



CURSO DE DIREITO

CAUÃ FOCCHESATTO CASTAÑON

**ANÁLISE DO TRATAMENTO DE DADOS PESSOAIS NA
DEFENSORIA PÚBLICA DO ESTADO DE MATO GROSSO (DPE-MT), COM FOCO
NA CONFORMIDADE COM A LEI GERAL DE
PROTEÇÃO DE DADOS (LGPD)**

**Cuiabá/MT
2025**

CURSO DE DIREITO

CAUÃ FOCCHESATTO CASTAÑON

**ANÁLISE DO TRATAMENTO DE DADOS PESSOAIS NA
DEFENSORIA PÚBLICA DO ESTADO DE MATO GROSSO (DPE-MT), COM FOCO
NA CONFORMIDADE COM A LEI GERAL DE
PROTEÇÃO DE DADOS (LGPD)**

Trabalho de Conclusão de Curso
apresentado à Banca Avaliadora do
Departamento de Direito, da Faculdade
FASIPE Cuiabá, como requisito parcial
para a obtenção do título de Bacharel em
Direito.

Orientadora: Prof. Ma. Giovana César
Schnerer

**Cuiabá/MT
2025**

CAUÃ FOCCHESATTO CASTANÕN

**ANÁLISE DO TRATAMENTO DE DADOS PESSOAIS NA
DEFENSORIA PÚBLICA DO ESTADO DE MATO GROSSO (DPE-MT), COM FOCO
NA CONFORMIDADE COM A LEI GERAL DE
PROTEÇÃO DE DADOS (LGPD)**

Trabalho de Conclusão de Curso apresentado à Banca Avaliadora do Curso de Direito da Faculdade Fasipe Cuiabá como requisito parcial para a obtenção do título de Bacharel em Direito.

Aprovado em ____/____/_____.

Prof. Ma. GIOVANA CÉSAR SCHERNER
Professora Orientadora
Departamento de Direito – FASIPE CPA

NOME EXAMINADOR
Professor Avaliador
Departamento de Direito – FASIPE CPA

NOME EXAMINADOR
Professor Avaliador
Departamento de Direito – FASIPE CPA

OLMIR BAMPI JÚNIOR
Coordenador do curso de Direito – FASIPE CPA

Cuiabá/MT
2025

DEDICATÓRIA

Dedico este trabalho a minha família, base de tudo que sou, pelo amor incondicional, pelas palavras de incentivo e por nunca deixarem que eu desistisse dos meus sonhos. Agradeço por cada gesto de apoio, por cada sacrifício silencioso e por acreditarem em mim mesmo nos momentos em que eu duvidei.

Também dedico a todos os amigos e pessoas queridas que, de alguma forma, caminharam comigo nesta trajetória, oferecendo força, compreensão e companhia. Sem vocês, esta conquista não teria o mesmo significado.

AGRADECIMENTOS

Agradeço, primeiramente, a Deus, por ter me guiado e sustentado em cada etapa desta jornada.

Ao meu pai e a minha mãe, por todo amor, dedicação e pelos valores que me ensinaram, sendo sempre meu alicerce.

A minha namorada, pelo apoio incondicional, paciência e carinho nos momentos em que mais precisei. Sua presença tornou tudo mais leve.

Aos meus irmãos, por compartilharem comigo a vida, os aprendizados e os sonhos.

Aos meus avós maternos, que sempre me incentivaram com palavras de encorajamento e gestos de amor.

Aos meus avós paternos, com carinho especial à minha querida avó, que partiu recentemente, mas permanece viva em meu coração e em minhas lembranças.

Ao meu tio Fernando, por todo apoio, ensinamento e pelas oportunidades que me proporcionou ao longo da vida. Seu exemplo e confiança em mim fizeram toda a diferença.

A minha madrastra e ao meu padrasto, pelo acolhimento, incentivo e cuidado, que contribuíram muito nesta caminhada.

À minha orientadora Giovana César Scherner, pelo apoio, pela excelente orientação e pela atenção dedicada ao longo de todo o processo. Sua contribuição foi essencial para a realização deste trabalho.

A todos vocês, minha mais sincera gratidão. Esta conquista também é de vocês.

CASTANÕN, Cauã Focchesatto. Análise do tratamento de dados pessoais na Defensoria Pública do Estado de Mato Grosso (DPE-MT), com foco na conformidade com a lei geral de proteção de dados (LGPD). 2025. 52 folhas. Trabalho de Conclusão de Curso – Faculdade Fasipe Cuiabá.

RESUMO

O presente Trabalho de Conclusão de Curso, intitulado "Análise do tratamento de dados pessoais na Defensoria Pública do Estado de Mato Grosso (DPE-MT), com foco na conformidade com a Lei Geral de Proteção de Dados (LGPD)", aborda a crescente importância da proteção de dados pessoais diante do avanço da internet e da coleta massiva de informações. Destaca-se, nesse contexto, a necessidade de segurança e responsabilidade no tratamento de dados, especialmente no setor público. A Defensoria Pública do Estado de Mato Grosso, por atuar diretamente com dados sensíveis de pessoas em situação de vulnerabilidade, é o foco desta análise. A LGPD estabelece diretrizes para garantir o sigilo e a proteção das informações pessoais, sendo a conformidade não apenas um dever legal, mas também uma exigência ética, essencial para fortalecer a confiança social e assegurar o acesso à justiça. Este trabalho busca discutir como a DPE-MT tem se adequado à LGPD, identificando os principais desafios enfrentados e propondo soluções. A relevância do tema está na necessidade de promover o tratamento responsável de dados de cidadãos que dependem da atuação da instituição, alinhando-a aos princípios de justiça social e cidadania. A fundamentação teórica explora a evolução do direito à privacidade e os conceitos centrais da LGPD, como dados pessoais e sensíveis, tratamento de dados, agentes de tratamento (controlador, operador e encarregado), princípios, bases legais, direitos dos titulares e sanções administrativas. Também se examina a aplicação da proteção de dados no setor público e o papel da Autoridade Nacional de Proteção de Dados (ANPD). A DPE-MT trata diariamente um grande volume de dados pessoais, especialmente por meio de sistemas como Solar, PJe e SEEU. Para buscar a conformidade, a instituição implementou medidas como o Plano de Proteção de Dados Pessoais, a nomeação de um encarregado (DPO), a Política de Privacidade e Proteção de Dados, o fortalecimento do Sistema de Controle Interno e a criação de canais para o exercício dos direitos dos titulares. Além disso, mapeou os dados tratados e o ciclo de vida dessas informações, bem como as hipóteses legais de compartilhamento com outros órgãos. Apesar dos avanços, a DPE-MT ainda enfrenta desafios. Entre eles, destacam-se a infraestrutura tecnológica defasada, a falta de cultura de privacidade, a necessidade de capacitação contínua, a integração complexa entre sistemas, a ausência formal da Avaliação de Impacto à Proteção de Dados e fragilidades na gestão do ciclo de vida. Algumas medidas, como controle de acesso e plano de resposta a incidentes, já foram adotadas, mas ainda demandam aprimoramento. A pesquisa, de natureza qualitativa e exploratória, adota o estudo de caso da DPE-MT, com base em revisão bibliográfica e análise documental de políticas internas e registros. Ao final, conclui-se que a DPE-MT avançou significativamente na conformidade com a LGPD, mas ainda enfrenta obstáculos operacionais e estruturais. A conformidade é um processo contínuo, que representa não apenas obediência à lei, mas um compromisso ético com a dignidade da pessoa humana e a confiança social.

Palavras-chave: LGPD, Proteção de Dados, Defensoria Pública, Setor Público.

CASTANÕN, Cauã Focchesatto. Analysis of the processing of personal data in the Public Defender's Office of the State of Mato Grosso (DPE-MT), with a focus on compliance with the general data protection law (LGPD). 2025. 52 sheets. Final Paper – Fasipe College Cuiabá.

ABSTRACT

The present Course Completion Paper, entitled "Analysis of the Processing of Personal Data by the Public Defender's Office of the State of Mato Grosso (DPE-MT), with a Focus on Compliance with the General Data Protection Law (LGPD)", addresses the growing importance of personal data protection in the face of increasing internet use and the massive collection of information. In this context, the need for security and responsibility in data processing is highlighted, especially in the public sector. The Public Defender's Office of the State of Mato Grosso, which deals directly with sensitive data from people in vulnerable situations, is the focus of this analysis. The LGPD establishes guidelines to ensure the confidentiality and protection of personal information, with compliance being not only a legal duty but also an ethical requirement, essential for strengthening public trust and ensuring access to justice. This study aims to discuss how DPE-MT has adapted to the LGPD, identifying the main challenges faced and proposing practical solutions. The relevance of the topic lies in the need to promote the responsible handling of data from citizens who depend on the institution's services, aligning it with the principles of social justice and citizenship. The theoretical framework explores the evolution of the right to privacy and the core concepts of the LGPD, such as personal and sensitive data, data processing, data processing agents (controller, operator, and data protection officer), principles, legal bases, data subjects' rights, and administrative sanctions. It also examines data protection in the public sector and the role of the National Data Protection Authority (ANPD). DPE-MT handles a large volume of personal data on a daily basis, especially through systems such as Solar, PJe, and SEEU. To achieve compliance, the institution has implemented measures such as the Personal Data Protection Plan, the appointment of a Data Protection Officer (DPO), the Privacy and Data Protection Policy, the strengthening of its Internal Control System, and the creation of channels for the exercise of data subjects' rights. Additionally, it mapped the types of data processed and their life cycles, as well as the legal grounds for sharing data with other public bodies. Despite these advances, DPE-MT still faces challenges. These include outdated technological infrastructure, a lack of a privacy-focused culture, the need for continuous staff training, complex system integration, the absence of a formal Data Protection Impact Assessment (DPIA), and weaknesses in data lifecycle management. Some measures, such as access control and incident response planning, have already been adopted but still require improvement. This is a qualitative and exploratory research, using the case study of DPE-MT, based on bibliographic review and documentary analysis of internal policies and records. In conclusion, the study finds that DPE-MT has made significant progress in complying with the LGPD but still faces operational and structural obstacles. Compliance should be seen as an ongoing process that represents not only legal adherence but also an ethical commitment to human dignity and public trust.

Keywords: LGPD, Data Protection, Public Defender's Office, Public Sector.

SUMÁRIO

1	INTRODUÇÃO.....	9
2	FUNDAMENTAÇÃO TEÓRICA	12
	2.1 Proteção de Dados Pessoais e Privacidade.....	13
	2.1.1 Dados Pessoais e Sensíveis.....	15
	2.1.2 Princípios da Proteção de Dados.....	16
	2.1.3 A Lei Geral de Proteção de Dados (LGPD)	17
	2.1.4 Controlador, Operador, Encarregado (DPO).....	19
	2.1.5 Base Legais para Tratamento de Dados Pessoais	21
	2.1.6 Direitos dos Titulares de Dados Pessoais	22
	2.1.7 Obrigações dos Agentes de Tratamento	23
	2.1.8 Sanções Administrativas da LGPD	25
	2.2 Proteção de Dados no Setor Público	26
	2.2.1 Aplicabilidade da LGPD aos Órgãos Públicos	26
	2.2.2 Desafios e Responsabilidades no Tratamento De Dados	26
	2.2.3 Transparência e Equilíbrio com o Acesso à Informação.....	27
	2.2.4 Promoção da Cultura de Proteção de Dados.....	27
	2.3 Desafios da Administração Pública na Implementação da LGPD.....	27
	2.4 Papel da Autoridade Nacional de Proteção de Dados (ANPD) no Setor Público ...	29
3	A DEFENSORIA PÚBLICA DO ESTADO DE MATO GROSSO (DPE-MT) E O	
	TRATAMENTO DE DADOS PESSOAIS	31
	3.1 Caracterização Institucional da DPE-MT	33
	3.2 Fluxo dos Atendimentos na Defensoria Pública do Estado de Mato Grosso (DPE-	
	MT)	34
	3.2.1 Modalidades de Atendimento	34
	3.2.2 Sistemas Utilizados no Fluxo de Atendimento e Processamento	34
	3.2.3 Etapas do Fluxo de Atendimento	35
	3.2.4 Benefícios do Modelo Multicanal.....	35
	3.3 Mapeamento dos Dados na DPE-MT.....	36
	3.4 Ciclo de Vida dos Dados na Defensoria Pública do Estado de Mato Grosso (DPE-	
	MT)	37
	3.5 Bases Legais na Atuação da Defensoria Pública do Estado de Mato Grosso (DPE-	
	MT)	39
	3.6 Riscos, Vulnerabilidades e Desafios no Tratamento de Dados na DPE-MT	40
	3.7 Desafios Operacionais e Tecnológicos na DPE-MT.....	41
	3.7.1 Sistemas Integrados (Solar, PJE, SEEU).....	42
	3.7.2 Segurança da Informação	42
	3.7.3 Cultura Organizacional.....	43
	3.8 Análise Conformidade da DPE-MT com a LGPD: Avanços, Desafios e	
	Perspectivas.	43
4	CONSIDERAÇÕES FINAIS	47

REFERÊNCIAS.....	49
-------------------------	-----------

1 INTRODUÇÃO

Nos últimos anos, houve um aumento significativo na população de usuários da Internet e as informações de alguma forma foram abundantes e facilmente acessíveis, o que pode estar relacionado à conveniência que a Internet traz. O cenário aqui é que, com a tecnologia aprimorada, mais dados são coletados e compartilhados entre interações entre humanos e dispositivos, aumentando assim o volume de dados armazenados e processados, levantando dúvidas sobre a segurança dos dados. O impacto da Internet dependeu muito das atividades diárias das pessoas.

