

A Dicotomia entre Segurança Pública e Privacidade Individual

RAPHAEL ARISTÓTELES FREITAS
LUCAS RICIERI ANDRADE PAIVA
RENATA FREITAS SILVEIRA
JOÃO EMMANUEL D'ALKMIN NEVES

Resumo

Este artigo tem como objetivo analisar a tensão entre segurança pública e privacidade individual no contexto do uso de tecnologias de vigilância urbana, com ênfase na Internet das Coisas (IoT), bem como avaliar o nível de conhecimento e de confiança da população em relação à legislação. A partir de revisão bibliográfica e levantamento de campo realizado por meio de questionário online, investigou-se a percepção de cidadãos brasileiros sobre a coleta de dados pessoais em espaços públicos e seu grau de familiaridade com a Lei Geral de Proteção de Dados (LGPD). Os resultados indicam que, embora haja aceitação moderada do uso de tecnologias inteligentes para fins de segurança, há presença de desconfiança significativa quanto à efetividade da LGPD na proteção dos dados pessoais. Além disso, a maioria dos participantes demonstrou baixo nível de familiaridade com a legislação. Conclui-se que o avanço das tecnologias de vigilância deve ser acompanhado por transparência, fiscalização e educação digital, para equilibrar inovação tecnológica e garantias fundamentais.

Palavras-chave: IoT; LGPD; Privacidade; Segurança; Vigilância.

The Dichotomy between Public Security and Individual Privacy

Abstract

This article aims to analyze the tension between public security and individual privacy in the context of urban surveillance technologies, with an emphasis on the Internet of Things (IoT), as well as to assess the population's level of knowledge and trust regarding data protection legislation. Based on a literature review and a field study conducted through an online questionnaire, the research investigated Brazilian citizens' perceptions of the collection of personal data in public spaces and their degree of familiarity with the General Data Protection Law (LGPD). The results indicate that, although there is moderate acceptance of the use of smart technologies for security purposes, there is significant distrust regarding the effectiveness of the LGPD in protecting personal data. Furthermore, most participants demonstrated a low level of familiarity with the legislation. It is concluded that the advancement of surveillance technologies should be accompanied by transparency, oversight, and digital education in order to balance technological innovation and fundamental rights.

Keywords: IoT; LGPD; Privacy; Security; Surveillance.

1 INTRODUÇÃO

Diante das constantes mudanças no mundo digital, a tecnologia se torna cada vez mais influente no cotidiano, fortalecendo o que Castells (2018) chama de revolução informacional, caracterizada pela integração tecnológica que molda profundamente as estruturas sociais, econômicas e culturais. Nos últimos anos, se observou a crescente adoção de tecnologias tanto pelo setor público quanto pelo privado, especialmente com o uso da Internet das Coisas (IoT) no monitoramento e na gestão de ambientes urbanos e institucionais.

A IoT é uma rede inteligente de dispositivos, veículos, máquinas e outros físicos equipados com sensores, sistemas eletrônicos e conexão com a internet, permitindo a coleta e a troca de dados em tempo real. Essa conectividade permite o controle remoto dos dispositivos e promove uma integração mais eficiente entre os mundos físico e virtual, otimizando processos e ampliando a precisão das operações (Gokhale; Bhat; Bhat, 2018).

No entanto, mesmo com benefícios proporcionados pela IoT, surge um desafio em crescimento: proteger a privacidade dos usuários. A expansão da conectividade e a complexidade das infraestruturas digitais tornam mais difícil controlar o fluxo de informações pessoais e garantir seu uso adequado (Santos, 2016).

No Brasil, a Lei nº 13.709 de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), estabelece diretrizes para assegurar a privacidade e o tratamento adequado de dados por entes públicos e privados (Lima Rapôso *et al.*, 2019). Todavia, como destacam os mesmos autores, ainda há um debate significativo sobre a aplicabilidade e a efetividade da LGPD diante do avanço acelerado das tecnologias de informação, especialmente devido à insegurança jurídica sobre a transparência e a conformidade dos protocolos de uso de dados.

No cenário latino-americano, cresce também o uso de tecnologias como o reconhecimento facial na segurança pública, o que exige regulamentação alinhada aos direitos humanos e às legislações de proteção de dados presentes em países como Brasil, Colômbia, México e Equador. Essas normas estabelecem princípios de proporcionalidade, licitude e segurança para o tratamento de dados, exigindo consentimento do titular, salvo exceções previstas por lei (Badillo, 2023).

Diante desse contexto, surge a seguinte questão central: em que medida os brasileiros concordam com a coleta de dados pessoais por tecnologias IoT para fins de segurança pública? Para responder a essa questão, o estudo busca investigar a percepção da população brasileira acerca do uso desses dispositivos no âmbito da segurança pública.

A relevância desta pesquisa está no crescimento acelerado do uso de tecnologias IoT por órgãos de segurança pública e na necessidade de compreender como a população percebe esse processo. Considerando que muitos brasileiros ainda conhecem pouco a LGPD, torna-se fundamental avaliar se existe confiança na legislação para protegê-los contra o uso indevido dessas informações. Assim, compreender o nível de aceitação, preocupação e conhecimento dos cidadãos sobre o tema contribui para debates sobre transparência, governança de dados e políticas públicas mais alinhadas às garantias individuais.

2 REFERENCIAL TEÓRICO

Este capítulo apresenta os fundamentos teóricos que sustentam a presente investigação, abordando conceitos relacionados à Internet das Coisas, segurança da informação e privacidade de dados no contexto das tecnologias de vigilância urbana. Inicialmente, discute-se a relação

entre IoT e os desafios de proteção de dados, seguida da análise de aspectos legais e sociais associados ao uso dessas tecnologias.

2.1 Expansão IoT e Transformações na Segurança Pública

A Internet das Coisas refere-se à interconexão de dispositivos físicos capazes de coletar, processar e transmitir dados por meio da internet, incluindo sensores, câmeras inteligentes, sistemas de monitoramento urbano e plataformas de reconhecimento facial. No contexto da segurança pública, essas tecnologias têm sido incorporadas como instrumentos de monitoramento contínuo e análise preditiva, ampliando a capacidade estatal de vigilância e resposta a eventos urbanos. Embora a LGPD atribua centralidade ao consentimento como instrumento de proteção da autodeterminação informativa (Oliveira; Vega, 2024), Cordeiro e Sobral (2024) questionam sua efetividade em contextos de IoT, nos quais a coleta de dados ocorre de maneira difusa e muitas vezes imperceptível ao titular das informações.

Sob essa perspectiva, a expansão da IoT altera significativamente a dinâmica tradicional da segurança da informação, uma vez que multiplica os pontos de coleta e processamento de dados sensíveis. A interconectividade massiva amplia a chamada “superfície de ataque”, mas essa transformação não se limita a um desafio técnico. Trata-se de uma mudança estrutural na forma como dados são produzidos e apropriados, na qual a coleta contínua e difusa reduz a capacidade de controle do indivíduo sobre suas próprias informações. Nesse contexto, a segurança da informação deixa de ser apenas um problema de proteção de sistemas e passa a envolver disputas sobre controle, responsabilidade e governança de dados, tornando mais complexa a gestão de riscos e vulnerabilidades.

