FACIAL RECOGNITION IN BRAZILIAN PUBLIC SECURITY
ethical challenges, regulatory gaps, and proposals for a national legal framework

Simone Pereira Duarte Ferreira *
Luiz Honorato da Silva Júnior **

ABSTRACT: This article critically examines the regulatory and ethical challenges involved in the use of facial recognition (FR) technologies in Brazilian public security. The investigation is based on a systematic literature review and documentary analysis, revealing a significant regulatory gap. This void compromises not only the protection of personal data but also institutional transparency and the legitimacy of the state's use of such technologies. In a country historically marked by deep social and racial inequalities, the risks associated with algorithmic discrimination, indiscriminate surveillance, and violations of fundamental rights become even more concerning. The study seeks to understand how different countries have addressed these issues, drawing on regulatory models adopted in the European Union, the United States, and China. Based on this comparative analysis, the article proposes guidelines for the development of a national regulatory framework that promotes ethical and responsible governance of technology. Key elements include the implementation of audit mechanisms, oversight by independent bodies, and commitment to the operational efficiency of security forces. The conclusion is that Brazil must adopt a flexible regulatory model guided by principles such as proportionality, transparency, and accountability, ensuring a balance between technological innovation and the protection of constitutional rights and guarantees.

Keywords: facial recognition; public security; artificial intelligence; data protection; algorithmic bias.

DOI: https://doi.org/10.36776/ribsp.v9i23.338

Recebido em 13 de outubro de 2025.	Aprovado em 2 de abril de 2026.

* Polícia Civil do Distrito Federal (PCDF). CV Lattes: http://lattes.cnpq.br/5535676000951497 .
** Universidade de Brasília (UnB). Orcid: https://orcid.org/0000-0002-2840-3579 . CV Lattes: http://lattes.cnpq.br/1741285388725128

RECONHECIMENTO FACIAL NA SEGURANÇA PÚBLICA BRASILEIRA
desafios regulatórios, riscos éticos e propostas para um marco legal eficaz

RESUMO: Este artigo analisa de forma crítica os desafios regulatórios e éticos que envolvem a aplicação de tecnologias de reconhecimento facial na segurança pública brasileira. A investigação parte de uma revisão sistemática da literatura e de uma análise documental, revelando a existência de um vácuo normativo significativo. Essa lacuna compromete não apenas a proteção de dados pessoais, mas também a transparência institucional e a legitimidade do uso dessa tecnologia por órgãos estatais. Em um país historicamente marcado por profundas desigualdades sociais e raciais, os riscos associados à discriminação algorítmica, à vigilância indiscriminada e à violação de direitos fundamentais tornam-se ainda mais preocupantes. A pesquisa busca compreender como diferentes países têm enfrentado esses dilemas, tomando como referência os modelos regulatórios adotados na União Europeia, nos Estados Unidos e na China. A partir dessa comparação, propõem-se diretrizes voltadas à construção de um marco regulatório nacional que promova uma governança ética e responsável da tecnologia. Entre os elementos essenciais estão a existência de mecanismos de auditoria, a supervisão por órgãos independentes e o compromisso com a eficiência operacional das forças de segurança. Conclui-se que o Brasil precisa adotar um modelo regulatório flexível, orientado por princípios como a proporcionalidade, a transparência e a accountability, garantindo o equilíbrio entre inovação tecnológica e a preservação dos direitos e garantias constitucionais.

Palavras-chave: reconhecimento facial; segurança pública; inteligência artificial; proteção de dados; viés algorítmico.

1. INTRODUCTION

The rapid advancement of artificial intelligence (AI) has driven the development of technologies aimed at public security, among which facial recognition (FR) stands out as one of the most controversial. Used by police forces to identify suspects, locate missing persons, and support criminal investigations, FR is often seen as a promise for modernizing mechanisms of social control and crime prevention. However, its adoption in Brazil has occurred in a decentralized manner, without specific regulatory support, which raises serious concerns regarding the legality of its use, the protection of personal data, and the safeguarding of fundamental rights (Zuboff, 2019; Melo & Serra, 2022).

The absence of a national regulatory framework governing the use of facial recognition by public agents creates legal uncertainty for both technology operators and monitored citizens. Beyond legal uncertainties, there are significant ethical implications, such as the risk of mass surveillance, the potential reinforcement of structural inequalities through algorithmic bias, and the lack of effective mechanisms for transparency and oversight. While countries such as the European Union and the United States have adopted regulatory models with varying degrees of rigor and scope, Brazil remains faced with a normative vacuum that hinders the safe, fair, and efficient implementation of this technology (Buiten, 2019; Buolamwini & Gebru, 2018; Melo & Serra, 2022).

