
A APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) NOS SISTEMAS DE MONITORAMENTO E INTELIGÊNCIA DA SEGURANÇA PÚBLICA MUNICIPAL DE JATAÍ/GO: DESAFIOS JURÍDICOS E A PROTEÇÃO DOS DIREITOS FUNDAMENTAIS

Jackson Porn Martins ¹

Cyro Morioka²

RESUMO

Este artigo científico analisa a aplicação da Lei Geral de Proteção de Dados (LGPD) nos sistemas de monitoramento e inteligência da segurança pública municipal de Jataí, Goiás, considerando os desafios decorrentes da utilização de tecnologias voltadas à prevenção e repressão da criminalidade. A pesquisa explora os aspectos jurídicos relacionados à coleta, ao tratamento, ao armazenamento, ao compartilhamento e à proteção de dados pessoais no âmbito das atividades desenvolvidas pelos órgãos municipais de segurança pública, examinando a compatibilidade dessas práticas com os princípios, direitos e garantias estabelecidos pela Lei nº 13.709/2018. O estudo também aborda a proteção dos direitos fundamentais dos cidadãos, especialmente os direitos à privacidade, à intimidade, à liberdade e à autodeterminação informativa, diante da crescente utilização de sistemas de videomonitoramento, bancos de dados integrados e ferramentas de inteligência.

A pesquisa adota abordagem qualitativa, baseada em revisão bibliográfica, análise da legislação vigente, doutrina especializada e jurisprudência pertinente, buscando compreender os limites e as possibilidades da aplicação da LGPD no contexto da segurança pública municipal. Além disso, investiga as exceções previstas na própria legislação para atividades de segurança pública e discute a necessidade de harmonização entre a eficiência das ações estatais e a preservação dos direitos fundamentais. Busca-se identificar as melhores práticas para o tratamento de dados pessoais, os principais desafios enfrentados pela administração pública municipal e os potenciais gargalos para a conformidade com a LGPD, especialmente quanto à governança de dados, à segurança da informação, à transparência, ao controle de acesso e à responsabilização dos agentes públicos. Ao final, propõem-se reflexões sobre a necessidade de regulamentação específica para o setor, o fortalecimento de mecanismos de fiscalização e controle, bem como a capacitação contínua dos servidores envolvidos nas atividades de monitoramento e inteligência, visando assegurar maior segurança jurídica, eficiência administrativa e proteção dos direitos dos cidadãos.

Palavras-chave: LGPD. Segurança Pública Municipal. Monitoramento Inteligente. Direitos Fundamentais. Jataí-GO.

ABSTRACT

This scientific article analyzes the application of the Brazilian General Data Protection Law (LGPD) in the monitoring and intelligence systems of municipal public security in Jataí, Goiás, considering the legal challenges arising from the use of technologies aimed at crime prevention and law enforcement. The research examines the legal aspects related to the

Endereço: Av. Prof. Edvan Assis Melo, 1075 - Centro, Jataí - GO, 75800-001.

collection, processing, storage, sharing, and protection of personal data within the activities carried out by municipal public security agencies, assessing the compatibility of these practices with the principles, rights, and guarantees established by Law No. 13,709/2018. The study also addresses the protection of citizens' fundamental rights, particularly the rights to privacy, intimacy, freedom, and informational self-determination, in light of the increasing use of video surveillance systems, integrated databases, and intelligence tools.

The research adopts a qualitative approach based on a literature review, analysis of the applicable legislation, specialized legal doctrine, and relevant case law, seeking to understand the limits and possibilities of applying the LGPD within the context of municipal public security. Furthermore, it examines the legal exceptions established by the LGPD for public security activities and discusses the need to balance the effectiveness of governmental actions with the protection of fundamental rights. The study seeks to identify best practices for the processing of personal data, the main challenges faced by municipal public administration, and potential bottlenecks in achieving compliance with the LGPD, particularly regarding data governance, information security, transparency, access control, and the accountability of public officials. Finally, it proposes reflections on the need for specific regulations for the public security sector, the strengthening of oversight and control mechanisms, and the continuous training of public servants involved in monitoring and intelligence activities, aiming to ensure greater legal certainty, administrative efficiency, and the effective protection of citizens' fundamental rights.

Keywords: LGPD. Municipal Public Security. Intelligent Monitoring. Fundamental Rights. Jataí-GO.

1. INTRODUÇÃO

A transformação digital impulsionou a segurança pública, tornando as tecnologias de vigilância e análise de dados ferramentas cruciais na prevenção e repressão criminal. Sistemas de videomonitoramento, reconhecimento facial e inteligência de dados oferecem capacidades significativas para mapear atividades suspeitas e otimizar recursos. Contudo, essa expansão na

¹ Acadêmico de Direito da Faculdade de Gestão e Inovação – FGI. Jackson Porn Martins

² Prof. Orientador: Cyro Morioka

coleta e processamento de informações pessoais por órgãos estatais levanta preocupações substanciais quanto à salvaguarda da privacidade e de outros direitos fundamentais dos cidadãos.

Neste cenário, a Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018) estabelece um marco regulatório essencial para o tratamento de dados pessoais no Brasil. Inspirada em modelos internacionais, como o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, a LGPD visa garantir a privacidade e os direitos fundamentais, ditando regras para a coleta, armazenamento, uso, compartilhamento e descarte de dados pessoais.

À vista disso, o presente trabalho investiga a aplicação da LGPD no âmbito dos sistemas de monitoramento e inteligência da segurança pública municipal de Jataí, Goiás. A escolha do município se justifica pela sua relevância regional e pela crescente adoção de tecnologias de vigilância em seu território. O objetivo primordial é delinear os desafios jurídicos que a LGPD impõe a esses sistemas e analisar como sua implementação efetiva contribui para a proteção dos direitos fundamentais.

Nesse escopo, a segurança pública, constitucionalmente definida como dever do Estado e direito e responsabilidade de todos (Art. 144 da CF/88), tem se valido cada vez mais de ferramentas tecnológicas que geram e tratam grandes volumes de dados. No entanto, a ausência de uma legislação específica para o tratamento de dados pessoais para fins de segurança pública (o chamado “Artigo 4º” da LGPD, que trata da exceção de segurança pública e defesa nacional) cria uma lacuna normativa que precisa ser preenchida pela interpretação sistemática da lei e dos princípios constitucionais.

A relevância deste estudo reside na necessidade de fornecer um guia prático e teórico para a atuação municipal, que está na linha de frente da implementação dessas tecnologias. A conformidade com a LGPD não é apenas uma obrigação legal, mas um mecanismo de legitimação da atuação estatal, garantindo que a busca pela segurança não se traduza em um Estado de vigilância desproporcional. Assim, a importância desta pesquisa consolida-se na perspectiva de assegurar que a modernização administrativa de Jataí caminhe lado a lado com a segurança jurídica.

Diante dessas considerações, emerge o problema que orienta a presente pesquisa: quais são os principais desafios jurídicos e operacionais impostos pela Lei Geral de Proteção de Dados (LGPD) aos sistemas de monitoramento e inteligência da segurança pública

municipal de Jataí/GO, e como a conformidade com a lei pode ser alcançada para garantir a proteção dos direitos fundamentais?