Dessa forma, o modelo clássico da segurança da informação, fundamentado nos princípios de Confidencialidade, Integridade e Disponibilidade, adquire papel estratégico ampliado. Contudo, sua aplicação em ambientes de IoT voltados à segurança pública revela limitações importantes, uma vez que tais princípios, embora essenciais, não são suficientes para responder aos desafios relacionados à coleta massiva, à opacidade dos sistemas e à assimetria de poder entre Estado e indivíduos. Assim, eventuais falhas nesses pilares não apenas expõem sistemas a vulnerabilidades técnicas, mas também podem resultar em impactos diretos sobre direitos fundamentais e sobre a própria legitimidade das práticas de vigilância.

Desafios semelhantes podem ser observados em outras infraestruturas críticas digitalizadas, como as *Smart Grids*, que integram sistemas físicos e redes informacionais para otimizar a gestão energética. Conforme demonstrado por Alves *et al.* (2025), a interconectividade massiva nessas redes amplia vulnerabilidades cibernéticas, exigindo documentação rigorosa das arquiteturas e demanda governança contínua para mitigação de riscos. Tal paralelo reforça que a expansão da IoT, independentemente do setor, não representa apenas avanço operacional, mas também aumento da complexidade na gestão da segurança da informação e da responsabilidade institucional. Adicionalmente, Cordeiro e Sobral (2024) ressaltam que a multiplicidade de agentes envolvidos no ecossistema IoT, incluindo desenvolvedores, operadores públicos e fornecedores privados, dificulta a definição clara de responsabilidades no tratamento de dados, o que fragiliza a aplicação prática das garantias previstas na LGPD.

2.2 Vigilância Digital, Reconhecimento Facial e Impactos Sociais

Impulsionada por avanços em inteligência artificial e *Big Data*, a vigilância digital assumiu espaço rapidamente em ambientes urbanos, sendo aplicada ao monitoramento

preditivo, controle de muralhas virtuais, localização de indivíduos procurados e policiamento em tempo real (Badillo, 2023). O uso de tecnologias de reconhecimento facial (FRT) materializa essa lógica, ao permitir a identificação biométrica automatizada em massa. No entanto, essa expansão não deve ser interpretada apenas como avanço tecnológico, mas como uma reconfiguração das relações de poder entre Estado e cidadão, conforme discutido por Lyon (2003). Nesse sentido, a vigilância deixa de operar exclusivamente como instrumento de segurança e passa a atuar como mecanismo potencial de controle social, especialmente em contextos marcados por desigualdade estrutural.

Todavia, a literatura aponta que a adoção acelerada dessas tecnologias na América Latina ocorre, em muitos casos, com níveis limitados de transparência e auditoria institucional. Segundo Badillo (2023), a implementação de sistemas FRT em contextos de desigualdade social pode expor agravantes de vigilância desproporcional e discriminação algorítmica. Sob essa perspectiva, a vigilância digital transcende para um processo político e social, capaz de ressignificar as fronteiras entre segurança, controle estatal e direitos fundamentais. No contexto europeu, Gültekin-Várkonyi (2024) destaca a centralidade das avaliações de impacto como instrumento preventivo de mitigação de riscos. Tal perspectiva reforça a necessidade de que instrumentos similares previstos na LGPD sejam efetivamente implementados no contexto brasileiro. Conforme discutido por Fontes e Lütge (2022), as tecnologias de vigilância reforçam relações de poder e ampliam mecanismos de controle social em espaços públicos.

Observa-se, portanto, uma discrepância entre a expansão pragmática dessas tecnologias em contextos latino-americanos e a abordagem europeia baseada em governança de risco e proporcionalidade estrita. Essa diferença não é meramente regulatória, mas revela assimetrias institucionais que podem resultar na adoção de tecnologias invasivas sem mecanismos adequados de controle, ampliando riscos à garantia de direitos fundamentais. Segundo Lyon (2003), a vigilância contemporânea atua como mecanismo de classificação social, influenciando dinâmicas de inclusão e exclusão.

2.3 Privacidade, Direitos Fundamentais e Regulação

A coleta de dados biométricos, como imagens faciais, se encontra na categoria de dados sensíveis, cuja proteção é assegurada por marcos regulatórios como o Regulamento Geral de Proteção de Dados da União Europeia (GDPR) e a Lei Geral de Proteção de Dados brasileira (LGPD). Tais legislações estabelecem parâmetros como finalidade, necessidade, adequação e proporcionalidade no processamento de informações pessoais, buscando evitar abusos e fortalecer autodeterminação informativa, especialmente em ambientes digitais. No Brasil, iniciativas legislativas como o Projeto de Lei nº 1.515/2022 buscam regulamentar o uso de dados pessoais em contextos de segurança pública (Brasil, 2022).

Entretanto, a aplicação desses marcos no contexto da segurança pública apresenta desafios estruturais. As exceções previstas na LGPD para atividades de segurança e investigação criminal podem, na prática, ampliar margens de discricionariedade estatal, criando zonas de ambiguidade regulatória e fragilizando a previsibilidade jurídica. Esse cenário levanta questionamentos sobre até que ponto tais exceções comprometem a efetividade das garantias legais, especialmente em contextos de vigilância em larga escala.

De acordo com De Paula *et al.* (2024), iniciativas legislativas voltadas ao compartilhamento de dados sensíveis entre órgãos de segurança ainda carecem de maior amadurecimento normativo e de debate público, o que evidencia lacunas na construção de mecanismos institucionais robustos. Nesse sentido, a existência de um arcabouço jurídico formal não assegura, por si só, a proteção de direitos fundamentais, uma vez que sua efetividade

depende diretamente da implementação de instrumentos concretos de fiscalização, transparência e responsabilização estatal.

Além disso, Bu (2021) sustenta que a adoção de tecnologias como o reconhecimento facial deve ser precedida de análises de impacto em direitos fundamentais, consultas públicas e auditorias independentes. Na ausência desses instrumentos, o uso dessas ferramentas pode comprometer direitos como privacidade, liberdade individual de expressão e igualdade, especialmente em contextos de vigilância em massa.

2.4 Síntese e Lacuna

A literatura analisada aponta que a implantação de tecnologias IoT emergentes e reconhecimento facial na segurança pública produz uma tensão estrutural entre eficiência operacional e preservação de direitos fundamentais. Enquanto parte dos estudos enfatiza o potencial dessas ferramentas para aprimorar políticas de segurança, outros autores destacam riscos associados à ampliação da vigilância estatal e à fragilidade de mecanismos de controle institucional (Badillo, 2023; Bu, 2021).

