

APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS - LGPD NA ELABORAÇÃO DE BOLETINS DE ATENDIMENTO DA POLÍCIA MILITAR, TANTO NAS OCORRÊNCIAS QUANTO NOS PROCESSOS E PROCEDIMENTOS ADMINISTRATIVOS DISCIPLINARES INTERNOS DA PMPA

Michel Soares Veras¹
Vilson da Silva Gomes²
Misael Pinheiro Oliveira³
Carlos Henrique Ribeiro Soares⁴

RESUMO: A crescente digitalização dos sistemas de segurança pública tem ampliado a eficiência operacional das instituições policiais, ao mesmo tempo em que impõe novos desafios relacionados à proteção de dados pessoais. Nesse contexto, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) surge como importante instrumento de garantia dos direitos fundamentais à privacidade e à proteção das informações dos cidadãos. O presente artigo tem por objetivo analisar a aplicação da LGPD na elaboração dos Boletins de Atendimento da Polícia Militar do Pará, bem como nos procedimentos administrativos disciplinares e investigatórios internos da Corporação, incluindo sindicâncias, Inquéritos Policiais Militares, Procedimentos Administrativos Disciplinares Simplificados, Conselhos de Justificação e Conselhos de Disciplina. A pesquisa adota abordagem qualitativa, de natureza bibliográfica e documental, fundamentada na legislação vigente, na doutrina especializada e em normativos institucionais relacionados à atividade policial militar. Inicialmente, examina-se a aplicabilidade relativa da LGPD às atividades de segurança pública, considerando a exceção prevista no artigo 4º, inciso III, da referida lei, sem afastar a observância dos princípios constitucionais da legalidade, finalidade, necessidade e segurança da informação. Em seguida, analisa-se o fluxo de tratamento de dados pessoais durante o atendimento de ocorrências policiais, destacando a necessidade de restringir a coleta e o compartilhamento de informações ao estritamente necessário para a atividade-fim da instituição. Também são abordadas as garantias especiais conferidas a crianças e adolescentes, em conformidade com o Estatuto da Criança e do Adolescente. O estudo demonstra que a adoção de protocolos adequados de proteção de dados contribui para a preservação da cadeia de custódia das informações, reduzindo riscos de vazamentos, responsabilizações disciplinares e demandas judiciais. Conclui-se que a proteção de dados não constitui obstáculo à atuação policial, mas mecanismo de fortalecimento institucional e de segurança jurídica para os profissionais de segurança pública, promovendo maior eficiência, transparência e legitimidade no exercício das funções constitucionais da Polícia Militar do Pará.

Palavras-chave: Lei Geral de Proteção de Dados. Segurança Pública. Polícia Militar do Pará. Boletim de Atendimento. Procedimentos Administrativos Disciplinares. Proteção de Dados Pessoais. Segurança Jurídica.

¹Licenciatura Plena em Geografia/ Policial Militar. Universidade norte do Paraná - UNOPAR / Faculdade Única Docência em Geografia e Práticas Pedagógicas. Polícia Militar do Estado do Pará (PMPA).

²Ensino Médio Completo / Policial Militar Escola Estadual de Ensino Fund e Médio Prof. Acy de Jesus Neves de Barros Pereira / Polícia Militar do Estado do Pará (PMPA).

³Bacharel em Direito / Policial Militar, Centro Universitário Luterano de Santarém (CEULS/ULBRA) / Polícia Militar do Estado do Pará (PMPA).

⁴Pós-graduação Lato Sensu, Direito Administrativo/ Policial Militar Faculdade Integrada de Ensino Superior de Colinas (FIESC) / Polícia Militar do Estado do Pará (PMPA).

ABSTRACT: The increasing digitalization of public security systems has enhanced the operational efficiency of law enforcement agencies while simultaneously creating new challenges related to the protection of personal data. In this context, the Brazilian General Data Protection Law (Law No. 13,709/2018) emerges as an important instrument for safeguarding the fundamental rights to privacy and personal data protection. This article aims to analyze the application of the General Data Protection Law in the preparation of Police Service Reports within the Military Police of the State of Pará, as well as in internal disciplinary and investigative administrative procedures, including administrative inquiries, Military Police Investigations, Simplified Disciplinary Administrative Procedures, Boards of Justification, and Disciplinary Councils. The study adopts a qualitative approach, based on bibliographic and documentary research, supported by current legislation, specialized doctrine, and institutional regulations related to military police activities. Initially, the study examines the relative applicability of the General Data Protection Law to public security activities, considering the exception established in Article 4, Item III of the law, without disregarding the constitutional principles of legality, purpose limitation, necessity, and information security. Subsequently, it analyzes the flow of personal data processing during police operations, emphasizing the need to limit the collection and sharing of information to what is strictly necessary for institutional purposes. Special attention is also given to the protection of children and adolescents, in accordance with the Brazilian Child and Adolescent Statute. The findings demonstrate that the adoption of appropriate data protection protocols contributes to preserving the chain of custody of information, reducing risks of data breaches, disciplinary liability, and judicial disputes. The study concludes that data protection should not be viewed as an obstacle to police work, but rather as a mechanism for institutional strengthening and legal certainty for public security professionals, promoting greater efficiency, transparency, and legitimacy in the performance of the constitutional duties of the Military Police of Pará.

2

Keywords: General Data Protection Law. Public Security. Military Police of Pará. Police Service Report. Disciplinary Administrative Procedures. Personal Data Protection. Legal Certainty. Information Security.

1 INTRODUÇÃO

A transformação digital das instituições públicas modificou significativamente a forma como são realizados os procedimentos administrativos e operacionais, especialmente no âmbito da Segurança Pública. A substituição gradual dos registros físicos por sistemas informatizados ampliou a eficiência na produção, armazenamento e compartilhamento de informações, fortalecendo a integração entre os órgãos responsáveis pela persecução penal e pela defesa social. Nesse contexto, a Polícia Militar do Pará (PMPA) incorporou ferramentas digitais para o registro de ocorrências, elaboração de Boletins de Atendimento e tramitação de procedimentos administrativos, tornando o tratamento de dados pessoais parte essencial de sua atividade institucional.

Paralelamente a esse processo, a proteção de dados pessoais passou a ocupar posição de destaque no ordenamento jurídico brasileiro com a promulgação da Lei nº 13.709/2018,

denominada Lei Geral de Proteção de Dados Pessoais (LGPD). A legislação estabeleceu princípios e diretrizes para o tratamento de dados pessoais, buscando assegurar os direitos fundamentais à privacidade, à intimidade e à autodeterminação informativa. Embora a LGPD preveja tratamento diferenciado para atividades relacionadas à segurança pública, à defesa nacional e à investigação criminal, seus fundamentos permanecem relevantes para orientar a atuação dos órgãos policiais, especialmente diante do elevado volume de informações pessoais e sensíveis diariamente manipuladas.

