PROTEÇÃO DE DADOS E VIGILÂNCIA NA SEGURANÇA PÚBLICA BRASILEIRA: DESAFIOS NA APLICABILIDADE DA LGPD (2020-2024)

DATA PROTECTION AND SURVEILLANCE IN BRAZILIAN PUBLIC SECURITY: CHALLENGES IN THE APPLICABILITY OF THE LGPD (2020–2024)

Nícolas Lobo Lobato
Virgínia de Melo Dantas Trinks

RESUMO

O uso de tecnologias de vigilância pelas forças de segurança pública brasileiras coexiste em um contexto de lacuna regulatória para o tratamento de dados pessoais após a entrada em vigor da Lei Geral de Proteção de Dados (LGPD). Este cenário apresenta o problema de como a exclusão legal para o tratamento de dados na segurança pública impacta a aplicação dos princípios da LGPD e quais as implicações para direitos fundamentais e segurança jurídica. O estudo objetiva analisar a produção científica e normativa sobre esta temática no período 2020-2024, identificando os desafios jurídicos, técnicos e institucionais frutos desta exclusão legal. Ademais, tem-se como objetivos específicos mapear o arcabouço normativo brasileiro, caracterizar o uso dessas tecnologias, analisar os desafios enfrentados para garantir a proteção de dados pessoais e privacidade, quando o Estado implementa tecnologias de vigilância, no âmbito da segurança pública e levantar o conhecimento mais recente e avançado dentro da temática e as perspectivas para a regulamentação do tratamento de dados pessoais na segurança pública no Brasil. A pesquisa possui relevância para a academia ao oferecer uma sistematização do conhecimento produzido sobre um tema pouco explorado na literatura jurídica brasileira. Socialmente, contribui para o debate sobre políticas públicas que equilibrem a segurança e os direitos fundamentais constitucionalmente previstos.

Palavras-chave: LGPD, segurança pública, tecnologias de vigilância, proteção de dados.

ABSTRACT

The use of surveillance technologies by Brazilian public security forces coexists within a regulatory gap concerning the processing of personal data following the enactment of the General Data Protection Law (LGPD). This scenario raises the issue of how the legal exclusion of data processing for public security purposes affects the application of LGPD principles and what implications this holds for fundamental rights and legal certainty. It is argued that, despite the explicit exclusion of data processing for public security purposes from the LGPD's scope, its principles and the constitutionally recognized fundamental right to data protection may serve as indirect parameters to assess the legitimacy of such technologies. This study aims to analyze the scientific and regulatory output on this topic from 2020 to 2024, identifying the legal, technical, and institutional challenges arising from this legal exclusion. Moreover, its specific objectives include mapping the Brazilian regulatory framework, characterizing the use of such technologies, analyzing the challenges in ensuring personal data protection

and privacy when the State deploys surveillance technologies within the scope of public security, and identifying the most recent and advanced knowledge in the field, along with prospects for the regulation of personal data processing in public security in Brazil. The research is academically relevant by offering a systematization of the knowledge produced on a subject that remains underexplored in Brazilian legal literature. Socially, it contributes to the debate on public policies that seek to balance security and constitutionally guaranteed fundamental rights.

Keywords: LGPD, public security, surveillance technologies, data protection.

1 INTRODUÇÃO

O período entre 2020 e 2024 marca uma fase importante para a proteção de dados pessoais no Brasil, caracterizada pela implementação da Lei Geral de Proteção de Dados (LGPD) e pela crescente adoção de tecnologias de vigilância na segurança pública (Dalsenter, 2020) e (Menke; Levenfus, 2021). Neste contexto, o uso de sistemas de reconhecimento facial e câmeras corporais pelas forças policiais tem suscitado debates sobre privacidade e direitos fundamentais (Genghini; Oliveira; Fabretti, 2023) e (Santos, 2023).

A entrada em vigor da LGPD trouxe um paradoxo significativo: enquanto estabelece um marco regulatório abrangente para o tratamento de dados pessoais, exclui explicitamente de seu escopo as atividades de segurança pública, defesa nacional e investigação criminal (Nielsson; Rosa, 2023) e (Porto; Oliveira, 2021). Esta exclusão cria um vácuo regulatório particularmente problemático diante da expansão do uso de tecnologias de vigilância pelo Estado (Fernandes; Resende, 2023).

Neste cenário, emerge o seguinte problema de pesquisa: como a ausência de legislação específica para o tratamento de dados pessoais na segurança pública brasileira (2020-2024) impacta a aplicação dos princípios da LGPD no uso de tecnologias de vigilância e quais as implicações para direitos fundamentais e para segurança jurídica?

A hipótese que norteia esta investigação sugere que, apesar da exclusão do tratamento de dados para segurança pública do escopo da LGPD, seus princípios e o direito fundamental à proteção de dados podem servir como parâmetros indiretos para avaliar a legitimidade do uso de tecnologias de vigilância, criando um padrão mínimo de proteção mesmo na ausência de legislação específica.

Sustenta-se que, mesmo com a exclusão expressa do tratamento de dados para fins de segurança pública do escopo da LGPD, seus princípios e o direito

fundamental à proteção de dados constitucionalmente reconhecidos podem servir como parâmetros indiretos para avaliar a legitimidade dessas tecnologias.

O objetivo geral deste trabalho é analisar a produção científica sobre a aplicabilidade da LGPD no contexto do uso de tecnologias de vigilância na segurança pública brasileira entre 2020 e 2024, identificando os desafios jurídicos, técnicos e institucionais decorrentes da ausência de legislação específica.

Como objetivos específicos, busca-se: mapear o arcabouço normativo da proteção de dados no Brasil, com ênfase na LGPD e suas disposições relativas à segurança pública; caracterizar o uso de tecnologias de vigilância na segurança pública brasileira; comparar os desafios entre garantir a proteção de dados pessoais no contexto de necessidade de ampliação da vigilância estatal pelas forças de segurança pública; e levantar perspectivas para a regulamentação do tratamento de dados na segurança pública.

A urgência desta temática é corroborada pela crescente produção acadêmica e pelos desdobramentos normativos recentes. Conforme apontado por Wimmer (2021), a intensificação da coleta e do compartilhamento de dados pessoais decorrente da pandemia de Covid-19 evidenciou a ausência de critérios claros quanto às possibilidades e aos limites para o compartilhamento e uso secundário de dados pessoais no âmbito do poder público, fator que justificou e impulsionou debates e ações regulatórias no período.

Como resultado dos desafios e lacunas identificados, observa-se que, mesmo após o recorte temporal desta análise, o próprio Ministério da Justiça e Segurança Pública editou normativas como a Portaria MJSP Nº 961, de 24 de junho de 2025, que busca estabelecer diretrizes sobre o uso de soluções de tecnologia da informação em atividades de investigação criminal e inteligência de segurança pública, demonstrando a pertinência e a continuidade da problemática abordada.

Este trabalho segue a estrutura de um artigo científico, estruturado com introdução na seção 1, metodologia na seção 2, referencial teórico na seção 3, análise dos resultados na seção 4; discussões na seção 5; e, por fim, as conclusões na seção 6.

2 METODOLOGIA

A presente investigação se estrutura como uma pesquisa de natureza qualitativa, com caráter exploratório e abordagem predominantemente bibliográfica e documental. O objetivo geral deste estudo é analisar a produção científica sobre a aplicabilidade da LGPD no contexto do uso de tecnologias de vigilância na segurança pública brasileira entre 2020 e 2024, identificando os desafios jurídicos, técnicos e institucionais decorrentes da ausência de legislação específica.

O recorte temporal é justificado pelo amadurecimento do debate jurídico e acadêmico sobre a matéria, a partir de 2020, impulsionado pela promulgação da Emenda Constitucional nº 115/2022, que elevou a proteção de dados pessoais a direito fundamental, e pela discussão em torno do Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Persecução Penal (também conhecida como “LGPD Penal”).

As fontes de pesquisa abrangem produções científicas publicadas em periódicos especializados, bem como, defendidas em programas de pós-graduação, a legislação nacional pertinente (como a própria LGPD – Lei nº 13.709/2018, o Marco Civil da Internet – Lei nº 12.965/2014 e a Lei de Acesso à Informação – Lei nº 12.527/2011), a jurisprudência dos tribunais superiores (com destaque para decisões do Supremo Tribunal Federal – STF) e relatórios institucionais relevantes produzidos por órgãos como a Autoridade Nacional de Proteção de Dados (ANPD), o Conselho Nacional de Justiça (CNJ) e organizações da sociedade civil.

Foram priorizadas publicações que abordassem a lacuna legislativa na área, os desafios éticos e discriminatórios no uso dessas tecnologias, e as discussões sobre a necessidade de regulamentação específica e salvaguardas. Em contrapartida, foram excluídos materiais que se desviassem do recorte temporal ou da temática central, como estudos focados exclusivamente em segurança privada ou em contextos internacionais sem direta implicação para o cenário brasileiro.