Evidencia-se que a presença de marcos regulatórios como a LGPD não elimina automaticamente as problemáticas associadas à coleta massiva de dados biométricos. Ao contrário, a coexistência entre expansão tecnológica e fragilidade na governança evidencia uma tensão estrutural entre inovação e proteção de direitos. Nesse cenário, a ausência de mecanismos efetivos de controle e transparência pode transformar instrumentos de segurança em dispositivos de vigilância ampliada, reforçando a necessidade de análise crítica não apenas normativa, mas também social e política.

3 METODOLOGIA

A presente seção detalha os procedimentos metodológicos adotados na condução da pesquisa, contemplando a caracterização do estudo, os meios utilizados, o instrumento de coleta de dados, o delineamento da amostra e as técnicas de análise empregadas. A estrutura metodológica foi definida de modo a assegurar consistência entre o referencial teórico apresentado e a proposta empírica de investigação da percepção social sobre o uso de tecnologias IoT na segurança pública.

3.1 Tipo de pesquisa e natureza

A presente pesquisa caracteriza-se como descritiva e exploratória, com abordagem quantitativa. É descritiva por buscar identificar e analisar percepções da população acerca da coleta de dados pessoais por tecnologias IoT no contexto da segurança pública. Para o desenvolvimento desta pesquisa, foram utilizados os métodos investigativos do tipo pesquisa bibliográfica e levantamento de campo. A pesquisa bibliográfica foi feita com base em livros, artigos científicos, publicações institucionais e documentos oficiais que abordam temas como a Lei Geral de Proteção de Dados (LGPD), Internet das Coisas (IoT) e segurança pública. Esse tipo de abordagem, conforme Gil (2008), é desenvolvido a partir da análise de materiais já publicados, sendo útil para compreender e fundamentar teoricamente o problema de pesquisa.

As questões foram elaboradas com base nos eixos teóricos discutidos na revisão de literatura, especialmente nos debates sobre governança de dados, consentimento informacional, vigilância digital e proporcionalidade regulatória. O instrumento foi estruturado de modo a

relacionar diretamente cada bloco temático aos objetivos específicos da pesquisa, garantindo coerência entre coleta e análise dos dados. A estrutura do instrumento foi construída de forma objetiva e padronizada, visando reduzir ambiguidades interpretativas. A coleta de dados foi realizada por meio de questionário estruturado, aplicado na plataforma Microsoft Forms. O instrumento foi composto por seis questões objetivas, sendo quatro de múltipla escolha e duas estruturadas em escala Likert, organizadas em três blocos temáticos: (i) percepção sobre IoT; (ii) conhecimento sobre LGPD; (iii) opiniões sobre vigilância urbana. O questionário teve como objetivo mensurar o nível de aceitação, percepção de risco e confiança regulatória dos participantes em relação ao uso de tecnologias IoT na segurança pública.

Nesse contexto, as questões em escala Likert foram estruturadas em cinco pontos, variando de 1 (discordo totalmente) a 5 (concordo totalmente), permitindo mensurar o grau de concordância dos participantes em relação às afirmações apresentadas. Os dados obtidos por meio dessas questões foram analisados por meio de média aritmética, possibilitando a identificação de tendências centrais nas percepções dos respondentes. Embora a escala Likert produza dados de natureza ordinal, a utilização da média é recorrente em estudos exploratórios, permitindo a identificação de padrões gerais de percepção.

Os dados foram analisados por meio de estatística descritiva, utilizando medidas de frequência absoluta e relativa para as questões objetivas, bem como medidas de tendência central (média aritmética) para as questões em escala Likert. Essa abordagem possibilita não apenas a organização dos dados, mas também a identificação de padrões de resposta e tendências gerais nas percepções dos participantes.

Embora não tenha sido realizada validação estatística formal do instrumento, sua construção foi fundamentada em literatura consolidada sobre o tema, o que contribui para sua validade de conteúdo. Ainda assim, a ausência de teste piloto estruturado constitui uma limitação metodológica, devendo os resultados ser interpretados à luz dessa restrição.

3.2 Amostra

A amostra foi composta por 60 participantes válidos, em sua maioria jovens adultos entre 18 e 30 anos, residentes em diferentes estados do Brasil. Trata-se de uma amostra não probabilística por conveniência, adequada para captar percepções iniciais sobre o tema. A escolha desse tipo de amostragem justifica-se pela natureza exploratória do estudo e pela intenção de obter um panorama preliminar das percepções sociais sobre a temática. Embora não permita generalizações estatísticas para a população brasileira, possibilita a identificação de padrões relevantes para análise.

A coleta foi realizada entre os dias 31 de maio e 7 de junho de 2025, com divulgação em fóruns de discussão sobre privacidade, ambientes universitários e por meio do compartilhamento espontâneo entre os próprios participantes. Os critérios de participação foram: ter 18 anos ou mais e residir no Brasil. Ao todo, 61 respostas foram coletadas, sendo uma desconsiderada por não atender ao critério de residência, resultando em 60 respostas válidas para análise. O número de participantes mostra-se compatível com a natureza exploratória da pesquisa, cujo objetivo não é produzir inferências estatísticas generalizáveis, mas identificar tendências iniciais de percepção social sobre o tema investigado. Em estudos de caráter descritivo, amostras reduzidas são consideradas adequadas para a obtenção de dados preliminares e para a identificação de padrões interpretativos relevantes.

Os dados foram analisados por meio de estatística descritiva, utilizando medidas de frequência absoluta e relativa para as questões objetivas, bem como medidas de tendência central (média aritmética) para as questões estruturadas em escala Likert. Essa abordagem

permitiu identificar padrões de resposta, níveis de concordância e tendências gerais nas percepções dos participantes.

As análises foram organizadas com base em categorias como faixa etária, escolaridade e estado de residência dos participantes. Quanto ao perfil sociodemográfico, observou-se predominância de jovens adultos entre 18 e 30 anos, com diferentes níveis de escolaridade e residentes em distintas regiões do país. A diversidade geográfica contribuiu para ampliar a heterogeneidade da amostra, ainda que não represente proporcionalmente a distribuição populacional brasileira.

3.3 Limitações metodológicas

A pesquisa apresenta limitações inerentes ao seu delineamento metodológico. A utilização de amostra não probabilística por conveniência pode gerar viés de auto-seleção, uma vez que os participantes aderiram voluntariamente ao questionário, o que pode resultar em maior concentração de indivíduos com interesse prévio no tema. Além disso, a predominância de jovens adultos pode influenciar os resultados, considerando possíveis diferenças geracionais na percepção sobre tecnologia e privacidade.

Outro limite refere-se à ausência de validação prévia formal do instrumento de coleta. Embora as questões tenham sido fundamentadas na literatura especializada, não houve aplicação de teste piloto estruturado, o que pode impactar a precisão na mensuração das percepções dos participantes. Dessa forma, os resultados devem ser interpretados como indicativos e exploratórios, não sendo passíveis de generalização estatística para a totalidade da população brasileira.