Escândalos recentes sobre vazamentos de dados de empresas como Facebook, Netshoes e Uber expuseram dados pessoais, incluindo nomes, endereços, números de cartão de crédito, entre outros, e realmente destacaram o quão frouxa é a segurança relacionada ao processamento de dados pessoais. Há uma grande necessidade de mecanismos de trabalho adequados para evitar que ocorram vazamentos, mantendo a segurança da confidencialidade das informações.

Agora mais do que nunca, o setor público tornou-se uma preocupação básica de proteção de dados pessoais, ainda mais para agências que recebem e salva e guardam informações sensíveis de grupos vulneráveis na sociedade, como a Defensoria Pública do Estado de Mato Grosso (DPE-MT). A proteção adequada das informações entregues pela Lei Geral de Proteção de Dados Pessoais (LGPD) lei n.º 13.709/2018 determina processos que garantem que as informações sejam devidamente protegidas em sigilo e em observância aos direitos do indivíduo a quem as informações pertencem. A conformidade com as diretrizes da LGPD torna não apenas uma obrigação legal, mas um requisito fundamental para o processamento de dados de forma ética e eficiente para que nenhum dano seja causado àqueles que estão sendo assistidos e para construir confiança no funcionamento da instituição.

O fluxo de informações institucionais aumenta a complexidade do gerenciamento de dados, incluindo todos os tipos de informações coletadas e processadas diariamente em todo

a instituição, a Defensoria Pública do Estado de Mato Grosso contem, Histórico de saúde, relatórios de violência doméstica, informações socioeconômicas são exemplos de alguns dados pessoais extremamente sensíveis tratados em serviços e processos legais. A investigação de dados pode expor os assistidos a riscos extremamente severos, ou seja, violação de sua privacidade, discriminação e estigmatização. A direção de informações contidas compromete seriamente a missão da Defensoria Pública de promover a justiça e proteger aqueles que mais precisam, afetando assim a qualidade do direito: o acesso à justiça.

A pesquisa pretende discutir como o DPE-MT está cumprindo com as demandas da LGPD, delineando os principais desafios enfrentados e propondo soluções pragmáticas para qualquer instituição reduzindo riscos e aprimorando sua conformidade legal. O estudo cobrirá aspectos sobre proteção de dados, incluindo quais tipos de infraestrutura tecnológica são usados, quais tipos de rotinas e procedimentos internos são implementados e que tipo de nível de treinamento os funcionários têm em relação às suas tarefas relacionadas à segurança da informação.

A relevância do assunto é evidenciada pela crescente necessidade de garantir a segurança de dados em organizações, por exemplo, como a DPE-MT que atende contato direto com indivíduos ou indivíduos socialmente desfavorecidos. Que as informações fornecidas sejam tratadas de forma responsável é de extrema importância, não apenas como um ato de conformidade legislativa, mas principalmente no monitoramento das ações da Defensoria Pública em consonância com os princípios de justiça social e cidadania. O estudo, portanto, pretende contribuir para melhorar a governança de dados dentro da DPE-MT, abrindo caminhos para uma administração mais segura, transparente e eficaz, ao mesmo tempo em que cumpre com os padrões legais e definidos pela LGPD.

Diante do exposto, esta pesquisa adotará uma abordagem qualitativa e exploratória, com o objetivo de analisar o tratamento de dados pessoais na Defensoria Pública do Estado de Mato Grosso (DPE-MT), à luz da Lei Geral de Proteção de Dados (LGPD). O estudo seguirá a metodologia proposta por Bastos e Ferreira, contemplando uma revisão bibliográfica aprofundada sobre a LGPD, seus princípios, os direitos dos titulares de dados e as obrigações dos controladores, bem como o papel da Autoridade Nacional de Proteção de Dados (ANPD).

Serão também examinadas legislações correlatas, como o Marco Civil da Internet, além de estudos voltados à aplicação da LGPD em instituições públicas, com ênfase na proteção de dados sensíveis de pessoas em situação de vulnerabilidade. A metodologia incluirá um estudo de caso da DPE-MT, com a análise da conformidade de seus processos internos como a coleta, o armazenamento, o uso e o descarte de dados em relação às exigências

legais.

A pesquisa envolverá ainda a análise documental das políticas internas da instituição, visando verificar seu alinhamento com a LGPD, especialmente no que diz respeito à transparência e à manutenção de registros das atividades de tratamento. Ao final, pretende-se mapear as práticas adotadas, identificar eventuais falhas e propor medidas de aprimoramento, fortalecendo a segurança da informação e promovendo uma atuação institucional mais responsável e ética.

2 FUNDAMENTAÇÃO TEÓRICA

Compreender o tratamento de dados pessoais, especialmente em uma instituição pública como a Defensoria Pública do Estado de Mato Grosso (DPE-MT), exige uma base sólida nos conceitos e princípios da proteção de dados, bem como na legislação pertinente. A seção de Fundamentação Teórica abordará o arcabouço jurídico e conceitual que suporta a análise proposta neste trabalho.

Inicialmente, será explorada a evolução histórica do direito à privacidade e à proteção de dados pessoais, desde sua origem até os marcos legais modernos que culminaram na Lei Geral de Proteção de Dados (LGPD) no Brasil, destacando a influência de movimentos internacionais e a consagração da proteção de dados como direito fundamental na Constituição Federa.

Em seguida, serão detalhados os principais conceitos trazidos pela LGPD, como a distinção entre dados pessoais e dados pessoais sensíveis, o que configura o tratamento de dados, e as figuras dos agentes de tratamento, incluindo o Controlador, o Operador e o Encarregado de Dados (DPO). A legislação estabelece princípios que devem nortear todo o tratamento de dados, como finalidade, adequação, necessidade, transparência, segurança, prevenção, não discriminação e responsabilização.

Serão também abordadas as bases legais que legitimam o tratamento de dados pessoais, conforme previsto na LGPD, que vão desde o consentimento do titular até o cumprimento de obrigações legais, a execução de políticas públicas e o legítimo interesse. Paralelamente, serão apresentados os direitos dos titulares de dados, que conferem aos indivíduos controle sobre suas informações, como o direito de confirmação da existência do tratamento, acesso, correção, anonimização, bloqueio ou eliminação, portabilidade, informação sobre compartilhamento e revogação do consentimento.

A Fundamentação Teórica também contemplará as obrigações dos agentes de tratamento, que incluem a adoção de medidas de segurança, garantia da transparência, respeito

aos direitos dos titulares e comunicação de incidentes de segurança. As sanções administrativas previstas na LGPD para o descumprimento das normas serão igualmente detalhadas.

Um foco específico será dado à proteção de dados no setor público, analisando a aplicabilidade da LGPD aos órgãos governamentais e os desafios inerentes a esse contexto, como a complexidade institucional, a necessidade de capacitação e cultura organizacional, a adequação tecnológica e a conciliação entre transparência e proteção de dados. O papel da Autoridade Nacional de Proteção de Dados (ANPD) na fiscalização e orientação do setor público será igualmente examinado.

Este embasamento teórico é essencial para situar a análise do tratamento de dados na Defensoria Pública do Estado de Mato Grosso (DPE-MT) dentro do contexto legal e técnico da proteção de dados, permitindo uma avaliação aprofundada de sua conformidade com a LGPD.

2.1 Proteção de Dados Pessoais e Privacidade

O direito à privacidade, tal como se compreende na atualidade, é fruto de um processo evolutivo que acompanha as transformações sociais, tecnológicas e jurídicas da humanidade. Inicialmente, nas sociedades antigas, como na Grécia e em Roma, não havia um reconhecimento formal da privacidade como direito. Existiam distinções entre os âmbitos público e privado, sobretudo na proteção do lar e da vida doméstica, mas essa proteção ocorria de forma consuetudinária, sem respaldo legal expresso.

O marco inicial do reconhecimento jurídico do direito à privacidade no mundo ocorre no ano de 1890, com a publicação do artigo “The Right to Privacy”, de Samuel D. Warren e Louis D. Brandeis, na Harvard Law Review. Neste trabalho, os autores defendem o direito de estar só (“the right to be let alone”), como uma necessidade decorrente das crescentes invasões promovidas, especialmente, pela imprensa sensacionalista da época. Este artigo é considerado pela doutrina como o nascimento do direito à privacidade na modernidade.

A consolidação internacional do direito à privacidade ocorre no período pós-Segunda Guerra Mundial, com a elaboração de documentos internacionais que buscam garantir a dignidade da pessoa humana. A Declaração Universal dos Direitos Humanos de 1948, em seu artigo 12, estabelece que "ninguém será sujeito a interferências arbitrárias em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem a ataques à sua honra e reputação". De igual forma, o Pacto Internacional dos Direitos Civis e Políticos de 1966, em seu artigo 17, reforça a proteção da vida privada e impõe aos Estados a obrigação de fornecer instrumentos jurídicos eficazes para a sua defesa.

Nas décadas de 1970 e 1980, com a evolução dos sistemas informatizados e a criação de bancos de dados, surgem novas preocupações relativas à proteção da privacidade no âmbito digital. Dessa forma, surgem as primeiras legislações específicas sobre proteção de dados pessoais, sendo pioneira a Alemanha, com uma lei aprovada no estado de Hessen, em 1970, seguida pela França, com a edição da Lei nº 78-17, de 1978, conhecida como “Loi Informatique et Libertés”.

No século XXI, a expansão das tecnologias digitais, o uso massivo da internet, das redes sociais, da economia dos dados e das tecnologias de inteligência artificial intensificam os desafios à proteção da privacidade. Nesse cenário, destaca-se a adoção do Regulamento Geral de Proteção de Dados (GDPR) pela União Europeia, em 2016, com entrada em vigor em 2018, que se tornou o principal marco internacional de referência na proteção de dados e na tutela da privacidade na era digital⁵.

No contexto brasileiro, a proteção da privacidade seguiu inicialmente uma lógica dispersa. O Código Civil de 1916 não previa, de forma expressa, o direito à privacidade, mas protegia aspectos relacionados, como a honra e a imagem. O grande marco jurídico ocorre com a promulgação da Constituição Federal de 1988, que consolida a proteção da privacidade como direito fundamental, nos seguintes termos:

Art. 5º, X – São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação.

Art. 5º, XII – Assegura a inviolabilidade do sigilo da correspondência, das comunicações telegráficas, de dados e das comunicações telefônicas, salvo por ordem judicial, nas hipóteses e na forma que a lei estabelecer.

Após a Constituição de 1988, diversas legislações específicas foram editadas, reforçando a proteção à privacidade e aos dados pessoais no Brasil. Entre elas, destacam-se:

- Lei nº 9.507/1997 (Lei do Habeas Data) – Que assegura ao cidadão o direito de acessar e corrigir informações pessoais mantidas em bancos de dados públicos ou privados.
- Lei nº 8.078/1990 (Código de Defesa do Consumidor) – Que garante aos consumidores a proteção de seus dados pessoais.
- Lei nº 12.965/2014 (Marco Civil da Internet) – Que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil, com ênfase na proteção da privacidade e dos dados pessoais.