A atividade policial militar exige a coleta, o armazenamento, o compartilhamento e a utilização de dados de vítimas, testemunhas, suspeitos e demais envolvidos em ocorrências. O tratamento inadequado dessas informações pode ocasionar violações de direitos fundamentais, responsabilizações administrativas e judiciais, além de comprometer a credibilidade institucional. Conforme destaca Carneiro (2023), a governança adequada dos dados constitui instrumento indispensável para reduzir riscos decorrentes do uso indevido das informações sob responsabilidade do Estado.

A relevância da temática é ampliada pela crescente utilização de bancos de dados integrados, dispositivos móveis e plataformas eletrônicas de comunicação entre os órgãos do sistema de justiça criminal. Esse fluxo contínuo de informações exige mecanismos capazes de assegurar não apenas a eficiência operacional, mas também a integridade, a confidencialidade e a rastreabilidade dos dados tratados durante toda a cadeia informacional.

Embora a proteção de dados tenha sido amplamente debatida no âmbito da Administração Pública e das relações privadas, ainda são reduzidos os estudos que analisam sua aplicação prática na elaboração dos Boletins de Atendimento e nos procedimentos administrativos disciplinares da Polícia Militar do Pará. Essa lacuna científica evidencia a necessidade de pesquisas voltadas às especificidades da atividade policial militar e aos desafios decorrentes da implementação de mecanismos de governança informacional nesse contexto.

Diante desse cenário, a presente pesquisa busca responder ao seguinte problema: de que forma os princípios da Lei Geral de Proteção de Dados Pessoais podem ser aplicados na elaboração dos Boletins de Atendimento e nos procedimentos administrativos internos da Polícia Militar do Pará, conciliando a proteção dos dados pessoais com a eficiência da atividade policial e a segurança jurídica dos agentes públicos?

Parte-se da hipótese de que a adoção de protocolos institucionais alinhados aos princípios da proteção de dados fortalece a segurança jurídica dos policiais militares, reduz riscos de

vazamentos de informações e contribui para o aperfeiçoamento da gestão informacional da Corporação, sem comprometer a efetividade das atividades constitucionais de preservação da ordem pública.

O objetivo geral consiste em analisar a aplicação da Lei Geral de Proteção de Dados Pessoais na elaboração dos Boletins de Atendimento da Polícia Militar do Pará e nos procedimentos administrativos internos da Corporação. Como objetivos específicos, pretende-se examinar a aplicabilidade da LGPD às atividades de segurança pública, identificar os limites para coleta e compartilhamento de informações pessoais no contexto policial, analisar a proteção de dados nos procedimentos administrativos disciplinares e apresentar propostas de aperfeiçoamento voltadas ao fortalecimento da governança informacional.

A pesquisa justifica-se pela necessidade de adequação das instituições policiais às exigências contemporâneas de proteção de dados e pela contribuição que pode oferecer ao aperfeiçoamento dos procedimentos administrativos e operacionais da Polícia Militar do Pará. Além disso, busca ampliar a produção científica sobre a aplicação da LGPD na atividade policial militar, oferecendo subsídios teóricos e práticos para o fortalecimento da segurança jurídica institucional.

Trata-se de pesquisa de abordagem qualitativa, desenvolvida por meio de revisão bibliográfica e documental, fundamentada na legislação vigente, na doutrina especializada, em publicações científicas e em normativos institucionais relacionados à proteção de dados e à atividade policial militar. Pretende-se demonstrar que a proteção de dados pessoais não constitui obstáculo ao exercício da função policial, mas representa importante instrumento de fortalecimento institucional, proteção dos direitos fundamentais e modernização da gestão da segurança pública.

4

2 A APLICABILIDADE RELATIVA DA LGPD NA ATIVIDADE POLICIAL

A crescente utilização de recursos tecnológicos pelas instituições de segurança pública tem promovido profundas transformações na forma como as informações são coletadas, armazenadas, compartilhadas e utilizadas durante o exercício das atividades policiais. A modernização dos sistemas de registro de ocorrências, a implementação de bancos de dados integrados e a utilização de plataformas digitais para comunicação entre órgãos governamentais passaram a desempenhar papel fundamental na eficiência das ações estatais voltadas à preservação da ordem pública e à proteção da sociedade. Nesse cenário, a proteção dos dados

possíveis passou a ocupar posição estratégica dentro da administração pública, especialmente após a entrada em vigor da Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (Brasil, 2018), a qual estabeleceu princípios e diretrizes destinados a assegurar a proteção dos direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade da pessoa natural.

Embora a LGPD tenha sido concebida para disciplinar o tratamento de dados pessoais em diversos setores da sociedade, o próprio legislador reconheceu que determinadas atividades estatais apresentam peculiaridades que exigem tratamento jurídico diferenciado. Em razão disso, o artigo 4º da legislação prevê hipóteses específicas nas quais suas disposições não se aplicam integralmente, incluindo atividades relacionadas à segurança pública, à defesa nacional, à segurança do Estado e à investigação criminal (Brasil, 2018). Tal previsão tem gerado amplos debates doutrinários acerca dos limites da atuação estatal e da forma pela qual os princípios da proteção de dados devem ser observados pelas instituições responsáveis pela segurança pública.

No âmbito da Polícia Militar do Pará, a discussão adquire relevância ainda maior em razão da natureza das atividades desempenhadas pela Corporação. O atendimento de ocorrências policiais exige contato permanente com informações pessoais de vítimas, testemunhas, autores de infrações penais, adolescentes em conflito com a lei e demais cidadãos envolvidos em situações que demandam intervenção estatal. A elaboração dos Boletins de Atendimento, relatórios operacionais e demais documentos administrativos pressupõe a coleta e o tratamento de informações que, muitas vezes, possuem caráter sensível e cuja divulgação inadequada pode acarretar prejuízos irreparáveis aos indivíduos envolvidos.

A interpretação equivocada da exceção prevista no artigo 4º da LGPD pode levar à falsa compreensão de que as atividades policiais estariam completamente afastadas das exigências relacionadas à proteção de dados pessoais. Entretanto, a doutrina especializada tem demonstrado que a exclusão da incidência integral da LGPD não afasta a necessidade de observância dos direitos fundamentais previstos na Constituição Federal. Conforme destaca Aras (2025), os órgãos de segurança pública permanecem submetidos aos princípios constitucionais da legalidade, proporcionalidade, necessidade e finalidade, devendo justificar adequadamente toda atividade de tratamento de dados realizada no exercício de suas atribuições institucionais.

A proteção de dados no contexto da atividade policial não deve ser compreendida como obstáculo à atuação operacional dos agentes de segurança pública. Pelo contrário, a observância

de protocolos adequados de tratamento da informação contribui para o fortalecimento da legitimidade institucional e para a ampliação da segurança jurídica dos profissionais responsáveis pela execução das políticas de defesa social. O tratamento adequado das informações reduz riscos de responsabilização administrativa, evita vazamentos de dados e fortalece a confiança da sociedade nas instituições encarregadas da manutenção da ordem pública (Costa, 2024).