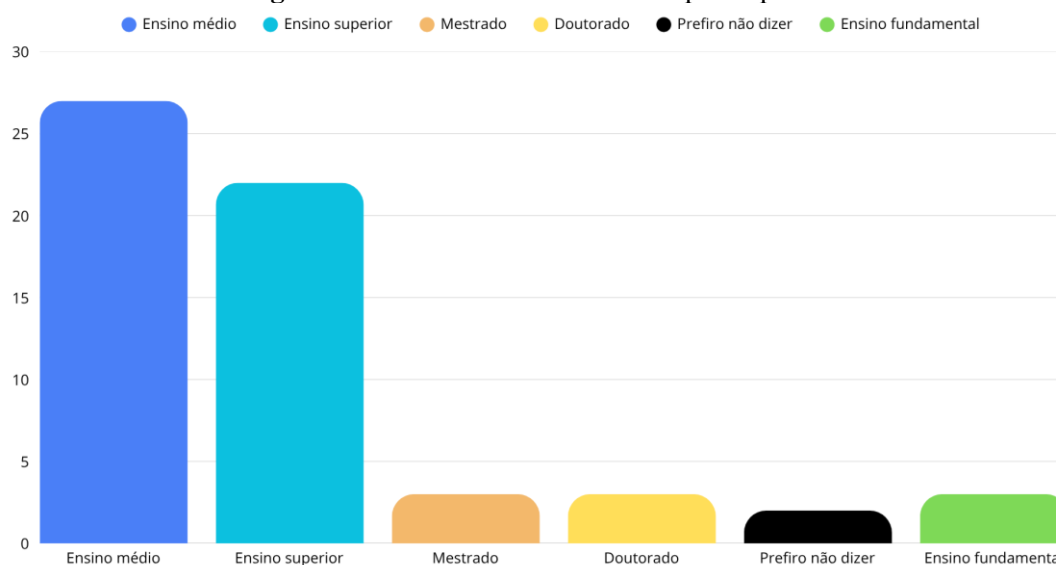
Adicionalmente, o uso de questionário online pode ter introduzido viés de cobertura, ao potencialmente excluir indivíduos com menor acesso à internet ou menor familiaridade com ferramentas digitais. Esse fator pode limitar a representatividade da amostra, especialmente em relação a grupos socialmente mais vulneráveis ou com menor inclusão digital.

4 RESULTADOS

A partir da análise dos dados coletados, podemos ter compreensão de como a população participante percebe a relação entre tecnologias de vigilância, como a Internet das Coisas (IoT), e a proteção da privacidade no contexto da segurança pública. De modo geral, resultados evidenciam consciência da presença e do uso de tecnologias inteligentes em espaços públicos, mas ainda marcada por um déficit de conhecimento legal e por sentimentos ambíguos quanto à proteção de seus dados pessoais.

Para entender com mais profundidade os resultados obtidos, é possível observar os gráficos a seguir gerados a partir dos dados coletados.

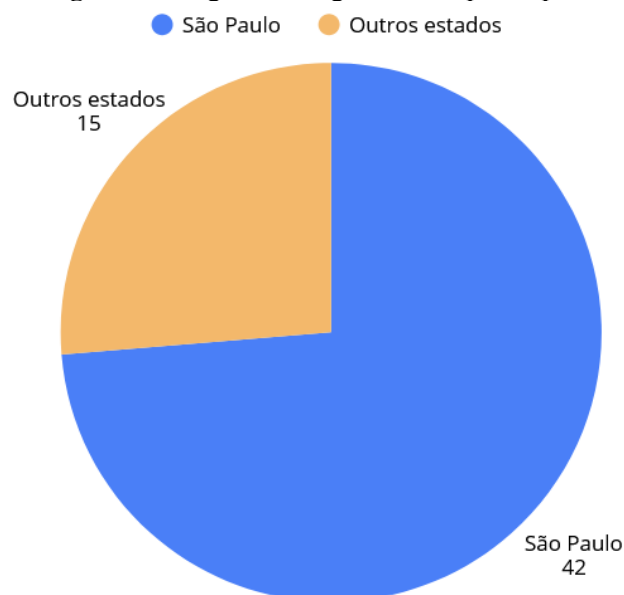
Figura 1 - Nível de escolaridade dos participantes



Fonte: Elaborado pelos autores (2025)

No que se refere ao nível de escolaridade, verifica-se na Figura 1, predominância de participantes com ensino médio e superior, indicando uma amostra com relativo acesso à educação formal. Esse perfil, quando analisado em conjunto, sugere a presença de indivíduos mais expostos a ambientes digitais e ao uso de tecnologias, o que pode influenciar diretamente a forma como percebem sistemas de vigilância e dispositivos IoT.

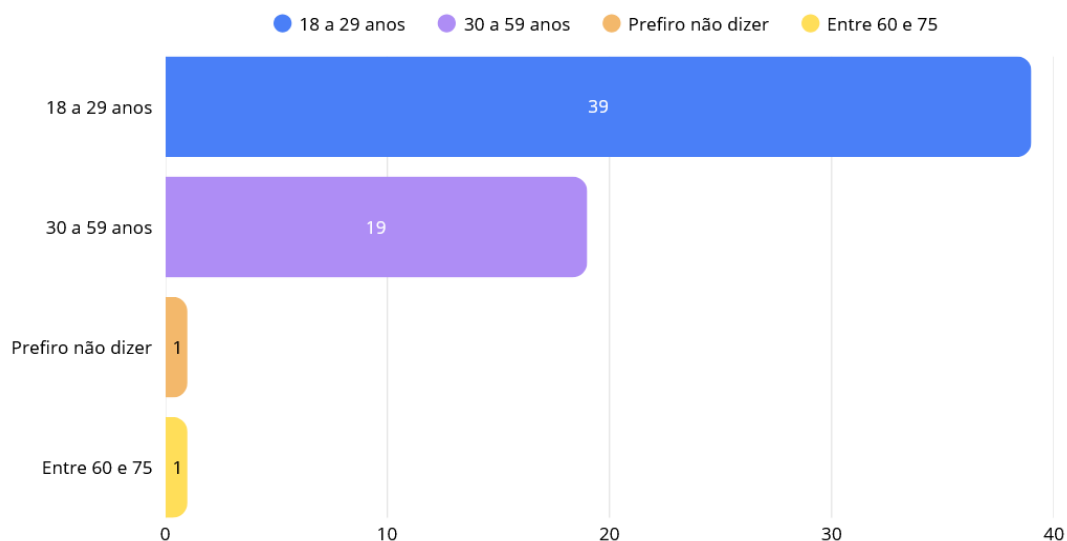
Figura 2 - Região demográfica dos participantes



Fonte: Elaborado pelos autores (2025)

Além disso, a concentração etária e geográfica evidencia possíveis limitações na representatividade da amostra, uma vez que a predominância de jovens adultos e de participantes de uma mesma região pode impactar a diversidade de percepções analisadas, especialmente em um tema sensível como privacidade e vigilância tecnológica, conforme verifica-se na Figura 2.