Os procedimentos de coleta de dados incluíram a pesquisa sistemática em bases acadêmicas, como *Scielo*, *Google Scholar* e repositórios de teses e dissertações de universidades brasileiras. A análise normativa focou na interpretação de artigos da Constituição Federal, da LGPD (especialmente o Art. 4º, III), no Anteprojeto de Lei para a Proteção de Dados Pessoais do Ministério da Justiça (versões de 2010/2015) e no Anteprojeto de Lei de Proteção de Dados Pessoais para Segurança Pública e Persecução Penal, além do Projeto de Lei n.º 1515/2022

(Azevedo et al., 2022). Já a análise jurisprudencial concentrou-se em decisões do Supremo Tribunal Federal que tratam da proteção de dados pessoais e seu compartilhamento com órgãos públicos.

As técnicas de análise empregadas consistiram na revisão da literatura, associada à análise de conteúdo, permitindo a identificação de padrões recorrentes, lacunas regulatórias e desafios jurídicos, éticos, técnicos e institucionais na aplicação das tecnologias de vigilância. A abordagem buscou compreender a complexidade da interação entre a ausência de um marco legal específico para o setor, o papel supletivo dos princípios da LGPD (como finalidade, adequação, necessidade, transparência, segurança, prevenção, não discriminação e responsabilização/prestação de contas) e as implicações para os direitos fundamentais e a segurança jurídica.

Ressalta-se que, como limitação da pesquisa, a investigação é restrita ao período de 2020 a 2024, o que pode não capturar todo o histórico de desenvolvimento das tecnologias de vigilância no Brasil. Adicionalmente, a escassez de jurisprudência consolidada em temas tão recentes e a dependência de produções acadêmicas e relatórios institucionais que, por vezes, ainda se encontram em estágio inicial de amadurecimento científico, representam desafios inerentes à pesquisa em temas de fronteira tecnológica e jurídica.

A própria discussão sobre a necessidade e o formato de uma LGPD Penal ainda está em andamento, evidenciando a fluidez e as incertezas normativas no campo. Contudo, a rigor metodológico, tais limitações são entendidas como parte integrante da própria natureza da pesquisa em temas dinâmicos, contribuindo para a conscientização sobre a complexidade da matéria e a necessidade contínua de diálogo entre o Direito, a tecnologia e a sociedade.

3 REFERENCIAL TEÓRICO

A proteção de dados pessoais no Brasil é regida por um cenário normativo complexo e em constante evolução, que busca equilibrar o avanço tecnológico com a salvaguarda de direitos fundamentais. Este sistema é composto por diversas normas, sendo a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018 (Brasil, 2018), o principal marco regulatório.

A LGPD, inspirada no Regulamento Geral de Proteção de Dados da União Europeia (GDPR), busca proteger os direitos de liberdade e privacidade das pessoas

naturais, bem como o livre desenvolvimento de sua personalidade. Neste sentido, a LGPD insere o Princípio da Finalidade como pilar fundamental, o qual condiciona a realização do tratamento para propósitos específicos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades (Wimmer, 2021), estabelecendo um limite para o uso de dados pessoais.

Além da LGPD, outras normas e decisões judiciais fundamentais complementam e enriquecem o arcabouço da proteção de dados no país, conforme demonstrado na Tabela 1.

Tabela 1: principais Normas Constitucionais e Legais sobre Proteção de Dados Pessoais no Brasil

Norma / Dispositivo	**Conteúdo / Garantia**
Constituição Federal de 1988, Art. 5º, Inciso X	Garante a inviolabilidade da intimidade, vida privada, honra e imagem, assegurando direito à indenização por dano material ou moral.
Constituição Federal de 1988, Art. 5º, Inciso XII	Assegura o sigilo de correspondência e comunicações, permitindo sua quebra apenas por ordem judicial para investigação criminal ou instrução processual penal.
Constituição Federal de 1988, Art. 5º, Inciso LXXIX	Reconhece expressamente a proteção de dados pessoais, inclusive nos meios digitais, como direito fundamental, conforme Lei nº 115/2022.
Marco Civil da Internet (Lei nº 12.965/2014)	Estabelece princípios, garantias, direitos e deveres para o uso da internet, destacando privacidade e proteção de dados pessoais.
Lei de Acesso à Informação (Lei nº 12.527/2011)	Regulamenta o direito de acesso à informação pública, exigindo transparência e respeito à privacidade, vida privada, honra, imagem e garantias individuais.

Fonte: Elaborado pelo autor (2025).

O Supremo Tribunal Federal (STF) tem desempenhado um papel fundamental na interpretação e aplicação da proteção de dados pessoais. Notadamente, no julgamento da Ação Direta de Inconstitucionalidade (ADI) 6.387, o STF reconheceu a existência de um direito fundamental autônomo à proteção de dados pessoais e à autodeterminação informacional. Tal reconhecimento é fundamental, pois, como Wimmer (2021) salienta ao analisar o contexto da pandemia de Covid-19, essa decisão criou as bases para uma análise mais detalhada do tema.

Assim, em decisões como a Arguição de Descumprimento de Preceito Fundamental (ADPF) 695 e a ADI 6.649, o STF estabeleceu parâmetros rigorosos para o compartilhamento de dados pessoais por órgãos públicos.

Na ADPF 695, o Ministro Relator expressou que não há uma autorização irrestrita no ordenamento jurídico brasileiro ao livre fluxo e compartilhamento de dados no Poder Público (Wimmer, 2021), exigindo que convênios e acordos de compartilhamento baseados em disposições genéricas parecem afigurar-se potencialmente lesivos às garantias individuais, dependendo das condições e riscos envolvidos. Tais decisões reforçam que o compartilhamento de dados não pode ser amplo e irrestrito, mas sim balizado por critérios de proporcionalidade e transparência, em consonância com o Princípio da Finalidade.

Apesar do amplo escopo da LGPD, é fundamental destacar que a lei prevê exceções específicas para o tratamento de dados pessoais quando este é realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, conforme dispõem as alíneas do inciso III do art. 4º da Lei.

Conforme o Art. 4º, § 1º, da LGPD, o tratamento de dados nestes contextos será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observando o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos na própria LGPD. Tal exclusão não é meramente formal, mas, na prática, cria um vácuo regulatório substancial na ausência de uma lei específica para esses setores, um ponto que será aprofundado na próxima subseção.

3.1 A exceção legal da LGPD para fins de segurança pública, defesa nacional e segurança do Estado

A Lei Geral de Proteção de Dados Pessoais (LGPD), apesar de seu escopo amplo e abrangente sobre o tratamento de dados pessoais no Brasil, prevê em seu Art. 4º, inciso III, uma exclusão específica de sua incidência integral para o tratamento de dados realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (Nielsson; Rosa, 2023).

Tal ressalva significa que, para essas finalidades específicas, as normas da LGPD não se aplicam em sua totalidade (Oliveira; Oliveira; Silveira, 2025). É importante notar que a exclusão se restringe aos propósitos exclusivos dessas atividades, vale dizer, se um órgão de segurança tratar dados para outras finalidades (e.g., recursos humanos), a LGPD se aplica plenamente (Alves; Valadão, 2022).

Embora a LGPD estabeleça essa exceção, ela não resulta em uma desproteção absoluta dos dados pessoais nestes setores. O §1º do Art. 4º da própria LGPD impõe que o tratamento de dados para as finalidades excepcionadas será regido por legislação específica, a qual deve prever medidas proporcionais e estritamente necessárias para atender ao interesse público, e, indispensavelmente, observar o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos na LGPD (Dalsenter, 2020). A interpretação dessas exceções deve

ser restritiva, dada a primazia da LGPD em proteger direitos fundamentais como a liberdade e a privacidade (Alves; Valadão, 2022).

Apesar da previsão de uma legislação específica, essa lei ainda está em tramitação. Essa omissão gera um evidente vazio legislativo e uma lacuna normativa (Pessoa, 2025), possibilitando livre interpretação sobre o acesso e tratamento de dados pessoais no âmbito penal e da segurança pública (Nielsson; Rosa, 2023).