O ápice desse processo evolutivo se dá com a edição da Lei nº 13.709/2018 (Lei Geral

de Proteção de Dados – LGPD), que estabelece normas sobre o tratamento de dados pessoais, tanto por pessoas naturais quanto jurídicas, de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade. A LGPD define princípios, direitos dos titulares de dados e deveres para os agentes de tratamento, além de criar a Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável pela fiscalização, orientação e aplicação de sanções.

Por fim, o Brasil dá um passo definitivo no reconhecimento da proteção de dados pessoais como direito fundamental ao promulgar, em 2022, a Emenda Constitucional nº 115, que inclui no texto do artigo 5º da Constituição Federal a seguinte redação: "é assegurada, nos termos da lei, a proteção de dados pessoais, inclusive nos meios digitais", o que evidencia a centralidade desse direito no ordenamento jurídico brasileiro contemporâneo.

Assim, percebe-se que a evolução histórica do direito à privacidade acompanha diretamente os avanços tecnológicos e sociais, refletindo a constante necessidade de proteção da dignidade da pessoa humana, especialmente no contexto da sociedade da informação e da economia digital.

2.1.1 Dados Pessoais e Sensíveis

A Lei Geral de Proteção de Dados Pessoais (LGPD), instituída pela Lei nº 13.709/2018, estabelece diretrizes e princípios para o tratamento de dados pessoais no Brasil, tanto no meio físico quanto no digital. Seu objetivo central é a proteção dos direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Segundo o artigo 5º, inciso I, da LGPD, dados pessoais são definidos como "informação relacionada a pessoa natural identificada ou identificável" (BRASIL, 2018). Isso significa que qualquer dado que permita, de forma direta ou indireta, identificar alguém é considerado dado pessoal. Esses dados podem ser classificados como diretamente identificáveis, quando isoladamente identificam o titular, ou indiretamente identificáveis, quando sua combinação com outras informações permite essa identificação.

Entre os principais exemplos de dados pessoais estão: nome completo, CPF, RG, data de nascimento, endereço residencial, telefone, e-mail, placa de veículo, dados bancários, geolocalização via GPS e o endereço de IP de dispositivos conectados à internet.

Por sua vez, os dados pessoais sensíveis correspondem a uma categoria especial de dados que demandam maior proteção, uma vez que dizem respeito a informações que podem gerar discriminação, constrangimento ou violação de direitos fundamentais, caso sejam tratados

de maneira inadequada. O artigo 5º, inciso II, da LGPD, conceitua dados sensíveis como aqueles relacionados à "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (BRASIL, 2018).

São exemplos de dados sensíveis: religião informada em cadastros, informações sobre saúde como prontuários médicos e laudos, dados sobre deficiências, dados biométricos (impressões digitais, reconhecimento facial, íris ocular), informações sobre orientação sexual, bem como filiação a partidos políticos ou sindicatos.

A distinção entre dados pessoais e dados sensíveis está no grau de proteção exigido e no potencial risco à privacidade do titular. Enquanto os dados pessoais identificam uma pessoa, os dados sensíveis revelam características íntimas que, se expostas ou utilizadas de forma indevida, podem gerar discriminação e constrangimento. Por essa razão, a LGPD impõe requisitos mais rigorosos para o tratamento de dados sensíveis, exigindo bases legais específicas e medidas técnicas e administrativas reforçadas por parte dos agentes de tratamento.

Compreender essa diferenciação é essencial para a efetiva aplicação da LGPD, garantindo, assim, a preservação dos direitos fundamentais dos titulares e a conformidade das organizações com a legislação vigente.

2.1.2 Princípios da Proteção de Dados

A Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, estabelece, em seu artigo 6º, os princípios que regem o tratamento de dados pessoais no Brasil. Esses princípios são fundamentais para assegurar que o tratamento de dados ocorra de forma ética, transparente e segura, respeitando os direitos fundamentais dos titulares, como a privacidade, a dignidade e a liberdade.

São ao todo dez princípios que devem ser observados por todos os agentes de tratamento, sejam eles públicos ou privados, sempre que realizarem atividades envolvendo dados pessoais. Cada princípio orienta e limita a atuação das organizações, assegurando que o uso dos dados seja feito de forma responsável.

Os principais princípios previstos na LGPD são:

- Finalidade: O tratamento de dados deve ocorrer para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

- Adequação: Os dados coletados devem ser compatíveis com as finalidades informadas ao titular, ou seja, é necessário que haja uma coerência entre o objetivo declarado e os dados efetivamente tratados.
- Necessidade: Estabelece que o tratamento deve se limitar ao mínimo necessário para a realização de suas finalidades, abrangendo dados pertinentes, proporcionais e não excessivos.
- Livre Acesso: Garante aos titulares dos dados a consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como a integralidade de seus dados pessoais.
- Qualidade dos Dados: Assegura que os dados pessoais estejam exatos, claros, relevantes e atualizados, de acordo com a necessidade e para o cumprimento da finalidade do tratamento.
- Transparência: Os titulares devem ser informados, de maneira clara, precisa e facilmente acessível, sobre os agentes de tratamento e sobre os dados que estão sendo tratados, bem como suas respectivas finalidades.
- Segurança: Determina a adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados, bem como de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.
- Prevenção: Exige a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais, atuando de forma proativa na mitigação de riscos.
- Não Discriminação: Impede o tratamento de dados para fins discriminatórios, ilícitos ou abusivos, protegendo, assim, a dignidade e os direitos dos titulares.
- Responsabilização e Prestação de Contas: O agente de tratamento deve demonstrar a adoção de medidas eficazes e capazes de comprovar o cumprimento da LGPD, bem como a eficácia dessas medidas.

Esses princípios atuam como diretrizes fundamentais para que as atividades de coleta, armazenamento, uso e compartilhamento de dados sejam realizadas de forma ética, responsável e em conformidade com a lei. A observância a esses princípios é essencial não apenas para proteger os titulares dos dados, mas também para fortalecer a confiança nas relações entre pessoas, empresas e instituições.

2.1.3 A Lei Geral de Proteção de Dados (LGPD)

A promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, no Brasil, foi impulsionada por diversos fatores, tanto no cenário nacional quanto internacional. A crescente digitalização das relações sociais, comerciais e institucionais, bem como o aumento do volume de dados pessoais circulando na internet e em ambientes físicos, expôs a necessidade urgente de uma legislação capaz de proteger os direitos fundamentais dos cidadãos, especialmente no que se refere à privacidade e à proteção de dados.

Internacionalmente, a entrada em vigor do Regulamento Geral de Proteção de Dados da União Europeia (GDPR), em maio de 2018, serviu como forte influência para a formulação da LGPD no Brasil. A ausência de uma legislação específica no país dificultava relações comerciais internacionais, uma vez que organizações brasileiras poderiam ser vistas como inseguras para o tratamento de dados pessoais em comparação com países que já possuíam marcos regulatórios robustos.

No âmbito nacional, o aumento dos casos de vazamentos de dados, fraudes digitais e uso indevido de informações pessoais também impulsionou o debate sobre a necessidade de proteger os cidadãos frente aos riscos gerados pela economia digital. A LGPD, portanto, surge como uma resposta normativa para assegurar a proteção dos direitos fundamentais, especialmente os direitos à privacidade, à intimidade, à liberdade e ao livre desenvolvimento da personalidade.

Além de suas motivações, a LGPD estabelece alguns conceitos fundamentais que norteiam toda a sua aplicação, sendo eles indispensáveis para a correta compreensão da lei.

- **Dados Pessoais**

De acordo com o artigo 5º, inciso I, da LGPD, dados pessoais são definidos como “informação relacionada a pessoa natural identificada ou identificável” (BRASIL, 2018). Ou seja, são todas aquelas informações que podem, de forma direta ou indireta, identificar um indivíduo. Esse conceito engloba dados como nome, CPF, RG, e-mail, endereço, número de telefone, placa de veículo, IP, localização geográfica, entre outros.

- **Dados Pessoais Sensíveis**

Conforme o artigo 5º, inciso II, da LGPD, dados sensíveis são aqueles que dizem respeito a “origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural” (BRASIL, 2018).

Os dados sensíveis exigem maior rigor no tratamento, pois envolvem informações que podem gerar discriminação, constrangimento ou qualquer forma de violação de direitos, caso sejam tratados de forma indevida.

- Tratamento de Dados

O conceito de tratamento está previsto no artigo 5º, inciso X, da LGPD, sendo definido como “toda operação realizada com dados pessoais”, o que inclui, mas não se limita a, as atividades de coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle da informação, modificação, comunicação, transferência, difusão ou extração (BRASIL, 2018).

Isso significa que qualquer ação realizada com dados pessoais, desde sua coleta até seu descarte, está submetida às regras e princípios estabelecidos na LGPD.

Assim, os conceitos de dados pessoais, dados sensíveis e tratamento de dados são os pilares fundamentais para a compreensão da LGPD, uma vez que estruturam os direitos dos titulares, as obrigações dos agentes de tratamento e os limites legais para o uso de informações pessoais.

2.1.4 Controlador, Operador, Encarregado (DPO)

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, além de definir princípios e conceitos relacionados ao tratamento de dados, também estabelece os papéis e as responsabilidades dos agentes que realizam esse tratamento. Três figuras são fundamentais na aplicação da LGPD: o Controlador, o Operador e o Encarregado, também conhecido como Data Protection Officer (DPO).

Cada um desses agentes possui funções específicas dentro do ciclo de vida dos dados pessoais, sendo imprescindível a correta identificação de suas atribuições para garantir a conformidade legal.

- Controlador

De acordo com o artigo 5º, inciso VI, da LGPD, o Controlador é definido como a “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais” (BRASIL, 2018).

Em outras palavras, é o agente responsável por determinar quais dados serão coletados, para quais finalidades serão utilizados e como serão tratados. O controlador assume o papel central na definição das diretrizes do tratamento dos dados, bem como na responsabilização legal pelos dados sob sua guarda.

Exemplos de controlador incluem empresas, órgãos públicos, entidades privadas, escolas, hospitais ou qualquer organização que defina como os dados de indivíduos serão

utilizados.

- Operador

Nos termos do artigo 5º, inciso VII, da LGPD, o Operador é a “pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador” (BRASIL, 2018).

O operador, portanto, executa atividades de tratamento dos dados seguindo as ordens e orientações do controlador, não tendo autonomia para decidir sobre as finalidades ou os meios desse tratamento.

Por exemplo, uma empresa de tecnologia contratada por uma instituição para armazenar dados em nuvem atua como operadora, pois apenas executa o processamento, armazenamento ou manipulação dos dados, conforme as determinações do controlador.

- Encarregado (DPO – Data Protection Officer)

O Encarregado, conhecido internacionalmente como Data Protection Officer (DPO), é definido no artigo 5º, inciso VIII, da LGPD como a “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)” (BRASIL, 2018).

O encarregado tem funções essenciais no processo de governança de dados, sendo responsável por:

- Aceitar reclamações e comunicações dos titulares dos dados;
- Prestar esclarecimentos e adotar providências;
- Receber comunicações da Autoridade Nacional de Proteção de Dados (ANPD) e repassar aos responsáveis internos;
- Orientar os funcionários e os contratados da entidade sobre as práticas de proteção de dados;
- Executar outras atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

O encarregado atua como uma ponte entre os titulares dos dados, o controlador e a ANPD, sendo um elemento central para assegurar a transparência e a conformidade no tratamento de dados pessoais.

A definição clara dos papéis de controlador, operador e encarregado (DPO) é essencial para a responsabilização no tratamento de dados e para a aplicação efetiva das normas de proteção previstas na LGPD.

2.1.5 Base Legais para Tratamento de Dados Pessoais

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, estabelece que toda atividade de tratamento de dados pessoais deve estar fundamentada em uma base legal. As bases legais funcionam como os fundamentos jurídicos que autorizam o tratamento de dados, garantindo que ele seja legítimo, transparente e em conformidade com os direitos dos titulares.