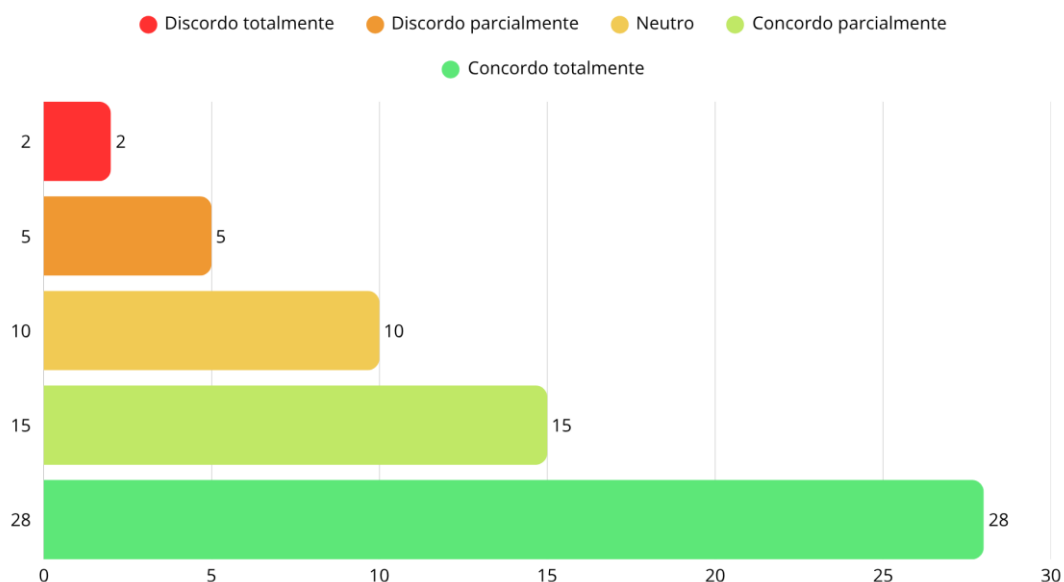
Figura 3 - Faixa etária dos participantes



Fonte: Elaborado pelos autores (2025)

Com base nos dados apresentados nas figuras, observa-se que a amostra é predominantemente composta por participantes residentes no estado de São Paulo, que representam a maior parcela dos respondentes, em comparação aos demais estados. Em relação à faixa etária, há predominância significativa de indivíduos entre 18 e 29 anos, entrevistados entre 30 e 59 anos, enquanto as demais categorias apresentam participação residual, conforme observa-se na Figura 3.

Figura 4 - Análise da concordância com o uso de IoT na segurança pública

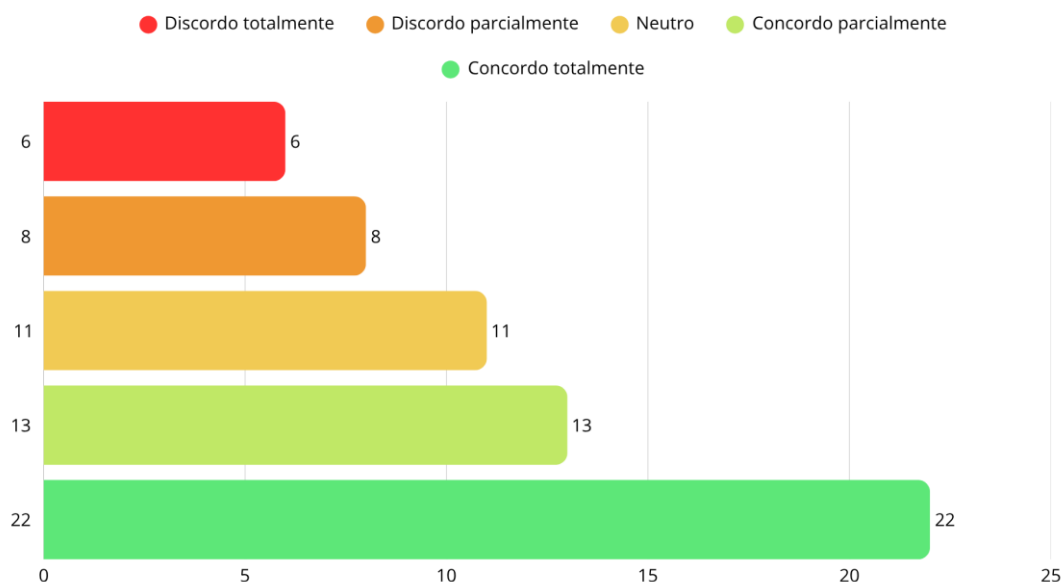


Fonte: Elaborado pelos autores (2025)

Quando foi questionado aos participantes “Você concorda com o uso de câmeras inteligentes (como reconhecimento facial) em locais públicos para fins de segurança?” obtém média de 4,03, indicando aceitação significativa dessas tecnologias. No entanto, esse resultado

não deve ser interpretado como legitimação irrestrita da vigilância digital. Ao contrário, ele sugere que a adesão está fortemente condicionada à percepção de utilidade imediata, especialmente associada à segurança pública, o que tende a sobrepor, no plano inicial, preocupações mais complexas relacionadas à privacidade, conforme verifica-se na Figura 4.

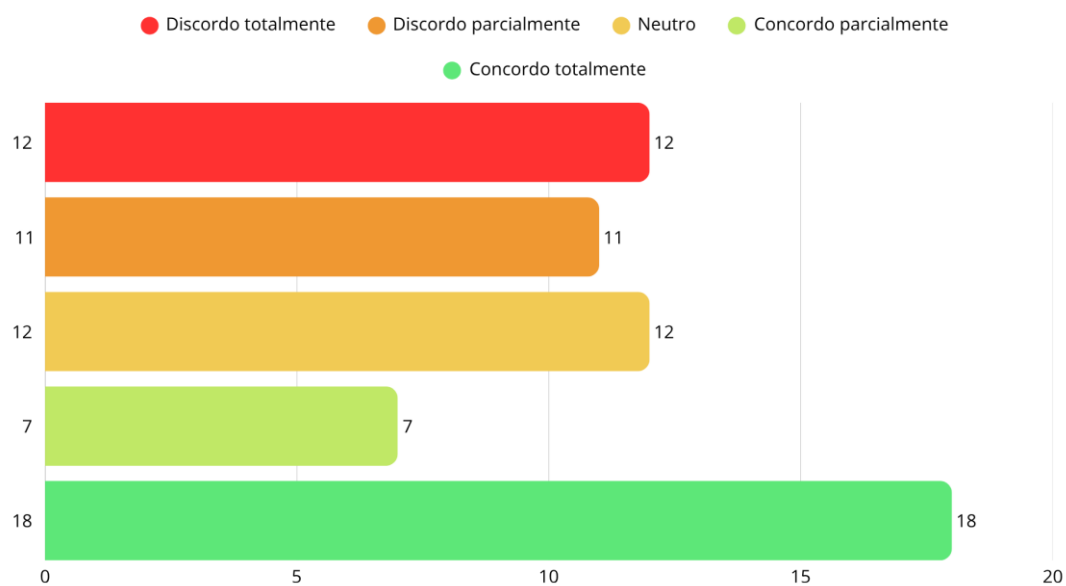
Figura 5 - Análise sobre o incentivo de uso de IoT



Fonte: Elaborado pelos autores (2025)

Com a pergunta “Você acredita que o uso de tecnologias como IoT (Internet das Coisas) deve ser incentivado na segurança pública, mesmo que isso implique em maior vigilância sobre os cidadãos?” apresenta uma classificação média de 3,62, indicando uma posição intermediária que não configura nem rejeição, nem adesão plena. Esse resultado sugere que o apoio à expansão dessas tecnologias é condicionado e pragmático, estando menos relacionado a uma confiança consolidada nos sistemas e mais à expectativa de benefícios imediatos associados à segurança, conforme observa-se na Figura 5.