Diante de tal lacuna legislativa no ordenamento jurídico brasileiro – uma vez que a LGPD excetua o tratamento de dados para fins exclusivos de segurança pública e persecução penal (Art. 4º, III) e exige legislação específica – identificaram-se diversos desafios no período de 2020 a 2024. Tais desafios estão majoritariamente ligados à ausência de um marco normativo que harmonize a proteção de dados com o interesse público. A tabela 2 apresenta tais desafios:

Tabela 2: Desafios identificados na literatura a partir da vigência da LGPD

Desafios	Referência
Incerteza jurídica e falta de balizas claras para a atuação dos órgãos de segurança e persecução penal no uso de dados pessoais, o que, em rigor, pode levar à imprevisibilidade pelo indivíduo sobre o uso de seus dados	(Pessoa, 2025) e (Bioni *et al.*, 2020)
Rápida e desregulamentada adoção de novas tecnologias, como o uso crescente de sistemas de reconhecimento facial, inteligência artificial e *big data* na segurança pública, acarretando riscos de vigilância em massa e controle excessivo sobre a população	(Araújo; Cardoso; Paula, 2021) e (Dalsenter, 2020)
Vulnerabilidade e risco de violação a direitos fundamentais (como privacidade, intimidade e o direito à não discriminação) decorrentes da falta de parâmetros legais e do potencial uso indevido de dados pessoais sensíveis	(Nielsson; Rosa, 2023)
Ocorrência e potencialização de vieses algorítmicos, especialmente em tecnologias como o reconhecimento facial, resultando em identificações erradas e na perpetuação da seletividade do sistema penal brasileiro, afetando desproporcionalmente grupos vulneráveis, como a população negra	(Battaglin; Vieira, 2020) e (Daguer; Borri; Soares, 2022)
Déficit de transparência e *accountability* no tratamento de dados, dificultando a prestação de contas pelo Estado e o controle social e democrático sobre as atividades policiais e de inteligência	(Nielsson; Rosa, 2023)
Incompatibilidade com padrões internacionais de segurança e tratamento de dados, o que afeta a eficiência investigativa dos órgãos brasileiros e a cooperação transnacional	(Nielsson; Rosa, 2023)

Fonte: Elaborado pelo autor (2025).

É importante ressaltar que, em resposta a esta lacuna e aos desafios identificados no período de 2020 a 2024, órgãos como o Ministério da Justiça e Segurança Pública têm emitido normas infralegais. Um exemplo notório é a Portaria MJSP Nº 961, de 24 de junho de 2025 (Brasil, 2025), que, embora posterior ao recorte temporal desta pesquisa, atesta a pertinência da discussão ao estabelecer diretrizes sobre o uso de soluções de tecnologia da informação em atividades de investigação criminal e inteligência de segurança pública, buscando alinhar a atuação dos órgãos aos princípios de proteção de dados, como o devido processo legal e a proteção de dados pessoais.

A tabela 3 explicita as consequências práticas da omissão legislativa.

Tabela 3: Problemas causados pela omissão legislativa

Problema	Referência
Ausência de uniformidade nacional nos sistemas de identificação criminal, como o reconhecimento facial, resultando em diferentes abordagens por cada estado.	(Araújo; Cardoso; Paula, 2021)
Imprevisibilidade para o cidadão sobre como seus dados serão utilizados.	(Bioni *et al.*, 2020)
Falta de bases legais claras e precisas para muitas intervenções informacionais do Estado, o que pode subverter o direito à autodeterminação informacional.	(Bioni *et al.*, 2020) e (Fernandes; Resende, 2023)
Dependência da doutrina e da jurisprudência para definir a extensão da proteção de dados, utilizando princípios jurídicos que são, por natureza, mais vagos e imprecisos na ausência de lei formal.	(Alves; Valadão, 2022)
Preocupação com o tratamento irrestrito de dados por tecnologias de vigilância de "alto risco" aos direitos fundamentais.	(Daguer; Borri; Soares, 2022) e (Marwell, 2024)
Situações em que as atividades de segurança pública são realizadas sem amparo legal adequado ou com base em normas processuais penais que não foram concebidas para o tratamento de dados.	(Bioni *et al.*, 2020) e (Marwell, 2024)

Fonte: Elaborado pelo autor (2025).

A doutrina majoritária aponta a urgência e a necessidade de uma legislação específica. Alguns autores classificam a omissão como um erro de legística (Aras, 2024), pois as sensíveis questões da segurança pública e persecução criminal deveriam ter sido regulamentadas simultaneamente à LGPD geral. A elaboração de uma Lei Geral de Proteção de Dados (LGPD) no âmbito da segurança pública e penal, frequentemente referida como "LGPD Penal", é vista como um instrumento normativo importante para garantir o direito fundamental da proteção de dados pessoais, preservando os direitos humanos e a integridade do indivíduo (Oliveira, Loryne Viana *et al.*, 2022).

Existem discussões em torno de anteprojetos e projetos de lei, como o Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Persecução Penal e o PL nº 1.515/2022 (Castro; Paula, 2022) e (Daguer; Borri; Soares, 2022). Tais projetos buscam suprir o vácuo legislativo e estabelecer parâmetros para o acesso, utilização e tratamento de dados pessoais, garantindo a segurança jurídica.

Contudo, há críticas sobre a supressão de garantias dos titulares e a excessiva ampliação do poder discricionário do Estado em algumas dessas propostas (Fernandes; Resende, 2023). O ideal é que a nova legislação seja alinhada aos princípios da reserva de lei e da proporcionalidade, que exigem autorização expressa em lei para qualquer intervenção estatal que afete direitos fundamentais, especialmente na era da vigilância massiva (Souza, 2022a).

O cenário atual, com a ausência de uma lei específica para o tratamento de dados pessoais na segurança pública e persecução penal, representa um grave déficit legislativo (Pessoa, 2025). Esse vácuo normativo acarreta riscos substanciais à legalidade, proporcionalidade e transparência nas práticas de vigilância. A tabela 4, a seguir, apresenta os riscos que a ausência de normas claras pode desencadear.

Tabela 4: riscos decorrentes da ausência de normas claras no tratamento de dados pessoais na segurança pública

Risco	Descrição	Referências
Discricionariedade excessiva	Atuação policial e investigativa sem limites definidos, podendo gerar abusos.	(Souza, 2022)
Insegurança jurídica	Cidadãos perdem controle sobre seus dados e não sabem como serão utilizados; órgãos operam em zona cinzenta.	(Bioni et al., 2020); (Patz; Piaia, 2022)
Violação de direitos fundamentais	Privacidade e não discriminação ameaçadas, especialmente com reconhecimento facial, que pode amplificar vieses e afetar grupos marginalizados.	(Kremer; Silva, 2022)
Uso de cláusulas gerais de autorização	Permite intervenções estatais imprevisíveis e sem limites, subvertendo a autodeterminação informacional.	(Souza, 2022)

Fonte: Elaborado pelo autor (2025).

Para superar tais riscos, é imprescindível a atuação do Poder Legislativo para suprir a lacuna e editar uma legislação específica, estabelecendo requisitos claros para o tratamento de dados pessoais que garantam o mínimo de restrição aos direitos fundamentais (Marwell, 2024). Além disso, os Tribunais Superiores precisam estar atentos à ilegalidade/ilegitimidade de intervenções sem fundamento legal e continuar exigindo a ação legislativa (Bioni *et al.*, 2020).

3.2. Caracterização do uso de tecnologias de vigilância na segurança pública (2020-2024)

No período de 2020 a 2024, alvo da presente pesquisa, verificou-se que o Brasil vivenciou uma expansão significativa no uso de tecnologias de vigilância na segurança pública, impulsionada pelo desenvolvimento da inteligência artificial (IA) e pela crescente captação de dados, embora com notáveis lacunas regulatórias (Bioni *et al.*, 2020). A digitalização da sociedade tem levado à utilização de diversas ferramentas que, se por um lado prometem maior eficiência na prevenção e repressão de crimes, por outro, levantam sérias questões sobre a proteção dos direitos fundamentais dos cidadãos (Battaglin; Vieira, 2020).

Durante a pesquisa, foram catalogadas as principais tecnologias de vigilância empregadas no cenário brasileiro, cuja regulamentação ainda se mostra incipiente, mas, em evolução. Um exemplo deste movimento regulatório, que reflete os debates do período de 2020-2024, é a Portaria MJSP Nº 961, de 24 de junho de 2025, que aborda o uso de tais soluções. Notadamente, esta Portaria estabelece diretrizes para soluções de inteligência artificial e impõe vedações específicas, como a de identificação biométrica à distância, em tempo real, em espaços acessíveis ao público, exceto em casos específicos e mediante autorização judicial (Brasil, 2025, Art. 10 e Art. 11, § 1º). Este detalhamento ilustra a complexidade e os desafios inerentes à gestão dessas ferramentas.

Diante disso, a Tabela 5 apresenta a catalogação das principais tecnologias de vigilância empregadas no cenário brasileiro.