O objetivo geral consiste em analisar a aplicação da LGPD nos sistemas de monitoramento e inteligência da segurança pública municipal de Jataí, Goiás, e propor diretrizes para a conformidade legal e a proteção dos direitos fundamentais. Como objetivos específicos, pretende-se: (i) examinar os princípios e as bases legais da LGPD aplicáveis ao tratamento de dados pelo Poder Público Municipal na área de segurança; (ii) analisar as tecnologias de monitoramento e inteligência utilizadas em Jataí sob a ótica da LGPD, com foco no tratamento de dados pessoais sensíveis (biométricos); (iii) discutir a colisão entre o interesse público na segurança e os direitos fundamentais de privacidade, intimidade e não discriminação; e (iv) propor medidas de governança de dados (RIPD, DPO e *Accountability*) que garantam a conformidade e a autenticidade da atuação municipal.

Com relação à metodologia, a investigação contemplou uma abordagem qualitativa e exploratória, utilizando o método de pesquisa bibliográfica e documental. O estudo é classificado como exploratório, pois busca proporcionar uma visão aprofundada sobre um tema complexo e relativamente novo no contexto municipal brasileiro: a intersecção entre LGPD e segurança pública. A natureza exploratória permite a formulação de hipóteses e a proposição de soluções para os desafios identificados.

O método de abordagem principal é o dedutivo, partindo da análise da legislação geral (LGPD e Constituição Federal) e da doutrina especializada para a aplicação e interpretação no caso específico da segurança pública municipal de Jataí. Portanto, as técnicas de pesquisa utilizadas incluem duas espécies de pesquisa, a saber, pesquisa bibliográfica, com levantamento de literatura especializada (livros, artigos científicos, teses e dissertações) sobre LGPD, proteção de dados no setor público, segurança pública e tecnologias de vigilância; e a pesquisa documental, a partir da análise da Lei nº 13.709/2018 (LGPD), da Constituição Federal de 1988, de resoluções e guias da Autoridade Nacional de Proteção de Dados (ANPD) e de jurisprudência relevante (STF e tribunais superiores) sobre o tema.

Esta análise do conteúdo está estruturada em três eixos principais: (i) Eixo Normativo: Focado nos princípios e bases legais da LGPD aplicáveis ao Poder Público; (ii) Eixo Tecnológico: Focado na natureza dos dados tratados pelos sistemas de monitoramento (videomonitoramento, reconhecimento facial e inteligência) e seus riscos; e (iii) Eixo Constitucional: Focado na harmonização entre o dever de segurança pública e a proteção dos direitos fundamentais (privacidade, liberdade e não discriminação). A combinação desses

eixos permite uma avaliação crítica e propositiva dos desafios de conformidade do município de Jataí.

Também, trata-se de uma pesquisa de campo (*in loco*), realizada com base na observação direta e levantamento de informações junto aos sistemas de monitoramento e às estruturas de segurança pública municipal de Jataí/GO, com o objetivo de compreender a dinâmica operacional das tecnologias utilizadas, os fluxos de tratamento de dados pessoais e os mecanismos administrativos adotados pelo município.

O percurso metodológico *in loco* permitiu relacionar os referenciais teóricos e normativos da LGPD com a realidade prática da atuação municipal, contribuindo para uma análise crítica sobre conformidade, riscos e proteção de direitos fundamentais.

Desta maneira, a fim de atingir os objetivos propostos, este trabalho encontra-se estruturado em capítulos sequenciais: inicialmente, o Capítulo 2 discute-se a LGPD na segurança pública, seguido, no Capítulo 3, por uma análise do tratamento dos dados pessoais pelo Poder Público. Na sequência, o Capítulo 4 detalha o sistema de monitoramento e a inteligência. No Capítulo 5, a LGPD e a proteção dos direitos fundamentais, já no Capítulo 6, os desafios jurídicos na aplicação da LGPD. Por fim, no Capítulo 7, tem-se as propostas de governança na aplicação da LGPD no contexto de Jataí, seguido pelas considerações finais. Assim, a combinação da pesquisa bibliográfica, documental e de campo permitiu uma análise abrangente da aplicação da Lei Geral de Proteção de Dados no contexto da segurança pública municipal de Jataí/GO. A integração entre os referenciais teóricos, os fundamentos normativos e a realidade operacional observada possibilitou identificar os desafios jurídicos, técnicos e institucionais relacionados ao tratamento de dados pessoais nos sistemas de monitoramento e inteligência. Desse modo, a metodologia adotada fornece o suporte necessário para a análise crítica desenvolvida nos capítulos subsequentes, permitindo avaliar o grau de conformidade das práticas municipais com a LGPD e propor medidas de governança capazes de conciliar a eficiência das políticas de segurança pública com a proteção dos direitos fundamentais dos cidadãos, especialmente a privacidade, a intimidade, a liberdade e a autodeterminação informativa.

2. A LGPD E OS PRINCÍPIOS DO TRATAMENTO DE DADOS NA SEGURANÇA PÚBLICA

A LGPD fundamenta-se em um conjunto de princípios que devem orientar todas as operações de tratamento de dados, sendo que sua compreensão aprofundada é indispensável para a aplicação no contexto da segurança pública. Para Doneda (2019), o tratamento de

dados pelo poder público deve observar parâmetros rigorosos de legitimidade e transparência, especialmente quando envolve atividades sensíveis como investigação criminal e segurança pública.

Diante disso, é importante destacar os princípios da LGPD, a saber, a finalidade, a necessidade e a adequação, essenciais para limitar o tratamento de dados ao estritamente necessário. Em sistemas de monitoramento municipal, isso significa que a coleta de imagens e informações deve estar vinculada a objetivos específicos, legítimos e transparentes. O poder público não pode utilizar dados pessoais para finalidades genéricas, indeterminadas ou incompatíveis com o escopo da segurança pública, sob pena de violar a proporcionalidade, princípio amplamente debatido pela doutrina, como aponta Brum (2025). Diante disso, é importante destacar os princípios da LGPD essenciais para limitar o tratamento de dados ao estritamente necessário.

A atuação do Poder Público Municipal, especialmente na área de segurança, deve ser pautada pelos dez princípios da LGPD, denominados de princípios fundamentais, que funcionam como balizadores éticos e legais para o uso de dados pessoais, conforme sintetizados na Tabela 1 a seguir:

Princípio	Descrição e Aplicação na Segurança Pública
Finalidade	Os dados devem ser coletados para propósitos legítimos, específicos e explícitos. Na segurança pública, a finalidade deve ser claramente definida (ex.: prevenção de crimes específicos), evitando a coleta genérica sem propósito concreto.
Adequação	Compatibilidade entre o tratamento de dados e as finalidades. Dados de segurança pública não podem ser utilizados para fins diversos (ex.: comerciais) sem base legal específica.
Necessidade	O tratamento de dados deve ser limitado ao mínimo indispensável para o alcance das finalidades. Exige questionar se a coleta é estritamente essencial para a prevenção ou repressão de crimes.