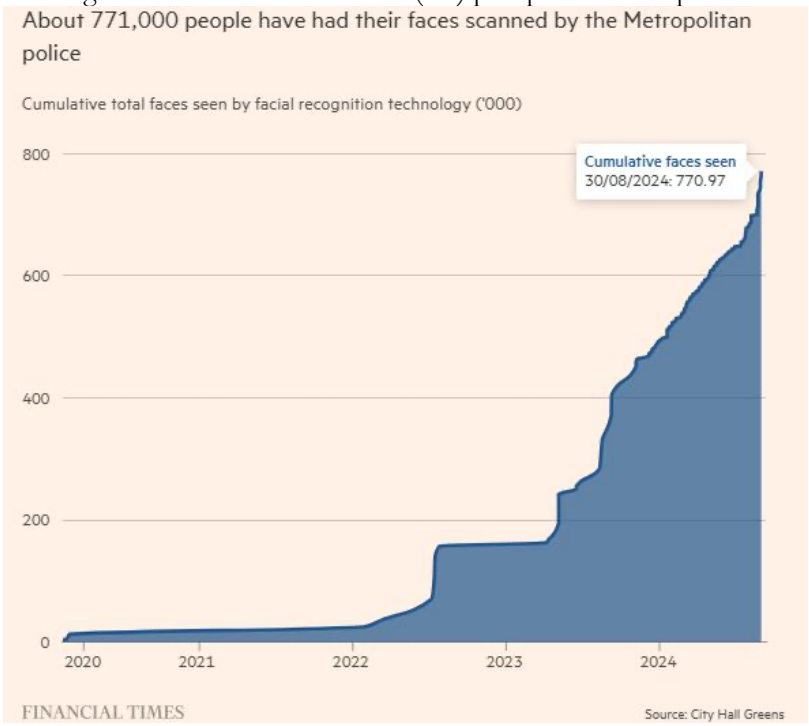
This article aims to analyze the regulatory gaps surrounding the use of facial recognition in Brazilian public security, discussing its ethical, legal, and operational impacts. Based on a systematic literature review and a documentary analysis of national and international regulations, the study compares different models of technological governance—with a focus on the European, North American, and Chinese contexts—and proposes guidelines for the construction of a national legal framework capable of balancing innovation, operational efficiency, and legal and ethical safeguards.

The relevance of this investigation lies in the urgency of establishing clear and effective regulatory parameters for the use of sensitive technologies such as FR, especially in a country marked by historical inequalities and fragile institutions. The absence of consistent guidelines undermines not only legal certainty and the efficiency of police action but also public trust in the adoption of technological solutions in the public sector. Thus, this work seeks to support the legislative debate and contribute to the formulation of a regulatory policy that ensures the responsible, proportional, and transparent use of facial recognition in Brazilian public security.

2. ETHICAL AND SOCIAL CHALLENGES AND THE REGULATORY VOID IN BRAZIL: RISKS OF THE LACK OF REGULATION IN THE USE OF FACIAL RECOGNITION TECHNOLOGIES

In public security, technology stands out for its potential to assist in the identification of suspects and the location of missing people, being used in police operations and urban monitoring systems. The *Financial Times* (2024) reported that the London Metropolitan Police carried out more than 117 operations using FR in just the first half of 2024 — three times more than in the previous four years — evidencing the rapid growth in the adoption of this tool in crime-fighting efforts (Figure 1). In addition, the technology has been applied to prevent fraud and increase security in financial transactions, as demonstrated by banking institutions that use facial biometrics for user authentication and transaction validation.

Figura 1 – Evolução do total acumulado de rostos escaneados pela tecnologia de reconhecimento facial (RF) pela polícia metropolitana



Fonte: Financial Times (2024).

Although FR offers significant benefits, its implementation faces technical and ethical challenges that must be considered. The accuracy of algorithms may be compromised by variations in image quality and by the functioning of machine learning models themselves. According to Sanchez-Moreno et al. (2021), FR systems are efficient in identifying and capturing suspects in surveillance scenarios but require rigorous calibration testing to minimize identification errors and algorithmic bias — that is, the system's tendency to show disproportionately higher error rates for certain demographic groups, such as women and Black people (Buolamwini & Gebru, 2018).

The use of FR technologies raises ethical questions, especially concerning privacy and the risk of mass surveillance. The adoption of the tool without clear guidelines can result in a constant monitoring environment, where the population loses autonomy over its own digital identity. Lyon (2018) warns that the normalization of surveillance systems negatively impacts individual freedoms, as citizens may be tracked without explicit consent. There are also concerns about the transparency and use of the databases feeding these systems, since the public often remains unaware of the criteria used for image collection and processing. Another relevant ethical issue involves algorithmic bias and the possibility of racial discrimination. Studies such as those by Buolamwini & Gebru (2018) show that FR systems have higher error rates when identifying individuals from specific racial groups, which may perpetuate structural inequalities. In Brazil, a survey conducted by the *Rede de Observatórios da Segurança* (2019) revealed that 90% of arrests made through facial monitoring between March and October 2019 involved Black people, underscoring the need for technical audits to ensure the technology is applied fairly and equitably.

The application of FR technologies in Brazilian public security occurs in a context of legal uncertainty due to the absence of a specific regulatory framework. Although the General Data Protection Law (LGPD – Law No. 13.709/2018) establishes guidelines for the processing of personal data, its applicability to the use of this technology in public security remains ambiguous. According to Melo & Serra (2023), the lack of clear regulation creates significant operational risks and ethical challenges, allowing for diverse interpretations regarding the legality of the tool and opening space for discriminatory practices. Buiten (2019) and Barroso (2024) also emphasize that the regulatory gap undermines the predictability of State actions and raises concerns about potential abuses and violations of fundamental rights.

The regulation of FR in Brazil faces the challenge of legislative fragmentation. Without a uniform national framework, states and municipalities have adopted their own regulations, often without standardized criteria for transparency, auditing, and independent oversight. The European Union's Artificial Intelligence Act (AI Act, 2024) demonstrates the importance of a structured set of regulations to ensure the safer and fairer use of such tools, highlighting the need for a similar model in Brazil. According to Veale & Borgesius (2021), this disparity undermines legal certainty for public agents and makes it difficult to define minimum guidelines that guarantee responsible use of the technology. In addition, Brundage et al. (2020) stress that the absence of regulatory requirements for continuous audits compromises the reliability of the systems, making them susceptible to failures and biases. A study by the *Observatório da Segurança* (2019) shows that the lack of regulatory standards can lead to systematic errors in the application of the technology, particularly harming historically marginalized groups, which reinforces the need for effective measures to prevent discrimination.