Tabela 5: principais tecnologias de vigilância

Tecnologia	Aplicações	Desafios/Críticas	Fontes
Reconhecimento Facial (RF) - detecta rostos, padroniza e extrai características para comparar com bancos de dados, emitindo pontuação de semelhança	Identificação em multidões, busca de criminosos, garantia de cumprimento de penas, prevenção de fraudes em transportes públicos, identificação de suspeitos em locais de crime	Altos índices de erro (92% na UEFA Champions League 2017, 90% carnaval carioca 2019), tendência preconceituosa contra mulheres negras, 90,5% dos presos por monitoramento facial no Brasil são negros Importante: A Portaria MJSP Nº 961/2025 (Brasil, 2025, Art. 11, § 1º) veda a identificação biométrica à distância, em tempo real, em espaços públicos, com exceções condicionadas à autorização judicial	Dalsenter, 2020; Araújo; Cardoso; Paula, 2021; Andréa; Silva; Gundim, 2022; Taute, 2020 Brasil, 2025
Videomonitoramento Inteligente e Câmeras Operacionais Portáteis (COPs/Bodycams) - câmeras de vigilância em espaços públicos e câmeras portáteis usadas por polícias militares	Documentar evidências, aumentar transparência e controle social, reduzir violência e uso excessivo da força, material para treinamento	Discricionariedade na ativação/interrupção das gravações, dificuldade de acesso aos dados, potencial desvio de finalidade, controvérsia sobre existência/fidedignidade das imagens	Galeano; Guareschi, 2023; Santos, 2023; Genghini; Oliveira; Fabretti, 2023
Bancos de Dados Biométricos - grandes bases de dados biométricos para vigilância em massa	Reconhecimento facial, cadastros nacionais de pessoas condenadas, registro de medidas protetivas	Preocupações sobre privacidade, acurácia depende da qualidade dos bancos de dados	Taute, 2020; Araujo; Araujo Junior; Albuquerque, 2023; Souza, 2022
Sistemas Preditivos e de Análise Comportamental (Policiamento Preditivo) - análise de grandes volumes de dados e IA para prever crimes e traçar estratégias	Previsão de crimes, otimização de recursos, identificação de padrões suspeitos, mapeamento de locais e horários de incidência criminal	Risco de enviesamento/discriminação de grupos sociais, classificações automatizadas de comportamento suspeito/perigoso	Daguer; Borri; Soares, 2022; Fernandes; Resende, 2023; Taute, 2020
Plataformas de Integração de Dados (Interoperabilidade entre Órgãos) - integração de dados de diversas fontes para apoiar decisões em segurança pública	Combate ao crime organizado, furto de veículos, leitura de placas, análise de padrões	Ausência de transparência, necessidade de parâmetros rigorosos para compartilhamento de dados segundo STF, críticas à supervisão pública	Bioni et al., 2020; Marwell, 2024; Supremo Tribunal Federal, 2022; Pessoa, 2025

Fonte: Elaborado pelo autor (2025).

A análise da literatura evidencia um equilíbrio instável entre a busca por maior eficiência na ação do Estado e a necessidade de resguardar direitos fundamentais frente ao avanço dessas tecnologias (Daguer; Borri; Soares, 2022). Destaca-se ainda, que a Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018), inspirada no GDPR europeu, classifica dados biométricos como sensíveis (Battaglin; Vieira, 2020).

Embora a LGPD não se aplique integralmente a atividades de segurança pública e persecução penal (Art. 4º, III), ela exige que o tratamento de dados nesses contextos seja regido por legislação específica que preveja medidas proporcionais e estritamente necessárias, observando o devido processo legal e os princípios gerais

de proteção de dados (Taute, 2020), revelando, assim, uma lacuna normativa no ordenamento jurídico brasileiro (Daguer; Borri; Soares, 2022).

4 ANÁLISE DOS RESULTADOS

A implementação de tecnologias de vigilância pelo Estado no âmbito da segurança pública no Brasil enfrenta uma série de desafios complexos, que se manifestam nas esferas jurídica, técnica e institucional. Além disso, a governança dessas tecnologias levanta questões significativas relacionadas aos custos envolvidos.

Quanto aos desafios para a proteção de dados pessoais e privacidade na implementação de tecnologias de vigilância pelo Estado, temos que a digitalização crescente da sociedade e o uso massivo de tecnologias biométricas como o reconhecimento facial (RF) e as câmeras corporais (COP) pelas autoridades estatais têm intensificado o debate sobre o tema (Andréa; Silva; Gundim, 2022). A categorização, que abrange as esferas jurídica, técnica e institucional, é importante para compreender a complexidade da matéria, conforme detalhado na Tabela 6.

Tabela 6: categorização dos desafios na implementação de tecnologias de vigiância

Categoria	Desafio	Descrição com Referências
Jurídicos	Vácuo Normativo e Falta de Legislação Específica	A Lei Geral de Proteção de Dados (Lei nº 13.709/2018) exclui do seu âmbito de aplicação o tratamento de dados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (Nielsson; Rosa, 2023). Apesar da existência de um Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Persecução Penal (LGPD Penal), sua tramitação ainda pendente gera incerteza jurídica e ausência de balizas claras para a atuação estatal (Araújo; Cardoso; Paula, 2021). Iniciativas normativas como a Portaria MJSP Nº 961/2025 (Brasil, 2025) surgem como respostas infralegais, mas reiteram a necessidade de um marco legal mais robusto.
	Violação de Direitos Fundamentais	O uso indiscriminado de tecnologias de vigilância, como o reconhecimento facial (RF), ameaça direitos fundamentais como privacidade, intimidade, honra, imagem, liberdade de locomoção, igualdade e não discriminação (Andréa; Silva; Gundim, 2022). Dados biométricos, incluindo RF, são dados pessoais sensíveis e requerem maior rigor de proteção (Patz; Piaia, 2022).
	Ausência de Consentimento e Transparência	Frequentemente, a coleta de dados biométricos ocorre de forma compulsória, sem consentimento prévio, e sem transparência sobre coleta, uso, armazenamento e compartilhamento, dificultando a fiscalização social (Taute, 2020;(Instituto de Pesquisa em Direito e Tecnologia do Recife, 2024).
	Princípios da Proporcionalidade e Necessidade	O uso da tecnologia de RF deve ser proporcional e estritamente necessário ao interesse público, observando o devido processo legal (Fernandes, Maíra; Meggiolaro; Prates, 2022).
	Responsabilidade do Estado	O tratamento indevido de dados pessoais por órgãos públicos pode gerar responsabilidade civil do Estado e responsabilização dos agentes (Supremo Tribunal Federal, 2022b). A Portaria MJSP Nº 961/2025 (Brasil, 2025, Art. 15) expressamente prevê que o uso indevido das soluções de TI sujeitará o responsável à responsabilização administrativa, civil e criminal. A LGPD e propostas correlatas buscam delimitar essa responsabilização (Oliveira, et al., 2022).
	Impacto no Devido Processo Legal e Presunção de Inocência	A vigilância massiva e automatização de decisões podem comprometer o direito à ampla defesa e a presunção de inocência, especialmente diante de prisões equivocadas ou estigmatização (Daguer; Borri; Soares, 2022). A Portaria MJSP Nº 961/2025 (Brasil, 2025, Art. 2º, IV) busca mitigar esse risco

		ao valorizar o devido processo legal e o Art. 3º, IV, ao focar na cadeia de custódia da prova para manter a integridade de elementos informativos.
Técnicos	Vieses Algorítmicos e Discriminação	Algoritmos de RF treinados com dados enviesados tendem a apresentar erros e discriminação contra grupos vulneráveis, como negros, mulheres e pessoas não-binárias (Dalsenter, 2020). Há registros de prisões decorrentes de falhas nesses sistemas (Daguer; Borri; Soares, 2022).
	Acurácia e Confiabilidade	A confiabilidade da RF é controversa, demandando testes padronizados e independentes para aferição de taxas de erro (Instituto de Pesquisa em Direito e Tecnologia do Recife, 2024)
	Segurança dos Dados e Vazamentos	O armazenamento de grandes volumes de dados sensíveis amplia riscos de vazamento e acessos não autorizados, exigindo medidas técnicas e administrativas robustas (Nascimento; Barros; Pinto, 2024).
	Opacidade e Ininteligibilidade	A complexidade e autonomia da IA podem dificultar a compreensão e supervisão das decisões automatizadas, prejudicando o controle humano (Santos, 2023).
Institucionais	Falta de Órgão Central de Regulação e Fiscalização Efetivo	A ANPD, criada pela LGPD, não exerce coordenação efetiva sobre tecnologias de alto risco na segurança pública. O Anteprojeto da LGPD Penal prevê um Conselho Nacional de Proteção de Dados na Segurança Pública, com funções consultivas, deliberativas e fiscalizadoras (Araújo; Cardoso; Paula, 2021; Bioni et al., 2020). A Portaria MJSP Nº 961/2025 (Brasil, 2025, Art. 14) atribui o acesso aos logs a autoridades com competência legal para realizar o controle, mas sem especificar um órgão centralizador, ressaltando o desafio de fiscalização.
	Resistência Institucional à Regulação	Há resistência de corporações policiais e políticas estatais à adoção de mecanismos de responsabilização pelo uso indevido de tecnologias de vigilância (Galeano; Guareschi, 2023).
	Capacitação e Cultura de Proteção de Dados	Falta cultura consolidada de proteção de dados e capacitação profissional adequada entre operadores que tratam dados pessoais sensíveis, aumentando o risco de violações (Gunther; Comar; Rodrigues, 2020).
	Parcerias Público-Privadas Desreguladas	A terceirização do uso de RF à iniciativa privada, mesmo para fins legítimos, apresenta riscos pela ausência de controle sobre o uso real dos dados, que podem ser explorados comercialmente (Andréa; Silva; Gundim, 2022).
	Interesses Político-Criminais	A prioridade política-criminal na repressão tende a flexibilizar direitos e garantias em nome do combate ao crime, dificultando a implementação de salvaguardas rígidas (Macri Júnior; Macri; Frontini, 2023).