Livre Acesso	Garante ao titular o direito de acesso facilitado e gratuito sobre a totalidade de seus dados tratados.
Qualidade dos Dados	Assegura que os dados sejam exatos, íntegros, atualizados e relevantes. Dados incorretos podem levar a decisões equivocadas e à violação de direitos.
Transparência	Imposição de fornecer informações claras, precisas e acessíveis sobre o tratamento de dados. Em sistemas de vigilância, exige sinalização adequada e políticas de privacidade claras.
Segurança	Exige a adoção de medidas técnicas e administrativas para proteger os dados contra acessos não autorizados, perda, destruição ou alteração. Requisito crítico para dados sensíveis manuseados na segurança pública.
Prevenção	Adoção de medidas para evitar a ocorrência de danos em virtude do tratamento de dados pessoais, antecipando riscos e implementando salvaguardas.
Não Discriminação	Veda a realização de qualquer discriminação com base na origem dos dados ou na finalidade do tratamento, evitando que sistemas de inteligência reproduzam vieses.
Responsabilização e Prestação de Contas	O agente de tratamento (o município) deve ser capaz de demonstrar a observância e o cumprimento das normas de proteção de dados, documentando processos e políticas.

Tabela 1 – Princípios da LGPD e sua aplicação na Segurança Pública

2.1. O Binômio Necessidade-Proporcionalidade

Dentre os princípios, o binômio Necessidade-Proporcionalidade assume um papel central no contexto da segurança pública municipal. A LGPD exige que o tratamento de dados seja limitado ao estritamente necessário para o alcance da finalidade (necessidade). No caso de Jataí, cidade localizada no sudoeste do estado de Goiás, isso implica que o sistema de

monitoramento deve ser justificado pela real necessidade de segurança, e não por uma coleta indiscriminada.

A proporcionalidade, embora não seja um princípio autônomo na LGPD, está intrinsecamente ligada à necessidade e é um conceito fundamental do Direito Administrativo e Constitucional. Ela exige que o benefício social gerado pela coleta de dados (aumento da segurança) seja proporcional e se sobreponha aos potenciais riscos e à invasão da privacidade. O uso de tecnologias invasivas, como o reconhecimento facial, deve passar por um teste rigoroso de proporcionalidade, questionando se o mesmo resultado poderia ser alcançado por meios menos intrusivos.

2.2. A Importância da Transparência e da Responsabilização

A Transparência é vital para a legitimidade da atuação estatal. O cidadão deve ter clareza sobre quais dados estão sendo coletados, por quem e para qual propósito. A ausência de transparência em sistemas de vigilância pode gerar desconfiança e violar o direito fundamental à informação.

A Responsabilização e a Prestação de Contas (*Accountability*) impõem ao município o dever de demonstrar que todas as medidas de conformidade foram adotadas. Isso não se limita a ter políticas no papel, mas a comprovar a eficácia dessas políticas, por meio de auditorias, registros de tratamento e, principalmente, a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD).

2.3. Bases Legais Aplicáveis ao Tratamento de Dados pelo Poder Público

A LGPD estabelece bases legais específicas para o tratamento de dados pelo Poder Público, listadas no Art. 7º e detalhadas no Art. 23. Diferentemente do setor privado, o Poder Público não pode utilizar o “legítimo interesse” para o tratamento de dados com o objetivo de alcançar suas finalidades primárias. As diretrizes legais mais relevantes para a segurança pública municipal são:

a) Cumprimento de Obrigação Legal ou Regulatória (Art. 7º, II e Art. 23, I):

Este é o permissivo legal mais comumente invocado. O tratamento de dados é permitido quando o órgão público está obrigado por lei a realizar determinada atividade. No contexto da segurança pública, a Constituição Federal e leis infraconstitucionais impõem ao

município o dever de zelar pela segurança. No entanto, a doutrina e a ANPD alertam que essa dispositivo não pode ser interpretada de forma genérica. A mera atribuição constitucional de “prevenir e reprimir a criminalidade” não autoriza a coleta indiscriminada. É necessário que a lei ou regulamento específico detalhe a finalidade e a necessidade do tratamento de dados, vinculando-o a uma competência legal clara e delimitada.

b) Execução de Políticas Públicas (Art. 7º, III e Art. 23, I). Nesse aspecto, o tratamento de dados pode ocorrer para a execução de políticas públicas previstas em leis e regulamentos.

A segurança pública, quando estruturada como uma política pública municipal (ex.: planos de segurança, programas de videomonitoramento), pode utilizar esse critério. Para a validade desta hipótese normativa, a política pública deve ser formalizada, ter objetivos claros e o tratamento de dados deve ser estritamente necessário para a sua execução. O município de Jataí, ao implementar seu sistema de monitoramento, deve demonstrar que o tratamento de dados é um meio essencial para a concretização de uma política pública de segurança formalmente estabelecida.

c) Exercício Regular de Direitos em Processo (Art. 7º, VI). Em relação a esse fundamento, destaca-se o tratamento de dados para o exercício regular de direitos em processo judicial, administrativo ou arbitral, essa é a norma que justifica, por exemplo, o uso das imagens de videomonitoramento como prova em uma investigação policial ou processo judicial. É fundamental que o tratamento de dados seja limitado ao contexto do processo, não justificando a coleta proativa e generalizada de dados de toda a população. A LGPD busca evitar que a exceção se torne a regra, mantendo o foco na proteção do titular.

3. O TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO NO CONTEXTO DA SEGURANÇA URBANA: REFERENCIAL TEÓRICO E JURÍDICO

A crescente utilização de tecnologias de vigilância pelos entes públicos representa uma das transformações mais significativas no campo da segurança pública contemporânea.

Sistemas de videomonitoramento urbano, softwares de análise de imagens e ferramentas de inteligência artificial passaram a integrar as estratégias de prevenção e repressão à criminalidade em diversas cidades brasileiras. Contudo, de acordo com Doneda (2011) e Schertel Mendes (2021), a ampliação dessas tecnologias também impõe novos desafios jurídicos relacionados à proteção de dados pessoais e à preservação dos direitos fundamentais.

Sob esse prisma, a aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) aos sistemas de monitoramento urbano apresenta um conjunto complexo de desafios institucionais

e normativos. Embora a LGPD preveja hipóteses específicas de tratamento de dados pelo poder público, especialmente quando voltadas à segurança pública, tais atividades não estão isentas da observância dos princípios gerais da proteção de dados (Brasil, 2018).

Entre os principais desafios jurídicos destaca-se a necessidade de garantir que o tratamento de dados realizado pelos sistemas de videomonitoramento observe os princípios da finalidade, necessidade e proporcionalidade, previstos na legislação. Acompanhando as contribuições de Barbieri (2020), isso significa que a coleta de imagens e informações deve ocorrer exclusivamente para objetivos legítimos e claramente definidos, “evitando-se práticas de vigilância indiscriminada ou excessiva” (Barbieri, 2020, p.33).

Um ponto a ser destacado, se refere ao risco de monitoramento massivo da população, fenômeno que tem sido amplamente debatido pela doutrina contemporânea. A expansão das tecnologias de vigilância pode ampliar significativamente a capacidade do Estado de observar comportamentos individuais, o que exige a adoção de mecanismos rigorosos de controle institucional e governança de dados. Conforme observa Doneda (2011), o poder público deve atuar com especial cautela no tratamento de informações pessoais, justamente em razão da assimetria de poder existente entre o Estado e o cidadão.