Given this scenario, the creation of a federal regulatory framework emerges as an urgent necessity. Buiten (2019) highlights that a robust regulatory model must ensure transparency, fairness, and predictability in the application of FR technology. International experiences, such as those established by the European Union's AI Act, demonstrate that the implementation of clear rules reduces the risks associated with the indiscriminate use of technology and improves its reliability. However, until such

regulation is implemented in Brazil, technologies will continue to be applied without effective control. Brundage et al. (2020) warn that, without proper audits and oversight, citizens will remain vulnerable to potential abuses and errors, which may compromise the legitimacy and effectiveness of this technology in the country.

2.1 Legislation and Guidelines

The development of a national regulatory framework for the use of facial recognition (FR) technologies in public security must begin with the premise that technological innovation needs to be aligned with the constitutional principles of legality, proportionality, transparency, and the protection of fundamental rights. To this end, it is recommended that the regulation be structured around three central pillars: (i) transparency and accountability, through requirements for impact reports, publication of usage protocols, and social control mechanisms; (ii) independent oversight, with the creation or designation of a competent authority to supervise the use of the technology, conduct regular audits, and investigate complaints of abuse; and (iii) institutional accountability, with administrative and civil sanctions in cases of misuse, algorithmic discrimination, or violation of rights (Buiten, 2019).

In addition, it is essential that regulation establish minimum technical criteria for the adoption of FR systems, including accuracy standards, mitigation of algorithmic bias, and interoperability requirements for platforms used by different levels of government. International experience shows that effective regulatory models do not simply restrict or liberalize technology indiscriminately; instead, they propose intermediate paths that reconcile operational efficiency with ethical and legal safeguards. In this sense, a Brazilian regulatory model should be evidence-based, centered on the protection of human dignity, and adaptable to the pace of technological evolution.

2.1.1 The Brazilian Regulatory Landscape

Brazil still does not have a specific federal law regulating the use of facial recognition (FR) in public security. Although the General Data Protection Law (LGPD – Law No. 13.709/2018) establishes guidelines for the processing of personal data, its application to the use of artificial intelligence in this sector remains undefined. According to Azevedo et al. (2022), this gap prevents public agents from having clear parameters to operate the technology, which may result in both legal uncertainty and inconsistent application of facial capture and monitoring tools. The lack of regulation not only undermines legal predictability but also generates direct operational challenges for public security professionals, who must cope with uncertainty regarding the legality of their actions.

The absence of a uniform national regulation allows each state or municipality to define its own criteria for the use of technology, without necessarily following minimum standards of transparency or governance. As a result, the same system may be applied differently in different locations, creating distortions and uncertainty for technology operators.

In addition to the lack of standardization, the absence of mandatory technical audits and independent oversight increases the risk of improper monitoring and selective enforcement, as Cavoukian and Jonas (2012) warn. Without effective inspection mechanisms, there is no guarantee that the systems in use are being regularly reviewed to avoid biases or operational failures. This issue is particularly concerning in a context where, according to the National Council of Justice (2024), there are no national guidelines requiring recurring audits or impact reports for these systems, which may compromise their reliability and heighten the risk of misuse.

In this context, Freitas (2024) observes that the absence of regulation has not prevented the expansion of monitoring in cities such as São Paulo, where implementation occurs without formal guarantees of governance. This situation reinforces the need for a federal regulatory framework capable of ensuring not only transparent and predictable use but also mechanisms that safeguard fundamental rights. As Cavoukian (2009) highlights, any AI system applied to public policies must incorporate governance principles from its design, ensuring that privacy protection and civil rights are treated as priorities rather than secondary concerns.

Legal uncertainty directly affects public security professionals, who may be held accountable for potential privacy violations without having clear parameters for operating the technology. The lack of standardization in the implementation of FR systems exacerbates inequalities between states and municipalities, allowing each locality to establish its own criteria, often without minimum guarantees of governance and transparency.

2.1.2 International Experiences and Lessons for Brazil

International experience shows that countries that have established specific regulatory frameworks for FR enjoy greater control over its use and mitigate risks related to privacy and discrimination. The distinction between the regulatory models of the United States and the European Union (EU) in AI is widely discussed in the academic literature. Buiten (2019) and Veale & Zuiderveen Borgesius (2021) point out that the U.S. adopts a minimal regulation approach, encouraging innovation and allowing the market to self-regulate, while the EU opts for a more prescriptive approach, based on risk assessment and the protection of fundamental rights.

The European Union, through the *Artificial Intelligence Act* (AI Act, 2024), classified FR as a high-risk technology, imposing strict restrictions on its implementation, requiring transparency, frequent audits, and impact assessments before its use. Complementarily, the *General Data Protection Regulation* (GDPR, 2018) establishes rigorous requirements for consent and the protection of personal data, ensuring that applications of this technology respect fundamental principles of privacy and fairness. According to Floridi et al. (2018), the European model is based on the idea that AI must comply with pre-existing ethical and legal principles, ensuring transparency, accountability, and human oversight.

On the other hand, *Executive Order 13859*, enacted in the U.S., is a milestone in the federal government's AI strategy. It establishes guidelines for AI development without imposing significant

regulatory barriers (U.S. Government, 2019). According to Bryson (2019), this vision is sustained by the argument that excessive regulation could inhibit technological progress and undermine U.S. competitiveness in the global arena.