Fonte: Elaborado pelo autor (2025).

Os custos relacionados à implementação de tecnologias de vigilância integram os desafios de governança, principalmente quanto à sustentabilidade financeira e à conformidade com a LGPD e outras normas (Costa, 2024; Paiva; Lanzillo, 2023).

As referências consultadas mencionam alguns valores e sua natureza, mas não discriminam explicitamente as despesas de aquisição de hardware em relação à manutenção de software. A seguir, a Tabela 7 sintetiza os principais aspectos econômicos identificados na literatura, com as respectivas descrições e fontes.

Tabela 7: custos para implementação de tecnologias de vigilância

Aspecto Econômico/Financeiro	Descrição com Referências
Custos de Implementação de Projetos	Projetos que envolvem tratamento de dados pessoais, como sistemas de reconhecimento facial, acarretam custos significativos (Souza, 2022b). A detecção prévia de ameaças e o desenvolvimento de salvaguardas antes da implementação podem reduzir esses custos.
Investimento em Infraestrutura Digital	O Ministério da Justiça investiu milhões de reais em infraestrutura digital para facilitar a integração e análise de grandes volumes de dados na segurança pública, incluindo tecnologias como Big Data e Inteligência Artificial (Costa, 2024).
Financiamento e Orçamento	Em democracias consolidadas, o compartilhamento de dados pode enfrentar riscos financeiros decorrentes de financiamento insuficiente ou instável, impactando a manutenção e aprimoramento dos sistemas (Supremo Tribunal Federal, 2022b).
Custo-Benefício da Interoperabilidade	A gestão de ferramentas digitais deve considerar o custo-benefício da interoperabilidade de informações e dados, sugerindo avaliação econômica para integração e manutenção (Supremo Tribunal Federal, 2022a).
Avaliação de Impacto Regulatório	Regulamentações sobre tecnologias de monitoramento devem ser acompanhadas de avaliação de impacto regulatório (Santos, 2021; Daguer; Borri; Soares, 2022), descrevendo

	escopo, capacidades tecnológicas e possíveis impactos desproporcionais sobre populações específicas (Araujo; Araujo Junior; Albuquerque, 2023).

Fonte: Elaborado pelo autor (2025).

Da análise da pesquisa, verificou-se que os custos de implementação das tecnologias de vigilância na segurança pública são um fator relevante nos desafios de governança, pois afetam a capacidade do Estado de garantir a conformidade e a segurança dos dados. No entanto, as fontes não detalham especificamente os custos de compra de hardware ou de manutenção de software, abordando-os mais amplamente como "custos de aplicação", "investimento em infraestrutura digital" ou "financiamento".

5 DISCUSSÃO DOS RESULTADOS

A presente pesquisa analisou como a ausência de legislação específica para o tratamento de dados pessoais no âmbito da segurança pública brasileira, no período de 2020 a 2024, afeta a aplicação dos princípios da Lei Geral de Proteção de Dados (LGPD) no uso de tecnologias de vigilância, e quais as implicações para os direitos fundamentais e a segurança jurídica.

A hipótese central que norteou este estudo postulava que, apesar da exclusão expressa do tratamento de dados para fins de segurança pública do escopo direto da LGPD, seus princípios e o direito fundamental à proteção de dados podem, ainda assim, servir como parâmetros indiretos para avaliar a legitimidade do uso de tecnologias de vigilância, estabelecendo um padrão mínimo de proteção na ausência de regulamentação específica. Com base na análise do arcabouço normativo, da caracterização do uso de tecnologias de vigilância, da comparação dos desafios e do levantamento de perspectivas regulatórias, a hipótese foi amplamente confirmada.

O reconhecimento da proteção de dados pessoais como um direito fundamental no Brasil, por meio da Emenda Constitucional nº 115/2022 e de decisões do Supremo Tribunal Federal (STF), como as proferidas nas ADIs 6.387 e 6.529 e ADPF 695 (Alves; Valadão, 2022), eleva a proteção da autodeterminação informacional a um patamar de inalienabilidade, impondo ao Estado um dever de abstenção e exigindo justificação especial para qualquer intervenção (Souza, 2022a).

Essa perspectiva é amplamente compartilhada na literatura, com Wimmer (2021) destacando que a autodeterminação informativa é comprometida caso indivíduos não saibam quais informações a seu respeito são conhecidas e para quais finalidades tais informações são coletadas e tratadas.

Este marco constitucional e jurisprudencial é importante, pois, mesmo que a LGPD em seu Art. 4º, inciso III, e § 1º, explicitamente exclua o tratamento de dados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais de sua aplicação direta, ela remete a necessidade de legislação específica que preveja medidas proporcionais e estritamente necessárias, observando o devido processo legal, os princípios gerais de proteção e os direitos do titular (Nielsson; Rosa, 2023).

A inexistência de lei específica para reger o tratamento de dados pessoais em atividades de segurança pública e persecução penal levou o Ministério da Justiça e Segurança Pública, no período pós-pesquisa, a editar normas de caráter infralegal para mitigar essa lacuna. Um exemplo é a Portaria MJSP nº 961, de 24 de junho de 2025, que estabelece diretrizes para o uso de soluções de tecnologia da informação em investigações criminais e inteligência.

As diretrizes nela fixadas são orientadas por valores como o respeito aos direitos e às garantias fundamentais, a inviolabilidade da intimidade e o direito à proteção de dados pessoais, além de imporem condições de legalidade, adequação, necessidade e proporcionalidade e preverem mecanismos de transparência e prestação de contas. Trata-se, entretanto, de instrumento administrativo que não substitui a legislação abrangente exigida pelo art. 4º, § 1º, da LGPD, evidenciando que o ordenamento jurídico ainda carece de um marco legal robusto para disciplinar o tema.

Diante do exposto, a ausência de legislação específica para o tratamento de dados pessoais na segurança pública brasileira, conforme previsto na LGPD, gera um vácuo normativo significativo (Araújo; Cardoso; Paula, 2021). Esta lacuna tem implicações diretas e profundas nos direitos fundamentais dos cidadãos e na segurança jurídica, pois sem parâmetros legais claros e detalhados, há um risco acentuado de uso abusivo das tecnologias de vigilância (Almeida, 2022), como o reconhecimento facial e as câmeras corporais, que já são amplamente utilizadas em diversas capitais brasileiras.

A falta de regulamentação específica permite que a atividade estatal seja conduzida com discricionariedade excessiva (Santos, Alexandre Claudino Simas, 2023) e (Supremo Tribunal Federal, 2022b), expondo os indivíduos a uma vigilância massiva e contínua que pode comprometer sua privacidade, intimidade,

autodeterminação informacional, e o livre desenvolvimento da personalidade (Souza, 2022a). Em tal contexto, a instrumentalização do direito penal e das políticas de segurança sem um contraponto regulatório robusto pode aprofundar as desigualdades sociais existentes (Santos, 2021).

Apesar do vácuo legislativo específico, a pesquisa demonstrou a possibilidade de aplicação indireta dos princípios da LGPD como salvaguardas essenciais. O STF, em suas decisões, tem consistentemente estabelecido que o tratamento de dados pessoais pelo Poder Público, mesmo em atividades de inteligência ou compartilhamento de informações, deve observar princípios como a finalidade legítima e explícita, adequação, necessidade, transparência e segurança (Supremo Tribunal Federal, 2022b).

Wimmer (2021) corrobora tal visão ao argumentar que a divisão informacional de poderes impede que o governo seja tratado como uma única unidade informacional, exigindo que as funções específicas de cada agência e a finalidade que conduziu à coleta dos dados determinem o acesso à informação. Este rigor também é refletido em iniciativas recentes, como a Portaria MJSP Nº 961/2025 (Brasil, 2025), que, embora infralegal, exige que a utilização de soluções de tecnologia seja proporcional e observe o dever de prevenção de riscos e as leis aplicáveis (Art. 10), além de impor controle de acesso, auditorias e logs de utilização (Cap. III e IV), consolidando a aplicação prática desses princípios.

Isso inclui a exigência de medidas proporcionais e estritamente necessárias para atender ao interesse público, a instauração de procedimento administrativo formal com motivação prévia, permitindo controle judicial, e a utilização de sistemas eletrônicos de segurança e registro de acesso para responsabilização em caso de abuso (Supremo Tribunal Federal, 2022b). Além disso, a Agência Nacional de Proteção de Dados (ANPD) pode emitir opiniões técnicas e recomendações, e solicitar relatórios de impacto à proteção de dados pessoais (RIPD) referentes às exceções do Art. 4º da LGPD (Costa, 2024).