O artigo 7º da LGPD prevê dez bases legais que autorizam o tratamento de dados pessoais, e o artigo 11 trata especificamente das bases legais para o tratamento de dados sensíveis, que demandam critérios ainda mais rigorosos.

As principais bases legais são:

- Consentimento

Ocorre quando o titular dos dados autoriza, de forma livre, informada e inequívoca, que seus dados sejam tratados para uma finalidade específica. O consentimento deve ser claro, destacável e pode ser revogado a qualquer momento pelo titular.

- Cumprimento de obrigação legal ou regulatória

Permite o tratamento de dados quando este for necessário para o cumprimento de uma obrigação imposta pela legislação ao controlador, como na guarda de documentos fiscais, exigida pela Receita Federal.

- Execução de políticas públicas

O tratamento é permitido quando necessário para a execução de políticas públicas previstas em leis, regulamentos ou contratos, principalmente por parte de órgãos públicos.

- Realização de estudos por órgãos de pesquisa

Autoriza o uso de dados para pesquisas, desde que garantida, sempre que possível, a anonimização dos dados pessoais.

- Execução de contrato ou de procedimentos preliminares relacionados

Permite o tratamento de dados necessário para a celebração, execução e gestão de contratos dos quais o titular seja parte, como contratos de prestação de serviços, de trabalho, de compra e venda, entre outros.

- Exercício regular de direitos em processo judicial, administrativo ou arbitral

Garante que dados possam ser tratados quando necessários para assegurar direitos em processos judiciais, administrativos ou arbitrais.

- Proteção da vida ou da incolumidade física do titular ou de terceiro

Permite o tratamento de dados para situações de emergência, como atendimentos

médicos, acidentes ou qualquer situação que envolva risco à vida ou à integridade física.

- Tutela da saúde

Autoriza o tratamento de dados, especialmente dados sensíveis, quando necessário para procedimentos realizados por profissionais da saúde, serviços de saúde ou autoridades sanitárias.

- Legítimo interesse

Ocorre quando o tratamento é necessário para atender interesses legítimos do controlador ou de terceiros, desde que não prejudiquem os direitos e liberdades fundamentais do titular. Essa base exige uma análise criteriosa, com avaliação de riscos e garantia de transparência.

- Proteção do crédito

Permite o tratamento de dados necessário para procedimentos de proteção ao crédito, como análise de score, cadastro em birôs de crédito, entre outros.

Essas bases legais visam assegurar que o tratamento de dados ocorra dentro dos limites legais, protegendo os direitos dos titulares e evitando abusos. É dever do controlador identificar, justificar e documentar a base legal que fundamenta cada operação de tratamento, promovendo, assim, uma cultura de responsabilidade, transparência e proteção de dados.

2.1.6 Direitos dos Titulares de Dados Pessoais

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, assegura aos titulares de dados uma série de direitos que visam garantir maior controle, transparência e segurança sobre o uso de suas informações pessoais. Esses direitos são fundamentais para a proteção da privacidade e para a promoção da autonomia do indivíduo no ambiente digital e fora dele.

Os principais direitos dos titulares previstos na LGPD, especialmente no artigo 18, são:

- Confirmação da existência do tratamento

O titular tem o direito de obter a confirmação sobre a existência ou não do tratamento de seus dados pessoais por parte do controlador.

- Acesso aos dados

O titular pode solicitar acesso aos seus dados pessoais que estejam sendo tratados, incluindo informações sobre as finalidades do tratamento, categorias de dados, compartilhamentos e o período de armazenamento.

- Correção de dados incompletos, inexatos ou desatualizados

O titular pode requerer a correção imediata de seus dados pessoais quando estes estiverem incorretos, incompletos ou desatualizados.

- Anonimização, bloqueio ou eliminação

Tem o direito de solicitar a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD.

- Portabilidade dos dados

O titular pode requerer a portabilidade de seus dados pessoais a outro fornecedor de serviço ou produto, mediante requisição expressa, em formato estruturado, interoperável e de fácil acesso.

- Eliminação dos dados tratados com consentimento

Pode solicitar a eliminação dos dados pessoais tratados com base no consentimento, exceto nas hipóteses de guarda legal, cumprimento de obrigação legal ou exercício regular de direitos.

- Informação sobre compartilhamento

O titular tem direito a ser informado sobre as entidades públicas e privadas com as quais seus dados foram compartilhados.

- Informação sobre a possibilidade de não fornecer consentimento e consequências

O titular deve ser informado sobre a possibilidade de não fornecer consentimento para o tratamento dos dados e as consequências da negativa.

- Revogação do consentimento

O titular pode revogar o consentimento previamente concedido, mediante manifestação expressa, conforme previsto na legislação.

- Reclamação junto à Autoridade Nacional de Proteção de Dados (ANPD)

Caso considere que seus direitos foram violados, o titular pode apresentar reclamação à ANPD para que sejam adotadas as providências cabíveis.

Esses direitos fortalecem a posição do titular, garantindo-lhe maior autonomia e controle sobre suas informações pessoais, além de exigir das organizações a adoção de práticas transparentes e responsáveis no tratamento dos dados.

2.1.7 Obrigações dos Agentes de Tratamento

Na estrutura da Lei Geral de Proteção de Dados Pessoais (LGPD), os agentes de

tratamento Controlador e Operador têm responsabilidades específicas para garantir a proteção dos dados pessoais e o cumprimento da legislação. O artigo 37 da LGPD estabelece as obrigações fundamentais desses agentes para assegurar a conformidade legal e a proteção dos direitos dos titulares.

- Adotar medidas de segurança, técnicas e administrativas

Os agentes de tratamento devem implementar medidas eficazes para proteger os dados pessoais contra acessos não autorizados, vazamentos, perdas, alterações ou qualquer forma de tratamento inadequado ou ilícito.

- Garantir a transparência

Devem informar aos titulares, de forma clara e acessível, sobre o tratamento realizado, incluindo finalidade, forma e duração do tratamento, bem como os direitos dos titulares.

- Respeitar os direitos dos titulares

É obrigação dos agentes assegurar que os direitos previstos na LGPD sejam respeitados, facilitando o exercício desses direitos, como acesso, correção, eliminação e portabilidade dos dados.

- Comunicar incidentes de segurança

Em caso de vazamento, acesso não autorizado ou qualquer incidente que possa comprometer os dados pessoais, os agentes devem comunicar a Autoridade Nacional de Proteção de Dados (ANPD) e os titulares afetados, conforme os prazos e procedimentos previstos na legislação.

- Manter registros das operações de tratamento

Os agentes devem manter registro das operações de tratamento realizadas, especialmente aquelas que possam representar riscos aos direitos dos titulares, para fins de auditoria e fiscalização.

- Observar os princípios da LGPD

Devem observar e aplicar os princípios da proteção de dados, como finalidade, adequação, necessidade, transparência, segurança, prevenção e responsabilização.

- Nomear o encarregado (DPO)

O controlador deve indicar um encarregado, ou Data Protection Officer (DPO), responsável por atuar como canal de comunicação entre o controlador, os titulares e a ANPD, zelando pela conformidade da entidade com a LGPD.

- Atender às determinações da ANPD

Os agentes devem colaborar com a Autoridade Nacional de Proteção de Dados em

processos de fiscalização, investigação e auditoria.

- Realizar avaliações de impacto

Sempre que aplicável, os agentes devem realizar avaliações de impacto à proteção de dados pessoais para identificar e mitigar riscos relacionados ao tratamento.

O cumprimento dessas obrigações é essencial para a construção de uma cultura organizacional de privacidade e proteção de dados, prevenindo riscos jurídicos e promovendo a confiança dos titulares e do mercado.

2.1.8 Sanções Administrativas da LGPD

A Lei Geral de Proteção de Dados Pessoais (LGPD) estabelece um conjunto de sanções administrativas para os agentes de tratamento que descumprirem suas disposições, com o objetivo de garantir o respeito à privacidade e à proteção dos dados pessoais. Essas sanções são aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD) e buscam promover a conformidade e a responsabilidade no tratamento de dados.

As principais sanções administrativas previstas no artigo 52 da LGPD são:

- Advertência

Advertência formal à empresa ou pessoa responsável, com indicação de prazo para adoção de medidas corretivas.

- Multa simples

Multa de até 2% do faturamento da pessoa jurídica, grupo ou conglomerado no Brasil no seu último exercício, limitada a R\$ 50 milhões por infração.

- Multa diária

Multa aplicada por dia de descumprimento da norma, respeitando o limite máximo estabelecido.

- Publicização da infração

Divulgação pública da infração após decisão final, para fins de transparência e prevenção.

- Bloqueio dos dados pessoais

Bloqueio dos dados pessoais relacionados à infração, impedindo seu tratamento até a regularização.

- Eliminação dos dados pessoais

Eliminação dos dados pessoais relacionados à infração, quando aplicável.

- Suspensão parcial do funcionamento do banco de dados

Suspensão temporária do tratamento de dados pessoais.

- Proibição parcial ou total do exercício de atividades relacionadas ao tratamento de dados

Restrição temporária ou definitiva das atividades do agente de tratamento relacionadas a dados pessoais.

Importância das sanções

As sanções administrativas possuem caráter educativo, punitivo e preventivo, incentivando as organizações a adotarem práticas responsáveis de proteção de dados. A aplicação das sanções considera a gravidade da infração, os danos causados, a boa-fé do agente, os esforços para mitigar o dano, entre outros aspectos.

Além das sanções administrativas, o descumprimento da LGPD pode acarretar responsabilidade civil e penal, reforçando a importância da conformidade com a lei.

2.2 Proteção de Dados no Setor Público

A aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) no setor público apresenta desafios singulares devido à complexidade das atividades governamentais e ao volume expressivo de dados pessoais tratados. Conforme destacam Tesser et al. (2021), o setor público deve observar os princípios da LGPD, ainda que algumas especificidades se façam necessárias diante da missão institucional dos órgãos públicos.

2.2.1 Aplicabilidade da LGPD aos Órgãos Públicos

Segundo Tesser et al. (2021, p. 45), “a LGPD abrange o tratamento de dados pessoais realizado por órgãos e entidades da administração pública direta e indireta, englobando todas as esferas federativas”. Isso implica que as informações pessoais tratadas no exercício da função pública estão submetidas às regras de proteção previstas na legislação, ressalvadas as hipóteses previstas em lei que autorizem tratamentos específicos.

Além disso, o livro enfatiza que a base legal mais utilizada no setor público é o “cumprimento de obrigação legal ou regulatória pelo controlador” (TESSER et al., 2021, p. 112), refletindo o caráter mandatário das atividades governamentais.

2.2.2 Desafios e Responsabilidades no Tratamento De Dados

Os autores apontam que a segurança dos dados e a transparência são aspectos centrais para o setor público. Como afirmam, “a proteção dos dados pessoais na administração pública exige a implementação de medidas técnicas e administrativas rigorosas, visando evitar vazamentos e assegurar os direitos dos titulares” (TESSER et al., 2021, p. 233).

Outro ponto relevante é a obrigatoriedade de nomeação do encarregado de dados (DPO), que funciona como elo entre os órgãos públicos, os titulares e a Autoridade Nacional de Proteção de Dados (ANPD), fortalecendo a governança e o controle do tratamento (TESSER et al., 2021, p. 180).

2.2.3 Transparência e Equilíbrio com o Acesso à Informação

Tesser e colaboradores (2021, p. 305) ressaltam que “a LGPD deve ser aplicada de forma harmônica com a Lei de Acesso à Informação (LAI), assegurando a transparência pública sem comprometer a privacidade dos cidadãos”. A adequada conciliação desses direitos é fundamental para garantir a accountability da administração pública e o respeito à privacidade.

2.2.4 Promoção da Cultura de Proteção de Dados

Por fim, o livro destaca que “a efetiva implementação da LGPD no setor público depende da construção de uma cultura organizacional que valorize a privacidade, com capacitação contínua de servidores e adoção de políticas internas robustas” (TESSER et al., 2021, p. 412). Essa cultura é essencial para garantir a confiança da sociedade e a proteção dos direitos fundamentais.