A relevância da temática também está relacionada à crescente integração entre os órgãos que compõem o sistema de justiça criminal. Atualmente, informações produzidas pela Polícia Militar frequentemente são compartilhadas com a Polícia Civil, Ministério Público, Poder Judiciário e demais entidades responsáveis pela persecução penal. Essa circulação de dados exige mecanismos capazes de garantir a integridade, autenticidade e confidencialidade das informações durante todo o fluxo institucional. A ausência de controles adequados pode comprometer investigações, gerar nulidades processuais e ocasionar violações aos direitos fundamentais dos cidadãos.

Outro aspecto que merece destaque refere-se à utilização crescente de dispositivos eletrônicos no cotidiano policial. Sistemas embarcados em viaturas, aplicativos institucionais, câmeras corporais, plataformas de consulta de antecedentes e bancos de dados integrados passaram a compor a rotina operacional dos agentes de segurança pública. Tais ferramentas ampliam significativamente a capacidade de resposta das instituições, mas também aumentam os riscos relacionados ao acesso indevido, compartilhamento não autorizado e utilização inadequada das informações armazenadas. Conforme observa Souza (2020), a governança informacional tornou-se elemento indispensável para garantir a efetividade e a legitimidade das atividades estatais relacionadas à segurança pública.

A preocupação com a proteção de dados torna-se ainda mais relevante quando envolve grupos vulneráveis, especialmente crianças e adolescentes. O Estatuto da Criança e do Adolescente estabelece regras específicas destinadas à preservação da identidade de menores envolvidos em procedimentos policiais, impondo restrições à divulgação de informações que possam resultar em exposição indevida ou estigmatização social (Brasil, 1990). Dessa forma, a atividade policial exige elevado grau de cautela na coleta, armazenamento e compartilhamento de dados relacionados a esse público.

A doutrina contemporânea tem sustentado que a ausência de uma legislação específica destinada ao tratamento de dados para fins de segurança pública não significa ausência de

controle jurídico. Pelo contrário, os princípios constitucionais e os fundamentos gerais da proteção de dados permanecem plenamente aplicáveis às instituições policiais, servindo como parâmetros para avaliação da legalidade das condutas administrativas e operacionais. Nesse sentido, Josino (2021) ressalta que a proteção dos dados pessoais deve ser compreendida como instrumento de fortalecimento democrático, capaz de compatibilizar a atuação estatal com a preservação dos direitos fundamentais.

A implementação de políticas internas de governança da informação também representa importante mecanismo de proteção institucional. A definição de protocolos para acesso a sistemas corporativos, o estabelecimento de critérios para compartilhamento de dados e a realização de treinamentos periódicos contribuem para a redução de incidentes de segurança e para a consolidação de uma cultura organizacional voltada à proteção das informações sob responsabilidade da administração pública. Segundo Paulo (2025), organizações públicas que investem em programas estruturados de governança de dados apresentam melhores índices de conformidade legal e menores riscos de responsabilização administrativa.

Diante desse contexto, torna-se evidente que a aplicação da LGPD às atividades policiais não pode ser analisada sob uma perspectiva simplificada. A existência de regras especiais para a segurança pública não elimina a necessidade de observância dos direitos fundamentais nem afasta a responsabilidade institucional pelo tratamento adequado das informações pessoais. Ao contrário, exige interpretação equilibrada capaz de harmonizar a eficiência operacional da atividade policial com a proteção da privacidade, da dignidade humana e da segurança jurídica dos agentes públicos. Assim, a compreensão da aplicabilidade relativa da LGPD na atividade policial constitui elemento essencial para o aperfeiçoamento dos procedimentos operacionais e administrativos da Polícia Militar do Pará, contribuindo para o fortalecimento da instituição e para a consolidação de práticas compatíveis com os desafios contemporâneos da proteção de dados e da segurança pública.

2.1 A Exceção do Artigo 4º, Inciso III, Alínea “a” da LGPD e a Atividade de Segurança Pública

A Lei Geral de Proteção de Dados Pessoais, instituída pela Lei nº 13.709/2018, estabeleceu um novo paradigma para o tratamento de dados pessoais no Brasil, regulamentando a forma pela qual informações relacionadas às pessoas naturais podem ser coletadas, armazenadas, compartilhadas e utilizadas por entidades públicas e privadas. Apesar da amplitude de sua aplicação, o próprio legislador reconheceu que determinadas atividades desenvolvidas pelo

Estado possuem características específicas que exigem tratamento normativo diferenciado. Em razão disso, o artigo 4º, inciso III, alínea “a”, da LGPD prevê que suas disposições não se aplicam integralmente ao tratamento de dados pessoais realizado para fins exclusivos de segurança pública (Brasil, 2018).

A existência dessa previsão legal tem gerado diferentes interpretações no meio jurídico e institucional. Em uma leitura superficial, poderia surgir o entendimento de que os órgãos de segurança pública estariam completamente dispensados da observância dos princípios relacionados à proteção de dados pessoais. Entretanto, a doutrina especializada tem demonstrado que essa interpretação não encontra respaldo no ordenamento jurídico brasileiro. A exclusão prevista na LGPD refere-se à sua incidência integral, não afastando a aplicação dos direitos e garantias fundamentais previstos na Constituição Federal, especialmente aqueles relacionados à dignidade da pessoa humana, à intimidade, à vida privada e à proteção da honra e da imagem dos cidadãos (Brasil, 1988).

No contexto da atividade policial militar, essa distinção possui relevância prática significativa. A Polícia Militar do Pará desenvolve atividades que demandam contato permanente com dados pessoais de vítimas, testemunhas, suspeitos, investigados e demais indivíduos envolvidos em ocorrências policiais. Durante a elaboração dos Boletins de Atendimento, por exemplo, são registradas informações como nome completo, filiação, endereço, números de documentos, contatos telefônicos e circunstâncias relacionadas aos fatos atendidos. Tais informações são indispensáveis para a atuação estatal, mas também exigem cuidados específicos para evitar exposições indevidas e utilização incompatível com a finalidade institucional.

Segundo Aras (2025), a exclusão prevista no artigo 4º da LGPD não deve ser compreendida como autorização para tratamentos indiscriminados de dados pessoais por parte dos órgãos de segurança pública. Mesmo diante da inexistência de uma legislação específica para o setor, os princípios constitucionais continuam funcionando como parâmetros de controle das atividades estatais. Dessa forma, toda coleta ou utilização de dados deve estar vinculada a uma finalidade legítima, compatível com as atribuições legais da instituição responsável pelo tratamento das informações.

A importância dessa interpretação torna-se ainda mais evidente diante da crescente digitalização dos sistemas de segurança pública. A utilização de plataformas eletrônicas, bancos de dados integrados, aplicativos institucionais e sistemas informatizados ampliou

significativamente a capacidade operacional das corporações policiais. Paralelamente, aumentaram os riscos relacionados ao acesso indevido, ao compartilhamento não autorizado e ao vazamento de informações pessoais. Conforme observa Souza (2020), a evolução tecnológica exige mecanismos cada vez mais robustos de governança informacional, especialmente em órgãos responsáveis pelo tratamento de grandes volumes de dados sensíveis.