Além disso, a ausência de regulamentações específicas no âmbito municipal representa um desafio adicional para a implementação adequada da LGPD. Para o pesquisador Bruno Bioni (2020), embora a legislação federal estabeleça princípios e diretrizes gerais, muitos aspectos operacionais do tratamento de dados dependem de normativas locais. Por exemplo, definição de prazos de armazenamento das imagens, critérios de compartilhamento de informações entre órgãos e protocolos de auditoria e controle de acesso aos sistemas (Bioni, 2020).

Outro aspecto de suma importância concerne à capacitação técnica e jurídica dos agentes públicos responsáveis pela operação dos sistemas de monitoramento. A jurista Caitlin Sampaio Mulholland (2020) enfatiza a importância da formação adequada, tanto voltada para a aquisição de conhecimentos tecnológicos quanto para a atualização de conhecimentos legais.

A correta aplicação da LGPD exige conhecimento não apenas das tecnologias utilizadas, mas também dos limites legais relacionados ao tratamento de dados pessoais. Sem essa formação adequada, aumenta-se o risco de práticas irregulares, como acesso indevido a informações, compartilhamento não autorizado de imagens ou utilização inadequada dos dados coletados (MULHOLLAND, 2020).

No campo constitucional, o debate sobre videomonitoramento urbano envolve a necessária ponderação entre dois valores fundamentais: de um lado, o direito à privacidade e à proteção de dados pessoais, assegurados pelo artigo 5º, incisos X e LXXIX da Constituição da República Federativa do Brasil de 1988; de outro, o dever do Estado de promover a segurança pública, previsto no artigo 144 da Constituição. Consequentemente, a harmonização desses direitos exige que a atuação estatal seja pautada pelos princípios da proporcionalidade, razoabilidade e legalidade³.

Nesse sentido, a jurisprudência do Supremo Tribunal Federal tem reconhecido que o tratamento de dados pessoais pelo poder público deve observar limites claros e fundamentação adequada, especialmente quando envolve a coleta massiva de informações. O reconhecimento do direito fundamental à proteção de dados reforça a necessidade de que sistemas de vigilância urbana sejam estruturados com mecanismos robustos de segurança da informação, governança de dados e controle institucional (STF, ADI 6387, 2020).

Nessa perspectiva, a implementação de sistemas de videomonitoramento municipal deve ser acompanhada de práticas voltadas à proteção da privacidade, transparência administrativa e responsabilização institucional. Segundo o jurista Canotilho (2003), somente por meio dessa abordagem equilibrada será possível conciliar a eficiência das tecnologias de segurança pública com a preservação dos direitos fundamentais dos cidadãos, garantindo que a inovação tecnológica permaneça alinhada aos princípios do Estado Democrático de Direito.

A partir da revisão doutrinária e da análise normativa realizada ao longo do trabalho, verificou-se que a LGPD representa um importante marco regulatório no ordenamento jurídico brasileiro, estabelecendo limites e parâmetros para o tratamento de dados pessoais tanto por entidades privadas quanto pelo poder público. No contexto da segurança pública, embora a legislação reconheça a necessidade de flexibilizações para o tratamento de dados voltado à prevenção e repressão de ilícitos, tais exceções não afastam a obrigação estatal de observar os princípios fundamentais da proteção de dados, especialmente aqueles relacionados à finalidade, necessidade, transparência e segurança da informação (Brasil, 2018).

A investigação também demonstrou que a incorporação de tecnologias de monitoramento urbano tem se tornado uma ferramenta relevante para o fortalecimento das políticas de segurança pública municipal. Sistemas de videomonitoramento, análise de dados

³ FONTE: SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de direito constitucional**. 11. ed. São Paulo: Saraiva, 2022.

e inteligência policial permitem maior capacidade de prevenção de crimes, apoio às investigações e gestão estratégica das ações de segurança (Barbieri, 2020). Nesse sentido, tais tecnologias representam instrumentos importantes para a promoção da ordem pública e para a proteção da coletividade.

Entretanto, consoantes as contribuições de Bioni (2020), o uso dessas ferramentas também impõe desafios significativos no campo jurídico e institucional:

A ampliação da capacidade estatal de coleta e tratamento de informações pessoais exige mecanismos robustos de governança de dados, controle institucional e proteção da privacidade. Sem a adoção de medidas adequadas de segurança da informação e de regulamentações claras sobre o uso dessas tecnologias, existe o risco de que sistemas de vigilância sejam utilizados de forma desproporcional ou incompatível com os direitos fundamentais garantidos pela Constituição Federal (BIONI, 2020).

A pesquisa empírica realizada por meio de visita técnica ao sistema de videomonitoramento do município de Jataí permitiu identificar que o poder público local já tem buscado implementar mecanismos tecnológicos voltados à proteção das informações coletadas. A presença de protocolos de criptografia, sistemas de autenticação reforçada, controle de acesso e mecanismos de segurança digital demonstra uma preocupação institucional com a integridade e a confidencialidade dos dados tratados. Tais medidas dialogam diretamente com os princípios de segurança e prevenção previstos na LGPD, contribuindo para reduzir riscos relacionados ao acesso indevido ou à utilização inadequada das informações (Brasil, 2018).

A proteção de dados pessoais foi elevada ao patamar de direito fundamental no ordenamento jurídico brasileiro por meio da Emenda Constitucional nº 115/2022, que inseriu no artigo 5º da Constituição Federal o inciso LXXIX, estabelecendo expressamente que “é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais”. Tal alteração constitucional reforçou a centralidade da tutela informacional no Estado Democrático de Direito e consolidou o entendimento de que a proteção de dados constitui desdobramento direto da dignidade da pessoa humana, da privacidade e da liberdade individual.

Nesse contexto, o Supremo Tribunal Federal, especialmente no julgamento da ADI 6387/DF, reconheceu a existência de um direito fundamental autônomo à proteção de dados pessoais, vinculado ao princípio da autodeterminação informativa, entendido como a prerrogativa conferida ao indivíduo de controlar a coleta, o tratamento, o armazenamento e o

compartilhamento de suas informações pessoais. A Corte assentou que o tratamento massivo de dados pelo Poder Público exige observância rigorosa aos princípios da finalidade, necessidade, proporcionalidade e transparência, sobretudo em contextos envolvendo tecnologias de vigilância e monitoramento estatal.

Dessa forma, a jurisprudência constitucional brasileira passou a consolidar a compreensão de que a atividade estatal relacionada à segurança pública não está imune aos limites impostos pelos direitos fundamentais, impondo ao Poder Público o dever de estruturar políticas de governança de dados compatíveis com os parâmetros constitucionais de proteção da privacidade e da autodeterminação informativa.

Apesar desses avanços, o estudo também evidenciou a necessidade de aprimoramento contínuo das políticas públicas relacionadas à governança de dados no âmbito municipal. A ausência de regulamentações específicas sobre o tratamento de dados em sistemas de monitoramento urbano, bem como a necessidade de capacitação adequada e permanente dos agentes públicos responsáveis pela operação dessas tecnologias, conforme anteriormente mencionado, representa desafios importantes para a plena implementação da LGPD no contexto da segurança pública local.