2.3 Desafios da Administração Pública na Implementação da LGPD

A implementação da Lei Geral de Proteção de Dados Pessoais (LGPD) na Administração Pública enfrenta desafios complexos e multifacetados, decorrentes das especificidades do setor, do volume e diversidade de dados tratados e da necessidade de conciliar proteção à privacidade com a transparência e eficiência administrativas. São elas:

- Complexidade institucional e estrutura organizacional

Conforme destacam Tesser et al. (2021, p. 356), a administração pública brasileira é composta por múltiplos órgãos e entidades distribuídos nas esferas federal, estadual e municipal, o que torna a uniformização das práticas de proteção de dados um desafio considerável. A ausência de estruturas consolidadas de governança de dados em muitos órgãos dificulta a implementação coordenada das normas da LGPD.

- Capacitação e cultura organizacional

Os autores ressaltam que a construção de uma cultura de proteção de dados é um dos principais desafios. “A sensibilização e capacitação dos servidores públicos são fundamentais para que as normas de proteção de dados sejam compreendidas e efetivamente aplicadas no cotidiano do serviço público” (TESSER et al., 2021, p.368). Contudo, a rotatividade de pessoal e a falta de treinamentos adequados podem comprometer essa construção cultural.

- Adequação tecnológica

A infraestrutura tecnológica dos órgãos públicos nem sempre está preparada para suportar as exigências da LGPD. Nessa mesma linha, Tesser e colaboradores (2021, p. 372) defendem que “a modernização dos sistemas e a adoção de ferramentas de segurança da informação são essenciais para a proteção dos dados pessoais, mas frequentemente encontram limitações orçamentárias e burocráticas”.

- Conciliar transparência com proteção de dados

Outro desafio relevante é a conciliação entre os princípios da transparência pública, previstos na Lei de Acesso à Informação, e da proteção da privacidade.

“É necessário que a administração pública implemente procedimentos que permitam o acesso à informação sem comprometer os direitos dos titulares, o que demanda um esforço constante de adequação normativa e prática” (TESSER et al., 2021, p. 379).

- Cumprimento dos prazos e das obrigações legais

A complexidade do cumprimento das obrigações previstas na LGPD, tais como a realização de avaliações de impacto à proteção de dados e a nomeação do encarregado (DPO), apresenta desafios operacionais. Os autores destacam que “o atendimento aos prazos legais impõe a necessidade de planejamento estratégico e recursos dedicados, nem sempre disponíveis nos órgãos públicos” (TESSER et al., 2021, p. 382).

- Fiscalização e sanções

Por fim, a fiscalização pela Autoridade Nacional de Proteção de Dados (ANPD) e a possibilidade de sanções administrativas geram um ambiente de pressão para a adequação, exigindo dos órgãos públicos mecanismos eficazes de controle e monitoramento contínuo (TESSER et al., 2021, p. 385).

2.4 Papel da Autoridade Nacional de Proteção de Dados (ANPD) no Setor Público

A Autoridade Nacional de Proteção de Dados (ANPD) é o órgão responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD) em todo o território nacional, incluindo o setor público.

No contexto da administração pública, a ANPD tem um papel fundamental na orientação, supervisão e regulação das práticas relacionadas ao tratamento de dados pessoais por órgãos e entidades governamentais. Entre suas principais atribuições estão:

Fiscalização e aplicação de sanções: A ANPD monitora e investiga eventuais infrações à LGPD cometidas por agentes públicos, podendo aplicar sanções administrativas, que vão desde advertências até multas e outras penalidades previstas na legislação.

Elaboração de normas e diretrizes: A Autoridade é responsável por editar normas complementares, procedimentos e diretrizes específicas para a proteção de dados pessoais no setor público, adequando a aplicação da LGPD às peculiaridades da administração pública.

Orientação e capacitação: A ANPD oferece orientações técnicas e jurídicas para que os órgãos públicos compreendam e implementem corretamente as regras da LGPD, promovendo também a capacitação de servidores e a disseminação de boas práticas.

Atuação consultiva: Atua como órgão consultivo para a elaboração e revisão de políticas públicas relacionadas à proteção de dados, garantindo que as novas iniciativas governamentais estejam em conformidade com a LGPD.

Recepção e tratamento de reclamações: A ANPD recebe denúncias e reclamações de

titulares de dados quanto ao tratamento inadequado de suas informações pessoais por órgãos públicos, assegurando o direito à reparação.

Dessa forma, a ANPD desempenha um papel estratégico para garantir a proteção dos dados pessoais na esfera pública, promovendo a transparência, a segurança e o respeito aos direitos fundamentais dos cidadãos.

3 A DEFENSORIA PÚBLICA DO ESTADO DE MATO GROSSO (DPE-MT) E O TRATAMENTO DE DADOS PESSOAIS

A Defensoria Pública do Estado de Mato Grosso (DPE-MT) desempenha papel fundamental na garantia do acesso à justiça e na defesa dos direitos dos cidadãos, especialmente daqueles em situação de vulnerabilidade. Em suas atividades, a DPE-MT realiza o tratamento de grande volume de dados pessoais e sensíveis de assistidos, servidores e terceiros, o que demanda atenção rigorosa às normas da Lei Geral de Proteção de Dados Pessoais (LGPD).

- Responsabilidades no tratamento de dados

A DPE-MT, como órgão público, está sujeita às obrigações estabelecidas pela LGPD, devendo garantir que o tratamento dos dados pessoais seja realizado de forma lícita, transparente e segura. Isso inclui a observância das bases legais previstas para o tratamento, como o cumprimento de obrigação legal, a execução de políticas públicas e o exercício regular de direitos.

- Plano de Proteção de Dados Pessoais (PPDP)

A implementação de um Plano de Proteção de Dados Pessoais (PPDP) pela Defensoria Pública do Estado de Mato Grosso é fundamental para garantir o alinhamento da instituição com a LGPD, respondendo às demandas legais e sociais por maior proteção à privacidade e segurança dos dados dos cidadãos. Instituído pela Resolução nº 018/2022-DPG do DPE-MT, o PPDP estabelece diretrizes essenciais para a conformidade, definindo padrões claros para o tratamento de dados pessoais. Além disso, atua como um instrumento estratégico de governança de dados, assegurando que as atividades que envolvem informações pessoais sejam realizadas de maneira segura, transparente e responsável (DPE-MT, 2022).

A conformidade com a LGPD e a criação do PPDP têm implicações significativas para o ambiente institucional da DPE-MT. Primeiramente, o plano orienta o mapeamento dos dados pessoais tratados pela instituição e a definição de fluxos e atores, estabelecendo um panorama completo de como essas informações são manejadas. Isso permite identificar e mitigar riscos de forma proativa, promovendo a segurança dos dados e evitando vazamentos ou acessos não autorizados, que poderiam comprometer tanto os cidadãos quanto a integridade institucional (ANPD, 2020).

- Encarregado de Proteção de Dados (DPO)

A LGPD exige que todas as instituições que tratam dados pessoais nomeiem um Encarregado de Proteção de Dados Pessoais (Data Protection Officer - DPO) (BRASIL, 2018). No caso do PPDP da DPE-MT, o DPO é designado para supervisionar o cumprimento da legislação, funcionando como um elo entre a instituição, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). Este papel é crucial para garantir a comunicação efetiva entre todas as partes interessadas e para reforçar a responsabilidade da DPE-MT em proteger os dados pessoais com os quais lida diariamente (DPE-MT, 2022).

- Governança e cultura de proteção de dados

O PPDP alinha-se com as melhores práticas recomendadas pelo *Guia de Desenvolvimento do Programa de Governança de Privacidade* da ANPD, que sugere a criação de políticas explícitas de proteção de dados, a definição de responsabilidades internas e a realização de treinamentos periódicos. Essas práticas visam construir uma cultura de privacidade e segurança dentro da instituição, assegurando que todos os funcionários compreendam a importância da proteção de dados e estejam capacitados para lidar com informações sensíveis de maneira adequada e segura (ANPD, 2020).

- Importância do PPDP para a DPE-MT

Assim, o PPDP da DPE-MT não apenas garante a conformidade legal, mas também fortalece a confiança do público na capacidade da instituição de proteger os dados pessoais de forma eficiente. Com a crescente digitalização dos serviços públicos, planos como o PPDP são essenciais para atender às expectativas da sociedade por transparência e segurança, mitigando

os riscos de violação de dados e promovendo um ambiente institucional mais responsável e consciente dos direitos de privacidade.

3.1 Caracterização Institucional da DPE-MT

A Defensoria Pública do Estado de Mato Grosso (DPE-MT) é uma instituição essencial à função jurisdicional do Estado, com autonomia funcional, administrativa e iniciativa própria de sua proposta orçamentária, conforme disposto no artigo 134 da Constituição Federal e regulamentado no âmbito estadual pela Lei Complementar nº 146/2003.

Sua missão institucional é promover e assegurar, de forma integral e gratuita, a orientação jurídica e a defesa dos direitos individuais e coletivos das pessoas em situação de vulnerabilidade social e econômica. A DPE-MT atua como instrumento de efetivação dos direitos humanos, da cidadania e do acesso à justiça, especialmente daqueles que não possuem recursos para custear a contratação de advogados particulares.

A DPE-MT está presente em diversas comarcas do Estado de Mato Grosso, levando atendimento jurídico às populações mais carentes. Atua nas áreas cível, criminal, família, infância e juventude, saúde, consumidor, violência doméstica, execução penal, direitos coletivos e difusos, entre outras.

Além da atuação judicial, a instituição exerce funções extrajudiciais, como mediação, conciliação, educação em direitos e promoção de políticas públicas, fortalecendo sua função social e preventiva. Sua estrutura da DPE-MT é composta por: Defensor Público-Geral: responsável pela gestão superior da instituição; Subdefensores Públicos-Gerais: que auxiliam na administração; Corregedoria-Geral: órgão de controle interno e disciplina; Ouvidoria-Geral Externa: canal de comunicação com a sociedade; Conselho Superior: órgão deliberativo superior; Núcleos Especializados e Núcleos de Atendimento: responsáveis pela atuação especializada em determinadas matérias ou grupos vulneráveis.

Conta também com servidores efetivos, comissionados, estagiários e colaboradores que dão suporte às atividades desenvolvidas pelos defensores públicos.

A DPE-MT se orienta por princípios como: Acesso à justiça; Promoção da cidadania; Defesa dos direitos humanos; Efetivação dos direitos fundamentais; Atuação gratuita, integral e de qualidade e Independência funcional dos defensores públicos.

Entre os desafios enfrentados estão a necessidade de expansão da presença em todo o território estadual, a constante modernização dos serviços, a capacitação dos quadros internos e, especialmente, a adequação às novas exigências legais, como o cumprimento da

Lei Geral de Proteção de Dados Pessoais (LGPD), que exige a adoção de políticas de segurança, transparência e governança no tratamento de dados pessoais.

A atuação da DPE-MT é indispensável para a promoção da dignidade da pessoa humana, para a defesa dos interesses dos grupos vulneráveis e para a construção de uma sociedade mais justa, inclusiva e democrática no Estado de Mato Grosso.

3.2 Fluxo dos Atendimentos na Defensoria Pública do Estado de Mato Grosso (DPE-MT)

A DPE-MT adota uma abordagem multicanal para atender à população, oferecendo diversas formas de contato para facilitar o acesso aos seus serviços. Os atendimentos podem ser realizados de forma presencial, virtual, por telefone e através de sistemas eletrônicos específicos.

3.2.1 Modalidades de Atendimento

O atendimento presencial é realizado nas unidades físicas da Defensoria Pública em todo o Estado de Mato Grosso. Ele é destinado ao público que prefere ou necessita de contato direto, especialmente em situações que exigem a entrega de documentos físicos, assinaturas ou quando há necessidade de uma orientação mais detalhada. Além disso, a instituição também oferece atendimento virtual, por meio da plataforma de atendimento remoto acessível no site institucional da DPE-MT. Esse canal permite a realização de triagens, orientações jurídicas, acompanhamento de processos e o envio de documentos digitalizados.

O atendimento virtual também é facilitado através dos e-mails institucionais de cada unidade. Outra opção disponível é o atendimento telefônico, presente em todas as unidades, que funciona como um canal para orientações, agendamento de atendimentos, esclarecimento de dúvidas e realização da triagem inicial. Algumas unidades oferecem ainda o atendimento via WhatsApp, proporcionando mais agilidade na comunicação, especialmente para o envio de informações e documentos de forma rápida e prática.

