa e não se enquadra na categoria de empresa, seria inadequado. Além disso, as penalidades disciplinares já existentes no Estatuto da Advocacia seriam ignoradas ou duplicadas, criando um sistema punitivo confuso.

4.2 Criação de Regulamentação Própria pela OAB

Esta via sugere que, diante de sua natureza e autonomia, a OAB criaria um sistema interno de proteção de dados, em analogia a sua regulação e mecanismos de prestação de contas financeiras. As consequências seriam:

- Reforço da Autonomia Institucional: Ao normatizar internamente a proteção de dados, a OAB reafirmaria sua independência e seu papel de autorregulação. Isso garantiria que as peculiaridades da advocacia, como o sigilo profissional, fossem devidamente consideradas na regulamentação;
- Harmonização com o Sigilo Profissional: A regulamentação interna poderia estabelecer critérios claros para a ponderação entre os direitos dos titulares de dados e o dever de sigilo do advogado. Os Tribunais de Ética e Disciplina (TEDs) seriam os responsáveis por julgar os casos de descumprimento, aplicando sanções disciplinares já previstas no Estatuto da Advocacia;

- Possível Diálogo com a ANPD: Embora a OAB não estaria subordinada, um diálogo poderia ser estabelecido para harmonizar as regulamentações internas com as diretrizes gerais da ANPD. A OAB poderia atuar como uma "autoridade setorial" na área jurídica, mantendo um canal de comunicação com a ANPD para troca de informações e cooperação técnica.

4.3 Judicialização da Questão

Este cenário ocorre se o diálogo entre a OAB e a ANPD não avançar. A questão seria levada ao poder judiciário, possivelmente chegaria ao STF, para uma resolução definitiva. As consequências seriam:

- Fortalecimento da Jurisprudência do STF: A judicialização reforçaria a jurisprudência já estabelecida sobre a natureza sui generis da OAB. O STF provavelmente reafirmaria a autonomia da OAB e a inviolabilidade da advocacia, estendendo esse entendimento para a relação com a LGPD e a ANPD;
- Morosidade e Insegurança Jurídica: O processo judicial seria lento, e a falta de uma definição clara durante esse período geraria insegurança jurídica para advogados, escritórios, titulares de dados e ao sistema OAB. Isso poderia resultar em um vazio regulatório por tempo indeterminado, prejudicando a proteção de dados.
- Solução Impositiva: A decisão judicial seria uma solução impositiva, que poderia não contemplar o diálogo e a cooperação que poderiam ser alcançados em um cenário de regulamentação própria. A falta de participação das instituições na construção da norma poderia levar a um resultado menos adequado às especificidades da advocacia.

Em suma, a criação de uma regulamentação própria pela OAB, em diálogo com a ANPD, parece ser o caminho mais promissor. Ele preservaria a autonomia da entidade, harmonizaria o sigilo profissional com a proteção de dados pessoais e ofereceria uma solução prática e eficaz, evitando os riscos de conflito e morosidade dos outros cenários.

5 – Considerações Finais

Essa lacuna, objeto deste texto (se a instituição OAB se subordina ou não à ANPD e se a advocacia deve ou não cumprir a LGPD), precisa ser dialogada e resolvida pelas instituições, pois independente do direcionamento futuro que será dado, atualmente, dados pessoais de funcionários e clientes são tratados a todo momento pelo sistema OAB e pela advocacia, sem direcionamento adequado, fiscalização ou possíveis sanções.

Essa realidade além de haver um aparente prejuízo aos titulares de dados, também gera desafios e indagações constantes aos parcos encarregados de dados nomeados no sistema OAB, pois algumas seccionais possuem encarregados de dados nomeados, titulares e suplentes, como é o caso da OAB-AM, ou seja, e qual caminho o encarregado de dados da OAB deve seguir?

A solicitação da OAB-AM não avançou junto a ANPD até o momento, pois o diálogo é o melhor caminho, de outra forma será necessário judicializar o assunto, mais o entendimento do STF em vários julgados, certamente será mantido e estendido a ANPD e a LGPD.

Usando como analogia o fato de a OAB ter normatizado internamente e criado seus critérios de aplicação e prestação de contas financeiro e aprovação. O mesmo pode ocorrer com o tratamento dos dados pessoais, sugere-se ao Conselho Federal da OAB internamente normatizar, fiscalizar, sancionar o que diz respeito a proteção de dados pessoais, ou seja, criar seus instrumentos normativos e mecanismos, à instituição OAB e por consequência aos sistemas OAB. Esse parece ser o melhor caminho.

Neste mesmo sentido sugere-se que o Conselho Federal da OAB crie a normatização à advocacia e escritórios, realizem a adequação a proteção de dados pessoais de seus clientes e funcionários, e em casos de inadequação, descumprimento a norma e incidentes de insegurança as sanções serem aplicadas pelos Tribunais de Ética e Disciplina do sistema OAB e as seguintes recomendações a OAB e a advocacia:

1. Funcionamento Prático:

- Estrutura de Governança: O Conselho Federal da OAB criaria um Comitê Nacional de Proteção de Dados. Esse comitê seria responsável por sugerir a regulamentação, além de servir como órgão consultivo e orientativo;
- Normatização Detalhada: A OAB elaboraria um provimento que detalhasse as obrigações de proteção de dados para todos os advogados e escritórios. Esse provimento incluiria diretrizes sobre coleta, tratamento, armazenamento, descarte e segurança da informação, adaptadas à realidade da advocacia;
- Fiscalização Interna: As seccionais da OAB teriam comissões específicas (como a já existente na OAB-AM) para atuar na fiscalização e na orientação dos profissionais e escritórios. Essas comissões não teriam um poder sancionatório direto, mas seriam responsáveis por investigar denúncias e encaminhar os casos aos TEDs;
- Encarregado de Dados: Cada seccional da OAB nomearia um Encarregado de Dados para ser o canal de comunicação entre os advogados, os titulares

de dados e a própria OAB. Esse Encarregado seria responsável por orientar sobre a aplicação das normas e mediar conflitos.

