



CENTRO DE ESTUDOS SUPERIORES DE ITAITUBA-LTDA
FACULDADE DE ITAITUBA-FAI
CURSO DE BACHARELADO EM DIREITO

AMANDA COUTINHO QUINTERO
TAMIRES RODRIGUES MOURA

**A TECNOLOGIA COMO ALIADA DA SEGURANÇA PÚBLICA:
o uso da inteligência artificial no combate ao crime**

Itaituba- PA

2025

AMANDA COUTINHO QUINTERO
TAMIRES RODRIGUES MOURA

**A TECNOLOGIA COMO ALIADA DA SEGURANÇA PÚBLICA:
o uso da inteligência artificial no combate ao crime**

Trabalho de Conclusão de Curso apresentado à
Faculdade de Itaituba para obtenção do título de
bacharel em direito.

Orientadora: Prof. Ma. Cintia de Souza Goulart.

Itaituba – PA

2025

QUINTERO, Amanda Coutinho; MOURA, Tamires Rodrigues.

A TECNOLOGIA COMO ALIADA DA SEGURANÇA PÚBLICA: o uso da inteligência artificial no combate ao crime/ Amanda Coutinho Moura; Tamires Rodrigues Moura– Itaituba: FAI, 2025.

42 fls.

Orientadora: Cintia de Souza Goulart

Trabalho de Conclusão de Curso (TCC) da Faculdade de Itaituba – FAI, Curso Bacharel em Direito, Itaituba, BR – PA, 2025.

1. 1. Direito Penal. 2. Tecnologia. 3. Segurança Pública I. GOULART, Cintia de Souza. II. Faculdade de Itaituba. Itaituba, BR – PA, 2025.

AMANDA COUTINHO QUINTERO
TAMIRES RODRIGUES MOURA

**A TECNOLOGIA COMO ALIADA DA SEGURANÇA PÚBLICA:
o uso da inteligência artificial no combate ao crime**

Trabalho de Conclusão de Curso apresentado à
Faculdade de Itaituba para obtenção do título de
bacharel em direito.

Orientadora: Prof. Ma. Cintia de Souza Goulart.

BANCA EXAMINADORA

Presidente/orientador: _____ Nota: _____

Prof^a. Ma. Cintia de Souza Goulart.

Avaliador(a) 1 : _____ Nota: _____

Avaliador(a) 2: _____ Nota: _____

Resultado: _____ Média: _____

Itaituba-PA, ____ de março de 2025.

Dedicatória: Dedicamos este trabalho a todas as pessoas que, com amor e apoio incondicional, foram fundamentais nas nossas jornadas. As nossas famílias, pelo constante incentivo e pela força que nos impulsionaram a seguir em frente, e a todos que acreditaram em nós.

AGRADECIMENTOS

Primeiramente, agradeço a **Deus** por me fortalecer e guiar em cada etapa desta caminhada acadêmica. Concluir esta jornada e este trabalho representa a concretização de um sonho, e nada disso seria possível sem o apoio e incentivo de pessoas tão especiais em minha vida.

Agradeço aos meus pais, **Antônio Quintero** e **Olinda Quintero**, que, mesmo de longe, me deram total apoio, ensinando-me desde cedo que o estudo é o melhor caminho para um futuro brilhante. Vocês dois foram, e sempre serão, minha fortaleza nos dias sombrios e foram fundamentais para que eu vencesse esta batalha.

Ao meu marido, **Natan**, que foi meu porto seguro nos dias mais difíceis. Nos momentos em que a exaustão tentava me vencer, você esteve lá, incansável, lembrando-me da minha força. Seu apoio foi essencial para que eu não desistisse.

Agradeço, com todo o meu amor, ao meu filho, **Nathan Kalléo**, que veio ao mundo durante esta jornada e se tornou minha maior motivação. Sua existência trouxe ainda mais sentido a cada esforço e me impulsionou a concluir esta etapa com ainda mais dedicação.

À minha amiga e parceira **Tamires Moura**, que, há cinco anos, compartilhava comigo os desafios do primeiro trabalho da faculdade e, juntas, agora celebramos a conclusão deste TCC, meu muito obrigada por toda essa caminhada.

Por fim, agradeço a todos os professores desta universidade, que me proporcionaram o conhecimento necessário para minha formação. Em especial, à nossa orientadora, **Cíntia**, cuja dedicação e orientação foram fundamentais para o desenvolvimento deste trabalho.

A todos que, de alguma forma, fizeram parte dessa caminhada, meu mais sincero agradecimento. Cada gesto de apoio, incentivo e compreensão foi essencial para que este trabalho se tornasse realidade. Levo comigo não apenas o conhecimento adquirido, mas também a gratidão por cada pessoa que contribuiu para esta conquista.

Amanda Coutinho Quintero

AGRADECIMENTOS

Primeiramente, agradeço a **Deus** por me fortalecer e guiar em cada etapa dessa caminhada. Agradeço aos meus pais, **Felipe Neri Moura** e **Shirley Rodrigues Moura**, que, mesmo de longe, me deram total apoio e me ensinaram, desde cedo, que o estudo é o melhor caminho.

À minha parceira, **Amanda Quintero**, por estar ao meu lado neste momento tão importante, e à nossa orientadora, **Cíntia**, pela dedicação e orientação na realização deste trabalho.

Tamires Rodrigues Moura

RESUMO

O presente trabalho, analisa as inovações e tecnologias atualmente incorporadas à segurança pública, abordando seus impactos e desafios, bem como a importância do uso da tecnologia e a responsabilidade sobre o uso de dados e sua proteção. Embora as tecnologias possam auxiliar as autoridades no combate ao crime, elas trazem à tona questões sobre o uso de dados pessoais.

Portanto, é fundamental assegurar que seu uso seja conduzido de maneira ética e profissional, tendo em vista que com a interligação de sistemas, dados que antes eram pertencentes a um órgão passaram a ser disponibilizados para todo um sistema, diante desta primícia, o presente estudo busca compreender e analisar os meios aos quais a tecnologia é benéfica para a segurança e as medidas utilizadas para assegurar a segurança dos dados utilizados.

A metodologia empregada consiste em uma pesquisa bibliográfica, fundamentada em fontes confiáveis, com ênfase nos impactos e desafios apresentados por essas tecnologias, assim como em possíveis problemas ligados à privacidade. É necessário realizar mais investigações nesse domínio para aprofundar a compreensão dos desafios e oportunidades associados.

Palavras-chave: Tecnologias de segurança pública. Políticas. Proteção de dados. Ética. Responsabilidade. Impactos.

ABSTRACT

The present study analyzes the innovations and technologies currently incorporated into public security, addressing their impacts and challenges, as well as the importance of technology usage and the responsibility for data usage and protection. Although technologies can assist authorities in combating crime, they raise concerns about the use of personal data.

Therefore, it is essential to ensure that their use is conducted ethically and professionally, considering that with the interconnection of systems, data that previously belonged to a single entity has become available to an entire system. In light of this premise, the present study seeks to understand and analyze the ways in which technology benefits security and the measures used to ensure the security of the data employed.

The methodology employed consists of a bibliographic research based on reliable sources, emphasizing the impacts and challenges posed by these technologies, as well as potential privacy-related issues. Further investigations in this field are necessary to deepen the understanding of the challenges and opportunities involved.

Keywords: Public security technologies. Policies. Data protection. Ethics. Responsibility. Impacts.

LISTA DE QUADROS

Quadro 1 – Demonstrativo dos trabalhos de produção científica.	36
---	----

SUMÁRIO

1 INTRODUÇÃO	11
2. FUNDAMENTAÇÃO TEÓRICA	13
2.1 A HISTÓRIA DA TECNOLOGIA NA SEGURANÇA PÚBLICA	13
2.2 A TECNOLOGIA APLICADA NA SEGURANÇA PÚBLICA	16
2.1.1 Caso Henry Borel	22
2.1.2 Caso Marielle Franco	24
2.3 OS DIREITOS FUNDAMENTAIS E A PRIVACIDADE NA SEGURANÇA DIGITAL	25
2.4 NECESSIDADE DE PROTEÇÃO DE DADOS SOB A LUZ DA LGPD – LEI DE PROTEÇÃO DE DADOS	27
2.4.1 Importância da LGPD na Segurança Pública	29
2.4.2 Uso da LGPD para Coibir o Vazamento de Dados por Servidores Públicos	30
2.4.3 A Visão da Corrente Utilitarista em relação a LGPD	32
3 METODOLOGIA	34
3.1 TIPO DE PESQUISA	34
4 RESULTADOS E DISCUSSÃO	36
REFERÊNCIAS	42

1 INTRODUÇÃO

Este trabalho de pesquisa científica tem o intuito de identificar e analisar o tema em questão, sobre tecnologia como aliada da segurança pública, observando o uso da inteligência artificial no combate ao crime. Haja vista que a tecnologia tem desempenhado um papel importante no combate à criminalidade e na melhoria da segurança da população brasileira.

A abordagem à temática em questão se justifica pela incorporação de sistemas de monitoramento, uma das estratégias adotadas para coibir a criminalidade, assim como a implementação de softwares de reconhecimento facial e de análises de placas de veículos, aos quais utilizam bancos de dados para análises criminais.