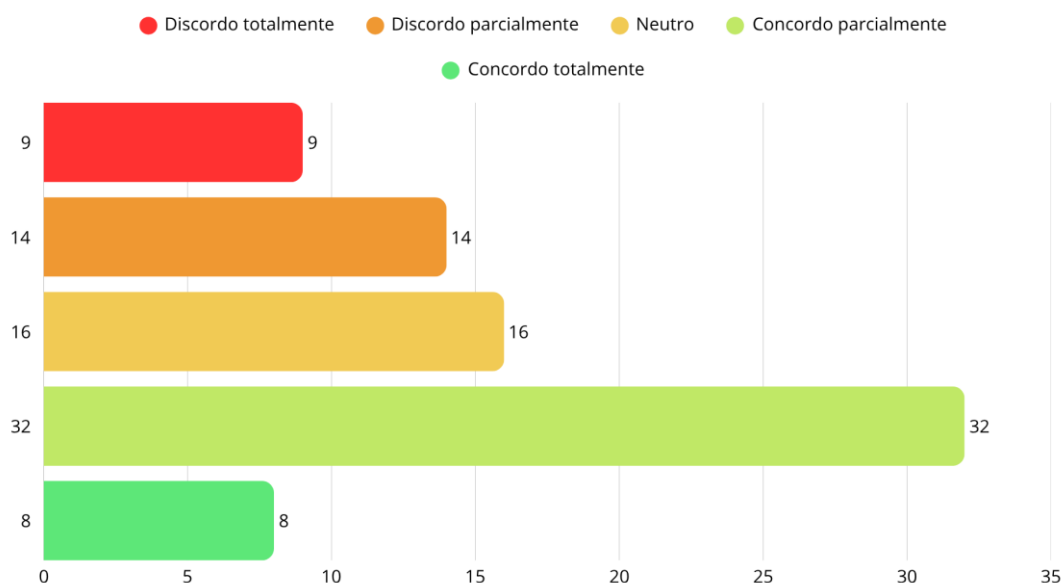
Figura 6 - Análise sacrifício da própria privacidade



Fonte: Elaborado pelos autores (2025)

Já a questão “Você concordaria em abrir mão de parte da sua privacidade em troca de mais segurança nos espaços públicos?” revela a classificação média de 3,13, demonstrando maior resistência do público em renunciar sua privacidade individual, relutância percebida de forma parecida entre os estados, mas resultado ainda mostra alta ambiguidade, sendo minimamente mais aceito em outros estados, conforme verifica-se na Figura 6. Sob a ótica da Segurança da Informação, esse dado reforça a centralidade do princípio da confidencialidade e escancara a preocupação social com práticas de monitoramento em massa com o uso indiscriminado de dados sensíveis, como biometria.

Figura 7 - Conhecimento da LGPD

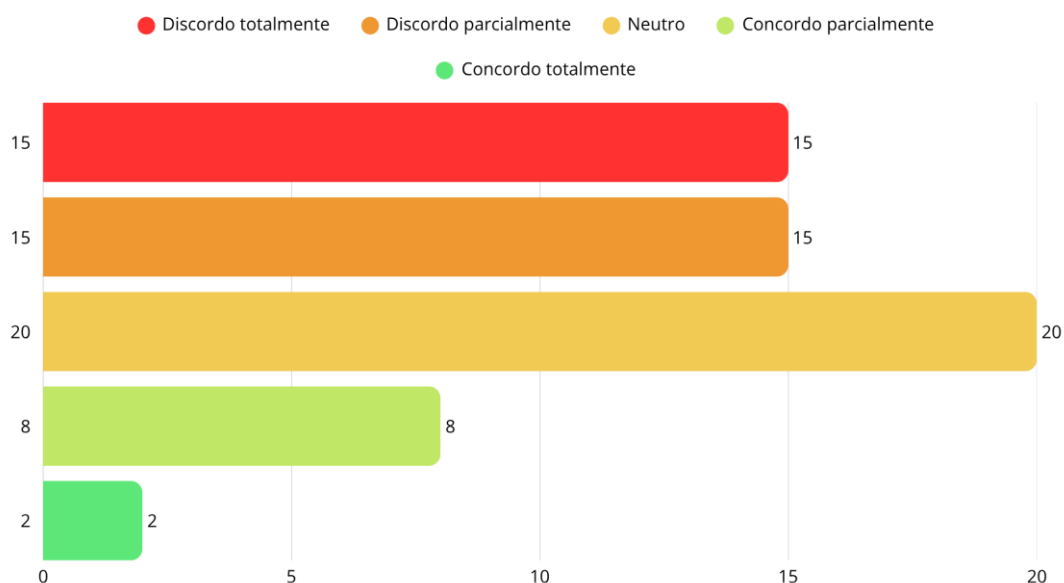


Fonte: Elaborado pelos autores (2025)

Com os dados coletados pela questão “Você considera que tem conhecimento suficiente sobre a Lei Geral de Proteção de Dados (LGPD)?”, classificação média de 2.95, a figura 5 mostra que os participantes em sua maioria se sentem pouco familiarizados com a LGPD, confirmando a hipótese inicial da pesquisa e está alinhado com os estudos que apresentam o letramento limitado no âmbito jurídico e digital da população brasileira em relação com a proteção de dados pessoais (De Paula *et al.*, 2024).

A distribuição das respostas demonstra que a maior parte dos participantes se concentrou na alternativa “concordo parcialmente”, seguida por respostas neutras e de discordância parcial. As opções “discordo totalmente” e “concordo totalmente” aparecem em menor frequência, indicando menor polarização nas extremidades. Esse padrão evidencia uma tendência dos respondentes a se posicionarem de forma intermediária quanto ao seu nível de conhecimento sobre a LGPD, conforme apresentado na Figura 7.