No âmbito da Polícia Militar do Pará, a observância desses cuidados possui impacto direto na segurança jurídica dos próprios policiais militares. O acesso a sistemas corporativos deve ocorrer exclusivamente para finalidades relacionadas ao serviço público. Consultas realizadas por interesse pessoal, curiosidade ou qualquer finalidade estranha à atividade institucional podem caracterizar desvio funcional e gerar responsabilização administrativa, disciplinar e até criminal. A proteção de dados, nesse sentido, não representa apenas garantia aos cidadãos, mas também instrumento de proteção para os agentes públicos que atuam dentro dos limites legais estabelecidos.

Outro aspecto relevante refere-se à necessidade de preservação da confiança social nas instituições de segurança pública. A legitimidade da atuação policial está diretamente relacionada à capacidade da instituição de proteger tanto a ordem pública quanto os direitos fundamentais da população. Quando informações pessoais são tratadas de forma inadequada, surgem riscos de questionamentos judiciais, prejuízos à imagem institucional e redução da credibilidade da corporação perante a sociedade. Conforme destaca Josino (2021), a proteção de dados constitui elemento essencial para a consolidação de modelos democráticos de segurança pública, nos quais eficiência operacional e respeito aos direitos fundamentais devem coexistir de maneira equilibrada.

A discussão também se relaciona à ausência de uma legislação específica destinada ao tratamento de dados para fins de segurança pública e persecução penal. Desde a entrada em vigor da LGPD, diversos estudiosos têm defendido a necessidade de criação de um marco regulatório próprio para disciplinar o tratamento de informações pelas instituições policiais e demais órgãos envolvidos na investigação criminal. O Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Persecução Penal surgiu justamente com o objetivo de preencher essa lacuna normativa, estabelecendo regras específicas para compatibilizar a eficiência das atividades estatais com a proteção dos direitos individuais (Brasil, 2020).

Enquanto essa regulamentação específica não é consolidada, as instituições policiais devem adotar medidas internas capazes de garantir a utilização adequada das informações sob

sua responsabilidade. Protocolos de acesso a sistemas, controles de compartilhamento de dados, capacitação permanente dos agentes e mecanismos de auditoria representam instrumentos importantes para reduzir riscos e fortalecer a conformidade institucional. Essas medidas contribuem para a construção de uma cultura organizacional baseada na responsabilidade informacional e na proteção dos direitos fundamentais.

Além disso, o próprio Boletim Geral nº 5/2026 da Polícia Militar do Pará reforça a necessidade de que as pesquisas científicas produzidas no âmbito da Corporação apresentem contribuições relevantes para as atividades institucionais e para a melhoria dos serviços prestados à sociedade. Nesse contexto, a discussão sobre proteção de dados e segurança jurídica mostra-se plenamente compatível com a missão institucional da PMPA, especialmente por propor mecanismos destinados ao aperfeiçoamento dos procedimentos operacionais e administrativos da Corporação.

Portanto, a exceção prevista no artigo 4º, inciso III, alínea “a”, da LGPD não afasta a responsabilidade dos órgãos de segurança pública em relação à proteção dos dados pessoais tratados no exercício de suas funções. Ao contrário, exige interpretação equilibrada que permita compatibilizar a efetividade da atividade policial com a preservação dos direitos fundamentais dos cidadãos. No âmbito da Polícia Militar do Pará, essa compreensão contribui para o fortalecimento institucional, para a ampliação da segurança jurídica dos agentes públicos e para a construção de práticas operacionais alinhadas aos desafios contemporâneos da proteção de dados e da defesa social.

10

2.2 O Princípio da Finalidade e da Necessidade na Elaboração dos Boletins de Atendimento da Polícia Militar do Pará

Entre os fundamentos que orientam a proteção de dados pessoais no ordenamento jurídico brasileiro, destacam-se os princípios da finalidade e da necessidade, considerados elementos essenciais para garantir que o tratamento das informações ocorra de maneira legítima, proporcional e compatível com os direitos fundamentais dos cidadãos. Embora a Lei Geral de Proteção de Dados Pessoais preveja tratamento diferenciado para as atividades de segurança pública, os referidos princípios permanecem como importantes parâmetros de interpretação para a atuação dos órgãos policiais, especialmente diante do elevado volume de informações pessoais manipuladas diariamente pelas instituições responsáveis pela preservação da ordem pública (Brasil, 2018).

No âmbito da Polícia Militar do Pará, a aplicação desses princípios assume relevância prática significativa durante a elaboração dos Boletins de Atendimento, documentos que registram formalmente os fatos observados pelas guarnições durante o atendimento de ocorrências. Esses registros constituem instrumentos fundamentais para a comunicação institucional, para o encaminhamento das informações à Polícia Civil e para a formação de elementos informativos que poderão subsidiar investigações, processos administrativos e procedimentos judiciais. Em razão dessa importância, a coleta e o tratamento dos dados pessoais inseridos nesses documentos devem observar critérios rigorosos de adequação e necessidade.

O princípio da finalidade estabelece que os dados pessoais devem ser coletados para objetivos específicos, legítimos e claramente relacionados às atribuições institucionais do órgão responsável pelo tratamento das informações. Na atividade policial militar, isso significa que toda informação registrada em um Boletim de Atendimento deve possuir relação direta com a ocorrência atendida e com as finalidades legais da atuação estatal. Dados obtidos sem justificativa operacional ou desvinculados do contexto da ocorrência não encontram respaldo nos princípios que orientam a proteção das informações pessoais e podem representar risco tanto para os cidadãos quanto para a própria instituição.

Durante o atendimento de uma ocorrência policial, é comum que os agentes necessitem registrar informações referentes às vítimas, testemunhas, autores de infrações e demais pessoas envolvidas nos fatos. Nome completo, endereço, filiação, documentos de identificação, contatos telefônicos e informações circunstanciais frequentemente são indispensáveis para a correta formalização da ocorrência. Entretanto, a legitimidade dessa coleta decorre justamente da finalidade institucional que justifica sua obtenção. Conforme destaca Nora (2021), a atividade policial exige o tratamento de dados pessoais como instrumento indispensável à preservação da ordem pública, mas essa necessidade não elimina a obrigação de restringir a coleta ao estritamente necessário para o cumprimento da missão institucional.

Associado à finalidade encontra-se o princípio da necessidade, segundo o qual o tratamento de dados deve limitar-se ao mínimo indispensável para atingir o objetivo pretendido. Em outras palavras, os órgãos públicos devem evitar a coleta excessiva de informações quando estas não forem essenciais para a execução de suas atribuições legais. No contexto dos Boletins de Atendimento da Polícia Militar do Pará, esse princípio impõe aos agentes públicos a responsabilidade de registrar apenas os elementos relevantes para a compreensão dos fatos e para a adoção das providências cabíveis.