2. Princípios Orientadores:

A regulamentação interna da OAB seria guiada por princípios que harmonizam a LGPD com as peculiaridades da advocacia, como:

- Inviolabilidade e Confidencialidade: O principal princípio seria a garantia da inviolabilidade profissional e do sigilo de dados, conforme previstos na Constituição Federal e no Estatuto da Advocacia. A norma interna da OAB reforçaria que o sigilo profissional é um dever ético e legal;
- Transparência e Acesso: A regulamentação estabeleceria que, apesar do sigilo profissional, o advogado deve ser transparente sobre como os dados do cliente são tratados. Seria necessário um procedimento para que o titular de dados possa exercer seus direitos de acesso, correção ou eliminação, desde que não infrinjam o sigilo profissional ou o dever de custódia de documentos;
- Responsabilidade e Accountability: A norma interna da OAB reforçaria a responsabilidade do advogado e do escritório de advocacia em demonstrar a conformidade com as regras de proteção de dados. Isso incluiria a adoção de medidas de segurança e a criação de registros de tratamento.

3. Harmonização com o Sigilo Profissional:

A harmonização dos direitos do titular de dados com o sigilo profissional seria o maior desafio. Para isso, a regulamentação da OAB criaria um procedimento de ponderação:

- Solicitação de Titulares: Quando um titular de dados (como um ex-cliente) solicitasse acesso ou eliminação de seus dados, o advogado avaliaria a solicitação sob a ótica da Proteção de dados pessoais e do Estatuto da Advocacia;
- Ponderação do Sigilo: O advogado teria o dever de proteger as informações que estão sob sigilo profissional, como estratégias jurídicas, correspondências confidenciais ou documentos que possam prejudicar o cliente em potencial. Nesses casos, o advogado poderia negar o acesso ou a eliminação, explicando ao titular o motivo da recusa com base no dever de sigilo;
- Mediação da OAB: Em caso de conflito, o titular de dados poderia recorrer à comissão da OAB, que atuaria como mediadora para encontrar uma solução que respeite o sigilo profissional sem ferir os direitos fundamentais do titular.

4. Preparação dos Tribunais de Ética e Disciplina (TEDs):

Os TEDs seriam o ponto de aplicação das sanções. Para se prepararem, seriam necessárias as seguintes ações:

- Formação Continuada: Os membros dos TEDs passariam por cursos de capacitação em proteção de dados, segurança da informação e LGPD, para que pudessem julgar os casos com conhecimento técnico;
- Manual de Procedimentos: Seria criado um manual que orientaria os TEDs sobre como lidar com denúncias de incidentes de segurança, tratamento indevido ou descumprimento das normas internas. Esse manual detalharia o rito processual e as sanções aplicáveis;
- Sanções Adaptadas: As sanções aplicadas pelos TEDs seriam as já existentes no Estatuto da Advocacia, como advertência, censura, suspensão ou até mesmo exclusão dos quadros da Ordem, a depender da gravidade da infração. A norma interna da OAB estabeleceria uma gradação para a aplicação dessas sanções, levando em conta o dolo, o prejuízo causado e a reincidência.

Referências

BRASIL. *Lei nº 13.709, de 2018*. Lei Geral de Proteção de Dados. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm . Acesso em: 25/05/2025;

BRASIL. *Nota Técnica nº. 03/2023/CGF/ANPD*. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/nota-tecnica-no-3-2023-cgf-anpd.pdf. Acesso em: 25/05/2025 ;

BRASIL. *Resolução CD/ANPD Nº 15, de 24 de abril de 2024*. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024. Acesso em: 25/05/2025;

BRASIL. *Resolução CD/ANPD Nº 01, de 28 de outubro de 2021*. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no1-2021 . Acesso em: 25/05/2025.

BRASIL. *Resolução CD/ANPD Nº 4, de 24 de fevereiro de 2023*. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077. Acesso em: 25/05/2025;

BRASIL. *Constituição Federal de 1988*. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm .Acesso em: 25/05/2025;

OAB – Ordem dos Advogados do Brasil. *Decreto nº. 19.408/1930*. Reorganiza a Corte de Apelação. Disponível em: https://www.oab.org.br/historiaoab/inicio.htm#criacaoordem . Acesso em: 25/05/2025;

BRASIL. *Lei nº 8.906/1994*. Estatuto da Advocacia e a Ordem dos Advogados do Brasil (OAB). Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8906.htm .Acesso em: 25/05/2025;

Migalhas. *OAB/AM pede para não ser subordinada à ANPD*. Disponível em: https://www.migalhas.com.br/quentes/350010/oab-am-pede-para-nao-ser-subordinada-a-anpd;

Rede Amazonense de Proteção de Dados

Tribunal de Justiça do Estado do Amazonas

Íkono.
PUBLICAÇÕES