Em contrapartida, a problemática condizente à pesquisa se verifica diante dos desafios que caracterizam o cenário brasileiro, a busca por soluções que aliem eficiência e inovação tornou-se indispensável. Nesse sentido, a tecnologia emerge como uma aliada estratégica, oferecendo ferramentas capazes de transformar a forma como o Estado previne, combate e investiga crimes.

No que concerne ao objetivo geral da pesquisa, este busca analisar os pontos principais referente à tecnologia como aliada da segurança pública, identificando as problemáticas que permeiam tal descrição. Por outro lado, em se tratando dos objetivos específicos, condizem em observar e verificar o uso da inteligência artificial no combate ao crime. Tendo em vista que, conforme aponta Costa (2024), a incorporação de tecnologias avançadas no âmbito da segurança pública representa uma oportunidade significativa para reduzir os índices de criminalidade e ampliar a sensação de segurança entre a população.

No que diz respeito à metodologia aplicada à pesquisa, foi utilizada estudo exploratório e descritivo, pois visa aprofundar o conhecimento sobre a pesquisa

Segundo Oliveira e Santos (2020), a implementação de tecnologias não apenas fortalece a capacidade de resposta das forças de segurança, mas também possibilita uma gestão mais eficiente dos recursos disponíveis. Contudo, essa evolução traz consigo desafios éticos e operacionais que precisam ser enfrentados.

No contexto brasileiro, a aplicação de tecnologias voltadas para a segurança pública ainda enfrenta barreiras significativas, como desigualdades regionais, restrições orçamentárias e preocupações relacionadas à privacidade. Apesar dessas dificuldades, iniciativas como o uso de drones para o monitoramento de áreas de risco,

a integração de bancos de dados biométricos e a aplicação de inteligência artificial em investigações têm mostrado resultados promissores em diversas regiões do país (SILVA, 2022). A estrutura é fundamental para compreender como essas tecnologias estão sendo empregadas, quais impactos estão gerando e quais são as perspectivas para o futuro.

Destarte, a pesquisa se estrutura em analisar o impacto da tecnologia na segurança pública no Brasil, considerando suas potencialidades, limitações e implicações sociais. Por meio de uma abordagem crítica e multidisciplinar, busca-se contribuir para o debate sobre como a inovação tecnológica pode ser utilizada de maneira ética e eficaz, promovendo um ambiente mais seguro para todos.

2. FUNDAMENTAÇÃO TEÓRICA

2.1 A HISTÓRIA DA TECNOLOGIA NA SEGURANÇA PÚBLICA

Desde o início das civilizações, a segurança era uma preocupação do cotidiano coletivo. Numa época ao qual o homem vivia em bandos e comunidades, eles utilizavam desse sistema coletivo para revezar em vigilância e proteger-se de invasões e ameaças, utilizando métodos simples de vigilância.

Segundo Durant (2001), as primeiras comunidades humanas desenvolveram métodos de defesa para proteger suas terras e recursos, como a construção de muralhas e a formação de grupos armados, frequentemente organizados de forma improvisada para lidar com ameaças externas.

Diante dessa estrutura de sociedade, a defesa era baseada na cooperação entre os membros da comunidade, à medida que o homem foi se desenvolvendo e deixando de ser nômade e passando a construir as fortificações, muralhas e torres, aos quais eram construídas para proteger os habitantes de ataques externos.

Conforme as civilizações evoluíam, ocorreu a necessidade de se ter as instituições de Segurança Pública, as quais começaram a surgir na Roma antiga. Conforme Gat (2006), em 27 a.C., durante o governo de Augusto, foi criada a Cohortes Urbanae, que era uma força paramilitar destinada a manter a ordem pública dentro da cidade de Roma. Além disso, os eles eram responsáveis pela prevenção de incêndios e pela segurança noturna, aos quais foram considerados uma das primeiras forças policiais.

Esses homens tinham a responsabilidade de garantir o cumprimento das leis locais, utilizando a força física e a ameaça de sanções penais. Essas primeiras corporações voltadas para a preservação da ordem tinham seus membros e estruturas organizacionais inspirados nas corporações militares. Embora nem todas fossem efetivamente militares, eles possuíam a tarefa de impor a ordem e a disciplina no meio social.

Embora rudimentares, esse controle é um dos percussores dos meios de segurança utilizados na nossa sociedade atual, assim como a forma que os antigos egípcios faziam longas descrições textuais detalhadas das características físicas das pessoas como uma forma de identificação, hoje utilizada na nossa sociedade atual em diversas áreas, como a segurança pública, onde através das características de

uma pessoa podemos obter um retrato falado.

Os babilônicos utilizavam impressões digitais em argila para identificar os autores dos escritos cuneiformes. Esse método, apesar de arcaico se baseava na primícia de que uma digital é única, inviabilizando e repelindo possíveis falsificações. Com o avanço do homem, sociedade e o desenvolvimento da tecnologia, no início do século XVII, ocorreu com a institucionalização das corporações de Segurança Pública, as quais começaram a se estabelecer na Europa durante a Idade Moderna.

Segundo Emsley (2010), a criação da Metropolitan Police em 1829, em Londres, representou um marco na institucionalização das corporações de segurança pública. Foi a primeira força policial moderna organizada com base em princípios como uniformidade, hierarquia e prevenção de crimes, servindo de modelo para outros países.

Neste período, ocorreu a introdução de lanternas e uniformes padronizados para os policiais, aos quais ajudavam a identificar a autoridade, assim como possibilitava o monitoramento noturno da guarda.

No século XIX, se deu início a criação e desenvolvimento de tecnologias mais avançadas, como a invenção do telégrafo, ferramenta que veio a facilitar os meios de comunicação entre pessoas. Segundo Júnior (2009), o telégrafo contribuiu para a centralização do controle policial, permitindo que as autoridades coordenassem ações em grande escala e monitorassem atividades em diferentes regiões de maneira quase instantânea.

Além disso, nesta época começaram a surgir a implementação de seus primeiros sistemas de registro criminal, ao quais auxiliavam na descrição de informações sobre criminosos e suas atividades. Dado o início do século XX, e o avanço e descobertas de novas tecnologias eletrônicas e da computação, ouve a expansão de tecnologias aplicadas à segurança.

Como o uso de câmeras de vigilância, sendo implementados primeiramente para uso particular por pessoas de poder aquisitivo elevado, adquirido posteriormente para o monitoramento de vigilância das cidades, assim como aquisição de sistemas integrados de comunicação, ao quais permitiram o uso e cruzamento de dados interligados, trazendo uma interligação entre os dados e as agências.

Com o início da era da internet e implementação e desenvolvimento de tecnologias móveis no final do século XX e início do XXI, novas ferramentas foram desenvolvidas para melhorar a vida da pessoas e consequentemente acabaram

sendo utilizadas para a segurança pública.

Como a implementação de câmeras de Monitoramento e Vigilância, que passaram a permitir e monitorar áreas públicas e privadas, e o uso de reconhecimento facial e ferramentas como Clearview AI aos quais ajudam a identificar suspeitos a partir de imagens ou vídeos e o uso de Drones que equipados com câmeras, são usados para monitoramento aéreo e coleta de informações em áreas remotas que não poderiam adentrar sem essas ferramentas.

Com os avanços da internet, ao longo das últimas décadas, ela se tornou uma ferramenta essencial para o acesso à informação e no dos meios de comunicação, sendo um elemento essencial para a sociedade. Apesar dos benefícios proporcionados, a popularização da rede mundial de computadores também trouxe consigo um aumento expressivo nos crimes cibernéticos.

De acordo com dados recentes, a expansão do acesso à internet contribuiu para a ampliação do alcance e da complexidade dos crimes cibernéticos. A globalização da conectividade permitiu que criminosos agissem em escala internacional, muitas vezes explorando lacunas legislativas entre diferentes países. Além disso, a anonimidade oferecida pelo ambiente digital facilita a atuação de indivíduos e organizações criminosas, tornando mais difícil a identificação e responsabilização dos autores.

Segundo Silva (2017), o Brasil está entre os países mais afetados por crimes cibernéticos, com destaque para golpes de clonagem de aplicativos de mensagens e invasões de contas bancárias. Esses crimes têm causado prejuízos financeiros significativos, além de impactos psicológicos e sociais nas vítimas.

Diante deste problema, ocorre a necessidade de combate a esses crimes. Primeiramente, destaca-se a importância de investimentos em tecnologia e infraestrutura para fortalecer os sistemas de segurança cibernética. Ferramentas como inteligência artificial e algoritmos de aprendizado de máquina têm se mostrado promissoras na identificação de padrões de comportamento criminoso e na antecipação de ataques (SOUZA; FERREIRA, 2021).

Além disso, é essencial a criação de legislações específicas que acompanhem a evolução tecnológica e possibilitem a punição adequada dos responsáveis por crimes digitais, bem como a cooperação internacional entre países para lidar com delitos cibernéticos transnacionais (OLIVEIRA, 2019).

Outro aspecto fundamental é a capacitação de profissionais especializados em

segurança cibernética, tanto no setor público quanto no privado. Delegacias especializadas, como as Divisões de Crimes Cibernéticos, devem ser fortalecidas com recursos humanos e tecnológicos para garantir a eficácia das investigações.

Paralelamente, campanhas de conscientização destinadas à população podem desempenhar um papel crucial na prevenção desses crimes, educando os usuários a respeito de práticas seguras no uso da internet. Segundo dados do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.BR, 2022), grande parte dos ataques cibernéticos ocorre devido à falta de conhecimento dos usuários sobre medidas básicas de segurança.