In the U.S., AI regulation is strongly tied to national security and the maintenance of global leadership in the sector. As Allen & Chan (2019) note, the U.S. strategy seeks to prevent geopolitical adversaries, such as China, from dominating AI development, which justifies the emphasis on intellectual property protection and cybersecurity. In contrast, the EU is more concerned with the social and ethical impacts of AI. Studies such as those by Wachter, Mittelstadt & Floridi (2017) emphasize the need for regulatory oversight to prevent algorithmic discrimination and privacy violations. For Veale (2021), the European approach is grounded in risk-based regulation, which seeks to balance innovation with the protection of fundamental rights.

China, in turn, adopts a vertical AI regulatory approach, with specific laws for issues such as facial recognition and surveillance, integrated into a state control system aimed at public security and social stability (Taeihagh, 2021). Key features include the public registration of AI systems, mandatory ethical assessments, and rigorous oversight, often associated with mass surveillance technologies such as the *Social Credit System*. Unlike the EU, which prioritizes fundamental rights, and the U.S., which emphasizes innovation, the Chinese model raises ethical concerns about privacy and individual freedoms but demonstrates the effectiveness of specific regulations in mitigating technical and operational risks.

The choice between a more flexible, innovation-oriented model (like that of the U.S.), a more regulated and legally secure model (like that of the EU), or a state-controlled model (like that of China) has direct implications for Brazil. According to Carini (2020), Brazil should adopt a hybrid model, considering the need to foster innovation without neglecting ethical and legal aspects, while learning from international experiences to establish specific regulations that balance technological efficiency and the protection of fundamental rights.

2.1.3 Legislative Initiatives in Brazil

The regulation of AI in Brazil has been the subject of debate across different fronts and spheres, but it still lacks detailed norms for high-impact applications such as FR in public security. The country has a set of laws and policies aimed at fostering digital innovation, but none provide specific guidelines for the application of these technologies in police operations and public surveillance.

Among the main existing regulations, the Innovation Law (*Law No. 10.973/2004*) stands out, as it encourages scientific and technological research but does not address ethical and operational issues of AI use in public security. Similarly, the Marco Civil da Internet (*Law No. 12.965/2014*) establishes general principles for data protection and privacy.

The Brazilian Strategy for Digital Transformation (E-Digital), instituted in 2018, also sought to promote the advancement of digital technologies, including AI, but did not provide a specific regulatory

framework for its application in public security. The Brazilian Artificial Intelligence Strategy (EBIA), launched later, represented a step forward by acknowledging the need for regulation but still failed to establish clear guidelines for facial recognition, demonstrating that Brazil remains behind in structuring regulations that ensure governance and transparency in the application of this technology.

Among the more recent initiatives, the most noteworthy is Bill No. 1515/2022, which proposes the creation of a General Law on the Protection of Personal Data for purposes of public security, national defense, and criminal prosecution. The bill seeks to fill the gaps left by the LGPD, establishing specific parameters for the use of biometric data and automated decision-making in the public sector. However, there are still critical points to be improved, especially regarding the requirement of judicial authorization for the processing of sensitive data and the prohibition of fully automated decisions, which may compromise the efficiency of technology in security operations.

2.1.4 Bill No. 1515/2022: Limitations on the Actions of Security Forces and Impacts on Innovation

According to the analysis by the Laboratory of Public Policy and Internet (LAPIN), Bill No. 1515/2022 emerges as an attempt to fill the gap left by the LGPD, proposing specific guidelines for the processing of personal data in the context of public security, national defense, and criminal prosecution. However, although it represents progress in regulating these technologies, the bill presents critical points that may limit both the performance of security forces and technological innovation in the sector.

The same LAPIN Technical Note highlights one of the most debated aspects: the requirement of judicial authorization for the processing of sensitive data, including facial biometrics. While this measure seeks to ensure greater control and privacy protection, its strict application may compromise the efficiency of public security operations, especially in emergency situations that demand rapid responses. The time required to obtain judicial authorizations may become an operational obstacle, reducing the effectiveness of investigations and police actions based on technology.

In addition, the bill prohibits exclusively automated decisions, requiring that any analysis performed by artificial intelligence undergo human validation. This restriction directly impacts the use of real-time facial recognition systems, as it prevents the technology from operating autonomously to identify suspects or criminal patterns in large volumes of data. Although human oversight is essential to avoid algorithmic bias and ensure greater reliability, the absolute requirement of human intervention may overburden security forces and reduce agility in operations.

Another point that deserves attention is the rigidity in the rules for data sharing between public bodies and private entities. The bill establishes that any transfer of information between different institutions requires detailed justification and, in some cases, judicial authorization. This bureaucratization may hinder cooperation among different security forces, limiting the integration of databases and interoperability between intelligence systems. Consequently, the lack of an efficient flow of information may compromise criminal investigations and joint actions that depend on the exchange of data among institutions.

The proposed regulation also establishes limits for the storage of biometric data, requiring their deletion after fulfilling the purpose for which they were collected. Castro and Paula (2021) point out that this requirement may be problematic in long-term investigations, where the preservation of historical records is essential for the analysis of criminal patterns and the identification of repeat offenders. The absence of a clause allowing extended data storage for strategic security purposes may undermine the continuity and effectiveness of investigations, as well as hinder the creation of integrated national databases.