Com efeito, destaca-se que a modernização tecnológica da segurança pública municipal não deve ser compreendida apenas como um avanço operacional, mas também como um desafio jurídico e ético que demanda constante reflexão e aprimoramento institucional (Doneda, 2020). A efetiva aplicação da Lei Geral de Proteção de Dados no contexto das políticas de segurança pública constitui, portanto, um passo fundamental para garantir que a inovação tecnológica caminhe lado a lado com a proteção da dignidade humana, da privacidade e das liberdades individuais.

4. SISTEMAS DE MONITORAMENTO E INTELIGÊNCIA EM JATAÍ: ANÁLISE TECNOLÓGICA E JURÍDICA

O desenvolvimento de sistemas de monitoramento e inteligência urbana impõe relevantes desafios jurídicos relacionados à proteção de dados pessoais e aos direitos fundamentais. Conforme sustentam Doneda (2019) e Mendes (2021), a crescente capacidade tecnológica de coleta e tratamento de informações demanda mecanismos de controle capazes de limitar excessos estatais. Nesse contexto, os sistemas de videomonitoramento implementados em Jataí devem observar os princípios da finalidade, necessidade, adequação e

proporcionalidade previstos na LGPD, assegurando equilíbrio entre segurança pública e proteção da privacidade.

Nesse cenário, os sistemas de monitoramento e inteligência na segurança pública municipal de Jataí abrangem um amplo espectro de tecnologias, cuja análise jurídica é crucial para a conformidade com a LGPD. A seguir, estão listadas as características dos principais espectros tecnológicos identificados em Jataí/GO:

a) Videomonitoramento e a Coleta de Dados Pessoais – o videomonitoramento, com câmeras de alta resolução e capacidade de gravação noturna, é a forma mais comum de coleta de dados pessoais na segurança pública municipal. As imagens capturadas, por permitirem a identificação de indivíduos, são consideradas dados pessoais. Já a coleta e o tratamento de dados em larga escala por esses sistemas levantam questões críticas sobre a necessidade e a proporcionalidade da vigilância, especialmente em relação a cidadãos não envolvidos em atividades ilícitas. A LGPD exige que a cidade de Jataí defina claramente o período de retenção dessas imagens, o protocolo de acesso e o descarte seguro, em observância ao princípio da limitação do tratamento.

b) O Desafio do Reconhecimento Facial e Dados Biométricos – o uso de tecnologias mais avançadas, como o reconhecimento facial, representa um desafio ainda maior. Dados biométricos (como a face) são considerados dados pessoais sensíveis pela LGPD (art. 5º, II), e seu tratamento é submetido a regras mais rigorosas. Para o tratamento de dados sensíveis, o Poder Público deve se ater às bases legais específicas do art. 11, sendo a mais aplicável o cumprimento de obrigação legal ou regulatória (art. 11, II, “a”) ou a execução de diretrizes (art. 11, II, “b”). A implementação do reconhecimento facial em Jataí, mesmo que para fins de segurança pública, deve ser precedida de um Relatório de Impacto à Proteção de Dados Pessoais (RIPD) que demonstre a estrita necessidade, a proporcionalidade e a mitigação de riscos, especialmente o risco de discriminação e vigilância em massa. A tecnologia de reconhecimento facial, por sua natureza, pode levar a decisões automatizadas que afetam direitos, exigindo transparência e a possibilidade de revisão humana, conforme o Art. 20 da LGPD.

c) Sistemas de Inteligência e Análise Preditiva – os sistemas de inteligência que realizam a análise de grandes volumes de dados (Big Data) de diversas fontes (redes sociais, registros públicos, dados de tráfego) para prever crimes e subsidiar tomadas de decisão, também estão sob o escopo da LGPD. O tratamento de dados para fins de inteligência deve respeitar o princípio da Não Discriminação, evitando que algoritmos reproduzam ou

perpetuem vieses sociais e raciais, o que é um risco inerente a sistemas preditivos. A LGPD exige que o município garanta a qualidade dos dados utilizados, pois dados incorretos ou desatualizados podem levar a decisões equivocadas e injustas contra o cidadão.

4.1. Percurso metodológico “*in loco*” e observação empírica do sistema de videomonitoramento municipal

Em relação às etapas metodológicas previstas nesta pesquisa, especialmente no que se refere à observação empírica das estruturas utilizadas pela segurança pública municipal, foi realizada visita técnica ao setor responsável pelo sistema de videomonitoramento do município de Jataí, Goiás. A atividade teve como objetivo compreender, de forma prática, a estrutura tecnológica empregada pelo poder público para a captação, processamento e armazenamento de dados provenientes do monitoramento urbano.

Essa etapa empírica está alinhada à proposta metodológica exploratória do estudo, que busca analisar a aplicação concreta dos mecanismos de vigilância tecnológica no contexto municipal, isso permite confrontar a realidade operacional com os parâmetros normativos estabelecidos pela Lei Geral de Proteção de Dados – LGPD.

Durante a visita técnica, foi possível constatar que o município dispõe de um sistema de videomonitoramento composto por aproximadamente 67 câmeras distribuídas em diferentes pontos da cidade, estrategicamente posicionadas em locais considerados sensíveis do ponto de vista da segurança pública. A definição desses pontos de instalação não ocorre de forma arbitrária, mas sim a partir da análise de dados relacionados à incidência de “manchas criminais”, registros de ocorrências policiais e estatísticas de acidentes de trânsito. Esse modelo de planejamento demonstra a adoção de uma lógica orientada por dados e inteligência aplicada à segurança pública, permitindo que o sistema de monitoramento atue de maneira preventiva e estratégica na mitigação de riscos e na promoção da segurança urbana.

No que se refere à infraestrutura tecnológica e à proteção das informações coletadas, verificou-se que o sistema possui um conjunto de mecanismos voltados à proteção dos dados armazenados e transmitidos, evidenciando a adoção de práticas compatíveis com os princípios de segurança da informação. Entre as medidas observadas, destaca-se a utilização de chaves criptográficas proprietárias, responsáveis por garantir a proteção dos fluxos de comunicação entre os dispositivos de captura de imagens e os servidores responsáveis pelo armazenamento das informações.

Além disso, identificou-se a utilização de protocolos seguros de transmissão de dados, como o SSL (*Secure Socket Layer*), que assegura a integridade e confidencialidade das informações trafegadas na rede. Também foi verificada a implementação de criptografia baseada no padrão AES (*Advanced Encryption Standard*), amplamente reconhecida como uma das tecnologias mais robustas no campo da segurança da informação para proteção de dados sensíveis.

Outro aspecto relevante observado durante a visita refere-se à adoção de políticas de controle de acesso ao sistema, incluindo padrões seguros para criação e gerenciamento de senhas, bem como a implementação de mecanismos de autenticação em dois fatores (dupla autenticação). Esse recurso constitui uma camada adicional de proteção, dificultando acessos não autorizados e fortalecendo o controle sobre os usuários que operam a plataforma de monitoramento.