A observância do princípio da necessidade contribui significativamente para a redução dos riscos relacionados à exposição indevida de informações pessoais. Quanto maior o volume de dados armazenados sem justificativa concreta, maiores serão as possibilidades de utilização inadequada, compartilhamento indevido ou vazamento de informações. Conforme observa Costa (2024), a minimização dos dados coletados constitui uma das estratégias mais eficazes para fortalecer a segurança informacional das instituições públicas e reduzir potenciais responsabilidades decorrentes de incidentes envolvendo informações pessoais.

A aplicação desses princípios torna-se ainda mais relevante diante da crescente digitalização dos procedimentos operacionais adotados pelas instituições policiais. A utilização de sistemas informatizados para elaboração de registros operacionais ampliou a capacidade de armazenamento e compartilhamento de informações, permitindo que os dados coletados em uma ocorrência sejam rapidamente disponibilizados para diferentes órgãos da administração pública. Embora essa integração represente importante avanço para a eficiência da segurança pública, também exige maior rigor na definição das informações que efetivamente precisam ser registradas e compartilhadas.

A proteção especial conferida a crianças e adolescentes constitui outro exemplo da importância dos princípios da finalidade e da necessidade. O Estatuto da Criança e do Adolescente estabelece regras específicas destinadas à preservação da identidade e da dignidade dos menores envolvidos em procedimentos policiais (Brasil, 1990). Nesses casos, a coleta e o registro das informações devem observar critérios ainda mais restritivos, evitando qualquer exposição desnecessária que possa comprometer o desenvolvimento social, psicológico ou familiar dos envolvidos. A utilização inadequada desses dados pode resultar não apenas em responsabilização administrativa, mas também em violações aos direitos fundamentais assegurados pela legislação protetiva.

Outro aspecto relevante refere-se ao compartilhamento das informações constantes nos Boletins de Atendimento. A finalidade que legitima a coleta dos dados também deve orientar sua transmissão aos demais órgãos envolvidos no sistema de justiça criminal. Informações obtidas durante a atividade policial devem ser encaminhadas exclusivamente por meios institucionais e para autoridades legalmente competentes. O uso de aplicativos não oficiais, grupos informais de mensagens ou qualquer outro canal desprovido de mecanismos adequados de segurança aumenta significativamente os riscos de vazamento e compromete a integridade da cadeia de custódia informacional.

Nesse contexto, torna-se fundamental que a Polícia Militar do Pará desenvolva protocolos internos capazes de orientar seus integrantes quanto à correta aplicação dos princípios da finalidade e da necessidade. A criação de procedimentos operacionais padronizados, associada à realização de treinamentos periódicos, contribui para uniformizar condutas e reduzir interpretações equivocadas acerca do tratamento de dados pessoais no ambiente institucional. Segundo Paulo (2025), a consolidação de programas de governança informacional representa medida indispensável para garantir conformidade legal e eficiência administrativa nas organizações públicas.

Além dos benefícios relacionados à proteção dos cidadãos, a observância desses princípios também fortalece a segurança jurídica dos próprios policiais militares. Quando a coleta e o tratamento das informações ocorrem dentro dos limites legais e institucionais estabelecidos, reduzem-se significativamente os riscos de questionamentos administrativos, disciplinares e judiciais. Dessa forma, a proteção de dados deixa de ser compreendida apenas como obrigação normativa e passa a constituir instrumento de proteção funcional para os agentes responsáveis pela execução das atividades de segurança pública.

O próprio Boletim Geral nº 5/2026 da Polícia Militar do Pará estabelece que os trabalhos científicos produzidos no âmbito da Corporação devem apresentar relevância institucional e contribuir para o aperfeiçoamento das atividades administrativas e operacionais da PMPA. Sob essa perspectiva, a adoção de práticas voltadas à observância dos princípios da finalidade e da necessidade apresenta potencial para fortalecer a gestão das informações institucionais, aprimorar os procedimentos operacionais e reduzir riscos associados ao tratamento inadequado de dados pessoais.

Dessa forma, verifica-se que os princípios da finalidade e da necessidade constituem importantes instrumentos para orientar a elaboração dos Boletins de Atendimento da Polícia Militar do Pará. Sua observância contribui para a proteção dos direitos fundamentais dos cidadãos, fortalece a legitimidade institucional da Corporação e amplia a segurança jurídica dos policiais militares, demonstrando que a eficiência operacional e a proteção de dados pessoais podem coexistir de maneira harmoniosa dentro das atividades de segurança pública.

2.3 A Proteção de Dados como Instrumento de Segurança Jurídica para o Policial Militar

A proteção de dados pessoais tem sido frequentemente associada à defesa dos direitos individuais dos cidadãos, especialmente no que se refere à privacidade, à intimidade e ao controle das informações pessoais. Entretanto, no contexto da segurança pública, essa temática também possui relevante dimensão institucional, uma vez que a adoção de práticas adequadas de tratamento de dados representa importante mecanismo de proteção para os próprios agentes públicos responsáveis pela execução das atividades policiais. No âmbito da Polícia Militar do Pará, a observância dos princípios relacionados à proteção de dados contribui diretamente para a ampliação da segurança jurídica dos policiais militares, reduzindo riscos de responsabilização administrativa, disciplinar, civil e penal decorrentes do tratamento inadequado das informações obtidas durante o serviço.

A atividade policial exige contato permanente com dados pessoais de diversas naturezas. Durante uma única ocorrência, o policial militar pode coletar informações de vítimas, testemunhas, suspeitos, adolescentes, familiares e demais envolvidos, registrando elementos que posteriormente integrarão Boletins de Atendimento, relatórios operacionais, comunicações internas e procedimentos administrativos. A correta utilização dessas informações torna-se fundamental para garantir a legitimidade da atuação estatal e preservar a credibilidade institucional da Corporação. Nesse cenário, a proteção de dados deve ser compreendida não apenas como obrigação legal, mas também como ferramenta de proteção funcional para os integrantes da Polícia Militar.

14

A segurança jurídica pode ser compreendida como a garantia de que a atuação do agente público ocorrerá dentro de parâmetros previamente estabelecidos pela legislação e pelos regulamentos institucionais, reduzindo incertezas e proporcionando previsibilidade quanto às consequências de seus atos. Quando existem normas claras sobre coleta, armazenamento, compartilhamento e utilização de dados pessoais, os policiais militares passam a dispor de referências objetivas para orientar suas decisões durante o exercício da atividade operacional. Conforme observa Carneiro (2023), a existência de mecanismos de governança informacional contribui para reduzir falhas procedimentais e fortalecer a conformidade institucional no tratamento das informações.