3.2.2 Sistemas Utilizados no Fluxo de Atendimento e Processamento

A Defensoria Pública do Estado de Mato Grosso conta com diversos sistemas que auxiliam tanto na gestão interna quanto na atuação finalística. O Sistema Solar é uma ferramenta interna utilizada para o controle de atendimentos, movimentações processuais,

gestão de demandas e elaboração de estatísticas. Por meio dele, são registrados os dados dos assistidos, realizado o acompanhamento dos casos e gerenciado todo o fluxo institucional.

Outro sistema essencial é o Pje (Processo Judicial Eletrônico), utilizado no âmbito do Poder Judiciário, que permite aos defensores públicos peticionar, acompanhar e atuar nos processos de forma digital, tanto na 1ª quanto na 2ª instâncias.

No âmbito da execução penal, utiliza-se o SEEU (Sistema Eletrônico de Execução Unificado), um sistema de abrangência nacional que possibilita o acompanhamento e a gestão das execuções penais, facilitando o controle de penas, progressões e demais direitos dos reeducandos. Além desses, a instituição também faz uso de sistemas de apoio e comunicação, como os e-mails institucionais e plataformas de videoconferência a exemplo do Zoom, Google Meet ou similares, que são utilizados para audiências, reuniões e atendimentos remotos. Soma-se a isso o sistema interno de protocolo, responsável pela gestão documental e pelo controle dos processos administrativos.

3.2.3 Etapas do Fluxo de Atendimento

O atendimento na Defensoria Pública do Estado de Mato Grosso inicia-se com a triagem, que pode ser realizada de forma presencial, por telefone ou virtual. Nessa etapa, verifica-se se o cidadão se enquadra nos critérios de vulnerabilidade e se a sua demanda é de competência da instituição.

A depender da natureza e da complexidade do caso, o atendimento pode ocorrer de forma imediata ou ser agendado para uma análise mais detalhada. Na sequência, o cidadão é atendido por um defensor público, que realizará a análise da situação apresentada, prestará a devida orientação jurídica e, sempre que possível, buscará uma solução extrajudicial. Caso não seja possível resolver de forma conciliatória, poderá ser promovido o ajuizamento da demanda.

O acompanhamento processual é feito por meio dos sistemas Solar, Pje, SEEU e outras plataformas, que permitem o monitoramento do andamento do caso. Ao longo de todo o processo, o assistido é devidamente informado sobre os atos processuais, os desdobramentos da sua demanda e sobre eventuais providências que sejam necessárias.

3.2.4 Benefícios do Modelo Multicanal

A atuação da Defensoria Pública do Estado de Mato Grosso, por meio de seus diversos canais e sistemas, proporciona maior acessibilidade e inclusão, especialmente para pessoas que

vivem em regiões distantes ou de difícil acesso. Essa dinâmica contribui para a redução de deslocamentos e de custos para os assistidos, além de garantir mais agilidade tanto no atendimento quanto na tramitação dos processos.

Todo esse processo reflete a modernização institucional da Defensoria, que se mantém alinhada às diretrizes de transformação digital dos serviços públicos, buscando oferecer um atendimento mais eficiente, célere e acessível à população.

3.3 Mapeamento dos Dados na DPE-MT

O mapeamento de dados na Defensoria Pública do Estado de Mato Grosso (DPE-MT) constitui uma etapa fundamental no processo de adequação à Lei Geral de Proteção de Dados Pessoais (LGPD), sendo indispensável tanto para assegurar a conformidade legal quanto para garantir a proteção e a segurança das informações pessoais tratadas pela instituição. Essa atividade possibilita a identificação dos dados coletados, a forma como são utilizados, os locais onde estão armazenados e quem possui acesso a eles, promovendo, assim, maior transparência e controle dos riscos envolvidos.

Considerando a natureza de suas atribuições, a DPE-MT lida com dados de diversos titulares, tanto no âmbito de sua atuação jurídica quanto na gestão administrativa. Esses dados são tratados com a finalidade de viabilizar o cumprimento da missão institucional de prestar assistência jurídica integral e gratuita à população em situação de vulnerabilidade, além de atender às demandas internas relacionadas à gestão de pessoal, contratos e atividades administrativas.

O tratamento de dados pessoais na DPE-MT abrange diferentes categorias, incluindo dados dos assistidos, como informações cadastrais (nome, CPF, RG, endereço, telefone e e-mail), dados socioeconômicos (renda, ocupação, composição familiar e outros indicadores de vulnerabilidade) e dados sensíveis, quando estritamente necessários, como informações de saúde, condição de deficiência, origem racial ou étnica, orientação sexual, filiação a organizações e situação penal, além dos dados processuais constantes nos autos judiciais e administrativos e de documentos pessoais como RG, CPF, certidões, comprovantes de residência, laudos médicos e declarações.

Também são tratados dados de servidores, estagiários e colaboradores terceirizados, incluindo informações cadastrais e funcionais (nome, CPF, RG, endereço, telefone e e-mail), dados financeiros (informações bancárias para pagamento de salários, auxílios, benefícios e obrigações previdenciárias), dados administrativos (histórico funcional, registros de ponto,

licenças, afastamentos, termos de posse, avaliações de desempenho, entre outros) e dados sensíveis, especialmente informações relativas à saúde e dados de dependentes, sempre que necessários ao cumprimento de obrigações legais e trabalhistas.

Além disso, a instituição trata dados de terceiros, como advogados, peritos, fornecedores, conveniados e testemunhas, que incluem informações cadastrais (nome, CPF ou CNPJ, endereço, telefone e e-mail), dados profissionais (como número de inscrição na OAB, registros em conselhos profissionais e certificados), dados bancários para viabilizar pagamentos e informações constantes nos processos judiciais, administrativos e procedimentos internos.

O tratamento desses dados ocorre com finalidades legítimas e específicas, alinhadas diretamente às atribuições institucionais da Defensoria Pública. Entre as principais finalidades estão a prestação de assistência jurídica integral e gratuita, a execução de atividades administrativas e operacionais, a gestão de recursos humanos, contratos e convênios, a atuação em processos judiciais e extrajudiciais, o cumprimento de obrigações legais e regulatórias, bem como o acompanhamento de demandas, a elaboração de relatórios e o cumprimento de metas institucionais.

O mapeamento dos dados permite não apenas a compreensão dos fluxos informacionais e das bases legais aplicáveis, mas também a adoção de medidas técnicas e administrativas capazes de assegurar a segurança, a confidencialidade e a integridade das informações. Esse processo é fundamental para a identificação e mitigação de riscos associados ao tratamento de dados pessoais, contribuindo diretamente para o cumprimento dos princípios da LGPD, como finalidade, adequação, necessidade, segurança e prestação de contas. Além disso, promove maior transparência em relação aos titulares dos dados e aos órgãos de controle, reforçando o compromisso da DPE-MT com a privacidade, a proteção de dados e a governança da informação no âmbito institucional.

3.4 Ciclo de Vida dos Dados na Defensoria Pública do Estado de Mato Grosso (DPE-MT)

O ciclo de vida dos dados na Defensoria Pública do Estado de Mato Grosso (DPE-MT) abrange todas as etapas pelas quais os dados pessoais passam, desde a sua coleta até o seu descarte ou arquivamento. A gestão adequada desse ciclo é essencial para assegurar a proteção dos dados, a conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD) e a efetividade das atividades institucionais. Cada fase desse processo demanda a adoção de medidas específicas que garantam a privacidade, a segurança e o tratamento correto das informações, sempre em consonância com os princípios da transparência, necessidade,

finalidade e prevenção.

A coleta dos dados ocorre durante os atendimentos presenciais, por meio de formulários digitais, por telefone e também através dos sistemas internos e externos utilizados pela DPE-MT, como o SOLAR, o PJe e o SEEU. Nessa etapa, são reunidos dados cadastrais, processuais, socioeconômicos e, quando necessário, dados sensíveis, todos diretamente vinculados às finalidades institucionais, seja na prestação de assistência jurídica, seja na gestão administrativa.

Após a coleta, os dados são armazenados em formatos físico como documentos, dossiês e fichas ou digital, por meio de bancos de dados, sistemas internos e plataformas processuais. A Defensoria Pública adota rigorosas medidas de segurança para proteger essas informações contra acessos não autorizados, perdas, vazamentos ou qualquer outro tipo de incidente. Esse armazenamento ocorre apenas pelo tempo necessário ao cumprimento da finalidade para a qual os dados foram coletados, respeitando os prazos legais, regulamentares ou contratuais aplicáveis.

No exercício de sua função institucional, a DPE-MT também realiza o compartilhamento de dados pessoais com diversos órgãos públicos e entidades parceiras, sempre que isso se fizer necessário e devidamente justificado. Entre os principais destinatários desse compartilhamento estão o Poder Judiciário do Estado de Mato Grosso (TJMT), o Ministério Público do Estado de Mato Grosso (MPE), as Delegacias de Polícia e demais órgãos de segurança pública, além de instituições de saúde, assistência social e outros integrantes da rede de proteção. Esse compartilhamento também pode ocorrer com outros órgãos públicos e entidades, sempre que indispensável para a defesa dos interesses dos assistidos ou para o cumprimento de obrigações legais. Todo esse processo é realizado de forma segura, observando as finalidades específicas e as bases legais estabelecidas na LGPD.

Por fim, quando a necessidade do tratamento dos dados se encerra, eles podem ser arquivados ou eliminados. O arquivamento ocorre nos casos em que há interesse histórico, legal ou institucional, ou ainda para garantir o cumprimento de prazos prescricionais, sempre em conformidade com as disposições da Lei de Arquivos Públicos (Lei nº 8.159/1991) e das normativas internas da DPE-MT. Já a eliminação dos dados ocorre quando não há mais necessidade de sua manutenção e desde que não haja impedimento legal. Esse procedimento deve ser realizado de forma segura, garantindo que os dados sejam destruídos de maneira definitiva, sem possibilidade de recuperação, resguardando assim a privacidade e a segurança dos titulares das informações.

3.5 Bases Legais na Atuação da Defensoria Pública do Estado de Mato Grosso (DPE-MT)

A atuação da Defensoria Pública do Estado de Mato Grosso (DPE-MT) envolve, de forma essencial e indissociável de sua missão institucional, o tratamento de dados pessoais e dados sensíveis. A coleta, utilização, armazenamento e compartilhamento dessas informações são fundamentais para garantir a efetividade da assistência jurídica gratuita e integral aos cidadãos em situação de vulnerabilidade, estando, portanto, plenamente respaldados pelas bases legais previstas na Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais (LGPD).

A conformidade da DPE-MT com a LGPD fundamenta-se, principalmente, nos artigos 7º e 23, que tratam das hipóteses legais para o tratamento de dados pessoais no âmbito do setor público. Nos termos do artigo 23, os órgãos e entidades públicas podem tratar dados pessoais sempre que esse tratamento for necessário para a execução de políticas públicas previstas em leis e regulamentos, bem como quando estiver respaldado em contratos, convênios ou outros instrumentos congêneres. Da mesma forma, o tratamento é autorizado quando se destina à proteção do interesse público e na persecução do interesse legítimo da administração pública.

Além disso, o artigo 7º da LGPD, aplicado conjuntamente ao artigo 23, permite que o tratamento de dados pela DPE-MT ocorra em situações como o cumprimento de obrigação legal ou regulatória, a execução de políticas públicas respaldadas por normas legais, a realização de estudos por órgãos de pesquisa, desde que, sempre que possível, com anonimização dos dados, a proteção da vida ou da incolumidade física do titular ou de terceiros, a tutela da saúde no âmbito de procedimentos realizados por profissionais ou serviços de saúde, a execução de contratos ou de procedimentos preliminares relacionados, e, ainda, no legítimo interesse público ou do controlador, desde que observados os limites legais.