A obrigatoriedade de elaborar RIPD para operações de alto risco, incluindo as tecnologias de vigilância, é fundamental para mitigar danos e garantir a conformidade (Supremo Tribunal Federal, 2022b). Tais princípios funcionam como uma salvaguarda mínima, mas seus limites são evidentes: eles são, por natureza, vagos e imprecisos sem uma lei que os concretize com regras detalhadas para coleta, armazenamento,

uso e compartilhamento de dados, bem como sanções claras (Alves; Valadão, 2022). Sem essa especificação, a aplicação se torna casuística e sujeita a interpretações que podem não garantir a efetiva proteção dos direitos.

Dada a confirmação da hipótese e as graves implicações da lacuna normativa, as perspectivas e recomendações para uma futura regulamentação específica são urgentes. A prioridade deve ser a aprovação de uma LGPD Penal que preencha esse vácuo legislativo, oferecendo segurança jurídica tanto para as autoridades quanto para os cidadãos (Alves; Valadão, 2022). A tabela 8 apresenta sugestões de diretrizes para esta legislação.

Tabela 8: sugestões de diretrizes para uma futura LGPD Penal

Diretriz	Descrição com Referências
Definição do Escopo	É necessário estabelecer definições claras sobre o escopo do tratamento de dados, especificando as finalidades e capacidades das tecnologias de vigilância (Souza, 2022a). A Portaria MJSP Nº 961/2025 (Brasil, 2025, Art. 2º, V; Art. 3º, I; Art. 10) reitera a indispensabilidade desses princípios na aplicação das tecnologias de TI.
Proporcionalidade e Necessidade	Os princípios da proporcionalidade e necessidade devem constituir balizas inafastáveis, limitando o uso de dados ao estritamente indispensável (Supremo Tribunal Federal, 2022b).
Relatórios e Análises de Impacto	Tornar obrigatória a elaboração de Relatórios de Impacto à Proteção de Dados (RIPD) e Análises de Impacto Regulatório (AIR) para tecnologias de alto risco, acompanhados de consulta pública e transparência na tomada de decisão (Supremo Tribunal Federal, 2022a)
Transparência	Garantir a transparência na coleta, uso e compartilhamento de dados, com informações claras e acessíveis sobre procedimentos e práticas adotadas por órgãos públicos (Supremo Tribunal Federal, 2022b). A Portaria MJSP Nº 961/2025 (Brasil, 2025, Art. 2º, VIII; Art. 3º, VI) prevê mecanismos de transparência e transparência das contratações, respectivamente.
Responsabilização e Controle	Prever mecanismos robustos de responsabilização e controle, como a criação de órgão supervisor multissetorial (ex.: Conselho Nacional de Proteção de Dados na Segurança Pública ou ampliação do poder fiscalizatório do CNJ), auditorias independentes, sistemas auditáveis e aplicação de sanções civis, administrativas e criminais para tratamento ilícito (Supremo Tribunal Federal, 2022a) e (Supremo Tribunal Federal, 2022b). A Portaria MJSP Nº 961/2025 (Brasil, 2025, Cap. III, IV e Art. 15) estabelece obrigações claras para órgãos gestores, registros de log e responsabilização em caso de uso indevido.
Viés Algorítmico	Abordar o problema do viés algorítmico, fomentando a criação de algoritmos imparciais que assegurem a isonomia nas decisões automatizadas (Souza, 2022b). A Portaria MJSP Nº 961/2025 (Brasil, 2025, Art. 10, Parágrafo único) prevê revisão dos resultados da inferência algorítmica na hipótese de haver risco de lesão a direitos fundamentais.
Modelo das Duas Portas	Adotar o modelo das duas portas no compartilhamento de dados entre diferentes esferas e finalidades, de forma a impedir o uso indiscriminado de dados coletados para finalidades específicas (Souza, 2022a) e (Bioni *et al.*, 2020). A Portaria MJSP Nº 961/2025 (Brasil, 2025, Art. 7º, § 1º) demonstra um avanço nesse sentido ao condicionar o uso de soluções de TI para obtenção de dados sigilosos a decisão judicial específica, exigindo indicação do procedimento investigativo e cópia da decisão.
Contextualização Nacional	Considerar as peculiaridades do contexto brasileiro, evitando a simples transposição de modelos estrangeiros e promovendo o desenvolvimento tecnológico autóctone (Oliveira et al., 2022).
Participação Social	Incentivar o diálogo multissetorial e a participação da sociedade civil na formulação e fiscalização das políticas de segurança pública que envolvem o uso de tecnologias (Instituto de Pesquisa em Direito e Tecnologia do Recife, 2024)

Fonte: Elaborado pelo autor (2025).

Em suma, a proteção de dados na segurança pública brasileira é um campo de intensa tensão entre a busca por eficiência estatal e a garantia de direitos fundamentais. A LGPD e seu reconhecimento constitucional como direito fundamental fornecem o alicerce principiológico para a proteção, mas a efetividade plena dependerá da promulgação de uma legislação específica (a LGPD Penal) que, de forma coerente com o Estado Democrático de Direito, harmonize esses interesses,

estabeleça balizas claras e promova mecanismos de controle e responsabilização, assegurando que o avanço tecnológico não se traduza em uma sociedade de vigilância em detrimento das liberdades individuais.

6 CONCLUSÃO

A presente pesquisa teve por objetivo analisar de que forma a ausência de legislação específica para o tratamento de dados pessoais na segurança pública brasileira, no período de 2020 a 2024, afeta a aplicação dos princípios da Lei Geral de Proteção de Dados (LGPD) no uso de tecnologias de vigilância, bem como identificar as implicações jurídicas e constitucionais dessa lacuna para os direitos fundamentais e para a segurança jurídica.

Para alcançar tal propósito, foram mapeados o arcabouço normativo brasileiro, caracterizado o uso das principais tecnologias de vigilância empregadas pelas forças de segurança pública, comparados os desafios entre a proteção de dados pessoais e a expansão da vigilância estatal, bem como, levantadas as perspectivas para a regulamentação futura do tratamento de dados no setor.

A análise realizada confirmou integralmente a hipótese da pesquisa, segundo a qual, ainda que o artigo 4º, inciso III, da LGPD exclua do seu escopo direto o tratamento de dados pessoais para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou persecução penal, os princípios da LGPD, aliados ao direito fundamental à proteção de dados pessoais consagrado pela Emenda Constitucional nº 115/2022, mantêm aplicabilidade indireta e funcionam como balizas de legitimidade para o uso das tecnologias de vigilância pelo Estado (Nielsson; Rosa, 2023; Alves; Valadão, 2022; Costa, 2024).

Ademais, os princípios — finalidade, adequação, necessidade, transparência, segurança, prevenção, não discriminação e responsabilização — assumem papel estruturante e vinculante para a Administração Pública, devendo orientar o tratamento de dados pessoais, mesmo quando realizado sob a justificativa da segurança pública. Tal entendimento decorre da natureza constitucionalmente qualificada da proteção de dados pessoais, reconhecida pelo Supremo Tribunal Federal em precedentes paradigmáticos, como as decisões proferidas nas ADPF 695 e ADI 6.529, que estabeleceram a obrigatoriedade da adoção de medidas proporcionais, estritamente

necessárias e previamente motivadas, com sistemas de segurança e registros de acesso auditáveis (Supremo Tribunal Federal, 2022b).

Constatou-se que a inexistência de legislação específica para reger o tratamento de dados pessoais na segurança pública produz um cenário de insegurança jurídica tanto para os cidadãos, desprovidos de garantias concretas de controle sobre suas informações, quanto para os próprios agentes estatais, que operam em ambiente normativo difuso e incerto (Marwell, 2024; Pessoa, 2025). Tal omissão legislativa amplia a discricionariedade administrativa e permite a implementação de políticas de vigilância com potencial violador da privacidade, intimidade, igualdade e autodeterminação informacional (Souza, 2022a; Bioni et al., 2020).

O estudo também demonstrou que a lacuna normativa favorece a vigilância massiva e contínua de cidadãos, sem critérios claros de legalidade, finalidade ou proporcionalidade (Santos, Alexandre Claudino Simas, 2023), e potencializa riscos de viés algorítmico e discriminação em razão do uso de tecnologias, tais como o reconhecimento facial e os sistemas de policiamento preditivo, que tendem a reproduzir padrões históricos de seletividade penal (Daguer; Borri; Soares, 2022; Almeida, 2022).