Também foram identificados mecanismos de controle de acesso físico e lógico aos sistemas, com a existência de portas de acesso convencionais devidamente controladas e restrição de uso apenas a operadores autorizados. Esse conjunto de medidas demonstra a adoção de uma arquitetura de segurança estruturada em múltiplas camadas de proteção, estratégia conhecida na área de tecnologia da informação como modelo de defesa em profundidade, que busca reduzir vulnerabilidades e ampliar a proteção dos sistemas contra eventuais incidentes de segurança.

Sob a perspectiva jurídica, tais mecanismos dialogam diretamente com os princípios da segurança e da prevenção previstos na Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que determinam a adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados, vazamentos, perda ou tratamento inadequado. Conforme destaca Bioni (2021), a implementação de práticas robustas de segurança da informação constitui elemento essencial para garantir a efetividade da proteção de dados no âmbito das atividades estatais.

Dessa forma, a observação empírica realizada durante a visita técnica evidencia que o sistema de videomonitoramento municipal de Jataí apresenta um ciclo estruturado de proteção das informações, integrando medidas tecnológicas, operacionais e administrativas voltadas à preservação da integridade, confidencialidade e disponibilidade dos dados coletados. Tais práticas contribuem para reduzir riscos relacionados ao tratamento de dados pessoais e reforçam a necessidade de que sistemas de vigilância urbana sejam permanentemente avaliados sob a ótica da governança de dados e da proteção dos direitos fundamentais.

Por fim, destaca-se que a adoção dessas medidas representa um avanço importante na estruturação da segurança digital no âmbito municipal. Entretanto, considerando a constante evolução das tecnologias de vigilância e dos riscos associados ao tratamento de informações pessoais, torna-se imprescindível que o poder público mantenha processos contínuos de avaliação, atualização tecnológica e capacitação dos agentes responsáveis pela operação dos sistemas, garantindo que o uso dessas ferramentas permaneça alinhado aos princípios do Estado Democrático de Direito e às garantias constitucionais de privacidade e proteção de dados.

5. LGPD E A PROTEÇÃO DOS DIREITOS FUNDAMENTAIS: A COLISÃO DE INTERESSES

A aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) está diretamente relacionada à tutela dos direitos fundamentais assegurados pela Constituição Federal de 1988, especialmente aqueles vinculados à privacidade, liberdade, intimidade e não discriminação. Nesse contexto, emerge a necessidade de harmonização entre o interesse público voltado à segurança e os direitos individuais dos cidadãos, sobretudo diante da crescente utilização de sistemas tecnológicos de monitoramento e inteligência pelo Poder Público.

O direito à privacidade, previsto no artigo 5º, inciso X, da Constituição Federal, protege a esfera individual contra interferências indevidas do Estado e de terceiros. A coleta indiscriminada de dados pessoais em sistemas de videomonitoramento, reconhecimento facial e inteligência artificial pode configurar invasão à esfera privada do indivíduo, principalmente quando inexistem critérios claros de finalidade, necessidade e proporcionalidade. Nesse sentido, a LGPD surge como importante instrumento normativo de limitação da atividade estatal, ao estabelecer princípios voltados à proteção dos titulares de dados pessoais.

Conforme leciona Doneda (2019), a proteção de dados pessoais representa uma evolução da própria concepção de privacidade, passando a exigir mecanismos de controle sobre o fluxo de informações relativas ao indivíduo. Para o autor, o tratamento de dados deve observar limites compatíveis com os direitos fundamentais, evitando práticas excessivas de vigilância e monitoramento social. Assim, a atuação estatal no âmbito da segurança pública não pode ocorrer de forma irrestrita, devendo respeitar garantias constitucionais e parâmetros legais de proteção informacional.

A intimidade, igualmente protegida pela Constituição Federal, resguarda aspectos pessoais da vida privada e das relações individuais. A LGPD fortalece essa proteção ao exigir

transparência quanto à coleta e utilização de dados, além de impor restrições ao compartilhamento e armazenamento indiscriminado de informações pessoais. Segundo Mendes (2021), a proteção de dados pessoais constitui instrumento essencial para a preservação da dignidade da pessoa humana e da autodeterminação informativa, permitindo ao indivíduo maior controle sobre suas informações e sobre a forma como elas são utilizadas pelo Estado e pelo setor privado.

Outro aspecto relevante refere-se ao denominado “*efeito chilling*” ou efeito inibidor, fenômeno caracterizado pela alteração comportamental do cidadão diante da sensação permanente de vigilância. Em ambientes monitorados constantemente, indivíduos podem restringir sua liberdade de expressão, associação e circulação por receio de interpretações equivocadas, monitoramento abusivo ou eventual fichamento estatal. Tal cenário demonstra que o excesso de vigilância pode comprometer o exercício pleno das liberdades públicas, produzindo efeitos incompatíveis com o Estado Democrático de Direito. Diante desse cenário, a LGPD atua como mecanismo de mitigação desses riscos ao estabelecer garantias de controle, finalidade e limitação no tratamento de dados pessoais.

Sob à ótica do direito à liberdade, previsto no artigo 5º, caput, da Constituição Federal, observa-se o fenômeno do efeito inibidor que compreende não apenas a liberdade de locomoção, mas também as liberdades de expressão, reunião e associação. A utilização de sistemas inteligentes de monitoramento deve, portanto, observar limites jurídicos rigorosos, de modo a impedir práticas que induzam à autocensura ou restrinjam comportamentos legítimos dos cidadãos em espaços públicos. A proteção de dados pessoais revela-se, assim, instrumento indispensável para assegurar o equilíbrio entre segurança pública e preservação das liberdades individuais.

Além disso, destaca-se a importância do princípio da não discriminação, previsto no artigo 6º, inciso IX, da LGPD. O emprego de tecnologias de inteligência artificial e reconhecimento facial na segurança pública exige mecanismos de auditabilidade e controle capazes de prevenir discriminações indevidas baseadas em raça, gênero, condição social ou origem étnica. A ausência de transparência algorítmica pode potencializar práticas discriminatórias incompatíveis com os objetivos fundamentais da República previstos no artigo 3º, inciso IV, da Constituição Federal, especialmente no que se refere à promoção do bem de todos sem preconceitos ou quaisquer formas de discriminação.

Dessa forma, observa-se que a implementação de sistemas de monitoramento e inteligência demanda constante ponderação entre a proteção da coletividade e a preservação

dos direitos fundamentais. A LGPD, ao estabelecer princípios como finalidade, adequação, necessidade, transparência e não discriminação, constitui importante instrumento jurídico de contenção de excessos estatais, contribuindo para que o avanço tecnológico ocorra em conformidade com os valores constitucionais e com a dignidade da pessoa humana.

6. DESAFIOS JURÍDICOS E OPERACIONAIS NA APLICAÇÃO DA LGPD EM JATAÍ

A implementação da LGPD nos sistemas de segurança pública do município de Jataí representa um importante desafio jurídico e operacional para a administração pública contemporânea. O avanço das tecnologias de vigilância e monitoramento, especialmente por meio de câmeras e bancos de dados digitais, exige que o poder público concilie eficiência na segurança pública com a preservação dos direitos fundamentais dos cidadãos. Nesse contexto, a proteção de dados pessoais passa a integrar o conjunto de garantias constitucionais relacionadas à dignidade da pessoa humana, à privacidade e à liberdade individual.