Por fim, a integração da inteligência artificial (IA) nas operações de segurança pública está moldando uma nova forma de vigilância e segurança, tendo em vista que se utiliza programas para analisar grandes volumes de dados coletados por câmeras, sensores e redes sociais, ajudando a inibir comportamentos criminosos e identificar suspeitos com maior precisão. Embora essa tecnologia ofereça benefícios significativos em termos de eficiência e eficácia, também levanta questões éticas relacionadas à privacidade e ao uso responsável dos dados.

2.2 A TECNOLOGIA APLICADA NA SEGURANÇA PÚBLICA

Desde a invenção do telégrafo, ao qual foi inventado por Samuel Morse, junto com o apoio de seus colaboradores Leonard Gale e Alfred Vail, em 1837, o principal propósito do telégrafo era permitir a comunicação rápida a longas distâncias, algo que era impossível na época sem depender de mensageiros físicos, apesar de existirem formas rudimentares de comunicação telegráfica antes disso, como os sistemas ópticos (baseados em sinais visuais), Morse foi o responsável por criar o telégrafo elétrico, que utilizava pulsos elétricos para transmitir mensagens por meio de fios.

A invenção do telégrafo foi o início do uso da tecnologia aplicada a segurança, sendo um dos marcos na história das inovações, possibilitando não só a comunicação, mas a eficiência das forças policiais.

Com esse marco, tivemos uma evolução até chegarmos ao uso de inteligência artificial, o uso de tecnologias vêm alterando a forma como as forças policiais, se integram e ajudam na nossa sociedade, seja em solução ou prevenção de casos. No início do século XX, as forças policiais começaram a adotar sistemas de comunicação mais eficientes, assim conseguindo uma forma mais rápida aos casos policiais e

alertas de crimes.

O uso do rádio, naquela época se tornou algo indispensável para coordenar as operações, fazendo com que os policiais se comunicassem instantaneamente entre si e com as centrais de comando. Essa inovação possibilitou que as emergências e demandas fossem atendidas rapidamente e melhorou o gerenciamento das operações policiais.

Com a modernização e otimização dos sistemas policiais, podemos visualizar o quanto a tecnologia tem inovado na segurança pública no Brasil, seja promovendo a integração entre órgãos e melhorando a eficiência das operações. Investimentos em monitoramento e reconhecimento facial têm contribuído para a redução da criminalidade, mas desafios como a privacidade e a transparência permanecem.

Um exemplo de investimento em tecnologia que também visa facilitar o acesso aos serviços públicos. É o estado do Rio de Janeiro, que busca se integralizar com monitoramentos de câmeras, patrulhamento de drones em áreas da cidade com maior taxa de criminalidade, reconhecimento facial, pois, em sua capital tem um dos índices mais violentos de criminalidade do nosso país, diante do número crescente da criminalidade, o uso de dados e a utilização de plataformas de monitoramento se tornaram indispensáveis para garantir a segurança dos cidadãos.

Um dos meios mais comuns de monitoramento é a utilização de câmeras de vigilância nas áreas urbanas. Essas câmeras permitem monitorar atividades suspeitas, ajudando na prevenção de crimes e na identificação de suspeitos após um incidente. Além disso, o armazenamento digital das imagens facilita o trabalho investigativo, facilitando a revisão das gravações, pela autoridade policial em busca de evidências.

É fato inarrável, que a tecnologia é fundamental nos tempos modernos, aliando-se ao patrulhamento, acaba melhorando a eficiência na segurança pública, permitindo através da análise mais rápida, uma melhor leitura dos dados. Os meios de arquivamento digital possibilitam que os bancos de dados armazenem recursos e provas, facilitando o uso em casos policiais. A análise desses dados permite identificar tendências, otimizar patrulhas e direcionar recursos para áreas com maior índice de criminalidade.

Uma outra ferramenta utilizada com o auxílio das câmeras, é o reconhecimento facial, ao qual a partir de um vídeo ou foto, escaneia seu rosto procurando em um banco de dados, podendo apontar algum criminoso que esteja foragido, a partir do

scanner facial.

De acordo com um levantamento realizado pelo Fórum Brasileiro de Segurança Pública (FBSP), até 2022, pelo menos 20 estados brasileiros já haviam implementado sistemas de reconhecimento facial em suas operações policiais. O principal objetivo dessa tecnologia é identificar suspeitos que possuem mandados de prisão em aberto, facilitando a captura de criminosos.

Na cidade de Salvador, o uso de câmeras com reconhecimento facial foi responsável pela prisão de 134 pessoas entre 2018 e 2021 (FBSP, 2022). Segundo Santos e Almeida (2020), a tecnologia de reconhecimento facial tem se mostrado uma aliada importante no fortalecimento das ações de policiamento ostensivo e na identificação de foragidos da justiça.

No entanto, o enviesamento em sistemas de reconhecimento (como reconhecimento facial, de voz ou imagens) ocorre quando o modelo de aprendizado de máquina ou inteligência artificial apresenta um desempenho desigual para diferentes grupos ou categorias. Esse viés pode surgir devido a problemas nos dados usados para treinar o modelo, nas escolhas feitas durante o desenvolvimento ou até nos próprios algoritmos.

O que causa o viés em sistemas de reconhecimento? Devido aos dados utilizados, o sistema aprende a partir dos dados fornecidos durante o treinamento. Se esses dados não representarem adequadamente toda a diversidade do mundo real, o modelo terá dificuldade em generalizar. Por exemplo: Um sistema de reconhecimento facial treinado majoritariamente com imagens de pessoas brancas pode ter dificuldade em identificar rostos de pessoas negras. Um estudo conduzido pelo National Institute of Standards and Technology (NIST) demonstrou que:

Sistemas de reconhecimento facial frequentemente apresentam desempenho desigual entre grupos demográficos. Em particular, as taxas de erro podem ser até 100 vezes maiores para rostos de pessoas negras e asiáticas em comparação com rostos de pessoas brancas, destacando a necessidade de maior diversidade nos dados de treinamento e auditorias regulares (NIST, 2019).

Um estudo estadunidense feito pela MIT Media Lab, conduzido em 2018 pela pesquisadora Joy Buolamwini e sua equipe, é um dos mais importantes no campo da inteligência artificial, especialmente no que diz respeito a viés racial e de gênero em sistemas de reconhecimento facial.

O principal objetivo do estudo era investigar como os sistemas de reconhecimento facial se comportavam em diferentes grupos demográficos, especialmente em relação a raça (tonalidade de pele) e gênero (homens e mulheres). Nesta análise, o sistema obteve taxa mínima de erro para homens, inferiores a 1% e para mulheres negras chegou a 34%.

O estudo identificou que a maioria dos sistemas utilizados por grandes empresas de tecnologia, como IBM, Microsoft e Meta, utilizam imagens de pessoas brancas que levou a um desempenho desigual para outros grupos raciais e constatou que os algoritmos não eram projetados para lidar com a diversidade global de características faciais, sendo sujeito a falhas.

Diante deste problemas, temos como exemplos prisões equivocadas, devido a reconhecimentos falhos, causados muita das vezes por falhas em sua estrutura organizacional, aos quais não investem o suficiente para atualização em seu sistema operacional tendo como consequência prisões indevidas, feitas mediante a mandados de prisões vencidos, aos quais devido não são devidamente atualizados, ocasionando prisões injustas.

Há casos em que pessoas foram presas porque o sistema de reconhecimento facial as identificou como procuradas, mas o mandado de prisão já havia expirado ou sido revogado.

Isso ocorre porque os sistemas policiais nem sempre verificam a validade do mandado antes de realizar a prisão. O uso de tecnologias como o reconhecimento facial amplifica os erros já existentes nos bancos de dados. Por exemplo: Uma pessoa com um mandado vencido pode ser identificada erroneamente como criminosa.

O sistema pode confundir pessoas com rostos semelhantes, especialmente em populações marginalizadas. Segundo Souza (2020):

A combinação de mandados de prisão vencidos com sistemas de reconhecimento facial pouco precisos tem levado a erros graves na segurança pública brasileira. Pessoas inocentes são presas por crimes que não cometeram, muitas vezes devido a identificações incorretas ou mandados desatualizados nos bancos de dados policiais. Esses casos afetam, em sua maioria, grupos vulneráveis, como negros e pardos, reforçando desigualdades raciais e sociais já existentes no país (SOUZA, 2020, p. 45).

Os presentes dados evidenciam a necessidade de uma análise mais efetiva, antes de qualquer prisão ou abordagem. Sendo necessário um maior cuidado e

atualização no sistema de dados para evitar abordagens e prisões erradas.

Com a chegada da inteligência artificial (IA), ocorreu uma revolução na forma como a segurança otimizou seus meios para facilitar o processo de denúncia por parte da população.

Com o uso da tecnologia, tivemos o acesso a aplicativos móveis e a sites online, desenvolvidos para ajudar a facilitar denúncias, sendo possível que os cidadãos relatem incidentes ou forneçam informações sobre atividades suspeitas.

Diante da globalização, onde até o lugar mais remoto é alcançado por torres e satélites, facilitando o uso de drones, aos quais tem auxiliado no combate a criminalidade, adentrando locais de difícil acesso, onde o patrulhamento não poderia chegar, permitindo que os policiais monitorem sem se expor ao perigo.