Apesar desta lacuna, a pesquisa confirmou que os princípios da LGPD podem e devem ser aplicados como parâmetros indiretos de controle da legalidade e da proporcionalidade. O Supremo Tribunal Federal, ao decidir sobre o compartilhamento de dados entre órgãos públicos, reconheceu que o tratamento de informações pessoais deve observar as garantias constitucionais de finalidade legítima, necessidade, transparência e segurança (Supremo Tribunal Federal, 2022b). Wimmer (2021) reforça esse entendimento ao sustentar que a divisão informacional de poderes impede o fluxo indiscriminado de dados dentro do Estado, exigindo que cada órgão fundamente o acesso em sua competência e finalidade específica.

Em complemento, a Portaria MJSP nº 961, de 24 de junho de 2025 (Brasil, 2025), ainda que posterior ao período analisado, confirma a relevância do tema ao estabelecer diretrizes sobre o uso de tecnologias da informação nas atividades de investigação criminal e inteligência, prevendo princípios como proporcionalidade, prevenção de riscos e responsabilização, bem como exigindo registros de logs e auditorias. Entretanto, trata-se de norma infralegal, de eficácia limitada, que não

substitui a reserva de lei exigida pelo § 1º do art. 4º da LGPD, permanecendo a necessidade de uma regulamentação setorial robusta.

A partir dos achados da pesquisa, tornam-se evidentes os efeitos práticos e teóricos da lacuna legislativa:

a) ausência de parâmetros uniformes para o tratamento de dados pelas forças de segurança;

b) descompasso com padrões internacionais de proteção e cooperação jurídica;

c) fragilidade institucional de controle e fiscalização; e

d) risco de erosão gradual das garantias fundamentais e do princípio da legalidade.

Para mitigar esses riscos, impõe-se a aprovação de uma Lei Geral de Proteção de Dados Pessoais para Segurança Pública e Persecução Penal (LGPD Penal), dotada de densidade normativa e compatível com a Constituição Federal. Tal legislação deve incorporar, como diretrizes, as recomendações já delineadas pela doutrina e jurisprudência (Souza, 2022a; Supremo Tribunal Federal, 2022a; Pessoa, 2025):

1. Definição clara do escopo e das finalidades do tratamento de dados, com delimitação precisa das hipóteses legais de coleta e uso;
2. Exigência de Relatórios de Impacto à Proteção de Dados (RIPD) e Análises de Impacto Regulatório (AIR) para tecnologias de alto risco (Santos, 2021; Daguer; Borri; Soares, 2022);
3. Estabelecimento de mecanismos de responsabilização e controle, com auditorias independentes e sanções administrativas, civis e penais;
4. Criação de órgão supervisor multissetorial ou fortalecimento da competência fiscalizatória da Autoridade Nacional de Proteção de Dados (ANPD);
5. Mitigação de vieses algorítmicos, mediante testes de acurácia e revisão humana obrigatória (Souza, 2022b);
6. Participação social e transparência ativa, garantindo o controle democrático das políticas de vigilância (Instituto de Pesquisa em Direito e Tecnologia do Recife, 2024);

7. Promoção de uma cultura institucional de proteção de dados, com capacitação de agentes públicos e políticas de governança informacional (Paiva; Lanzillo, 2023).

A efetividade dessa futura legislação dependerá da capacidade do Estado em demonstrar *accountability*, adotando mecanismos de prevenção de riscos e prestação de contas compatíveis com os princípios da legalidade, moralidade, publicidade, eficiência e proporcionalidade, previstos no art. 37 da Constituição Federal.

Do ponto de vista científico, este trabalho contribui para o amadurecimento do debate sobre a interseção entre Direito, tecnologia e segurança pública, oferecendo subsídios teóricos e empíricos à formulação de políticas públicas baseadas em evidências e na proteção dos direitos fundamentais. No plano institucional, a pesquisa evidencia a necessidade de governança pública digital responsável, fundada na transparência e na proporcionalidade do poder de vigilância estatal.

Conclui-se, portanto, que a aplicabilidade indireta dos princípios da LGPD constitui, no presente cenário, a principal salvaguarda jurídica contra práticas estatais de vigilância desproporcionais ou não regulamentadas. Os princípios devem ser compreendidos como instrumentos de limitação do poder estatal, destinados a assegurar que o avanço tecnológico não se converta em um instrumento de restrição arbitrária das liberdades civis.

Enquanto não sobrevier uma legislação específica, cabe ao Poder Judiciário, à ANPD e aos demais órgãos de controle, zelar pela observância da proporcionalidade e da legítima finalidade, garantindo que a segurança pública se realize dentro dos marcos do Estado Democrático de Direito. A consolidação de uma LGPD Penal, portanto, não é apenas uma demanda regulatória, mas uma exigência constitucional para o equilíbrio entre proteção de dados, segurança pública e direitos humanos no Brasil contemporâneo.

REFERÊNCIAS

ALMEIDA, Eduarda Costa. Os grandes irmãos: o uso de tecnologias de reconhecimento facial para persecução penal. **Revista Brasileira de Segurança Pública**, [*s. l.*], v. 16, n. 2, p. 264–283, 23 mar. 2022. https://doi.org/10.31060/rbsp.2022.v16.n2.1377.

ALVES, Fabricio da Mota; VALADÃO, Rodrigo Borges. Proteção de Dados Pessoais na Segurança Pública. [*s. l.*], 23 dez. 2022. Disponível em: https://www.migalhas.com.br/coluna/dados-publicos/379087/protecao-de-dados-pessoais-na-seguranca-public.

ANDRÉA, Gianfranco Faggin Mastro; SILVA, Denis Cortiz da; GUNDIM, Wagner Wilson Deiró. Tecnologia de reconhecimento facial como política de segurança pública: o caso do metrô de São Paulo. **Revista da Faculdade de Direito do Sul de Minas**, [*s. l.*], v. 38, n. 2, p. 279–298, 23 set. 2022. .

ARAS, Vladimir. Aplicabilidade da LGPD às atividades de segurança pública e persecução penal. 30 abr. 2024. **JOTA Jornalismo**. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/aplicabilidade-da-lgpd-as-atividades-de-seguranca-publica-e-persecucao-penal. Acesso em: 17 jun. 2025.

ARAÚJO, Romulo de Aguiar; CARDOSO, Naiara Deperon; PAULA, Marcélia de. Regulação e uso do reconhecimento facial na segurança pública do brasil. **Revista de Doutrina Jur**, [*s. l.*], v. 112, 5 out. 2021. .

AZEVEDO, Cynthia Picolo Gonzaga de; LIMA, Eliz Marina Bariviera de; SILVA, Felipe Rocha da; RODRIGUES,Gustavo Ramos; DUTRA, Luiza Corrêa de Magalhães; SANTARÉM, Paulo Renáda Silva; RODRIGUES, Victor Barbieri Vieira Rodrigues. **Nota técnica: análise comparativa entre o anteprojeto de LGPD penal e o PL 1515/2022**. Instituto de Referência em Internet e Sociedade (IRIS) e Laboratório de Políticas Públicas e Internet (LAPIN), novembro de 2022. Disponível em: <bit.ly/3U0OuU0> . Acesso em: 30 10 2025.

BATTAGLIN, Maria Fernanda Battaglin; VIEIRA, João Víctor Vieira. Problematizando o direito à privacidade e à proteção de dados pes-soais em face da vigilância biométrica. **Teknokultura. Revista de Cultura Digital y Movimientos Sociales**, [*s. l.*], v. 17, n. 2, p. 204–213, 9 set. 2020. https://doi.org/10.5209/tekn.69479.

BIONI, Bruno; EILBERG, Daniela Dora; CUNHA, Brenda; SALIBA, Pedro; VERGILI, Gabriela. **Proteção de dados no campo penal e de segurança pública: nota técnica sobre o anteprojeto de lei de proteção de dados para a segurança pública e investigação criminal**. S~ ao Paulo: Associação Data Privacy Brasil de Pesquisa, 2020.

BRASIL. **Ministério da Justiça. Secretaria Nacional do Consumidor; Secretaria de Assuntos Legislativos.** *Anteprojeto de lei de proteção de dados pessoais*. Brasília, 2015.

BRASIL. **Câmara dos Deputados. Comissão de Juristas responsável pela elaboração de anteprojeto de lei de proteção de dados para segurança pública e persecução penal.** *Anteprojeto de Lei de Proteção de Dados Pessoais para segurança pública e persecução penal*. Brasília, 2020. Disponível em: https://static.poder360.com.br/2020/11/DADOS-Anteprojeto-comissao-protecao-dados-seguranca-persecucao-FINAL.pdf. Acesso em: 30 out. 2025.

BRASIL. **Câmara dos Deputados.** *Projeto de Lei nº 1.515, de 2022* (Deputado Coronel Armando). Brasília, 7 jun. 2022. Lei de proteção de dados pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública e de investigação e repressão de infrações penais. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2189976&filename=Avulso%20PL%201515/2022. Acesso em: 30 out. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**, 14 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 19 jun. 2025.