A crescente digitalização dos sistemas de segurança pública ampliou significativamente a quantidade de dados disponíveis aos agentes policiais. Sistemas de consulta de antecedentes, bancos de dados integrados, registros de ocorrências, plataformas de inteligência e aplicativos institucionais passaram a fazer parte da rotina operacional das corporações. Embora essas

ferramentas representem importante avanço tecnológico, também aumentam a responsabilidade dos usuários quanto à correta utilização das informações acessadas. O uso inadequado dos sistemas corporativos pode gerar consequências administrativas graves, especialmente quando as consultas são realizadas por interesse pessoal, curiosidade ou finalidade incompatível com o serviço público.

Nesse contexto, a observância dos princípios da proteção de dados funciona como mecanismo preventivo contra condutas que possam resultar em responsabilização funcional. O policial que realiza consultas exclusivamente para fins institucionais, registra apenas as informações necessárias à ocorrência e compartilha dados por canais oficiais atua dentro dos limites estabelecidos pela legislação e pelos regulamentos internos. Essa postura reduz significativamente os riscos de questionamentos futuros e fortalece a legitimidade das ações desenvolvidas durante o serviço operacional.

A proteção de dados também se relaciona diretamente com a preservação da cadeia de custódia informacional. As informações coletadas no local da ocorrência frequentemente servem de base para investigações criminais, processos administrativos e procedimentos judiciais. Qualquer alteração indevida, compartilhamento inadequado ou perda desses dados pode comprometer a confiabilidade das informações e gerar prejuízos à persecução penal e à própria atividade administrativa. Segundo Josino (2021), a proteção adequada dos dados constitui requisito indispensável para assegurar a integridade das informações utilizadas pelos órgãos de segurança pública.

A necessidade de observância rigorosa desses procedimentos torna-se ainda mais evidente diante da crescente preocupação social com a privacidade e a proteção das informações pessoais. Casos de vazamentos de dados envolvendo órgãos públicos têm gerado repercussões negativas, ações judiciais e questionamentos acerca da capacidade estatal de proteger as informações sob sua responsabilidade. Nesse cenário, a adoção de protocolos institucionais voltados à proteção de dados contribui para fortalecer a confiança da sociedade nas instituições de segurança pública e para preservar a imagem da Polícia Militar do Pará.

A doutrina especializada tem destacado que a proteção de dados deve ser compreendida como componente essencial da governança pública contemporânea. Nesse sentido, Paulo (2025) afirma:

[...] a governança de dados no setor público não pode ser tratada apenas como exigência tecnológica ou burocrática. Trata-se de instrumento estratégico para assegurar transparência, integridade institucional e responsabilização adequada dos agentes

envolvidos no tratamento das informações. A implementação de políticas claras de controle de acesso, rastreabilidade das operações realizadas nos sistemas corporativos, capacitação permanente dos servidores e monitoramento contínuo dos fluxos informacionais contribui significativamente para a redução de incidentes de segurança. Além disso, fortalece a confiança da sociedade nas instituições públicas e promove maior segurança jurídica para os profissionais que desempenham suas funções de acordo com os procedimentos legalmente estabelecidos, reduzindo riscos de responsabilização decorrentes de falhas operacionais ou administrativas relacionadas ao tratamento inadequado de dados pessoais (Paulo, 2025, p. 87).

A reflexão apresentada demonstra que a proteção de dados não deve ser compreendida como elemento externo à atividade policial, mas como parte integrante dos mecanismos de gestão e controle institucional. A adoção de boas práticas relacionadas ao tratamento das informações contribui para a prevenção de incidentes, para a preservação da legalidade administrativa e para o fortalecimento da segurança jurídica dos profissionais responsáveis pela execução das atividades de segurança pública.

No âmbito da Polícia Militar do Pará, a implementação de programas permanentes de capacitação sobre proteção de dados pode representar importante estratégia de fortalecimento institucional. A inclusão da temática nos cursos de formação, habilitação e aperfeiçoamento profissional possibilita que os policiais militares compreendam os limites legais relacionados ao tratamento das informações e desenvolvam competências adequadas para utilização dos sistemas corporativos. Essa medida encontra respaldo nos critérios de relevância institucional previstos pelo Boletim Geral nº 5/2026, que valoriza pesquisas capazes de contribuir para o aperfeiçoamento das atividades administrativas e operacionais da Corporação.

Além da capacitação, a criação de protocolos específicos para compartilhamento de dados entre a Polícia Militar, a Polícia Civil e demais órgãos integrantes do sistema de justiça criminal pode reduzir significativamente os riscos de vazamentos e falhas procedimentais. A utilização exclusiva de sistemas oficiais, associada ao controle de acessos e à rastreabilidade das operações realizadas, fortalece a cadeia de custódia das informações e amplia a confiabilidade dos registros produzidos pela instituição.

Dessa forma, verifica-se que a proteção de dados pessoais transcende a simples observância de normas legais, constituindo importante instrumento de fortalecimento institucional e de proteção funcional para os integrantes da Polícia Militar do Pará. A adoção de práticas alinhadas aos princípios da finalidade, necessidade, segurança e responsabilidade contribui para a preservação dos direitos fundamentais dos cidadãos, para a redução dos riscos de responsabilização administrativa e para o aumento da segurança jurídica dos policiais militares. Nesse contexto, a proteção de dados revela-se elemento indispensável para a

construção de uma segurança pública moderna, eficiente e compatível com as exigências contemporâneas da administração pública e da defesa social.

3 METODOLOGIA

A presente pesquisa caracteriza-se como aplicada, por buscar produzir conhecimentos voltados à solução de problemas concretos relacionados ao tratamento de dados pessoais na elaboração dos Boletins de Atendimento e nos procedimentos administrativos disciplinares e investigatórios da Polícia Militar do Pará (PMPA). Quanto aos objetivos, classifica-se como descritiva e exploratória. É descritiva por analisar os procedimentos de tratamento de dados pessoais no contexto da atividade policial militar e exploratória por abordar temática ainda pouco desenvolvida na literatura nacional, especialmente no que se refere à aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) no âmbito da Polícia Militar.

Adotou-se abordagem qualitativa, considerada a mais adequada para compreender os aspectos jurídicos, institucionais e operacionais relacionados à proteção de dados pessoais na segurança pública. Conforme Marconi e Lakatos (2021), a pesquisa qualitativa possibilita interpretar fenômenos complexos a partir da análise de documentos, normas e produções científicas, permitindo compreender as relações entre o ordenamento jurídico e a realidade institucional. A opção por esse método justifica-se pela natureza do objeto investigado, que exige análise interpretativa da legislação, da doutrina e dos procedimentos administrativos adotados pela PMPA.

17

Quanto aos procedimentos técnicos, realizou-se pesquisa bibliográfica e documental. A pesquisa bibliográfica fundamentou-se na análise de livros, artigos científicos, dissertações, teses e demais publicações especializadas sobre proteção de dados pessoais, segurança pública, governança da informação e atividade policial. A pesquisa documental concentrou-se na análise da Constituição da República Federativa do Brasil de 1988, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), da Lei nº 8.069/1990 (Estatuto da Criança e do Adolescente), do Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Persecução Penal, bem como de normas e documentos institucionais da Polícia Militar do Pará relacionados ao tratamento de informações e à atividade administrativa.