Conforme destaca Doneda (2019), a proteção de dados deve ser compreendida como um direito fundamental autônomo, indispensável ao Estado Democrático de Direito.

Um dos principais desafios enfrentados pelo município refere-se à fundamentação legal para a coleta massiva de dados pessoais em sistemas de monitoramento urbano. Embora a LGPD autorize o tratamento de dados para o cumprimento de obrigação legal e execução de políticas públicas, há questionamentos sobre a legitimidade da coleta indiscriminada de informações baseada apenas na atribuição genérica de prevenção e repressão à criminalidade. O consentimento individual mostra-se inviável em cenários de vigilância coletiva, tornando necessária a adoção de bases legais sólidas e devidamente justificadas (DONEDA, 2019, p. 195-200).

Nesse sentido, Mendes (2021) ressalta que o tratamento de dados pelo poder público deve observar rigorosamente os princípios da finalidade, adequação e necessidade, evitando excessos incompatíveis com a ordem constitucional. A atuação da Guarda Municipal de Jataí também se insere nesse debate jurídico, especialmente diante da jurisprudência consolidada pelo Supremo Tribunal Federal (STF). A Corte Suprema reconhece que as guardas municipais exercem atividade de segurança pública de maneira subsidiária e complementar, o que amplia sua responsabilidade quanto ao tratamento de dados pessoais.

Dessa forma, a utilização de sistemas de videomonitoramento e vigilância eletrônica pela Guarda Municipal deve ocorrer em conformidade com os limites impostos pela LGPD e pelos direitos fundamentais assegurados pela Constituição Federal. Além disso, a

jurisprudência do STF estabelece que abordagens pessoais e veiculares realizadas pela Guarda Municipal dependem da existência de fundada suspeita, vedando práticas arbitrárias e discriminatórias.

Por analogia, a coleta de dados pessoais em sistemas de monitoramento também deve respeitar critérios objetivos e proporcionais, não podendo ocorrer de forma genérica ou baseada em critérios subjetivos. A LGPD atua, portanto, como instrumento de reforço à legalidade administrativa, impondo limites à atuação estatal e prevenindo abusos relacionados à vigilância excessiva, com respaldo nos princípios da necessidade e da proporcionalidade previstos no artigo 6º da LGPD.

Consoante já mencionado, esses princípios funcionam como mecanismos de contenção contra o uso abusivo de tecnologias de vigilância em massa. A coleta de imagens, dados de localização e informações biométricas, como reconhecimento facial, exige que o município demonstre de forma objetiva a indispensabilidade da medida adotada. Segundo Doneda (2019), a proporcionalidade constitui elemento essencial para assegurar que o tratamento de dados não ultrapasse os limites estritamente necessários à finalidade pública pretendida.

No caso específico de Jataí, a instalação de câmeras em regiões com baixos índices de criminalidade pode suscitar questionamentos quanto à adequação e necessidade da vigilância implementada. Para legitimar tais medidas, o município deve apresentar estudos técnicos e dados estatísticos que demonstrem a efetiva necessidade da intervenção tecnológica. A ausência de fundamentação baseada em evidências transforma o monitoramento em prática invasiva e potencialmente violadora da privacidade dos cidadãos, contrariando os princípios estabelecidos pela LGPD.

A transparência na utilização dos sistemas de monitoramento também constitui obrigação indispensável para a administração pública. A LGPD determina que os titulares dos dados sejam devidamente informados sobre a existência de coleta e tratamento de informações pessoais. Isso implica a necessidade de instalação de placas informativas em áreas monitoradas, bem como a disponibilização de políticas de privacidade acessíveis e compreensíveis à população. Conforme observa Mendes (2021), a transparência fortalece a confiança institucional e contribui para o controle democrático das atividades estatais de vigilância.

No âmbito da governança de dados, destaca-se a importância do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), instrumento previsto pela Autoridade Nacional de Proteção de Dados (ANPD). O RIPD permite identificar riscos relacionados ao tratamento de

dados e estabelecer medidas preventivas capazes de minimizar violações à privacidade. Em Jataí, a elaboração desse relatório seria fundamental para garantir maior segurança jurídica e transparência na implementação ou ampliação dos sistemas de monitoramento. O documento deve conter informações detalhadas sobre a coleta, armazenamento e compartilhamento dos dados, além das medidas de segurança adotadas pelo município.

Outro elemento indispensável para a conformidade com a LGPD é a nomeação do Encarregado de Proteção de Dados, também conhecido como *Data Protection Officer* (DPO). Esse profissional atua como intermediário entre o município, os titulares dos dados e a Autoridade Nacional de Proteção de Dados. Em âmbito municipal, o DPO possui função estratégica, sendo responsável por orientar agentes públicos, fiscalizar o cumprimento da legislação e receber reclamações dos cidadãos. A capacitação contínua dos servidores públicos envolvidos no tratamento de dados também se revela essencial para evitar incidentes de segurança e práticas incompatíveis com a legislação vigente.

Por fim, o compartilhamento de dados entre órgãos públicos representa um dos maiores desafios operacionais relacionados à segurança pública municipal. Sobre esse ponto, o artigo 26 da LGPD estabelece os limites nos termos seguintes:

Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei (BRASIL, 2018, s.p.).

Isto posto, a integração entre Guarda Municipal, Polícia Militar e Polícia Civil exige a circulação de informações pessoais entre diferentes esferas governamentais. Embora o artigo 26 da LGPD autorize o compartilhamento para execução de ações governamentais, essa prática deve observar rigorosamente os princípios da finalidade, adequação e segurança. Assim, o município de Jataí deve formalizar convênios e termos de cooperação técnica que estabeleçam claramente os dados compartilhados, as finalidades específicas e as medidas de proteção exigidas dos órgãos receptores, assegurando a proteção dos direitos fundamentais da população.

7. PROPOSTAS DE GOVERNANÇA E DIRETRIZES PARA CONFORMIDADE EM JATAÍ

Para que o município de Jataí alcance a plena conformidade com a LGPD e garanta a proteção dos direitos fundamentais, propõe-se a adoção das seguintes diretrizes de governança de dados:

Criação de Política Municipal de Proteção de Dados	→ Criação de ato normativo municipal (Decreto ou Lei) para a Política Municipal de Proteção de Dados Pessoais (PMPD)
--	--

O ato normativo criará o Comitê Gestor de Proteção de Dados (CGPD), responsável pela supervisão da política; a nomeação formal do Encarregado de Dados (DPO); e a obrigatoriedade de realização do RIPD para novos projetos de tecnologia.

Implementação de medidas técnicas e organizacionais	→ Medidas técnicas com foco na segurança da informação.
---	---

As medidas técnicas incluem: (i) anonimização e pseudonimização, isto é, sempre que possível, os dados devem ser tratados de forma a não permitir a identificação direta do titular; (ii) controle de acesso com a implementação de mecanismos rigorosos de controle de acesso aos dados de monitoramento, limitando-o apenas a agentes autorizados e com registro de logs; (iii) criptografia para proteger dados em trânsito e em repouso, especialmente dados biométricos.