Another relevant aspect of the bill is the requirement of data protection impact reports for any operation involving the use of sensitive technologies, such as facial biometric monitoring. While this measure aims to ensure greater transparency and control over the use of technology, its indiscriminate application may generate excessive bureaucracy, hindering the adoption and implementation of new technological solutions. The absence of clear criteria regarding when and how these reports should be required may increase the administrative burden of security forces, without necessarily improving the protection of fundamental rights.

3. METHODOLOGY

This study adopts a qualitative and exploratory approach, based on documentary analysis and a systematic literature review, following the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) protocols. The choice of this methodology is justified by the need to understand the regulatory gaps and ethical challenges of facial recognition in Brazilian public security, establishing connections between national and international regulations and the academic production on the subject.

The qualitative approach makes it possible to explore normative, legal, and social aspects of the use of technology, while documentary analysis allows for a critical evaluation of applicable regulatory guidelines and norms. The systematic review was used to ensure the breadth and scientific rigor of the research, identifying patterns and trends in existing studies.

3.1 Process of Building the Theoretical Framework and Source Selection

The bibliographic survey was conducted in the CAPES Journal Portal[1], using descriptors selected as shown in Table 1. Strict inclusion and exclusion criteria were applied, considering peer-reviewed articles and documents published in Portuguese and English to ensure the academic quality of the analyzed material.

[1] The Portal de Periódicos da CAPES (Capes Journal Portal) is a Brazilian government-funded digital library maintained by the Coordination for the Improvement of Higher Education Personnel (CAPES), an agency of the Ministry of Education (MEC).
It provides access to a vast collection of scientific journals, e-books, dissertations, and databases covering all fields of knowledge. Available at: https://www.periodicos.capes.gov.br. Accessed: Sept. 22, 2025.

The initial search returned 15,431 results, which were refined using relevance filters, language (Portuguese and English), and peer review, resulting in 5,458 valid documents, as shown in Table 1.

Table 1 – Research Results in the CAPES Journal Portal
(with filters applied: Portuguese or English language and peer review)

ID	Descriptors / Keyword Combinations	Raw Results	Results after Filters
A	Artificial intelligence	7,080	—
B	Facial recognition	308	188
C	Artificial intelligence and facial recognition	8	3
D	Facial recognition and public security	5	5
E	Facial recognition and public policy	5	5
F	Artificial intelligence and facial recognition and public safety	27	16
G	Facial recognition and public safety	166	101
H	Facial recognition and public policy	184	144
I	Artificial intelligence and facial recognition	7,648	4,996
	Overall Total	**15,431**	**5,458**

Source: Prepared by the author based on data extracted from the CAPES Journal Portal (2024).

Rows A and I of Table 1 were excluded, as they dealt with general aspects of artificial intelligence, without a direct connection to the specific application of FR in public security. After this stage, 462 articles were exported in RIS format and imported into Mendeley Desktop software, where duplicates were removed. This process resulted in 200 unique articles, which were analyzed by title and abstract, culminating in the final selection of 158 documents for detailed analysis.

In addition to academic research, the methodology included technical, regulatory, and governmental documents of national and international relevance, broadening the scope of investigation. Among those analyzed were: Decree No. 63.552/2024 (Smart Sampa), which regulates the use of monitoring cameras in São Paulo, establishing guidelines for the ethical and transparent implementation of this technology; the General Data Protection Law (LGPD – Law No. 13.709/2018), which serves as a reference for the processing of personal data in Brazil, although it explicitly excludes public security issues; and the European Union's Artificial Intelligence Act guidelines. Documentary analysis made it possible to construct a comparative framework between the regulations in force in Brazil and international guidelines, enabling a critical assessment of the regulatory and ethical challenges of using the technology in public security.

3.2 Application of the PRISMA Protocol

To ensure transparency and rigor in the document selection process, the stages of the PRISMA protocol (Preferred Reporting Items for Systematic Reviews and Meta-Analyses), widely used in systematic reviews and meta-analyses, were followed. PRISMA provides a structured and replicable method, ensuring the careful selection of academic and documentary sources. Table 2 describes the protocol stages applied in the study, showing the refinement process of the analyzed literature.

Table 2 – Document Selection Process by the PRISMA Protocol

PRISMA Stage	Description	Number of Documents
1. Identification	Initial search in databases using descriptors and keywords.	15,431
2. Screening	Removal of duplicates and irrelevant documents based on title and abstract.	5,458
3. Eligibility	Application of inclusion and exclusion criteria (language, peer review, thematic relevance).	—
4. Inclusion	Documents selected for detailed analysis.	462
5. Duplicate Removal	Removal of duplicate documents after screening.	200
6. Title Analysis	Exclusion of documents with titles outside the scope.	158
7. Abstract Analysis	Abstract analysis to verify adherence to the topic.	—
8. Final Documents	Documents selected for the final analysis.	158

Source: Prepared by the author based on the stages of the PRISMA protocol (2024).

This methodological process ensured the adequacy and relevance of the analyzed materials, allowing for an in-depth and well-founded investigation of the regulations and regulatory challenges of FR in public security.

3.3 Selection and Criteria of Analyzed Documents

The selection of documents followed an intentional sampling model, as described by Patton (2015), prioritizing sources directly related to the central theme of the study. The model was adopted to ensure the inclusion of materials with analytical depth, avoiding statistical generalizations irrelevant to the regulatory and legal context.

Selection criteria adopted: thematic relevance; source reliability; timeliness; and data triangulation.

3.4 Data Analysis

Data analysis was conducted in two complementary stages, combining Systematic Literature Review and Documentary Analysis, as detailed below.