O reconhecimento facial tem sido utilizada como uma ferramenta na área da segurança pública. Com essa tecnologia, é possível identificar suspeitos de forma ágil em locais públicos ou durante investigações criminais. Apesar de sua eficiência comprovada em diversas situações, o uso do reconhecimento facial ainda levanta debates éticos, sobre o respeito à privacidade e ao risco de uso indevido.

Além disso, as agências de segurança têm investido em sistemas integrados para melhorar a coordenação de respostas em emergências que envolvem diferentes entidades, como por exemplo a polícia, os bombeiros e os serviços médicos. Esses sistemas promovem um fluxo contínuo de informações entre as equipes, permitindo uma maior facilidade em compartilhamento de informações.

Outro tipo de tecnologia utilizado é o uso de dispositivos móveis equipados com aplicativos específicos. Essas ferramentas oferecem acesso instantâneo a dados relevantes, como informações sobre suspeitos, histórico criminal e detalhes de ocorrências anteriores. Com isso, os policiais conseguem ter um maior controle sobre possíveis criminosos, possíveis mandatos e controle sobre carros roubados, além de consultas sobre documentos possivelmente vencidos.

Durante eventos públicos grandes ou manifestações, tecnologias como drones e câmeras térmicas são utilizadas para monitorar multidões e garantir a segurança dos participantes.

Essas ferramentas ajudam as autoridades a identificarem comportamentos suspeitos ou situações potencialmente perigosas antes que se tornem ameaças reais, ajudando assim a inibir possíveis ataques e reprimir roubos e outros delitos. O uso de sistemas de transporte inteligentes, estão sendo adotados em diversas cidades com

o objetivo de melhorar o fluxo do tráfego e aumentar a segurança nas vias.

Esse tipo de transporte é equipado com sensores e câmeras, esses sistemas permitem o monitoramento em tempo real das condições de trânsito, possibilitando a prevenção em possíveis acidentes e diminuindo o fluxo de pessoas aglomeradas, tendo em vista que o mesmo analisa as taxas de tráfego, auxiliando no cálculo da rota e evitando atrasos.

No âmbito da segurança pública, a tecnologia vem auxiliando e desempenhando um papel essencial, pois ela faz a junção entre diferentes agências governamentais.

O uso de plataformas digitais facilita o compartilhamento de informações entre polícias locais, estaduais e federais, fazendo com que haja uma maior efetividade no combate a criminalidade, tendo em vista o compartilhamento de informação, inibindo a criminalidade e a violência, fazendo com que as operações possam ter um apoio conjunto e sendo mais efetivas.

O uso do monitoramento de redes sociais, se tornou de suma importância para possíveis prevenções de crimes. Com o uso de softwares específicos, as autoridades conseguem analisar postagens públicas em busca de possíveis ameaças ou atividades criminosas planejadas, permitindo que intervenções sejam realizadas antes mesmo que possíveis crimes possam ocorrer.

Apesar dos benefícios citados com a implementação da tecnologia, o uso e monitoramento traz à tona questões éticas, aos quais envolvem a privacidade, a preocupação com as formas de vigilância excessiva, utilizando os meios citados e o acesso a dados sensíveis pessoais.

A forma como essas inovações são implementadas podem influenciar diretamente o relacionamento entre as forças de segurança e as comunidades que elas atendem.

Sendo de extrema necessidade a implementação de projetos que busquem promover a transparência e uma aproximação entre a sociedade as instituições responsáveis pela proteção da sociedade.

Com o avanço e as mudanças tecnológicas, é fundamental que as forças policiais sempre se mantenham atualizadas sobre as inovações no setor de segurança pública. Investir em pesquisa e desenvolvimento é essencial para que as agências possam adotar soluções que possam auxiliar no combate e prevenção de crimes e que transpareça para a sociedade o sentimento de segurança e privacidade.

Portanto, fica claro que a tecnologia é de grande importância, ao qual é uma grande aliada na segurança pública, sendo imprescindível no combate e repressão de crimes. Dessa forma, é relevante destacar casos recentes que receberam ampla cobertura pela mídia e tiveram auxílio de tecnologias para solucionar os devidos crimes. Alguns exemplos são: os casos de Henry Borel e Marielle Franco.

2.1.1 Caso Henry Borel

O presente caso é um exemplo emblemático de como o uso da tecnologia pode auxiliar nas investigações criminais, o caso do menino Henry Borel Medeiros, de 4 anos, ocorrido em 8 de março de 2021, a tecnologia desempenhou um papel fundamental na investigação, ajudando a desmontar as versões apresentadas pelos acusados e a revelar a verdade por trás da morte da criança.

A criança Henry foi levada ao hospital pelos pais, Monique Medeiros (mãe) e o então vereador Dr. Jairinho (padrasto), já sem vida. Eles alegaram que o menino havia caído da cama, mas a autópsia revelou múltiplas lesões graves, incompatíveis com essa versão. Essas descobertas levaram a polícia a investigar a possibilidade de homicídio, tendo como suspeitos Jairinho e Monique.

A investigação utilizou diversas ferramentas tecnológicas para reunir provas e esclarecer o que realmente aconteceu com Henry, sendo a análise das mensagens trocadas entre Monique Medeiros e a babá de Henry foi decisiva para o caso. A polícia acessou os celulares e recuperou conversas que revelaram episódios anteriores de agressões do padrasto contra o menino. Aos quais foram recuperadas mensagens onde a babá relatava que Henry demonstrava medo de Jairinho, chorava ao ficar sozinho com ele e apresentava marcas de agressões.

Sendo descoberto, uma conversa de 12 de fevereiro de 2021, onde a babá informou a Monique que Henry havia reclamado de dores após ficar sozinho com Jairinho e onde mostra que Monique não tomou providências para proteger o filho, demonstrando omissão.

Sendo imprescindíveis para a investigação pois as mensagens desmentiram as alegações de Monique de que desconhecia as agressões e mostraram que ela sabia do comportamento violento de Jairinho.

Outra prova ao qual foi descoberta por meio da tecnologia, foram as imagens das câmeras de segurança do prédio onde a família morava foram analisadas para

reconstruir os eventos da noite do crime, aos quais mostraram Monique e Jairinho levando Henry ao hospital durante a madrugada. Nas imagens de segurança, o casal não chega a demonstrar sinais de emergência ou desespero, o que chamou a atenção dos investigadores.

As imagens ajudaram a estabelecer a cronologia dos fatos e contradisseram as versões apresentadas pelos acusados. As câmeras ajudaram a refutar a narrativa inicial de que Henry teria caído da cama acidentalmente.

A polícia realizou perícias nos celulares de Monique e Jairinho, através de um equipamento israelense chamado Cellebrite Premium, que é uma ferramenta avançada de perícia digital capaz de acessar, recuperar e analisar dados, incluindo mensagens e imagens apagadas, de dispositivos eletrônicos como celulares.

Esse equipamento foi fundamental para a investigação, permitindo a recuperação de conversas e outros dados relevantes nos celulares das pessoas envolvidas, encontrando evidências adicionais que reforçaram a acusação. Pesquisas na internet feitas por Monique sobre "hematomas em crianças" e "como se defender juridicamente".

O Padrasto Jairinho, tentou apagar mensagens e registros que poderiam incriminá-lo. Conversas entre Monique e Jairinho indicavam que eles estavam preocupados em criar uma versão que sustentasse a tese de acidente.

E por último, a polícia usou dados de localização e registros telefônicos para verificar os movimentos de Monique e Jairinho no dia do crime. Os dados ajudaram a confirmar a presença de Jairinho no apartamento no momento do crime. Contradições entre os depoimentos dos acusados e os registros de localização foram evidenciadas.

O que ajudou no rastreamento e a reforçar a cronologia dos fatos e a desmontar as versões apresentadas pelos acusados. Monique Medeiros foi acusada de omissão e conivência com as agressões de Jairinho.

Dr. Jairinho foi acusado de homicídio triplamente qualificado (motivo torpe, meio cruel e impossibilidade de defesa da vítima). Ambos foram presos preventivamente em abril de 2021. Jairinho foi apontado como o autor das agressões que levaram à morte de Henry.

Monique foi acusada de negligência e de não proteger o filho, mesmo sabendo das agressões. O caso ainda tramita na Justiça, e o julgamento segue em andamento. Jairinho e Monique permanecem como réus e aguardam sentença.

Diante do presente caso, foi sancionada em 24 de maio de 2022, a Lei Henry

Borel, que estabelece medidas para combater a violência doméstica e familiar contra crianças e adolescentes no Brasil. A lei foi criada em homenagem ao menino Henry Borel Medeiros, de 4 anos, vítima de violência doméstica que resultou em sua morte em março de 2021.

O caso Henry Borel, merece destaque devido à sequência flagrante de erros cometidos, que só foram descobertos devido ao auxílio da tecnologia. No entanto, esse caso não foi o único em que a tecnologia desempenhou um papel central envolvendo a esfera penal.

2.1.2 Caso Marielle Franco

O caso Marielle Franco é um dos crimes mais emblemáticos e complexos da história recente do Brasil. Na qual a vereadora Marielle Franco e seu motorista, Anderson Gomes, foram assassinados no dia 14 de março de 2018, no Rio de Janeiro.