O levantamento bibliográfico foi realizado nas bases Google Scholar, SciELO, Portal de Periódicos CAPES e Biblioteca Digital Brasileira de Teses e Dissertações (BDTD), contemplando publicações produzidas entre 2018 e 2026, período correspondente à promulgação

da LGPD e ao desenvolvimento das principais discussões científicas sobre sua aplicação na segurança pública. Foram utilizados, isoladamente e de forma combinada, os descritores: "Lei Geral de Proteção de Dados", "LGPD", "proteção de dados pessoais", "segurança pública", "atividade policial militar", "Boletim de Atendimento", "governança de dados", "Polícia Militar" e "segurança da informação".

Como critérios de inclusão, foram selecionadas obras que abordassem diretamente a proteção de dados pessoais, a governança informacional, a atividade policial, a segurança pública e os impactos da LGPD no setor público. Foram excluídas publicações duplicadas, estudos sem relação direta com o objeto da pesquisa, trabalhos exclusivamente voltados ao tratamento de dados no setor privado e documentos que não apresentassem fundamentação técnico-científica compatível com os objetivos deste estudo.

Após a seleção das fontes, procedeu-se à leitura exploratória, seletiva e analítica do material, identificando conceitos, fundamentos jurídicos, entendimentos doutrinários e propostas relacionadas ao tratamento de dados pessoais na atividade policial militar. Posteriormente, realizou-se análise interpretativa e comparativa das informações obtidas, buscando estabelecer relações entre a legislação vigente, a literatura especializada e os procedimentos administrativos desenvolvidos pela Polícia Militar do Pará.

18

A análise dos dados ocorreu por meio da interpretação sistemática da legislação e da análise de conteúdo das obras selecionadas, permitindo identificar convergências entre os princípios da proteção de dados pessoais e as atribuições constitucionais da Polícia Militar. A partir dessa análise, foram discutidos os impactos da LGPD na elaboração dos Boletins de Atendimento, no compartilhamento de informações entre os órgãos do sistema de justiça criminal e nos procedimentos administrativos disciplinares, bem como propostas voltadas ao fortalecimento da governança informacional e da segurança jurídica institucional.

Por fim, os resultados foram organizados de forma a demonstrar que a adoção de práticas compatíveis com os princípios da proteção de dados pessoais pode contribuir para o aperfeiçoamento da gestão das informações, para a proteção dos direitos fundamentais dos cidadãos e para o fortalecimento institucional da Polícia Militar do Pará, sem comprometer a eficiência das atividades de segurança pública.

4 RESULTADOS E DISCUSSÃO

A análise da legislação, da doutrina especializada e dos normativos institucionais evidencia que a proteção de dados pessoais constitui importante instrumento de fortalecimento da atuação da Polícia Militar do Pará (PMPA). Embora a Lei Geral de Proteção de Dados Pessoais estabeleça regime jurídico diferenciado para as atividades de segurança pública, verificou-se que princípios como finalidade, necessidade, adequação, segurança e responsabilização podem orientar o tratamento das informações produzidas durante o atendimento de ocorrências e a condução dos procedimentos administrativos internos.

Os resultados demonstram que os Boletins de Atendimento representam um dos principais instrumentos de tratamento de dados pessoais na atividade policial militar, reunindo informações referentes a vítimas, testemunhas, investigados e demais envolvidos nas ocorrências. Em razão da natureza dessas informações, sua coleta, armazenamento e compartilhamento devem observar critérios compatíveis com a finalidade institucional e com a proteção dos direitos fundamentais.

Esse entendimento converge com Carneiro (2023), ao afirmar que a governança de dados constitui mecanismo essencial para reduzir vulnerabilidades informacionais e fortalecer a conformidade institucional. Da mesma forma, Costa (2024) sustenta que a observância dos princípios da proteção de dados contribui para minimizar riscos jurídicos decorrentes do tratamento inadequado das informações pelos órgãos de segurança pública.

19

Outro aspecto identificado refere-se à inexistência de protocolos específicos de governança informacional direcionados às peculiaridades da atividade policial militar. Embora a PMPA disponha de procedimentos administrativos e operacionais consolidados, a pesquisa evidenciou que a definição de diretrizes específicas para o tratamento de dados pessoais tende a ampliar a segurança jurídica dos agentes públicos e a uniformizar práticas institucionais. Esse resultado encontra respaldo em Josino (2021), que defende a adoção de mecanismos de controle compatíveis com os princípios constitucionais de proteção dos dados pessoais, mesmo nas hipóteses de tratamento relacionadas à segurança pública.

A pesquisa também permitiu verificar que o compartilhamento de informações entre a Polícia Militar, a Polícia Civil, o Ministério Público e o Poder Judiciário exige mecanismos que assegurem a integridade, a confidencialidade e a rastreabilidade dos dados durante todo o fluxo informacional. Nesse contexto, Paulo (2025) destaca que programas estruturados de governança de dados reduzem riscos de vazamentos, fortalecem a transparência institucional e ampliam a segurança jurídica dos agentes públicos.

No que se refere aos grupos vulneráveis, observou-se que a proteção das informações relativas a crianças e adolescentes demanda atenção especial em razão das garantias estabelecidas pelo Estatuto da Criança e do Adolescente. A adoção de protocolos específicos para esses casos contribui para evitar exposições indevidas e assegurar a proteção integral prevista na legislação brasileira.

Os resultados obtidos permitem concluir que a adoção de procedimentos alinhados aos princípios da proteção de dados produz benefícios institucionais relevantes, conforme sintetizado no gráfico 1

A implementação de práticas de governança informacional e de protocolos voltados à proteção de dados pessoais tende a fortalecer a atuação institucional da Polícia Militar do Pará, ampliar a segurança jurídica dos policiais militares e assegurar maior conformidade com os princípios constitucionais aplicáveis à Administração Pública. Os resultados também demonstram que a proteção de dados não representa obstáculo à atividade policial, mas instrumento de aperfeiçoamento da gestão pública e de fortalecimento da confiança social nas instituições de segurança.

Gráfico 1 - Benefícios esperados da aplicação da LGPD na PMPA



Fonte: Elaborado pelo autor (2026), a partir dos dados obtidos na revisão bibliográfica e documental da pesquisa.

Os resultados da pesquisa confirmam a hipótese inicialmente proposta, demonstrando que a adoção de práticas alinhadas aos princípios da proteção de dados pessoais fortalece a

segurança jurídica dos policiais militares, preserva os direitos fundamentais dos cidadãos e contribui para o aperfeiçoamento institucional da Polícia Militar do Pará. A análise evidenciou que a implementação de medidas de governança informacional reduz riscos de vazamentos de dados, amplia a confiabilidade dos registros e favorece a eficiência da gestão das informações produzidas durante as atividades policiais.