O tratamento de dados realizado pela DPE-MT é absolutamente legítimo e indispensável ao cumprimento de sua função constitucional de prestar assistência jurídica integral e gratuita, conforme preconiza o artigo 134 da Constituição Federal. No exercício dessa missão, a Defensoria precisa coletar, armazenar e, quando necessário, compartilhar informações essenciais para avaliar a hipossuficiência dos assistidos, elaborar petições, defesas, recursos e demais peças processuais, acompanhar processos judiciais e extrajudiciais e atuar, de forma ampla, na defesa dos direitos fundamentais da população vulnerável. Inclusive, o próprio site institucional da DPE-MT ressalta essa missão ao afirmar que sua atuação visa assegurar, de forma integral e gratuita, a orientação jurídica e a defesa dos direitos individuais e coletivos dos necessitados, em todos os graus de jurisdição, judicial e extrajudicialmente.

Portanto, a legitimidade do tratamento de dados pela instituição decorre diretamente da obrigação legal, do interesse público e da necessidade de efetivar os direitos fundamentais dos cidadãos assistidos.

Em razão da natureza dos serviços prestados, a DPE-MT frequentemente trata dados pessoais sensíveis, nos termos do artigo 5º, inciso II, da LGPD. Entre esses dados estão informações sobre origem racial ou étnica, condições de saúde física e mental, dados biométricos quando necessários para a identificação, convicções religiosas, informações relativas à situação econômica, patrimonial e social dos assistidos e, ainda, dados sobre orientação sexual, especialmente em casos que envolvem demandas de direito de família, violência ou outros contextos específicos.

O tratamento desses dados sensíveis é justificado tanto pelo exercício regular de direitos quanto pela necessidade de proteger os direitos fundamentais dos assistidos, implementar políticas públicas e cumprir os deveres institucionais da Defensoria Pública. A proteção e segurança dessas informações são asseguradas por meio de medidas técnicas e administrativas previstas no Plano de Proteção de Dados Pessoais (PPDP) da DPE-MT, instituído pela Resolução nº 018/2022-DPG, que estabelece diretrizes para um tratamento de dados adequado, seguro e transparente dentro da instituição.

3.6 Riscos, Vulnerabilidades e Desafios no Tratamento de Dados na DPE-MT

A implementação da Lei Geral de Proteção de Dados Pessoais (LGPD) na Defensoria Pública do Estado de Mato Grosso (DPE-MT) trouxe avanços significativos na proteção dos dados pessoais, mas também impôs uma série de desafios, riscos e vulnerabilidades que demandam atenção constante por parte da instituição.

Diante da sensibilidade dos dados tratados, sobretudo dados pessoais sensíveis, a DPE-MT enfrenta riscos específicos relacionados à natureza de suas atividades, que envolvem a defesa de pessoas em situação de vulnerabilidade social, econômica e jurídica.

Entre os principais riscos mapeados estão: Vazamento de dados que consiste na divulgação não autorizada de informações pessoais, seja por falha humana, ataques cibernéticos ou ausência de medidas adequadas de segurança, é um dos riscos mais críticos. Esse tipo de incidente pode acarretar danos irreparáveis aos titulares dos dados e comprometer a credibilidade da instituição (BRASIL, 2018; DPE-MT, 2022).

Também há o acesso indevido que vem a ser o risco de que pessoas não autorizadas, internas ou externas, tenham acesso a informações protegidas é relevante, especialmente

considerando que a DPE-MT lida com dados que envolvem processos judiciais, dados de saúde, informações financeiras e dados sensíveis de seus assistidos (DPE-MT, 2022).

E o tratamento excessivo de dados, ou seja, a coleta ou manutenção de dados além do necessário para a finalidade pretendida configura um risco tanto legal quanto ético. A LGPD estabelece os princípios da necessidade e da minimização, determinando que apenas os dados estritamente necessários devem ser tratados (BRASIL, 2018).

Conforme ressalta a Autoridade Nacional de Proteção de Dados (ANPD), as instituições públicas precisam adotar medidas técnicas e administrativas que garantam a proteção dos dados pessoais e previnam a ocorrência de incidentes, considerando as vulnerabilidades específicas do ambiente institucional (ANPD, 2020).

Quanto às vulnerabilidades, a Defensoria Pública, como outros órgãos públicos, enfrenta as mais comuns, tais como: Infraestrutura tecnológica defasada; Falta de cultura organizacional voltada à privacidade e proteção de dados; Necessidade constante de capacitação dos servidores, estagiários e terceirizados; Integração de diversos sistemas externos (PJE, SEEU, TJMT, entre outros), que ampliam a superfície de risco.

Essas vulnerabilidades são destacadas no Plano de Proteção de Dados Pessoais (PPDP) da própria instituição, que busca enfrentá-las com medidas preventivas, como o mapeamento de dados, a revisão de processos internos e a implementação de protocolos de segurança (DPE-MT, 2022).

3.7 Desafios Operacionais e Tecnológicos na DPE-MT

A adequação da Defensoria Pública do Estado de Mato Grosso (DPE-MT) às exigências da Lei Geral de Proteção de Dados Pessoais (LGPD) envolve não apenas questões jurídicas, mas também uma série de desafios operacionais e tecnológicos. Esses desafios estão diretamente relacionados à complexidade dos sistemas utilizados, à segurança da informação e à necessidade de transformação da cultura organizacional.

Os principais desafios enfrentados pela DPE-MT incluem:

- Adequação tecnológica: Investir em sistemas seguros e atualizados é essencial para reduzir riscos, mas enfrenta limitações orçamentárias e estruturais típicas da administração pública (PIRONTI, 2021).
- Capacitação contínua: A proteção de dados não se resume a soluções tecnológicas. É necessário que todos os colaboradores estejam treinados para lidar adequadamente com informações sensíveis (ANPD, 2020).

- Gestão de incidentes: Criar protocolos eficazes para identificar, comunicar e mitigar eventuais violações de dados é um desafio recorrente, exigindo planejamento, agilidade e transparência.
- Cultura organizacional: Promover a conscientização sobre a importância da privacidade e da proteção de dados ainda é um processo em construção, especialmente no setor público (PIRONTI, 2021).

Diante desse cenário, a atuação alinhada com o Plano de Proteção de Dados Pessoais (PPDP) da DPE-MT, a supervisão constante do Encarregado de Proteção de Dados (DPO) e a adoção das diretrizes da ANPD tornam-se fundamentais para mitigar riscos e fortalecer a governança de dados dentro da instituição.

3.7.1 Sistemas Integrados (Solar, PJE, SEEU)

A DPE-MT utiliza diversos sistemas, internos e externos, para gerenciar atendimentos e processos judiciais, garantindo maior eficiência e controle. Destacam-se o Solar, sistema próprio para cadastro e gestão processual interna; o PJe, plataforma do Poder Judiciário para tramitação eletrônica dos processos; e o SEEU, sistema nacional voltado ao acompanhamento das execuções penais.

Além desses sistemas, a Defensoria também integra ferramentas de comunicação institucional, como e-mails oficiais e plataformas de videoconferência, que facilitam atendimentos remotos, reuniões e audiências virtuais. Essa infraestrutura tecnológica permite uma atuação mais ágil, segura e transparente, alinhada às necessidades da população e às exigências legais, garantindo a continuidade dos serviços mesmo em situações de restrição de acesso presencial.

O desafio se apresenta na medida em que esses sistemas operam de forma integrada e muitas vezes compartilham dados sensíveis entre diferentes órgãos, como Ministério Público, Tribunal de Justiça e órgãos de segurança pública. Isso exige que a DPE-MT adote medidas rigorosas de segurança e controle sobre os fluxos de dados, garantindo que o compartilhamento esteja em conformidade com as bases legais da LGPD e que haja rastreabilidade e segurança nas operações (DPE-MT, 2022; PIRONTI, 2021).

3.7.2 Segurança da Informação

A segurança da informação é um dos principais pilares para a efetiva proteção dos

dados pessoais. A DPE-MT lida com informações altamente sensíveis, como dados de saúde, informações socioeconômicas, etnia, antecedentes criminais e detalhes de processos judiciais.

Entre os desafios enfrentados estão:

- Implementação de políticas robustas de segurança da informação;
- Proteção contra acessos indevidos e ataques cibernéticos;
- Gestão de credenciais de acesso nos sistemas integrados;
- Criação de planos de resposta a incidentes.

Conforme destacado pela ANPD (2020), a adoção de medidas técnicas, como criptografia, controle de acesso, backups seguros e monitoramento de redes, é fundamental para mitigar os riscos relacionados à segurança da informação. Além disso, a falta de investimentos tecnológicos suficientes no setor público dificulta a implementação de soluções avançadas (PIRONTI, 2021).

3.7.3 Cultura Organizacional

Outro desafio expressivo está relacionado à mudança da cultura organizacional. A proteção de dados pessoais não se limita a procedimentos técnicos ou jurídicos; ela depende fortemente da conscientização dos servidores, estagiários, terceirizados e membros da instituição.

Na DPE-MT, promover uma cultura de privacidade implica:

- Realização de treinamentos contínuos;
- Criação de procedimentos operacionais claros sobre o tratamento de dados;
- Sensibilização dos colaboradores quanto à responsabilidade no manuseio de informações pessoais;
- Fortalecimento do papel do Encarregado de Proteção de Dados (DPO) como agente de governança e educação interna (DPE-MT, 2022).

Conforme enfatiza Pironti (2021), sem uma cultura organizacional alinhada à proteção de dados, qualquer esforço tecnológico ou normativo se torna insuficiente. A proteção de dados deve ser um valor incorporado à missão institucional da DPE-MT.

3.8 Análise Conformidade da DPE-MT com a LGPD: Avanços, Desafios e Perspectivas.

A Defensoria Pública do Estado de Mato Grosso (DPE-MT) tem empreendido

esforços consistentes para se adequar à Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, cuja observância é obrigatória tanto para os setores público quanto privado. Desde a promulgação da norma, a instituição vem implementando medidas de alinhamento normativo e técnico, numa tentativa de internalizar os princípios da proteção de dados pessoais em sua estrutura organizacional. Esse movimento institucional encontra respaldo no artigo 5º, inciso LXXIX, da Constituição Federal, que eleva a proteção de dados à categoria de direito fundamental.

Como primeira medida de adequação, a DPE-MT elaborou um projeto institucional que priorizou as chamadas "áreas meio", com atenção especial para os setores de contratos, recursos humanos (RH) e tecnologia da informação (TI). Paralelamente, a instituição instituiu, por meio da Resolução nº 018/2022/DPG, a Política de Privacidade e Proteção de Dados Pessoais (PPPD), que estabelece princípios orientadores para o tratamento de dados, tais como finalidade, adequação, necessidade, segurança e responsabilização. Tal política não apenas formaliza as diretrizes gerais da LGPD no âmbito da DPE-MT, como também prevê a implementação de instrumentos de controle e prevenção de riscos, como planos de resposta a incidentes e ações de conscientização institucional.

Ainda no aspecto normativo, a DPE-MT criou o Sistema de Controle Interno (SCI), previsto na Resolução nº 038/2022/DPG, cuja abordagem se fundamenta na gestão de riscos e na prevenção de irregularidades. O SCI visa promover uma cultura de compliance e reforçar a governança institucional, alinhando-se aos princípios da LGPD. Adicionalmente, a instituição disponibiliza, em seu site institucional, um canal de atendimento para titulares de dados exercerem seus direitos, conforme disposto no artigo 18 da LGPD. Por meio de formulário eletrônico, é possível solicitar informações sobre o tratamento de dados pessoais, bem como requerer correções, atualizações ou eliminação de dados desnecessários.

Cumprindo o artigo 41 da LGPD, a DPE-MT nomeou formalmente um Encarregado de Proteção de Dados (Data Protection Officer – DPO), designando o servidor Marcus Vinícius Sousa Ventura para a função por meio do Ato nº 174/2023, publicado no Diário Oficial do Estado em 30 de outubro de 2023. A atuação do DPO como ponto focal entre a instituição, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) é essencial para a construção de uma estrutura organizacional capaz de responder de forma técnica e jurídica às demandas da LGPD.

Contudo, apesar desses avanços normativos e operacionais, persistem desafios estruturais que dificultam a plena conformidade da DPE-MT com a LGPD. O mapeamento institucional realizado pela própria Defensoria revelou que, embora haja diretrizes

estabelecidas, a execução prática ainda é afetada por limitações operacionais. Um dos pontos críticos mais relevantes diz respeito à ausência da Avaliação de Impacto à Proteção de Dados (Data Protection Impact Assessment – DPIA). Embora prevista na PPPD e considerada uma ferramenta essencial para a identificação e mitigação de riscos, a DPIA ainda não foi formalmente publicada, o que prejudica a capacidade da instituição de antever e prevenir riscos relacionados ao tratamento de dados.