Na noite de 14 de março de 2018, Marielle Franco havia participado de um evento chamado "Jovens Negras Movendo as Estruturas", no centro do Rio de Janeiro.

Após sair do evento, o carro onde ela estava foi alvejado por 13 tiros, na região do Estácio, zona norte do Rio, na qual ela e seu motorista, Anderson Gomes, morreram na hora. A assessora que também estava no veículo sobreviveu com ferimentos leves. A vítima era Vereadora pelo PSOL, foi eleita com mais de 46 mil votos em 2016.

Mulher negra, feminista, bissexual e oriunda da favela da Maré, Marielle era conhecida por sua luta contra a violência policial, a desigualdade social e a opressão das minorias e no momento de sua morte, Marielle era relatora de uma comissão que fiscalizava a intervenção federal no Rio de Janeiro, que havia colocado as forças armadas no controle da segurança pública do estado.

O caso exigiu uma investigação complexa, com o uso de diversas tecnologias para identificar os responsáveis, como Câmeras de Segurança, onde as imagens das câmeras de segurança foram analisadas para rastrear o carro utilizado pelos assassinos. Um Cobalt prata clonado, através das câmeras foi possível verificar que o veículo seguiu o carro de Marielle por cerca de 4 km antes do ataque, através dessa linha de investigação, a polícia veio a entrar em contato com a montadora do veículo ao qual levantou dados de que, na data do crime estava em

circulação cerca de 12.742 veículos da mesma cor e tipo, sendo 443 em circulação no Rio de Janeiro.

Também foi utilizado, software de reconhecimento facial para identificar possíveis suspeitos e a partir das imagens obtidas, foi possível verificar que horas antes do crime, foram captadas imagens do interior do mesmo veículo, ao qual foi possível através de triangulação de sinais e a análise de antenas de telefonia, onde os dados de localização de celulares foram cruzados para identificar aparelhos que estavam próximos ao local do crime no momento do ataque.

Isso ajudou a mapear possíveis suspeitos e confirmar a presença deles na cena do crime, a análise Forense. As balas usadas no crime pertenciam a um lote que havia sido adquirido pela Polícia Federal. Isso levantou suspeitas de envolvimento de agentes de segurança.

Devido as Interceptações telefônicas, a polícia interceptou ligações e mensagens de suspeitos para identificar conexões entre eles e o planejamento do crime. Com todo esse auxílio tecnológico, em março de 2019, um ano após o crime, dois ex-policiais militares foram presos e acusados de envolvimento no assassinato.

Embora os executores tenham sido identificados, a motivação e os mandantes do crime ainda são objeto de investigação. Em 2023, a Polícia Federal assumiu parte das investigações para dar continuidade ao caso.

O caso Marielle Franco é um exemplo de como a tecnologia pode ser usada para investigar crimes complexos por justiça no Brasil, podendo esclarecer e elucidar crimes que sem o uso da tecnologia poderia ficar sem resolução até os dias de hoje.

2.3 OS DIREITOS FUNDAMENTAIS E A PRIVACIDADE NA SEGURANÇA DIGITAL

Diante dos avanços tecnológicos, houve a necessidade das autoridades policiais em se adequar aos tempos modernos, trabalhando com ferramentas que podem melhorar a eficiência e a eficácia das operações. Entretanto, essas ferramentas trazem questões importantes a serem discutidas.

Com o uso de tecnologias na segurança pública como câmeras de vigilância, reconhecimento facial e análise de big data, ao se refere ao armazenamento, processamento e análise de grandes volumes de dados que são gerados em alta velocidade e em diferentes formatos, acabam levantando questões sobre privacidade, consentimento e discriminação.

Um das principais questões levantadas é o equilíbrio entre segurança e privacidade. O uso da vigilância em massa, facilitada por câmeras e drones, pode infringir o direito à privacidade dos cidadãos? Ocorre que muitas das vezes, as pessoas não estão cientes de que estão sendo monitoradas, o que gera questões a serem consideradas, até qual momento os cidadãos têm sua privacidade violada em nome da segurança?

O uso de reconhecimento facial, acaba sendo uma das principais ferramentas utilizadas pelas autoridades de segurança pública, ao qual utiliza algoritmos avançados para identificar pessoas a partir de imagens capturadas por câmeras, esse método tem sido aplicado em aeroportos, rodoviárias, estádios e outros espaços públicos de grande circulação.

O uso de reconhecimento facial pela polícia é uma tecnologia controversa. Embora possa ajudar a identificar suspeitos, também levanta preocupações sobre precisão e viés racial. Estudos mostram que esses sistemas podem falhar em identificar corretamente pessoas de grupos minoritários.

O que levanta outro ponto, o desafio ético e a questão do consentimento informado. Muitas tecnologias utilizadas na segurança pública são implementadas sem o conhecimento ou consentimento dos cidadãos. Isso gera um dilema ético sobre a legitimidade do uso dessas ferramentas e se as comunidades têm voz nas decisões que afetam sua segurança e privacidade.

A falta de transparência no uso de tecnologias pelas forças policiais pode comprometer a confiança da população em meio de segurança. Pois quando as comunidades não têm clareza sobre como essas ferramentas estão sendo utilizadas ou quais dados estão sendo coletados, é algo do ser humano, ter questionamentos sobre como esses dados estão sendo utilizados e as formas aos quais dados são repassados.

Além disso, surge questionamentos sobre como a coleta e análise de grandes volumes de dados traz consigo o risco de manipulação ou uso indevido das informações obtidas. Dados sensíveis podem acabar sendo utilizados para finalidades não previstas, como perseguições políticas ou até mesmo discriminação em processos judiciais

Outro ponto preocupante é a desigualdade no acesso às tecnologias de segurança pública. Em algumas comunidades, especialmente aquelas mais vulneráveis, o monitoramento pode ser mais intenso devido ao maior índice de

criminalidade, levantando posicionamentos de discriminação.

A automação de decisões no âmbito policial também levanta questões éticas importantes. Quando um erro grave ocorre em decorrência de uma decisão tomada por um algoritmo, quem deve ser responsabilizado? Esse dilema ressalta a importância de manter a supervisão humana nas operações e de garantir que haja responsabilidade ética em todas as etapas do processo.

A constante presença de tecnologias de vigilância nas comunidades pode ter impactos psicológicos significativos. A sensação de estar sendo observado o tempo todo pode gerar ansiedade e até mesmo um sentimento de opressão, criando um ambiente onde os cidadãos não se sentem plenamente seguros, mesmo em suas próprias comunidades.

Diante desses desafios, é essencial que a implementação de tecnologias na segurança pública seja acompanhada de políticas claras e bem definidas. Princípios como transparência, responsabilidade e respeito à privacidade devem estar no centro dessas iniciativas, garantindo que o uso da tecnologia seja equilibrado e alinhado aos direitos dos cidadãos.

2.4 NECESSIDADE DE PROTEÇÃO DE DADOS SOB A LUZ DA LGPD – LEI DE PROTEÇÃO DE DADOS

A LGPD representa um marco importante para a proteção da privacidade no Brasil. Ao estabelecer regras claras para o tratamento de dados pessoais, formalmente conhecida como Lei nº 13.709/2018, é a legislação brasileira que regula o tratamento de dados pessoais, tanto no setor público quanto no privado. Inspirada em legislações internacionais, como o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia.

A LGPD tem como objetivo principal garantir a privacidade e a proteção dos dados pessoais dos indivíduos, promovendo transparência e segurança nas práticas de coleta, armazenamento, uso e compartilhamento dessas informações. A LGPD foi criada para proteger os direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade da pessoa natural.

Essa lei busca equilibrar o uso de dados pessoais com a necessidade de inovação tecnológica, desenvolvimento econômico e prestação de serviços, garantindo que as informações dos cidadãos sejam tratadas de forma ética e segura.

De acordo com a LGPD, dados pessoais são qualquer informação que permita identificar, direta ou indiretamente, uma pessoa natural. Alguns exemplos incluem o Nome, CPF, RG, endereço, telefone, e-mail, tendo também os dados financeiros, como informações bancárias, os dados de localização, como o uso de GPS e as informações digitais, como endereços IP e cookies.

A LGPD também define uma categoria especial de dados chamada de dados sensíveis, que exige maior proteção. Esses incluem: Origem racial ou étnica, dados de saúde ou vida sexual e dados genéticos ou biométricos. Esses dados são considerados mais críticos porque, se mal utilizados, podem gerar discriminação ou violação de direitos fundamentais.

Diante dessa vertente, a mesma estabelece princípios que devem ser seguidos por qualquer organização que trate dados pessoais. Entre eles, destacam-se:

A Finalidade a qual os dados devem ser coletados para um propósito legítimo, específico e informado ao titular, o tratamento dos dados deve ser compatível com a finalidade informada e apenas os dados estritamente necessários para o objetivo pretendido devem ser coletados. O uso de forma transparente, os titulares têm direito de saber como seus dados estão sendo usados.

Observa-se que, ao tratar da intimidade, da vida privada, da honra e da imagem das pessoas, remete-se diretamente ao critério individual de cada ser humano. Por esse motivo, torna-se desafiador conceituar o que se entende por privacidade de forma universal.

Quando se discute a necessidade de proteção da privacidade, percebe-se que a legislação brasileira, bem como a Constituição Federal, estabelece punições para aqueles que violam a intimidade de terceiros. Essas punições incluem formas de reparação, como indenizações de natureza material e moral.