Figura 8 - Análise da suficiência da LGPD

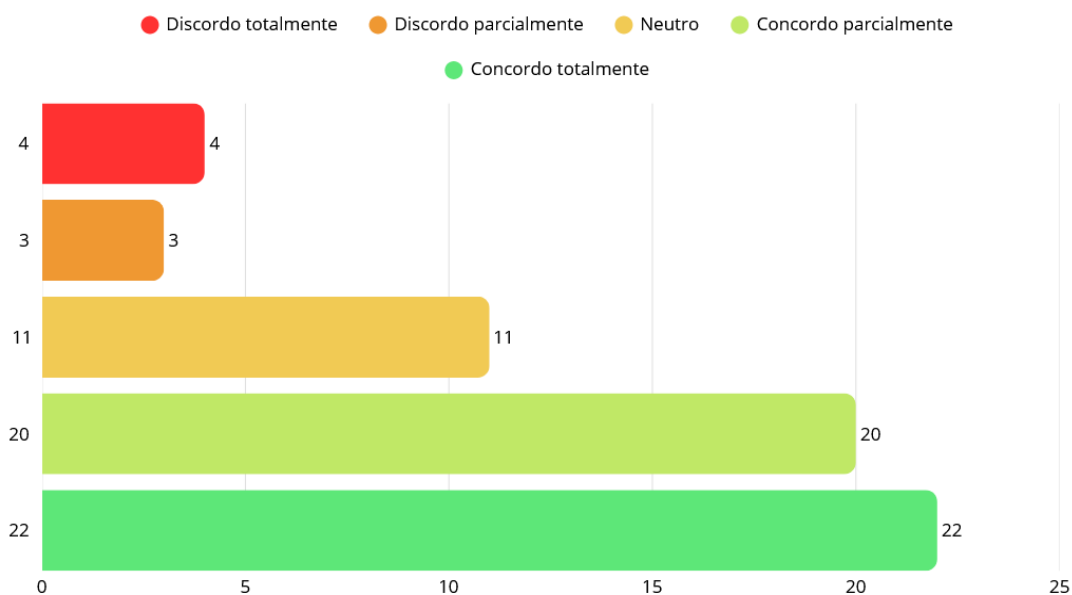


Fonte: Elaborado pelos autores (2025)

A questão “Você concorda que a Lei Geral de Proteção de Dados (LGPD) é suficiente para proteger os cidadãos frente ao avanço de tecnologias de vigilância?”, classificação média em 2,45, revelou que uma das hipóteses não se confirmou, pois, os participantes não se percebem protegidos pela lei diante do constante avanço das tecnologias como as IoTs, revelando alta desconfiança com a LGPD. Esse dado é relevante, pois relata uma percepção de fragilidade nos marcos legais, especialmente quando falado que a própria LGPD exclui, em seu artigo 4º, o tratamento de dados para fins de segurança pública.

A distribuição das respostas indica que a maior concentração de participantes se posicionou na alternativa neutra, seguida por níveis semelhantes de discordância total e discordância parcial. Em menor proporção, aparecem os respondentes que concordam parcialmente, enquanto a concordância total representa a menor frequência entre as opções. Esse padrão evidencia uma predominância de respostas centradas ou inclinadas à discordância em relação à suficiência da LGPD, conforme ilustrado na Figura 8.

Figura 9 - Ciência com relação aos dados coletados



Fonte: Elaborado pelos autores (2025)

Com a pergunta “Você reconhece que seus dados pessoais são coletados por câmeras, sensores e outros dispositivos IoT em espaços públicos para fins de segurança?” foi obtido a classificação média 3,88, confirmando o letramento digital dos participantes, que percebem que seus dados estão sendo utilizados em espaços públicos para fins de segurança.

Os resultados apresentados evidenciam uma dissociação entre aceitação das tecnologias IoT e preocupação com a integridade da privacidade. Mesmo que haja reconhecimento dos benefícios associados ao uso, a desconfiança aponta para riscos significativos no campo da Segurança da Informação, especialmente no que se refere à confidencialidade e integridade. Reforçamos as críticas antes citadas sobre a adoção acelerada de tecnologias sem controle ou auditoria independente adequada (Badillo, 2023). Sugerem necessidade de políticas públicas que apresentem fortalecimentos regulatórios, para equilíbrio da segurança pública com privacidade, conforme exibido na Figura 9.

5 DISCUSSÃO

Entende-se que os resultados apresentam um padrão consistente de ambiguidade: aceitação moderada ao uso de tecnologias IoT na segurança das cidades, contudo essa aceitação não se converte em confiança plena nos mecanismos de proteção dos dados coletados. A média obtida para a concordância do uso das câmeras inteligentes indica que os participantes percebem valor instrumental na tecnologia como suporte ao monitoramento, especialmente quando associada à segurança coletiva e à prevenção de riscos urbanos. Esse dado sugere que a utilidade percebida exerce influência significativa na legitimação social da vigilância tecnológica.

Entretanto, essa aceitação não deve ser interpretada como adesão irrestrita às práticas de vigilância. A média inferior registrada na questão relativa à disposição de abrir mão da privacidade demonstra que esse apoio é condicionado, refletindo uma percepção latente de risco associada à coleta massiva de dados. Esse comportamento pode ser compreendido como

resultado de uma tensão entre benefício coletivo e proteção individual, na qual os indivíduos reconhecem a utilidade da tecnologia, mas resistem à ampliação do controle sobre suas informações pessoais.

Paralelamente, o baixo nível de autopercepção de conhecimento sobre os marcos regulatórios, especialmente acerca da LGPD, não apenas evidencia um déficit de letramento jurídico-digital, mas também ajuda a explicar a desconfiança observada. A ausência de compreensão sobre os mecanismos legais de proteção pode reforçar a percepção de vulnerabilidade, contribuindo para a baixa confiança na capacidade do Estado em regular e fiscalizar o uso dessas tecnologias, conforme apontado por De Paula *et al.* (2024).

Nesse sentido, o conflito identificado entre aceitação tecnológica, desconfiança regulatória e consciência de vigilância revela uma dinâmica mais complexa do que uma simples adesão ou rejeição às tecnologias de monitoramento. Trata-se de um cenário em que a legitimidade da vigilância não depende exclusivamente de sua eficácia operacional, mas também da transparência institucional, da governança dos dados e da confiança social nos mecanismos de proteção. Assim, os resultados sugerem que a consolidação dessas tecnologias no contexto da segurança pública está diretamente condicionada à capacidade do Estado de equilibrar inovação tecnológica e garantia de direitos fundamentais.

6. CONSIDERAÇÕES FINAIS

Com essa investigação foi possível observar que a maioria dos participantes concorda moderadamente com o uso de dispositivos IoT para fins de segurança pública (média 4,03 em escala de 1 a 5), o que indica uma percepção positiva quanto à utilidade da tecnologia. No entanto, quando questionados sobre a disposição em renunciar sua privacidade em troca de segurança, a média foi significativamente menor, sugerindo que, embora reconheçam os potenciais benefícios dessas tecnologias, os participantes possuem postura relutante diante da perda de seu direito.