Além disso, a gestão do ciclo de vida dos dados pessoais, especialmente no que tange à eliminação segura e adequada de informações em meio físico ou digital, ainda apresenta fragilidades. O desafio da integração entre os diversos sistemas utilizados pela instituição como o SOLAR, o PJe, o SEEU e o SIPIA também é uma preocupação recorrente. Tais sistemas não foram originalmente concebidos com foco na privacidade e, por isso, a interoperabilidade entre eles representa uma ameaça à segurança e à rastreabilidade dos dados. Sobre esse ponto, Gonzalez e Morrison (2021, p. 143) alertam:

“A modernização tecnológica das instituições públicas é uma condição indispensável para a efetividade da LGPD. A ausência de interoperabilidade entre sistemas e a dependência de plataformas antigas inviabilizam o controle, o monitoramento e a rastreabilidade necessários para o cumprimento das obrigações legais relacionadas à proteção de dados” (Gonzalez e Morrison, 2021, p. 143).

A política de capacitação também é um aspecto que carece de maior aprofundamento. Embora a DPE-MT tenha promovido cursos, palestras e campanhas institucionais, ainda há carência de programas contínuos e sistematizados de formação em proteção de dados, sobretudo para servidores que atuam diretamente com informações sensíveis. O que se observa é uma abordagem pontual e fragmentada, o que contraria a orientação da literatura especializada. Segundo Silva e Pereira (2022, p. 128):

“A cultura de proteção de dados não se forma apenas com normativas internas ou com a nomeação de encarregados. É necessário investir, de forma contínua, na capacitação de todos os agentes que tratam dados, sob pena de tornar a política institucional um mero documento decorativo” (Silva e Pereira, 2022, p. 128).

Outras limitações também comprometem a efetividade das ações implementadas. As restrições orçamentárias impactam diretamente na aquisição de soluções tecnológicas como softwares de criptografia, anonimização e detecção de vazamentos. Da mesma forma, o corpo técnico da DPE-MT encontra-se aquém das necessidades da instituição, especialmente diante do crescimento da demanda por serviços jurídicos e do volume de dados sensíveis tratados diariamente. A concentração de responsabilidades no DPO, sem uma equipe multidisciplinar de apoio, revela um ponto estrutural crítico.

Apesar disso, a DPE-MT vem adotando medidas técnicas importantes, como o controle de acesso baseado no princípio da necessidade, segregação de perfis de usuários e monitoramento constante de sistemas como o SOLAR e a intranet institucional. Também está previsto um plano de resposta a incidentes, com procedimentos para notificação à ANPD e aos titulares em caso de violação de dados, conforme o artigo 48 da LGPD.

De modo geral, a experiência da DPE-MT evidencia os desafios enfrentados por instituições públicas na implementação de um programa robusto de governança de dados. Embora avanços tenham sido concretizados, ainda há um caminho extenso a ser trilhado para que a proteção de dados seja plenamente efetivada na cultura organizacional. Como bem sintetizam Gonzalez e Morrison (2021, p. 149):

“O maior desafio da LGPD não está na norma, mas na sua implementação. A lei trouxe à tona a urgência de uma reforma cultural no setor público, exigindo das instituições não apenas conformidade jurídica, mas mudanças estruturais, investimentos permanentes e consciência coletiva sobre o valor da privacidade” (Gonzalez e Morrison, 2021, p. 149).

4 CONSIDERAÇÕES FINAIS

Este trabalho teve como objetivo analisar a aplicabilidade da Lei Geral de Proteção de Dados Pessoais (LGPD) no contexto da Defensoria Pública do Estado de Mato Grosso (DPE-MT), destacando os desafios, avanços, riscos e medidas implementadas pela instituição na busca pela conformidade com a legislação.

Ao longo da pesquisa, foi possível constatar que a DPE-MT, alinhada às exigências da LGPD, avançou significativamente na institucionalização de práticas de governança de dados. A criação do Plano de Proteção de Dados Pessoais (PPDP), regulamentado pela Resolução nº 018/2022-DPG, e a nomeação do Encarregado de Dados (DPO) são marcos importantes no fortalecimento da cultura de privacidade dentro da instituição (DEFENSORIA PÚBLICA DO ESTADO DE MATO GROSSO, 2022).

Apesar desses avanços, foram identificados desafios relevantes, especialmente no que se refere às limitações tecnológicas, orçamentárias e de pessoal, além da necessidade de fortalecer práticas como avaliações de impacto (DPIA), controle do ciclo de vida dos dados e capacitação contínua dos colaboradores. Ademais, a integração dos sistemas (SOLAR, PJE, SEEU e outros) ainda carece de melhorias que garantam a segurança da informação e a rastreabilidade dos dados pessoais tratados (DPE-MT, 2024).

Por outro lado, também se percebe que a implementação da LGPD na DPE-MT não representa apenas um cumprimento legal, mas uma oportunidade para aprimorar a gestão institucional, fortalecer a relação de confiança com os assistidos e promover um ambiente mais seguro, transparente e ético no tratamento das informações (PIRONTI, 2021).

Diante dos resultados obtidos, sugere-se como linha para futuras pesquisas uma análise comparativa entre a adequação da LGPD na DPE-MT e em outras defensorias públicas do país, ou mesmo em diferentes órgãos públicos estaduais e federais. Essa comparação poderia revelar padrões, desafios comuns e boas práticas replicáveis, contribuindo para o desenvolvimento de uma governança de dados mais robusta no setor público.

Portanto, conclui-se que, embora haja um caminho percorrido, o processo de conformidade à LGPD é contínuo, exigindo monitoramento constante, atualização de práticas e investimentos em tecnologia, capacitação e cultura organizacional. A proteção de dados pessoais, sobretudo no setor público, não é apenas uma exigência normativa, mas um compromisso ético com a cidadania e com a dignidade da pessoa humana.

REFERÊNCIAS

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia de Elaboração de Programa de Governança em Privacidade**. Brasília: ANPD, 2022. Disponível em: <https://www.gov.br/anpd>. Acesso em: 23 out. 2024.

BASTOS, M. C. P.; FERREIRA, D. V. **Metodologia Científica**. Editora XYZ, 2020.

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

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 8.078, de 11 de setembro de 1990**. Código de Defesa do Consumidor. Diário Oficial da União, Brasília, DF, 12 set. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 23 out. 2024.

BRASIL. **Lei nº 9.507, de 12 de novembro de 1997**. Lei do Habeas Data. Diário Oficial da União, Brasília, DF, 13 nov. 1997. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9507.htm. Acesso em: 23 out. 2024.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Marco Civil da Internet. Diário Oficial da União, Brasília, DF, 24 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 23 out. 2024.

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. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 26 maio 2025.

BRASIL. **Lei nº 13.853, de 8 de julho de 2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a criação da Autoridade Nacional de Proteção de Dados. Diário Oficial da União, Brasília, 2019.

CUNHA, Rodrigo. **Governança e Boas Práticas de Proteção de Dados**. Belo Horizonte: Editora Fórum, 2020.

DEFENSORIA PÚBLICA DO ESTADO DE MATO GROSSO (DPE-MT). **Ata da primeira reunião ordinária do ano 2024 do Conselho Superior**. Cuiabá, 2024. Disponível em: https://www.defensoria.mt.def.br/dpmt/conteudo/documentos/1489-ATA_1__ROCS_ANO_2024_SESSAO_PRESENCIAL_EM_02_02_2024.pdf. Acesso em: 25 maio 2025.

DEFENSORIA PÚBLICA DO ESTADO DE MATO GROSSO (DPE-MT). **Encarregado de**

Dados. Cuiabá, 2023. Disponível em: <https://defensoria.mt.def.br/dpmt/lgpd/encarregado-de-dados>. Acesso em: 26 maio 2025.

DEFENSORIA PÚBLICA DO ESTADO DE MATO GROSSO (DPE-MT). **Formulário de Requisição de Direitos – LGPD.** Cuiabá, 2022. Disponível em: <https://defensoria.mt.def.br/dpmt/lgpd/formulario>. Acesso em: 25 maio 2025.

DEFENSORIA PÚBLICA DO ESTADO DE MATO GROSSO (DPE-MT). **Institucional.** Disponível em: <https://www.defensoria.mt.def.br/>. Acesso em: 25 maio 2025.

DEFENSORIA PÚBLICA DO ESTADO DE MATO GROSSO (DPE-MT). **Política de Privacidade e Proteção de Dados Pessoais (PPPD/DPE).** Cuiabá, 2022. Disponível em: <https://defensoria.mt.def.br/dpmt/lgpd/politica-de-privacidade-e-protecao-de-dados-pppd-dpe>. Acesso em: 26 maio 2025.

DEFENSORIA PÚBLICA DO ESTADO DE MATO GROSSO (DPE-MT). **Portal da LGPD na DPE-MT.** Cuiabá, 2024. Disponível em: <https://defensoria.mt.def.br/dpmt/lgpd>. Acesso em: 25 maio 2025.

DEFENSORIA PÚBLICA DO ESTADO DE MATO GROSSO (DPE-MT). **Resolução nº 018/2022-DPG. Institui o Plano de Proteção de Dados Pessoais (PPDP) no âmbito da DPE-MT.** Cuiabá, 2022. Disponível em: <https://www.defensoria.mt.def.br/>. Acesso em: 25 maio 2025.

DEFENSORIA PÚBLICA DO ESTADO DE MATO GROSSO (DPE-MT). **Sistema de Controle Interno da DPE-MT.** Cuiabá, 2022. Disponível em: <https://www.defensoria.mt.def.br/dpmt/sistema-de-controle-interno/o-sistema-de-controle-interno-da-dpe-mt>. Acesso em: 25 maio 2025.

FRANÇA. **Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.** Disponível em: <https://www.legifrance.gouv.fr/>. Acesso em: 25 mai. 2025.

GONZALEZ, J. C.; MORRISON, J. **Data Protection in the Digital Age: The Impact of the LGPD on Public Institutions.** Rio de Janeiro: Editora Jurídica, 2021.

MARQUES, Anderson; COSTA, Elisa; SOUZA, Fernanda. **Hipóteses Legais de Tratamento de Dados Pessoais.** São Paulo: Editora Jurídica, 2021.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos.** 1948. Disponível em: <https://www.un.org/pt/about-us/universal-declaration-of-human-rights>. Acesso em: 25 mai. 2025.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Pacto Internacional dos Direitos Cíveis e Políticos.** 1966. Disponível em: <https://www.ohchr.org/pt/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>. Acesso em: 25 mai. 2025.

PIRONTI, Rodrigo (coord.). **Lei Geral de Proteção de Dados no Setor Público.** 1. ed. Belo Horizonte: Fórum, 2021. ISBN 978-65-5518-141-8.

SECRETARIA DE ESTADO DE EDUCAÇÃO DE MATO GROSSO (SEDUC-MT). **Você conhece a Lei Geral de Proteção de Dados?** Cuiabá, 2022. Disponível em: <https://www3.seduc.mt.gov.br/voce-conhece-a-lei-geral-de-protecao-de-dados>. Acesso em: 25 maio 2025.

SILVA, Mariana; PEREIRA, João. **Tratamento de Dados Pessoais pelo Poder Público**. Rio de Janeiro: Editora Lumen Juris, 2022.

SILVA, R. A.; FERREIRA, L. C. **Privacidade e proteção de dados na era digital: reflexões sobre a LGPD**. Belo Horizonte: Editora Del Rey, 2022.

TESSER, André Luiz Bäuml et al. **Lei Geral de Proteção de Dados no Setor Público**. 1. ed. [S.l.]: [s.n.], 2021. 490 p. ISBN 978-65-5518-141-8.

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, Bruxelas, Bélgica, 4 maio 2016. Disponível em: <https://eur-lex.europa.eu/>. Acesso em: 25 mai. 2025.

WARREN, Samuel D.; BRANDEIS, Louis D. **The Right to Privacy**. Harvard Law Review, v. 4, n. 5, p. 193-220, Dec. 1890.