Nas constituições anteriores à de 1988, é possível identificar disposições que tratavam da proteção da privacidade. Contudo, essas proteções restringiam-se ao aspecto da inviolabilidade do domicílio e ao sigilo da correspondência.

Apenas com a Constituição de 1988, o direito à intimidade e à proteção da vida privada foi devidamente reconhecido e garantido como um direito fundamental.

No âmbito internacional, assim como no Brasil, percebe-se que a preocupação com o direito à privacidade intensificou-se ao longo do século XX, acompanhando os avanços da modernidade.

No caso brasileiro, essa evolução foi consolidada com a promulgação da

Convenção Interamericana de Direitos Humanos (CIDH, 1969), também conhecida como Pacto de San José da Costa Rica, por meio do Decreto nº 678, de 6 de novembro de 1992 (BRASIL, 1992). Esse marco internacional reforçou a proteção dos direitos humanos, incluindo o direito à privacidade.

Além disso, a legislação nacional também avançou nesse sentido. O Código de Defesa do Consumidor (Lei nº 8.078/1990) trouxe, em suas disposições, o direito de acesso às informações pessoais, fortalecendo a proteção da privacidade no contexto das relações de consumo.

Mais recentemente, com o advento da Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), buscou-se garantir a liberdade e a privacidade das pessoas, preenchendo uma lacuna legislativa existente no Brasil.

Essa lei, sancionada em 14 de agosto de 2018, tem como objetivo principal proteger os direitos fundamentais da liberdade, da privacidade e do livre desenvolvimento da personalidade da pessoa natural. Conforme disposto no artigo 1º da referida lei:

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural” (BRASIL, 2018).

É importante, contudo, destacar que a entrada em vigor da Lei nº 13.709/2018 não implica sua aplicação de forma absoluta. Isso ocorre porque outros princípios fundamentais devem ser considerados e equilibrados com o princípio da privacidade, assegurando que diferentes direitos sejam protegidos de maneira harmoniosa.

2.4.1 Importância da LGPD na Segurança Pública

A área da segurança pública é um campo sensível em que o uso de dados pessoais é essencial para a prevenção e repressão de crimes. A coleta, o armazenamento e o uso dessas informações precisam ser realizados de forma ética e responsável para evitar abusos.

A LGPD desempenha um papel crucial nesse contexto, pois ela protege os direitos dos cidadãos, ao estabelecer limites para o uso de dados pessoais, a LGPD

protege o direito à privacidade, evitando que informações sensíveis sejam utilizadas de forma discriminatória ou abusiva.

Previne o vazamento de dados, a LGPD exige que órgãos públicos implementem medidas de segurança robustas, como criptografia e controle de acesso, para proteger informações pessoais.

Garante a responsabilidade dos servidores público, a lei de LGPD, em seu art. 42, fala que o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo (BRASIL, 2018, art. 42). Este art. discute as formas e meios as quais os agentes são submetidos ao manuseio de dados, responsabilizando-os em caso de negligência ou má-fé.

O vazamento de dados, quando ocorre no âmbito da segurança pública, pode comprometer investigações, expor vítimas e testemunhas, além de violar direitos fundamentais.

2.4.2 Uso da LGPD para Coibir o Vazamento de Dados por Servidores Públicos

Com a implementação da Lei Geral de Proteção de Dados Pessoais (LGPD), instituída pela Lei nº 13.709/2018, regula o tratamento de dados pessoais no Brasil e estabelece diretrizes claras para prevenir o uso indevido de informações, especialmente por servidores públicos.

O vazamento de dados pessoais é uma prática que pode gerar graves consequências, como exposição de informações sensíveis, prejuízos à privacidade e violação de direitos fundamentais. Nesse contexto, a LGPD apresenta dispositivos legais que visam coibir essa prática, impondo responsabilidades aos agentes públicos e estabelecendo penalidades.

A LGPD estabelece princípios fundamentais para o tratamento de dados pessoais, que devem ser observados tanto por entidades privadas quanto públicas. Esses princípios estão descritos no art. 6º da LGPD e incluem os pilares para o tratamento de dados que são a finalidade que é o tratamento de dados e qual o propósito legítimo, específico e deve ser informado ao titular, evitando usos indevidos ou desnecessários.

A Necessidade ao qual deve-se limitar o tratamento de dados ao mínimo

necessário para atingir a finalidade pretendida. E a segurança, onde os servidores devem adotar medidas técnicas e administrativas para proteger os dados pessoais contra acessos não autorizados e vazamentos.

Ao qual é discutido em seu art. 23 da LGPD, na qual dispõe que o tratamento de dados pessoais que deve ser realizado para a execução de políticas públicas, respeitando os princípios da lei.

A referida lei obriga os agentes de tratamento a adotarem medidas técnicas e administrativas para garantir a segurança dos dados. Essas medidas incluem a implementação de sistemas de controle de acesso e o treinamento contínuo dos servidores públicos para evitar negligências ou abusos.

O texto legal reforça que os agentes de tratamento devem adotar medidas de segurança, vejamos:

Art. 46: "Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito" (BRASIL, 2018, art. 46)

Diante deste parágrafo, podemos compreender que a lei visa proteger os dados pessoais e a forma que o mesmo é manipulado, estipulando formas de restringir o acesso e tornar mais difícil o acesso e divulgação a terceiros.

Outra obrigação relevante está no art. 48, que exige a comunicação imediata de incidentes de segurança à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares dos dados. De acordo com o artigo, "o controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares" (BRASIL, 2018, art. 48).

Vale frisar que a LGPD em seu art. 52, prevê sanções administrativas para casos de descumprimento, vejamos:

Art. 52: "Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: I - advertência, com indicação de prazo para adoção de medidas corretivas; II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração; [...]" (BRASIL, 2018, art. 52).

No caso de servidores públicos, as penalidades podem incluir advertências, suspensão ou exoneração, dependendo da gravidade do vazamento, diante desta lei, fica claro o comprometimento em resguardar os direitos de privacidade dos cidadãos.

2.4.3 A Visão da Corrente Utilitarista em relação a LGPD

A LGPD pode ser analisada sob a ótica de pensadores que discutiram temas como controle, vigilância e liberdade individual, é uma lei que tem os mesmos princípios que estes distintos pensadores, aos quais mesmo em épocas distintas colocaram em suas obras, ideais de vigilância, controle e liberdade.

Michel Foucault, em sua obra *Vigiar e Punir* (1975), analisa o papel da vigilância como uma forma de controle social. Ele utiliza o conceito do Panóptico, idealizado por Jeremy Bentham, para explicar como a vigilância constante pode disciplinar os seres humanos e si próprio. No contexto da LGPD, a vigilância exercida pelo Estado sobre os cidadãos precisa ser equilibrada para não se transformar em um mecanismo opressor.

A LGPD atua como um contrapeso ao poder estatal, garantindo que a coleta e o uso de dados pessoais sejam realizados de forma transparente e ética. Segundo Foucault, "o poder é exercido mais eficazmente quando é invisível" (FOUCAULT, 1975). Neste mesmo sentido, a LGPD cria mecanismos para tornar o poder visível, exigindo que o Estado preste contas sobre o uso de informações privadas.

Não dando ao estado, o poder absoluto de controle sobre os dados, obrigando os seus operadores a prestar contas sobre como seus dados são utilizados e de que forma os mesmos serão repassados, fazendo assim uma interação e informação do usuário ao dono dos dados colhidos.

Jeremy Bentham, era um filósofo da corrente utilitarista, que idealizou o Panóptico, que seria uma estrutura arquitetônica que permite a vigilância constante de indivíduos sem que eles saibam quando estão sendo observados. O Panóptico neste caso é uma metáfora entre a relação da tecnologia e a privacidade na era digital.

A LGPD busca mitigar os efeitos negativos do "Panóptico digital", impondo limites à vigilância estatal e corporativa. Ao exigir consentimento e transparência no uso de dados, a LGPD garante que os cidadãos tenham controle sobre suas informações, reduzindo o sentimento de constante vigilância, tendo assim uma segurança de como esses dados serão tratados e utilizados.

John Stuart Mill, em seu livro chamado, Sobre a Liberdade (1859), defendia que a liberdade individual deve ser protegida contra a interferência do Estado, exceto quando há risco de danos a terceiros. A LGPD reflete esse princípio ao equilibrar a necessidade de segurança pública com o direito à privacidade, a lei veio para tentar inibir que apenas o estado tenha poder sobre estes dados, fazendo com que o mesmo venha ter obrigações com os cidadãos e transparência sobre seu uso.

Stuart Mill argumenta que "o único propósito pelo qual o poder pode ser exercido legitimamente sobre qualquer membro de uma comunidade civilizada, contra a sua vontade, é para prevenir danos a outros" (MILL, 1859). No contexto da LGPD, isso significa que o Estado só pode tratar dados pessoais quando for estritamente necessário para proteger a sociedade, respeitando os direitos individuais.

Diante disso, fica claro que a Lei Geral de Proteção de Dados Pessoais (LGPD) é um avanço na proteção da privacidade e na promoção da segurança pública no Brasil. Ao estabelecer regras claras para o tratamento de dados, a LGPD protege os direitos fundamentais dos cidadãos e responsabiliza os agentes públicos por eventuais abusos.