BRASIL, Ministério da Justiça e Segurança Pública. Portaria MJSP Nº 961, de 24 de junho de 2025. Estabelece diretrizes sobre uso de soluções de tecnologia da informação aplicadas às atividades de investigação criminal e inteligência de segurança pública. 24 jun. 2025. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-mjsp-n-961-de-24-de-junho-de-2025-638661609.

CASTRO, Katia Shimizu de; PAULA, Luciana Veiga de. O reconhecimento biométrico facial e a utilização pelo Poder Público. **Revista de Direito Internacional e Globalização Econômica**, [*s. l.*], v. 9, n. 9, p. 339–354, 28 dez. 2022. https://doi.org/10.23925/2526-6284/2022.v9n9.60092.

COSTA, Rafael Di Lorenzo. Lei geral de proteção de dados e a atividade de inteligência em segurança pública: uma análise profícua entre a privacidade individual e a segurança coletiva. **RECIMA21 - Revista Científica Multidisciplinar - ISSN 2675-6218**, [*s. l.*], v. 5, n. 10, p. e5105813, 14 out. 2024. https://doi.org/10.47820/recima21.v5i10.5813.

DAGUER, Beatriz; BORRI, Luiz Antonio; SOARES, Rafael Junior. O reconhecimento facial na segurança pública e a proteção de dados pessoais como garantia fundamental. [*s. l.*], v. 16, 2022. .

DALSENTER, Thamis. Reconhecimento Facial: laissez-faire, regular ou banir? **Migalhas**, [*s. l.*], 16 jul. 2020. .

FARIAS, Bruno Gomes De. Tecnologia e vigilância: uso da tecnologia como instrumento de controle social no Brasil. **Revista Políticas Públicas & Cidades**, [*s. l.*], v. 14, n. 3, p. e1860, 16 jun. 2025. https://doi.org/10.23900/2359-1552v14n3-28-2025.

FERNANDES, Fernando Andrade; RESENDE, Ana Paula Bougleux Andrade. Regulamentação do tratamento automatizado de dados pessoais em matéria penal. **Suprema - Revista de Estudos Constitucionais**, [*s. l.*], v. 3, n. 1, p. 471–500, 30 jun. 2023. https://doi.org/10.53798/suprema.2023.v3.n1.a207.

GENGHINI, Marco Aurélio Barberato; OLIVEIRA, Diogenes Wagner Silveira Esteves de; FABRETTI, Humberto Barrionuevo. O uso da câmera operacional portátil (COP) na polícia militar do estado de São Paulo: um diálogo entre segurança, privacidade e cidadania. **Revista de Direitos e Garantias Fundamentais**, [*s. l.*], v. 24, n. 3, p. 273–304, 4 dez. 2023. https://doi.org/10.18759/rdgf.v24i3.2310.

INSTITUTO DE PESQUISA EM DIREITO E TECNOLOGIA DO RECIFE. **Revelando rostos, ocultando sujeitos: como a implementação do reconhecimento facial fere direitos garantidos na Constituição Federal**. [*S. l.*: *s. n.*], 2 fev. 2024. Disponível em: https://ip.rec.br/publicacoes/nota-tecnica-revelando-rostos-ocultando-sujeitos-como-

a-implementacao-do-reconhecimento-facial-fere-direitos-garantidos-na-constituicao-federal/.

MARWELL, Daniel Bastos. **Direito fundamental à proteção de dados no campo penal: a atualização nos bancos de dados na Polícia Civil do Distrito Federal**. 2024. 366 f. Doutorado Acadêmico em Direito Constitucional – Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, Brasília, 2024. Disponível em: https://repositorio.idp.edu.br//handle/123456789/5271. Acesso em: 6 maio 2025.

MENKE, Fabiano; LEVENFUS, Sílvia. O reconhecimento facial no setor público e a proteção de dados pessoais. [*s. l.*], , p. 138–157, 2021. .

NIELSSON, Joice Graciele; ROSA, Milena Cereser Da. O direito fundamental da proteção de dados pessoais na segurança pública e âmbito penal: possibilidades e desafios. **Revista de Direito, Inovação, Propriedade Intelectual e Concorrência**, [*s. l.*], v. 8, n. 2, 15 fev. 2023. DOI 10.26668/IndexLawJournals/2526-0014/2022.v8i2.9293. Disponível em: https://indexlaw.org/index.php/revistadipic/article/view/9293. Acesso em: 21 fev. 2025.

OLIVEIRA, Marcos Martins de; OLIVEIRA, Maria Das Graças Macena Dias de; SILVEIRA, Daniel Barile da. Análise comparada da normas de proteção de dados do Brasil, da União Europeia e do Estado da Califórnia - EUA: LGPD x GDPR x CCPA. **Revista de Direito, Governança e Novas Tecnologias**, [*s. l.*], v. 10, n. 2, 10 mar. 2025. DOI 10.26668/IndexLawJournals/2526-0049/2024.v10i2.10923. Disponível em: https://indexlaw.org/index.php/revistadgnt/article/view/10923. Acesso em: 25 jun. 2025.

OLIVEIRA, Loryne Viana; CRIPPA, Margarete Esteves Nunes; LAURENTE GRADOS, \Itala Jeanette; HOLANDA, Tamires De Lima Carneiro. Aspectos ético-jurídicos e tecnológicos do emprego de reconhecimento facial na segurança pública no Brasil. **Revista Tecnologia e Sociedade**, [*s. l.*], v. 18, n. 50, p. 114, 2 jan. 2022. https://doi.org/10.3895/rts.v18n50.12968.

PAIVA, Thairone de Sousa; LANZILLO, Anderson Souza da Silva. Proteção de dados pessoais no Brasil: os limites da regulamentação e da regulação da LGPD no constitucionalismo digital brasileiro. **Revista Controle - Doutrina e Artigos**, [*s. l.*], v. 22, n. 1, p. 239–262, 11 dez. 2023. https://doi.org/10.32586/rcda.v22i1.865.

PESSOA, João Pedro Seefeldt. Entre a vigilância, a segurança pública e a privacidade: desafios regulatórios das tecnologias no contexto da proteção de dados pessoais. **CONTRIBUCIONES A LAS CIENCIAS SOCIALES**, [*s. l.*], v. 18, n. 6, p. e18553, 10 jun. 2025. https://doi.org/10.55905/revconv.18n.6-079.

PORTO, Victor Benigno; OLIVEIRA, Aldo José Barros Barata de. A proteção de dados e seus reflexos seara criminal. **Brazilian Journal of Development**, [*s. l.*], v. 7, n. 9, p. 87861–87884, 8 set. 2021. https://doi.org/10.34117/bjdv7n9-105.

SANTOS, Alexandre Claudino Simas. A regulamentação do uso de câmera corporais pelos órgãos de segurança pública e os reflexos na persecução penal: entre o efeito

civilizatório e a armadilha solucionista. **Revista de Criminologias e Politicas Criminais**, [*s. l.*], v. 9, n. 1, 1 ago. 2023. DOI 10.26668/IndexLawJournals/2526-0065/2023.v9i1.9686. Disponível em: https://indexlaw.org/index.php/revistacpc/article/view/9686. Acesso em: 17 jun. 2025.

SANTOS, Jéssica Guedes. Reconhecimento facial: entre a criminologia, a mídia e a LGPD penal. [*s. l.*], v. 2, n. 1, p. 214–232, jun. 2021.

SOUZA, Ricardo Calmona. A emenda constitucional nº 115 e o direito de proteção de dados na persecução penal: a (des) preocupação com a necessidade de uma "LGPD" penal. **Revista de Direito da Defensoria Pública do Estado do Rio de Janeiro**, [*s. l.*], , p. 109–122, 19 dez. 2022a. .

SOUZA, Ricardo Calmona. O reconhecimento facial na persecução penal: a supressão de garantias no presente e futuro do processo penal brasileiro. **Revista Acadêmica de Ciências Criminais da Fundação Getúlio Vargas**, [*s. l.*], , p. 71–87, 23 dez. 2022b. .

SUPREMO TRIBUNAL FEDERAL. **Ação Direta de Inconstitucionalidade no 6.649 - Distrito Federal**. [*S. l.*: *s. n.*], 15 set. 2022a.

SUPREMO TRIBUNAL FEDERAL. **Arguição de Descumprimento de Preceito Fundamental no 695 - Distrito Federal**. [*S. l.*: *s. n.*], 15 set. 2022b.

TAUTE, Fabian. Reconhecimento facial e suas controvérsias. 7 fev. 2020.

WIMMER, Miriam. Limites e possibilidade para o uso secundário de dados pessoais no poder público: lições da pandemia. **Revista Brasileira de Políticas Públicas**, [*s. l.*], v. 11, n. 1, 2 abr. 2021. DOI 10.5102/rbpp.v11i1.7136. Disponível em: https://www.publicacoes.uniceub.br/RBPP/article/view/7136. Acesso em: 1 set. 2025.