Na análise dos autores, essa tensão entre segurança e privacidade alerta para os riscos da implementação de sistemas de vigilância massiva em contextos sociais desiguais e sem garantias institucionais adequadas. A coleta de dados sensíveis, como imagens faciais, quando realizada sem fiscalização rigorosa e sem consentimento explícito, compromete princípios como liberdade, anonimato e não discriminação.

Outro aspecto relevante evidenciado com a pesquisa refere-se ao conhecimento acerca da Lei Geral de Proteção de Dados Pessoais (LGPD). A média de 2,95 indica que a maioria dos respondentes não se sente familiarizada com a legislação atual, podendo comprometer sua capacidade de reconhecer práticas abusivas no tratamento de dados que, em conjunto com a baixa confiança na eficácia da LGPD para protegê-los, sugere um desencontro entre a percepção pública sobre sua efetividade.

Os resultados confirmam parcialmente a hipótese inicial do estudo. Embora haja reconhecimento da presença das tecnologias de vigilância e aceitação moderada de sua aplicação, não se observa confiança equivalente nos mecanismos regulatórios que deveriam assegurar proteção jurídica. Essa informação fortalece os argumentos de que qualquer avanço tecnológico no campo da segurança pública deve seguir processos transparentes, fiscalizados e democraticamente discutidos.

Logo, o objetivo da pesquisa: analisar a percepção social sobre o uso de IoT na segurança pública em contraste com a proteção de dados, foi atingido ao constatar a coexistência de apoio tecnológico e ceticismo institucional.

Em contextos marcados por desigualdades estruturais e fragilidade institucional, a implementação de sistemas de monitoramento massivo pode ampliar riscos de uso indevido, discriminação e erosão de direitos, especialmente quando envolve o tratamento de dados sensíveis, como biometria facial.

Em termos práticos, os achados indicam a necessidade de fortalecimento das políticas públicas voltadas à transparência no tratamento de informações, ampliação do letramento digital e jurídico da população e implementação de mecanismos independentes de auditoria em sistemas de monitoramento. Para a área de Segurança da Informação, reforça-se a importância de princípios como confidencialidade, integridade e *accountability* como elementos estruturantes da governança tecnológica.

Por fim, como sugestão de pesquisas futuras, há de se analisar com levantamento de campo com grupo de participantes mais numerosos e mais bem distribuídos para ter uma visão mais fiel das percepções acerca do tema, com questões que explorem mais o entendimento dos conceitos pelos participantes e análise mais profunda dos aspectos sociais por trás das respostas.

REFERÊNCIAS

- ALVES, W. S. A.; BARBOZA, L. A.; MARQUES, J. F. S.; NEVES, J. E. D. A. Vulnerabilidade em Smart Grids. **Revista Tecnológica da Fatec Americana**, 2025, DOI: doi.org/10.47283/md2dpk85. Disponível em: fatec.edu.br/revista/index.php/RTecFatecAM/article/view/365. Acesso em: 17 mar. 2026.
- BADILLO, M. *Navigating the complexities of facial recognition for public security in Latin America*. Londres: International Bar Association, 2023. Disponível em: www.ibanet.org/facial-recognition-security-latin-america. Acesso em: 20 maio 2025.
- BRASIL. Câmara dos Deputados. **Projeto de Lei nº 1.515/2022**. Dispõe sobre a 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. Brasília, DF: Câmara dos Deputados, 2022. Disponível em: www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2326300&fichaAmigavel=nao. Acesso em: 20 maio 2025.
- BU, Q. The global governance on automated facial recognition (AFR): ethical and legal opportunities and privacy challenges. **International Cybersecurity Law Review**, v. 2, p. 113–145, 2021. DOI: doi.org/10.1365/s43439-021-00022-x. Disponível em: doi.org/10.1365/s43439-021-00022-x. Acesso em: 22 maio 2025.
- CASTELLS, M. **A sociedade em rede**. 11. ed. São Paulo: Paz e Terra, 2018. v. 1.
- CORDEIRO, A. A. de M.; SOBRAL, L. L. Desafios regulatórios da Lei Geral de Proteção de Dados (LGPD) para Internet das Coisas (IoT). **Revista Tecnologia**, v. 45, p. 1–11, 2024. DOI: doi.org/10.5020/23180730.2024.13998. Disponível em: doi.org/10.5020/23180730.2024.13998. Acesso em: 13 mar. 2026.
- DE PAULA, A. V.; DE BARROS, F.; RESENDE DE OLIVEIRA, L. A discriminação racial no sistema de reconhecimento facial no Brasil e seus impactos na política criminal. **Revista**

de Direitos Humanos e Desenvolvimento Social, v. 5, 2024. DOI: doi.org/10.24220/2675-9160v5a2024e13770. Disponível em: periodicos.puc-campinas.edu.br/direitoshumanos/article/view/13770. Acesso em: 31 maio 2025.

FONTES, A. C.; LÜTGE, C. Vigilância e relações de poder: o uso de tecnologias de reconhecimento facial e identificação biométrica a distância em espaço público e impactos na vida pública. **Direito Público**, v. 18, n. 100, 2022. Disponível em: www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/6203. Acesso em: 25 maio 2025.

GIL, A. C. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2008.

GOKHALE, P.; BHAT, O.; BHAT, S. **Introduction to IoT**. 2018. Disponível em: www.researchgate.net/publication/330114646_Introduction_to_IOT. Acesso em: 27 maio 2025.

GÜLTEKIN-VÁRKONYI, G. Navigating data governance risks: facial recognition in law enforcement under EU legislation. **Internet Policy Review**, v. 13, n. 3, 2024. Disponível em: policyreview.info/articles/analysis/data-governance-risks-facial-recognition. Acesso em: 13 mar. 2026.

LIMA RAPÔSO, C. F.; MELO DE LIMA, H.; DE OLIVEIRA JUNIOR, W. F.; FERREIRA SILVA, P. A.; BARROS, E. de S. LGPD – Lei Geral de Proteção de Dados Pessoais em tecnologia da informação: revisão sistemática. **RACE – Revista de Administração do Cesmac**, v. 4, p. 58–67, 2019. DOI: doi.org/10.3131/race.v4i0.1035. Disponível em: cesmac.emnuvens.com.br/administracao/article/view/1035. Acesso em: 25 maio 2025.

LYON, D. (org.). **Surveillance as social sorting: privacy, risk, and digital discrimination**. London: Routledge, 2003. Acesso em: 25 maio 2025.

OLIVEIRA, D. B. de; VEGA, G. C. M. A proteção da privacidade pela Lei Geral de Proteção de Dados (LGPD) na era da Internet das Coisas (IoT). **Revista de Direito**, v. 16, n. 2, p. 1–30, 2024. DOI: doi.org/10.32361/2024160219351. Disponível em: periodicos.ufv.br/revistadir/article/view/19351. Acesso em: 13 mar. 2026.

SANTOS, P. M. P. **Internet das coisas: o desafio da privacidade**. Setúbal: Instituto Politécnico de Setúbal, 2016. Disponível em: core.ac.uk/download/pdf/75985137.pdf. Acesso em: 27 maio 2025