Sob a ótica de pensadores como Foucault, Bentham e Mill, a LGPD representa um esforço para equilibrar o poder do Estado com as liberdades individuais, garantindo que a vigilância e o controle sejam exercidos de forma ética e transparente, tendo uma troca entre os cidadãos e o estado.

Tanto Foucault quanto Bentham destacam os perigos de sistemas de vigilância. A LGPD tenta mitigar esses riscos ao impor limites claros ao tratamento de dados. Mill e Bentham enfatizam a importância da liberdade individual e do bem-estar coletivo. A LGPD protege a privacidade como um direito essencial para a manutenção da liberdade em uma sociedade digital.

Em suma, a LGPD reflete preocupações éticas que estão no cerne das teorias desses pensadores, ao equilibrar os interesses de empresas e governos com os direitos dos indivíduos. Assim, a LGPD não apenas coíbe o vazamento de dados, mas também fortalece a confiança da sociedade nas instituições públicas, sendo imprescindível o auxílio dessas tecnologias para prevenir e reprimir possíveis crimes e divulgações de dados.

3 METODOLOGIA

3.1 TIPO DE PESQUISA

A pesquisa caracteriza-se como um estudo exploratório e descritivo, pois visa aprofundar o conhecimento sobre o tema. Segundo Gil (2002), as pesquisas exploratórias têm a finalidade de proporcionar maior familiaridade com o problema, visando torná-lo mais claro ou construir hipóteses, incluindo o levantamento bibliográfico. Por sua vez, Marconi e Lakatos (2017) afirmam que a pesquisa descritiva busca descrever as mais diversificadas características de uma população e, através disso, visa analisar e interpretar os dados que foram coletados.

Esta pesquisa utiliza uma abordagem qualitativa, buscando compreender em profundidade como a tecnologia passou por tantas mudanças e tornou-se parte do cotidiano, sendo uma ferramenta utilizada nos meios policiais para a prevenção de crimes. Para Denzin e Lincoln (2006), a pesquisa qualitativa envolve uma abordagem interpretativa do mundo, em que os pesquisadores estudam as coisas em seus cenários naturais, com o objetivo de entender os fenômenos em termos dos significados que as pessoas a eles conferem.

Por sua vez, Teixeira (2005) afirma que a pesquisa qualitativa busca diminuir a distância entre teoria e dados. Por utilizar a lógica da análise, essa pesquisa trata de salientar os fatos ao longo do tempo, permitindo uma vasta e sucinta compreensão da situação.

Esta pesquisa situa-se nas áreas do Direito Penal e da Criminologia, com destaque para as relações entre o sistema de justiça policial e a tecnologia como meio de prevenção de crimes, com principal foco na análise de como o uso inadequado e não ético dos dados pode afetar a população.

Sendo assim, é certo reconhecer a presença da pesquisa documental e bibliográfica. Esta “busca conhecer e analisar as contribuições culturais ou científicas do passado sobre determinado assunto, tema ou problema” (CERVO E BERVIAN, 1983).

Conforme Gil (2007), a pesquisa documental diferencia-se da pesquisa bibliográfica por utilizar: a) material que não recebeu, ainda, nenhum tratamento analítico:

a) como documentos arquivados em órgãos públicos e organizações privadas;

b) documentos como relatórios de pesquisa, tabelas estatísticas, relatórios de empresas etc.

4 RESULTADOS E DISCUSSÃO

Na presente pesquisa, foram encontrados vinte e cinco artigos, dos quais dez sujeitaram-se à análise. Como critério de exclusão e inclusão, foi levado em consideração o ano da publicação, com margem de dez anos, sendo que os artigos estão compreendidos entre os anos de 2014 e 2023. Para mais, investigou-se o bibliotecas eletrônicas científicas, como Scielo, Google Acadêmico e Banco de Teses e Dissertações da CAPES.

Teve-se em conta também as palavras-chaves percebidas nos estudos, citando como exemplos: tecnologia e processo penal. Para melhor representação dos artigos selecionados, abaixo desenvolveu-se um quadro comparativo, onde encontra-se o ano da publicação, tipo de pesquisa, nome do artigo e autor. Além disso, observa-se o objetivo, resultados e conclusões apreendidos das pesquisas.

Quadro 1 – Demonstrativo dos trabalhos de produção científica.

Nome/Autor/Ano/Tipo	Objetivo(s)	Resultados/Conclusões
TECNOLOGIA E SEGURANÇA PÚBLICA: UMA ANÁLISE DA APLICAÇÃO DAS NOVAS TECNOLOGIAS NO COMBATE À CRIMINALIDADE – LUCAS, Thiago (2014) Documental, Bibliográfica	Analisar como diferentes tecnologias, como softwares de gestão e ferramentas de monitoramento, são aplicadas pelas forças de segurança no Brasil para combater a criminalidade, destacando casos práticos e resultados obtidos.	Observou-se a necessidade de leis para fiscalização de como esses dados obtidos através de monitoramento são tratados, as formas que são analisados e seus resultados obtidos.
POLÍCIA E TECNOLOGIA: O IMPACTO DAS TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO NA SEGURANÇA PÚBLICA - SOUZA, André (2015) Bibliográfica, documental.	Analisar a transformação das práticas policiais com a introdução de tecnologias de informação e comunicação. O livro Discute como essas ferramentas podem otimizar a atuação policial e melhorar a relação com a comunidade.	Destacou-se a importância de respeitar os direitos fundamentais em frente a introdução da tecnologia em âmbito policial e a necessidade dessa importante ferramenta para segurança.
SEGURANÇA PÚBLICA E TECNOLOGIAS DA INFORMAÇÃO - ALMEIDA, José Carlos (2018) Pesquisa Exploratória, qualitativa	Verificou-se o papel das tecnologias da informação na segurança pública, abordando sua importância para a coleta e análise de dados, planejamento estratégico e tomada de decisões nas operações policiais.	Conclui-se que o presente artigo investiga o papel desenvolvido sobre o uso da tecnologia na segurança, abordando como é importante a análise sobre os dados coletados frente ao material obtido em parceria com o monitoramento com o uso da tecnologia.

O USO DE DRONES NA SEGURANÇA PÚBLICA: POTENCIALIDADES E DESAFIOS - SILVA, Mariana – (2019) Bibliográfica, descritiva	Estudar as potencialidades do uso de drones nas operações de segurança pública, como vigilância em áreas de difícil acesso, mas também aborda os desafios éticos e legais que essa tecnologia pode trazer.	Conclui-se que apesar da tecnologia ajudar e combater a criminalidade, tem se a necessidade de implantação de fiscalização, até quando é aceitável esse monitoramento e as imputações legais sobre essa vigilância.
A TECNOLOGIA COMO ALIADA DA SEGURANÇA PÚBLICA: ANÁLISE DO USO DE CÂMERAS DE VIGILÂNCIA – PEREIRA, Fernanda (2023). Pesquisa exploratória e documental.	Examinar a eficácia das câmeras de vigilância na prevenção e resolução de crimes, discutindo suas vantagens e limitações no contexto urbano brasileiro.	Observa-se os parâmetros entre a prevenção utilizando a tecnologia e as vertentes do monitoramento urbano, onde a ética se encaixa na utilização das imagens geradas.
BIG DATA E SEGURANÇA PÚBLICA: DESAFIOS E OPORTUNIDADES – OLIVEIRA, Rafael (2022). Pesquisa exploratória e qualitativa.	Estudar e analisar grandes volumes de dados pode ser utilizado para identificar padrões criminais, prever crimes e melhorar as estratégias policiais, além de abordar os desafios relacionados à privacidade e à ética.	Estuda e analisa os casos de levantamento de grandes volumes de dados com fins de prevenção e combate ao crime, abordando como isso se correlaciona com a ética e a proteção dos dados da população.
INTELIGÊNCIA ARTIFICIAL NA SEGURANÇA PÚBLICA: UMA NOVA ERA? - MARTINS, Carlos Eduardo (2018) – Bibliográfica e descritiva	Analisar o impacto da inteligência artificial nas operações policiais, abordando como algoritmos podem ser utilizados para prever crimes, otimizar recursos e melhorar a eficiência das investigações.	Conclui-se que as atividades policiais, ganharam uma grande ferramenta de monitoramento examinando a maneira que os algoritmos podem ser aplicados para antecipar crimes, aprimorar a alocação de recursos e aumentar a eficácia das investigações.
CYBERCRIME E A SEGURANÇA PÚBLICA NO BRASIL: DESAFIOS CONTEMPORÂNEOS - CASTRO, Luana. (2017) Explorativa e qualitativa	Verificar o crescimento do cibercrime no Brasil, discutindo os desafios que isso representa para as autoridades de segurança pública em termos de legislação, capacitação e recursos.	Analisar a ascensão do cibercrime no Brasil e debater os obstáculos sobre como as autoridades podem se utilizar dos presentes dados e quais os desafios, junto a legislação com relação aos meios utilizados e a preservação dos direitos junto a LPD.