Entre as principais medidas identificadas destacam-se a criação de protocolos específicos para o compartilhamento de dados entre os órgãos do sistema de segurança pública, a utilização prioritária de sistemas corporativos oficiais, o fortalecimento dos mecanismos de controle de acesso e auditoria, bem como a elaboração de Procedimentos Operacionais Padrão voltados ao tratamento de dados pessoais. A pesquisa também evidenciou a importância da capacitação permanente dos policiais militares em proteção de dados e segurança da informação, promovendo maior uniformidade dos procedimentos e reduzindo falhas decorrentes do uso inadequado das informações.

Outro aspecto relevante refere-se à necessidade de proteção reforçada dos dados de crianças e adolescentes, mediante protocolos específicos que assegurem o sigilo e restrinjam o acesso às informações. Constatou-se, ainda, que a consolidação de uma política institucional de governança de dados fortalece a gestão informacional, amplia a confiança da sociedade na Corporação e contribui para a modernização administrativa. Assim, a proteção de dados pessoais revela-se elemento estratégico para conciliar eficiência operacional, segurança jurídica e respeito aos direitos fundamentais no âmbito da segurança pública.

5 CONSIDERAÇÕES FINAIS

A presente pesquisa analisou a aplicação da Lei Geral de Proteção de Dados Pessoais na elaboração dos Boletins de Atendimento e nos procedimentos administrativos disciplinares e investigatórios da Polícia Militar do Pará, buscando verificar de que forma os princípios da proteção de dados podem contribuir para a segurança jurídica dos policiais militares e para o fortalecimento institucional da Corporação.

Os resultados demonstraram que, embora a Lei nº 13.709/2018 estabeleça tratamento diferenciado para as atividades de segurança pública, os princípios da finalidade, necessidade, adequação, segurança e responsabilização permanecem como importantes parâmetros para orientar o tratamento de dados pessoais no âmbito da Administração Pública. Sua observância

favorece a proteção dos direitos fundamentais dos cidadãos, reduz riscos decorrentes do uso inadequado das informações e fortalece a legitimidade da atuação estatal.

Também se verificou que os Boletins de Atendimento constituem instrumentos centrais no tratamento de dados pessoais durante a atividade policial, exigindo procedimentos compatíveis com a proteção da privacidade, a segurança da informação e a preservação da cadeia de custódia informacional. Da mesma forma, os procedimentos administrativos internos demandam mecanismos de governança capazes de assegurar controle, rastreabilidade e conformidade no tratamento das informações.

A hipótese inicialmente formulada foi confirmada, evidenciando que a implementação de protocolos institucionais voltados à proteção de dados contribui para ampliar a segurança jurídica dos policiais militares, aperfeiçoar a gestão das informações e fortalecer a atuação da Polícia Militar do Pará, sem comprometer a eficiência das atividades de preservação da ordem pública.

Entre as medidas identificadas como prioritárias destacam-se a elaboração de protocolos específicos para o tratamento e compartilhamento de dados pessoais, o fortalecimento dos mecanismos de controle de acesso aos sistemas corporativos, a capacitação permanente dos profissionais de segurança pública e a consolidação de políticas institucionais de governança informacional.

Como contribuição científica, este estudo amplia a discussão sobre a aplicação da LGPD no contexto da segurança pública, especialmente no âmbito da Polícia Militar do Pará, área ainda pouco explorada pela literatura especializada. Os resultados podem subsidiar futuras pesquisas e contribuir para o aperfeiçoamento de práticas administrativas e operacionais relacionadas à proteção de dados pessoais nas instituições policiais.

Conclui-se, portanto, que a proteção de dados pessoais deve ser compreendida como instrumento de fortalecimento institucional, capaz de conciliar eficiência operacional, segurança jurídica e respeito aos direitos fundamentais. A adoção de políticas de governança informacional representa medida estratégica para a modernização da gestão pública e para o aprimoramento das atividades desenvolvidas pelas instituições de segurança pública.

REFERÊNCIAS

ARAS, Vladimir. *A aplicabilidade da LGPD às atividades de segurança pública e de persecução penal*. 2024. Disponível em: <https://vladimiraras.blog>. Acesso em: 30 maio 2026.

ARAS, Vladimir. Proteção de dados pessoais em atividades de inteligência, segurança pública e processo penal brasileiro. *Revista Brasileira de Direito da Inteligência*, v. 5, n. 1, 2025.

BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil*. Brasília, DF: Senado Federal, 1988.

BRASIL. *Lei nº 8.069, de 13 de julho de 1990*. Estatuto da Criança e do Adolescente. Diário Oficial da União: Brasília, DF, 16 jul. 1990.

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

BRASIL. Câmara dos Deputados. Comissão de Juristas. *Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Persecução Penal*. Brasília, DF, 2020.

CARNEIRO, Plínio Maria. *A implementação da Lei Geral de Proteção de Dados Pessoais na governança do processo de pagamento de pessoal do comando do exército*. 2023.

COSTA, Rafael de Lima. Lei Geral de Proteção de Dados e a atividade de segurança pública: conflitos, limites e perspectivas jurídicas. *RECIMA21 - Revista Científica Multidisciplinar*, v. 5, n. 3, 2024.

D'OLIVEIRA, N. P. C. et al. Lei Geral de Proteção de Dados (LGPD): a relação entre informação, privacidade e proteção de dados. *Revista Digital de Biblioteconomia e Ciência da Informação*, v. 22, 2024. 23

JOSINO, Clarissa Nogueira. *Dados pessoais, segurança pública e investigação criminal: um panorama da proteção de dados e seus desafios regulatórios no Brasil*. Fortaleza: Universidade Federal do Ceará, 2021.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. *Fundamentos de metodologia científica*. 9. ed. São Paulo: Atlas, 2021.

NASCIMENTO, Heyder; ARAÚJO, Adrilayne; RAMOS, Edson. Zonas de abandono institucional: fragmentação dos mecanismos de resposta à violência doméstica perpetrada por policiais militares no Pará. *SSRN Electronic Journal*, 2026.

NORA, Heloísa Daniela. *Tratamento de dados pessoais e segurança pública: uma análise das polícias judiciárias paranaenses*. Curitiba, 2021.

PAULO, Francisco José Costa de. A governança pública na proteção de dados pessoais: desafios para as instituições policiais. *RECIMA21 - Revista Científica Multidisciplinar*, v. 6, n. 2, 2025.

SILVEIRA, Camila Rodrigues da et al. *Violência contra a mulher e proteção de dados: a padronização dos boletins de ocorrência à luz da Lei Geral de Proteção de Dados*. 2025.

SOUZA, Stefano Mozart P. Canedo de. *Possíveis impactos da LGPD na atividade de inteligência brasileira*. Brasília: Escola Nacional de Administração Pública, 2020.

GIL, Antonio Carlos. *Métodos e técnicas de pesquisa social*. 7. ed. São Paulo: Atlas, 2019.

POLÍCIA MILITAR DO PARÁ. *Boletim Geral nº 5, de 9 de janeiro de 2026*. Belém: PMPA, 2026.