First stage: Systematic Literature Review following PRISMA guidelines, prioritizing studies addressing:

i) Regulation of facial recognition in different contexts.

ii) Ethical and social impacts of technology.

iii) International experiences in regulatory governance.

This first stage enabled a comprehensive mapping of the academic and regulatory debate, providing input for comparative analysis between Brazil and other countries.

Second stage: Documentary Analysis, in which legal and regulatory documents were interpreted using the categorical content analysis technique, as per Bardin (2011). Three main axes were identified for categorizing the information:

i) Compatibility between facial recognition and LGPD: Analysis of legal provisions regulating the use of biometric data in Brazil and their implications for public security.

ii) Regulatory gaps in Brazil: Assessment of how the absence of specific norms impacts the adoption of the technology by security forces.

iii) International regulatory models: Comparison with the legislation of countries such as the United States and the European Union, identifying points of convergence and divergence.

The triangulation of data provided a critical and in-depth view of the regulation of the technology, highlighting challenges and opportunities for digital governance in Brazil.

3.5 Methodological Limitations

Despite the methodological rigor adopted, the research presents some limitations that need to be considered:

i. Dependence on public and academic sources: The absence of internal data from security forces limits the practical analysis of the technology's use.

ii. Rapid technological evolution: The field of facial recognition is in constant transformation, requiring continuous updates of the regulatory analysis.

iii. Normative variety in Brazil: Disparities among federal, state, and municipal norms make it difficult to create a unified regulatory framework.

Even with these limitations, the adopted methodology ensures transparency and scientific robustness. The application of the PRISMA protocol, combined with the use of strict selection and analysis criteria, strengthens the quality and reliability of the study's conclusions.

4. RESULTS AND FINAL DISCUSSIONS

Brazil still lacks a consolidated regulatory framework, which generates legal uncertainty for technology operators and practical limitations for its application in crime fighting. The absence of unified federal regulation fosters a fragmented scenario, allowing each state and municipality to establish its own rules, without guaranteeing a minimum level of operational security for law enforcement. In addition, the international comparison showed that the United States adopts a more pragmatic approach, allowing regulatory flexibility and ensuring that public security can use the technology without

excessive barriers. While the European Union classifies facial recognition as a high-risk technology and imposes strict restrictions, the U.S. has no single federal legislation, allowing states and municipalities to develop rules adapted to their reality. The U.S. model prioritizes public security and innovation, avoiding excessive requirements that could compromise the agility of police operations.

To illustrate the differences between national and international regulatory approaches in the use of FR technologies, Table 1 presents a comparison of the main regulatory aspects of Brazil, the European Union, and the United States. The analysis considers criteria such as the existence of a specific legal basis, the classification of the technology's risk level, the degree of regulatory detail, and the existence of partial or total bans. While Brazil still operates without a consolidated federal regulation, relying partially on the LGPD, the European Union advances with the AI Act, which imposes strict rules and recognizes FR as a high-risk technology. The United States, on the other hand, adopts a decentralized model, allowing states and municipalities to establish their own rules, with varying degrees of restriction and technical detail.

The comparison shown in Table 3 reveals a scenario of regulatory disparity that directly impacts the legal predictability and effectiveness of the use of facial recognition in public security. The European model, with a strong emphasis on fundamental rights protection and mandatory auditing, tends to prioritize ethics and legal certainty, although it may impose bureaucratic barriers to innovation. In contrast, the U.S. approach privileges regulatory flexibility and local autonomy, which favors innovation but may compromise standardization and rights protection. The Brazilian case presents a critical gap: the absence of a specific federal regulatory framework makes the scenario fragmented and unstable, exposing citizens to the risk of abuse and public operators to legal uncertainty. Thus, it becomes evident that Brazil needs to develop its own regulatory model that balances the pillars of technological innovation, operational efficiency, and constitutional safeguards.

Table 3 – Comparison of Facial Recognition Regulations

Criterion	Brazil (LGPD and state regulations)	European Union (AI Act)	United States (State regulations)
Legal basis	LGPD (no coverage for public security)	AI Act	State/local regulations
Associated risk	Undefined	High-risk technology	Variable by state
Specific regulation	Absent at federal level	Detailed regulatory framework	Depends on state legislation
Partial ban?	No	Yes, in certain contexts	Yes, in some states

Source: Prepared by the author based on LGPD (Brazil), AI Act (European Union), Executive Order 13859 (U.S.), and specialized literature (Melo & Serra, 2023; Veale & Borgesius, 2021; Allen & Chan, 2017).

In the U.S., regulation allows the technology to be used without the need for prior judicial authorization in several contexts, provided that minimum transparency and accountability guidelines are observed. In Brazil, however, the current approach excessively prioritizes individual rights, without considering that crime does not follow rules. Implementing a more flexible model would allow a faster

and more effective response, ensuring public security without compromising technology governance (Allen & Chan, 2017; Bryson, 2019).

4.1 Guidelines for a More Agile and Effective Regulatory Model

For facial recognition to be used efficiently and legally in Brazilian public security, it is essential to adopt a national regulatory framework that guarantees operational autonomy to security forces, reduces bureaucratic barriers, and strengthens the legal security of public agents. The current absence of unified legislation has resulted in divergent interpretations among states and municipalities, creating a regulatory environment of uncertainty that compromises the predictability and reliability of the technology in crime fighting (Melo & Serra, 2023). This regulatory fragmentation, in addition to weakening accountability mechanisms, makes it difficult to standardize technical and operational criteria for the use of the tool.