TECNOLOGIA E POLICIAMENTO COMUNITÁRIO: UM ESTUDO SOBRE A INTEGRAÇÃO ENTRE TECNOLOGIA E COMUNIDADE – REIS, GUSTAVO (2020). Pesquisa bibliográfica e documental.	Analisar como as tecnologias podem fortalecer o policiamento comunitário, promovendo maior interação entre a polícia e os cidadãos, além de melhorar a confiança mútua.	Observou-se que, com a devida interação social e a ajuda mútua da comunidade, é possível conviver harmoniosamente com a população, contando com a divulgação e a interação proporcionadas pela tecnologia.
O IMPACTO DAS REDES SOCIAIS NA SEGURANÇA PÚBLICA: O PAPEL DA INFORMAÇÃO EM TEMPO REAL – GARCIA, Ana Paula (2022). Pesquisa bibliográfica e documental.	Examinar como as redes sociais têm se tornado uma ferramenta importante na disseminação de informações sobre segurança pública, tanto para alertar sobre crimes quanto para mobilizar ações comunitárias.	Analisa as formas como as redes sociais e a internet desempenham um papel importante como veículos de informação, sendo utilizadas como ferramentas de alerta e prevenção de crimes.

Fonte: Dados de pesquisa (2025)

Ao iniciar este trabalho, foi considerado como as inovações tecnológicas poderiam auxiliar na segurança pública em seu controle preventivo e repressivo. No caso em questão, o uso da tecnologia torna-se uma ferramenta imprescindível, capaz de transformar a forma como o Estado previne, combate e investiga crimes.

Ao analisar a problemática apresentada, foram identificados alguns desafios relacionados ao uso da inteligência artificial. Por um lado, o uso de câmeras com reconhecimento facial representa um grande avanço tecnológico, pois esse sistema permite a identificação de criminosos em meio a grandes multidões, tendo alcançado excelentes resultados. Por outro lado, essa tecnologia ainda necessita de aprimoramento.

No entanto, a mesma máquina que realiza o reconhecimento facial de criminosos requer ajustes, como a inserção e programação de dados, para que não incorra em erros cometidos por humanos, como a identificação de pessoas por meio de um viés racista já estruturado na sociedade e também presente na abordagem policial. Um software não identifica quem mais comete crimes pela cor da pele, mas sim pelos dados que lhe são inseridos.

A troca de informações é essencial no que se refere aos mandados de prisão, sejam eles em aberto ou vencidos, pois qualquer equívoco na inserção de dados pode

resultar na prisão de uma pessoa inocente, havendo, portanto, a necessidade de zelo no tratamento dessas informações.

No que diz respeito à captação de sinais de telefones celulares por meio de antenas de operadoras de telefonia móvel, verifica-se a necessidade de tempo para mapear e localizar números exatos para investigação, além da exigência de autorizações judiciais para a busca e apreensão desses aparelhos, visando, ao final, a extração e triangulação de conversas e informações contidas nesses dispositivos para a elucidação de crimes. O trabalho de inteligência demanda pessoal treinado e maior investimento por parte da União, sendo necessário um repasse mais equitativo entre os estados brasileiros e as polícias Militar, Civil e Federal.

Por fim, a incorporação dessas tecnologias avançadas tem contribuído para a redução dos índices de criminalidade e para o aumento da sensação de segurança entre a população. Todavia, no uso dessas tecnologias, o zelo no acesso e na manipulação de dados exige atenção e cuidado, a fim de não comprometer a liberdade individual.

5 CONCLUSÃO

O presente trabalho buscou compreender como a tecnologia pode ajudar as forças de segurança pública e os desafios éticos enfrentados na modificação e implementação de softwares que visam auxiliar no monitoramento, processamento e combate à criminalidade.

De acordo com o relatório Justiça em Números 2023, aproximadamente 90% dos processos judiciais no Brasil já estão digitalizados, o que resultou em uma redução de até 35% no tempo médio de tramitação em comparação aos processos físicos. Além disso, o investimento em infraestrutura digital pelo Poder Judiciário cresceu 15%, totalizando R\$ 1,5 bilhão, demonstrando o compromisso com a implementação de soluções tecnológicas avançadas (CNJ, 2023).

Outro aspecto relevante é o impacto direto das tecnologias no monitoramento e prevenção de crimes. Segundo dados do CNJ, o uso de tornozeleiras eletrônicas reduziu em 68% os casos de reincidência em violência doméstica, enquanto dispositivos como aplicativos de proteção às vítimas evitaram mais de cinco mil agressões em 2023.

No âmbito da inteligência artificial, mais de 70% dos tribunais brasileiros já utilizam ferramentas baseadas em aprendizado de máquina, responsáveis por analisar mais de um milhão de processos e acelerar a resolução de casos acumulados. Essas ações, integradas ao programa Justiça 4.0, contribuíram para o julgamento de mais de 500 mil processos relacionados a crimes financeiros, evidenciando a importância da tecnologia para a promoção de justiça célere e eficiente (CNJ, 2024).

Entretanto, a análise das prisões injustas decorrentes de mandados de prisão vencidos e erros em sistemas de reconhecimento facial evidencia as fragilidades estruturais do sistema de segurança pública e justiça no Brasil. A coexistência de bancos de dados desatualizados, tecnologias enviesadas e a falta de regulamentação clara que visa punir esse tipo de violações graves dos direitos humanos, afetando principalmente grupos historicamente marginalizados, como negros e pardos.

Esses erros não apenas expõem pessoas inocentes ao constrangimento público e à privação injusta de liberdade, mas também reforçam desigualdades sociais e raciais, amplificando preconceitos já enraizados na sociedade brasileira. Além disso, a confiança da população nas instituições de segurança pública é profundamente

abalada, criando um ciclo de desconfiança e ineficiência.

Este trabalho conclui que a inovação tecnológica trouxe grandes benefícios e contribuiu de forma significativa para o auxílio e a prevenção na área da segurança pública. Contudo, foram evidenciados desafios relacionados à proteção de dados e à consolidação de leis para a fiscalização do tratamento e da utilização dos dados, bem como ao monitoramento da população.

Dessa forma, foram levantadas questões sobre segurança, tratamento de dados, monitoramento e utilização de softwares para fins de segurança, sendo esses aspectos de extrema importância para a sociedade, pois contribuem para a elucidação de casos, além de auxiliarem na prevenção e repressão de crimes. Assim, tornam-se indispensáveis no contexto atual.

REFERÊNCIAS

ALMEIDA, José Carlos. **Segurança pública e tecnologias da informação**. 2018.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 fev. 2025.

BUOLAMWINI, Joy; GEBRU, Timnit. **Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification**. Proceedings of Machine Learning Research, v. 81, p. 1-15, 2018. Disponível em: <https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>. Acesso em: 14 mar. 2025.

CASTRO, Luana. **Cybercrime e a segurança pública no Brasil: desafios contemporâneos**. 2017.

CERVO, A. L.; BERVIAN, P. A. **Metodologia científica**. 3. ed. São Paulo: McGraw-Hill, 1983.

COSTA, Ricardo. **Segurança pública, redes e governança**. São Paulo: SciELO Books, 2024.

DENZIN, N. K.; LINCOLN, Y. S. **O planejamento da pesquisa qualitativa: teorias e abordagens**. 2. ed. Porto Alegre: Artmed, 2006.

DURANT, Will. **A História da Civilização: Nossa herança oriental**. 2. ed. São Paulo: Editora Record, 2001.

EMSLEY, Clive. **The Birth of the English Police**. London: Bloomsbury Academic, 2010.

FERREIRA, Daniel de Souza Caliar; AARÃO, Melhym Pires. **Inteligência artificial e responsabilidade civil: algoritmos racistas no caso Google e o arcabouço jurídico brasileiro**. Disponível em: <https://revistaft.com.br/inteligencia-artificial-e-responsabilidade-civil-algoritmos-racistas-no-caso-google-e-o-arcabouco-juridico-brasileiro/>. Acesso em: 19 jan. 2025.

FERRÉS, Joan. **Televisão Subliminar: socialização mediante comunicações inadvertidas**. Porto Alegre: Edições Médicas Sul Ltd, 1996.

GARCIA, Ana Paula. **O impacto das redes sociais na segurança pública: o papel da informação em tempo real**. 2022.

GIL, A. C. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2002.

GIL, A. C. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2007.

JÚNIOR, A. L. S. **Fundamentos jurídicos da atividade policial**. São Paulo: Suprema Cultura, 2009.

LUCAS, Thiago. **Tecnologia e segurança pública: uma análise da aplicação das novas tecnologias no combate à criminalidade**. 2014.

MARCONI, M. A.; LAKATOS, E. M. **Fundamentos de metodologia científica**. 8. ed. São Paulo: Atlas, 2017.

MARTINS, Carlos Eduardo. **Inteligência artificial na segurança pública: uma nova era?** 2018.

OLIVEIRA, Rafael. **Big Data e segurança pública: desafios e oportunidades**. 2022.

PEREIRA, Fernanda. **A tecnologia como aliada da segurança pública: análise do uso de câmeras de vigilância**. 2023.

REIS, Gustavo. **Tecnologia e policiamento comunitário: um estudo sobre a integração entre tecnologia e a comunidade**. 2020.

SILVA, Ângelo Roberto. **Crimes cibernéticos**. São Paulo: Editora JH Mizuno, 2017.

SILVA, Mariana. **O uso de drones na segurança pública: potencialidades e desafios**. 2019.

SOUZA, André. **Polícia e tecnologia: o impacto das tecnologias de informação e comunicação na segurança pública**. 2015.

TEIXEIRA, S. J. **Pesquisa qualitativa em educação: fundamentos e abordagens**. São Paulo: Cortez, 2005.