Por sua vez, as medidas organizacionais incluem: (i) treinamento contínuo por meio de programas de capacitação para todos os agentes da Guarda Municipal e servidores envolvidos no tratamento de dados; (ii) protocolos de resposta a incidentes por intermédio da criação de um plano de resposta a incidentes de segurança, com comunicação imediata à ANPD e aos titulares, conforme o Art. 48 da LGPD.

Diretrizes para o uso de reconhecimento facial	→ Diretrizes em razão da natureza sensível dos dados biométricos.
--	---

O uso de reconhecimento facial deve seguir diretrizes estritas, tais como: (i) finalidade específica e delimitada, ou seja, o uso deve ser restrito a finalidades de alta

relevância, como a busca por foragidos ou pessoas desaparecidas, e não para vigilância em massa; (ii) auditoria e revisão, nos quais os algoritmos devem ser auditáveis para garantir a ausência de vieses discriminatórios; (iii) e transparência ativa, caracterizada pela publicação de relatórios periódicos sobre o uso da tecnologia, incluindo estatísticas de acertos e erros.

8. CONSIDERAÇÕES FINAIS

O presente estudo teve como objetivo analisar os desafios jurídicos decorrentes da aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) nos sistemas de monitoramento e inteligência da segurança pública municipal de Jataí, especialmente no que se refere à preservação dos direitos fundamentais dos cidadãos diante do avanço das tecnologias de vigilância. A pesquisa buscou compreender de que forma o uso de ferramentas tecnológicas voltadas à segurança pública pode ser compatibilizado com os princípios constitucionais da privacidade, da proteção de dados pessoais e da autodeterminação informativa.

A aplicação da LGPD nos sistemas de monitoramento e inteligência da segurança pública municipal de Jataí, Goiás, é um imperativo legal e constitucional. O desafio central é utilizar a tecnologia dentro dos limites da legalidade, da necessidade e da proporcionalidade. Por conseguinte, a pesquisa demonstrou que a conformidade com a LGPD exige que o município: (i) fundamente o tratamento de dados em bases legais estritas e específicas, evitando a interpretação genérica da “obrigação legal” e priorizando a Execução de Políticas Públicas formalizadas; (ii) aplique rigorosamente os princípios da Necessidade e Proporcionalidade, justificando a coleta massiva de dados e, em casos de tecnologias invasivas como o reconhecimento facial, realizando o RIPD para mitigar riscos; (iii) garanta a Transparência por meio de sinalização clara, políticas de privacidade acessíveis e a publicidade dos atos de tratamento; (iv) e, invista em Segurança e Governança, protegendo os dados contra incidentes, nomeando o DPO e demonstrando a conformidade (*Accountability*).

A LGPD atua como um instrumento de legitimação da atuação estatal, garantindo que a busca pela segurança pública não se sobreponha de forma desmedida aos direitos fundamentais de privacidade, intimidade e liberdade dos cidadãos de Jataí. A regulamentação

específica e a capacitação contínua dos agentes públicos são passos essenciais para transformar os desafios jurídicos em práticas de governança de dados que beneficiem toda a sociedade.

Ademais, destaca-se que a modernização tecnológica da segurança pública municipal não deve ser compreendida apenas como um avanço operacional, mas também como um desafio jurídico e ético que demanda constante reflexão e aprimoramento institucional. A efetiva aplicação da Lei Geral de Proteção de Dados no contexto das políticas de segurança pública constitui, portanto, um passo fundamental para garantir que a inovação tecnológica caminhe lado a lado com a proteção da dignidade humana, da privacidade e das liberdades individuais.

Em linhas de conclusão, portanto, espera-se que este trabalho contribua para o debate acadêmico e institucional sobre a governança de dados na segurança pública municipal, oferecendo subsídios teóricos e práticos para o desenvolvimento de políticas públicas que conciliem eficiência administrativa, segurança coletiva e respeito aos direitos fundamentais. Também, almeja-se colaborar para a ampliação e o aprofundamento das pesquisas acerca da temática, estimulando novas reflexões acadêmicas e investigações interdisciplinares que permitam compreender os desafios e as potencialidades da gestão de dados no âmbito da administração pública contemporânea.

REFERÊNCIAS BIBLIOGRÁFICAS

BARBIERI, Carlos. **Proteção de dados e segurança pública: desafios contemporâneos da vigilância estatal.** São Paulo: Thomson Reuters Brasil, 2020.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento.** 2. ed. Rio de Janeiro: Forense, 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Dispõe sobre a proteção de dados pessoais e dá outras providências. Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Último acesso em: 30 de abril de 2026.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Promulgada em 5 de outubro de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Último acesso em: 28 de abril de 2026.

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 e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF: Presidência da República, 2022. Disponível em: [Planalto - EC 115/2022](#). Último acesso em: 27 de abril de 2026.

BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade (ADI) 6387/DF. Relatora: Min. Rosa Weber. Julgamento em 07 maio 2020. Brasília, DF: STF, 2020. Disponível em: [STF - ADI 6387/DF](#). Último cesso em: 27 de abril de 2026.

BRUM, Ana Paula. **Direito e tecnologia:** desafios contemporâneos. Porto Alegre: Editora Jurídica, 2025.

CANOTILHO, José Joaquim Gomes. **Direito constitucional e teoria da constituição.** 7. ed. Coimbra: Almedina, 2003.

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

DONEDA, Danilo; PEREIRA, Laura Schertel. **Curso de Direito de Proteção de Dados.** 2. ed. Rio de Janeiro: Forense; São Paulo: MÉTODO, 2022.

GIL, Antônio Carlos. **Métodos e técnicas de pesquisa.** São Paulo: Editora Atlas, 2010.

JATAÍ. Lei Ordinária nº 4805 de 05 de Maio de 2025: Dispõe sobre princípios, regras e instrumentos para o Governo Digital no âmbito da Câmara Municipal de Jataí, buscando o aumento da eficiência e transparência pública e dá outras providências. Disponível em: <https://www.jatai.go.leg.br/L4805>. Acesso em: 30 de abril de 2026.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de metodologia científica.** 6ª edição. São Paulo: Atlas, 2009.

MENDES, Laura Schertel. **Proteção de dados pessoais:** fundamento, conceitos e modelo de aplicação. São Paulo: Thomson Reuters Brasil, 2021.

MENDES, Laura Schertel. **Vigilância e Proteção de Dados Pessoais no Brasil.** In: SILVA, A. M. S. (Org.). Temas Atuais de Direito Digital. São Paulo: Editora RT, 2019.

MENDES, Laura Schertel Ferreira; BIONI, Bruno Ricardo (coord.). **Tratado de proteção de dados pessoais.** Rio de Janeiro: Forense, 2021.

MULHOLLAND, Caitlin Sampaio. **Internet e contratação:** panorama das relações contratuais eletrônicas de consumo. Rio de Janeiro: Forense, 2020.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de direito constitucional.** 11. ed. São Paulo: Saraiva, 2022.