International experience demonstrates that more flexible, innovation-oriented regulatory models, such as the U.S. model, provide greater agility to public security operations without necessarily compromising technology governance. In the United States, the use of facial recognition by police bodies generally does not require prior judicial authorization, provided that basic principles of transparency, accountability, and compliance with state and local legislation are observed (Allen & Chan, 2017). In contrast, the European model—particularly the Artificial Intelligence Act—classifies facial recognition as a high-risk technology, requiring complex layers of auditing, impact assessment, and mandatory external oversight (Veale & Borgesius, 2021). Although intended to protect fundamental rights, this approach can, in practice, create barriers to immediate response in investigative contexts and in cases of flagrante delicto.

Given this, Brazil should consider relaxing certain bureaucratic requirements, such as waiving prior judicial authorization in real-time operations and granting immediate access to national identification databases. Smooth integration between public and private databases is essential to enable a dynamic and effective flow of information, allowing technology to act as a strategic differentiator in combating organized crime. This pragmatic view of technology governance does not imply the absence of control, but rather the adoption of proportional risk-based mechanisms, applying targeted audits only in cases of suspected abusive or improper use (Buiten, 2019).

In addition, it is necessary to review overly restrictive policies regarding the retention period of biometric data. While some European countries impose near-immediate deletion of such information, the Brazilian context—marked by high recidivism and violent crime—requires a more flexible approach. The creation of a national database focused on serious crimes and criminal organizations, with broader retention periods, could significantly enhance the State's ability to identify criminal patterns and anticipate risks.

Finally, Brazilian regulation should seek a balance between collective security and individual freedom, recognizing that the right to privacy, although fundamental, cannot be interpreted in an

absolute and isolated manner. Protecting society against real threats requires effective and technologically updated tools. Thus, a regulatory framework inspired by international best practices — such as the U.S. model, which combines operational autonomy and institutional accountability — can ensure that facial recognition is employed ethically, proportionally, and strategically, contributing to the strengthening of public security in the country (Bryson, 2019).

4.2. Reflection on Digital Governance and Public Security

Facial recognition should not be regarded as a threat to fundamental rights, but as a strategic tool for strengthening public security and the State's role in combating crime. When framed within a balanced and technically sound regulatory framework, the technology can operate in a proportional and transparent manner, contributing to the identification of suspects, crime prevention, and greater investigative effectiveness (Melo & Serra, 2023). In this sense, adopting an excessively restrictive stance — such as that of the European Union, which, through the Artificial Intelligence Act, classifies facial recognition as a high-risk technology and imposes strict regulatory layers of use, oversight, and auditing (Veale & Borgesius, 2021) — may render the practical application of the tool unfeasible in emergency contexts, indirectly benefiting organized criminal groups that take advantage of the State's operational gaps.

Unlike the European model, the United States has adopted a regulatory approach guided by the principle of "innovation with responsibility," in which the autonomy of public security agencies is preserved if minimum parameters of transparency and accountability are observed (Allen & Chan, 2017). This normative philosophy understands that technological effectiveness should not be undermined by excessive legal barriers, provided there is sufficient institutional oversight to prevent abuse. The U.S. model has demonstrated that it is possible to balance operational freedom and ethical governance without turning facial recognition into a bureaucratic or politically unfeasible instrument (Bryson, 2019).

In this context, Brazil should consider adopting a similar regulatory approach, one that recognizes the strategic potential of the technology and uses it as an ally in promoting public security. Regulation does not mean indiscriminate restriction, but rather the legal structuring of the technology's use based on criteria of proportionality, efficiency, and accountability. By integrating facial recognition into a public security policy guided by innovation, the country may reduce the impacts of crime without compromising fundamental rights — thus ensuring that the technology fulfills its role of collective protection and does not become hostage to regulatory excess.

5. CONCLUSIONS

The debate on the use of facial recognition in public security in Brazil is marked by a tension between the protection of fundamental rights and the need for technological innovation to strengthen

the State's response to crime. The absence of a consolidated and unified regulatory framework generates legal uncertainty, limits the effective use of the technology, and creates an environment of fragmentation, with states and municipalities adopting heterogeneous and often conflicting rules.

The international comparison carried out in this study reveals three different regulatory approaches: the European model, which treats facial recognition as a high-risk technology and subjects it to rigid restrictions; the U.S. model, which privileges operational autonomy and institutional accountability; and the Brazilian scenario, characterized by legal gaps and regulatory dispersion. Each of these models reflects distinct political and cultural conceptions regarding the balance between collective security and individual rights.

Brazil's challenge, therefore, is to construct a regulatory model that reconciles these dimensions, ensuring both the protection of constitutional guarantees and the operational effectiveness of public security agencies. For this, it is essential to establish clear and proportional rules, avoiding both the risks of indiscriminate use and the barriers created by excessive restrictions.

Facial recognition should not be interpreted as a threat, but as a technological tool whose ethical and efficient application depends on a coherent framework of governance. By adopting a regulatory perspective based on proportionality, transparency, and accountability, Brazil can take advantage of the potential of this technology in the fight against crime while preserving the fundamental rights of its citizens.

The reflection presented here points to the urgent need to overcome the current legal vacuum and move toward the construction of a national regulatory framework. This framework should not merely replicate foreign models but rather adapt international best practices to the Brazilian reality, considering the country's social, legal, and institutional specificities. Only in this way will it be possible to transform facial recognition into an instrument of security and digital governance, aligned with democratic principles and the demands of contemporary society.

REFERENCES

AI ACT. **Artificial Intelligence Act.** Regulamento da União Europeia (UE), v. 1689, 2024.

ALLEN, G.; CHAN, T. **Artificial intelligence and national security**. v. 132. Cambridge, MA: Belfer Center for Science and International Affairs, 2017. Disponível em: https://csdsafrica.org/wp-content/uploads/2020/06/AI-NatSec-final.pdf. Acesso em: 19 out. 2024.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **Inteligência artificial: conceitos e terminologia**. NBR ISO 22989. Rio de Janeiro: ABNT, 2023.

AZEVEDO, C. P. G. de; LIMA, E. M. B. de; SILVA, F. R. da; et al. **Nota técnica:** análise comparativa entre o anteprojeto de LGPD penal e o PL 1515/2022. Instituto de Referência em Internet e Sociedade (IRIS) e Laboratório de Políticas Públicas e Internet (LAPIN), nov. 2022. Disponível em: https://lapin.org.br. Acesso em: 18 out. 2024.

BAUER, M. W.; GASKELL, G. **Pesquisa qualitativa com texto, imagem e som:** um manual prático. Petrópolis: Vozes Limitada, 2017.

BARROSO, L. R. **Inteligência artificial, plataformas digitais e democracia**: Direito e tecnologia no mundo atual. Belo Horizonte: Fórum, 2024.

BINNS, R. Fairness in machine learning: Lessons from political philosophy. In: **Conference on fairness, accountability and transparency, 2018**, New York. Proceedings [...]. New York: PMLR, 2018. p. 149-159.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Marco Civil da Internet. Brasília, DF, 2014.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 2018.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 4.612/2019**. Disponível em: https://www.camara.leg.br. Acesso em: 10 nov. 2025.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 1515/2022**. Disponível em: https://www.camara.leg.br. Acesso em: dez. 2024.

BRUNDAGE, M.; AVIN, S.; WANG, J.; BELFIELD, H.; KRUEGER, G.; HADFIELD, G.; ANDERLJUNG, M. Toward trustworthy AI development: mechanisms for supporting verifiable claims. **arXiv preprint,** arXiv:2004.07213, 2020. Disponível em: https://arxiv.org/abs/2004.07213. Acesso em: 12 dez. 2024.

BUITEN, M. C. Towards intelligent regulation of artificial intelligence. **European Journal of Risk Regulation**, v. 10, n. 1, p. 41-59, 2019. Disponível em: https://www.cambridge.org/core/services/aop-cambridge-core/content/view/AF1AD1940B70DB88D2B24202EE933F1B/S1867299X19000084a.pdf/towards_intelligent_regulation_of_artificial_intelligence.pdf. Acesso em: 15 fev. 2025.

BUOLAMWINI, J.; GEBRU, T. Gender shades: Intersectional accuracy disparities in commercial gender classification. In: **conference on fairness, accountability and transparency, 2018**, New York. Proceedings [...]. New York: PMLR, 2018. p. 77-91.

BRYSON, J. J. The ethics of artificial intelligence. In: DUBBER, M. D.; PASQUALE, F.; DAS, S. (ed.). **The Oxford Handbook of Ethics of AI**. Oxford: Oxford University Press, 2019.

CAVOUKIAN, A. **Privacy by design:** the 7 foundational principles. Ontario: Information and Privacy Commissioner of Ontario, 2009.

CÓBE, R. M.; NONATO, L. G.; NOVAES, S. F.; ZIEBARTH, J. A. Rumo a uma política de Estado para inteligência artificial. **Revista USP**, n. 124, p. 37-48, 2020. DOI: https://doi.org/10.11606/issn.2316-9036.v0i124p37-48.

CRESWELL, J. W.; CRESWELL, J. D. **Projeto de pesquisa**: métodos qualitativo, quantitativo e misto. Porto Alegre: Penso, 2014.

CRESWELL, J. W.; CLARK, V. L. P. **Designing and conducting mixed methods research**. Los Angeles: Sage, 2017.

ESTADOS UNIDOS. Executive Order 13859: **Maintaining American Leadership in Artificial Intelligence**. 2019. Disponível em: https://www.presidency.ucsb.edu/documents/executive-order-13859-maintaining-american-leadership-artificial-intelligence. Acesso em: 15 fev. 2025.

FINANCIAL TIMES. Met police use of facial recognition in London surges. **Financial Times**, 19 out. 2024. Disponível em: https://www.ft.com/content/c33322a7-eba7-4299-8172-4ce1d4e88908.

FLORIDI, L. Information ethics, its nature and scope. **ACM SIGCAS Computers and Society**, v. 36, n. 3, p. 21-36, 2006. DOI: https://doi.org/10.1145/1167344.1167352.

FLORIDI, L. **The ethics of information**. Oxford: Oxford University Press, 2013.

FLORIDI, L. **The Fourth Revolution**: How the infosphere is reshaping human reality. Oxford: Oxford University Press, 2014.

FLORIDI, L. et al. AI4 People — an ethical framework for a good AI society: opportunities, risks, principles, and recommendations. **Minds and Machines**, v. 28, p. 689-707, 2018. Disponível em: https://link.springer.com/content/pdf/10.1007/s11023-018-9482-5.pdf. Acesso em: 15 fev. 2025.

FREITAS, H. Câmeras de reconhecimento facial se multiplicam em São Paulo: medida é aposta do governo estadual e da prefeitura para a área da segurança pública. **Veja São Paulo**, São Paulo, 27 maio 2024. Disponível em: https://vejasp.abril.com.br/cidades/cameras-reconhecimento-facial-sp/. Acesso em: 2 fev. 2025.