

# Evolution of Emerging Technologies in Police Intelligence: an integrated analysis of academic publications and patents in AI and biometric recognition

*Evolução das Tecnologias Emergentes na Inteligência Policial: análise integrada de produções acadêmicas e patentes em IA e Biometric Recognition*

Andreia Rodrigues Ferreira Baro<sup>1</sup>, João Paulo Albuquerque Souza<sup>2</sup>

<sup>1</sup>Federal University of Sergipe, São Cristóvão, Sergipe, Brazil

<sup>2</sup>Focus College, Cascavel, Paraná, Brazil

## Abstract

This article maps the evolution, from 2000 to 2025, of emerging technologies in police intelligence through an integrated analysis of academic publications and patents identified on The Lens platform. The literature review and patent search reveal studies on AI in investigations, biometric recognition, and predictive analytics. Employing descriptive statistics and systematic comparison, the work highlights the predominance of Anglophone centers, its interdisciplinary nature (Computer Science, Sociology, Law), and the gap between conceptual debate and practical application. It concludes by emphasizing the need for empirical validations in real-world operations, algorithmic bias assessments, and longitudinal case studies to guide the development of robust and responsible technological solutions for public safety.

Keywords: Data Mining; Public Safety Technologies; Predictive Analytics.

## Resumo

Este artigo mapeia a evolução, entre 2000 e 2025, de tecnologias emergentes na inteligência policial por meio de análise integrada de publicações acadêmicas e patentes identificadas na plataforma The Lens. A revisão bibliográfica e a prospecção de patentes revelam estudos sobre IA em investigações, Biometric Recognition e em análise preditiva. Empregando estatística descritiva e comparação sistemática, o trabalho destaca a predominância de centros anglófonos, o caráter interdisciplinar (Ciência da Computação, Sociologia, Direito) e o hiato entre debate conceitual e aplicação prática. Conclui-se que há necessidade de validações empíricas em operações reais, de avaliação de vieses algorítmicos e de estudos de caso longitudinais para orientar o desenvolvimento de soluções tecnológicas robustas e responsáveis em segurança pública.

Palavras-chave: Mineração de Dados; Tecnologias de Segurança Pública; Análise Preditiva.

Technology Area: Technology Foresight on Specific Topics.



## 1 Introduction

The growing complexity of contemporary crime, driven by globalization, the digitalization of human interactions, and the increasing sophistication of criminal networks, poses ever greater challenges for public security agencies. In this context, there has been a significant expansion in the use of emerging technologies, particularly those based on Artificial Intelligence (AI), machine learning, and data analytics, as strategic tools for combating criminal activity.

Artificial Intelligence and machine learning have radically transformed police investigative practices and military operations by enabling the large-scale processing of data and the rapid detection of criminal patterns. Technologies such as facial recognition, predictive policing systems, and intelligent surveillance platforms have become part of the technological arsenal of security agencies in numerous countries, reflecting advances generated through both academic research and patent-protected innovation.

Within this context, intelligence activities have become an essential function of security organizations, providing analytical support and advisory capabilities across multiple decision-making levels and establishing themselves as a central component in policy formulation and operational planning (Paz, 2022). Technological advances have enabled not only the automation of data collection and processing on a massive scale but also the predictive identification of patterns and suspicious behaviors with greater speed and accuracy. However, these technologies require careful attention to data quality, algorithmic bias, and continuous human oversight to ensure ethical and reliable outcomes (Rejas de la Peña et al., 2025).

According to Galdon Clavell (2018), technology plays a central role in modern policing practices, particularly in the management of urban security through tools such as video surveillance, crime mapping, biometric systems, and predictive analytics. However, before such solutions can be used effectively, it is necessary to address challenges related to the organizational structures responsible for managing them, their technical capabilities and expectations, as well as the social and urban impacts resulting from their implementation. The author emphasizes that the intersection of technology, society, and security requires a careful assessment of the external factors, both positive and negative, that influence their adoption and effectiveness.

According to Nissan (2012), the application of technologies such as data mining and network analysis in police investigations enables the extraction of hidden patterns and the reconstruction of relationships among entities. Techniques such as link analysis, which focuses on direct connections, and social network analysis, which emphasizes network metrics, facilitate inferences about suspicious behavior based on fragmented evidence.

Ontological approaches support the formalization of illicit economic schemes, while auditing methodologies employ data mining techniques to prioritize investigative targets in the fiscal domain by balancing risk criteria and operational feasibility. Complementing these approaches, the scope of computer science technologies applied to criminal investigations ranges from geospatial visualizations in Geographic Information Systems (GIS) to clustering algorithms and network analysis techniques. The integration of expertise from forensic psychology, criminology, and statistics is essential to ensure robust and operationally validated investigative projects (Ewart; Zeleznikow, 2006).

Similarly, the use of techniques such as link analysis and social network visualization has proven effective in mapping connections among suspects and criminal events. Soares and Pacífico (2023) highlight the growing participation of transnational actors in contemporary insecurity dynamics. Within the field of International Relations, the anarchic nature of the international system, characterized by the absence of a supranational authority, leads states, driven by insecurity, to strengthen their defensive capabilities. The realist logic traditionally associated with interstate rivalries has expanded in the era of globalization and complex interdependence to encompass non-state threats, exposing structural vulnerabilities within contemporary security systems.

Complementing this perspective, Barbosa (2002) argues that the terrorist attacks of September 11, 2001, catalyzed significant investments in surveillance, defense, and intelligence technologies, particularly in the United States, producing direct effects on the technological infrastructure currently employed in military and public security operations.

Within this context of technological expansion directed toward security, Sachoulidou (2023) observes that the application of artificial intelligence to police intelligence activities has become increasingly established as a means of predicting and interpreting human behavior, thereby influencing decisions related to investigation, arrest, and judicial proceedings. The author emphasizes, however, that this trend toward automation creates a tension between improving operational efficiency and preserving fundamental rights, particularly with respect to the presumption of innocence and due process of law. In response to these challenges, she advocates the implementation of procedural safeguards capable of ensuring transparency and fairness in the adoption of these technologies, warning of the risks associated with the arbitrary expansion of the concept of suspicion and the erosion of traditional legal guarantees.

Against this backdrop, this article presents a comparative and integrated analysis of academic production and patent records related to emerging technologies applied

to police intelligence between 2000 and 2025. This temporal scope is justified by the geopolitical transformations and the military, defense, and security innovations that emerged following the events of 2001. The study identifies the principal institutional and corporate actors, collaboration patterns, and areas with the greatest innovation potential. By comparing the scientific literature with patented inventions, it highlights technological trends and existing gaps while providing insights to support future research and the development of innovative solutions for public security.

## 2 Methodology

This study adopts a mixed-methods approach, combining qualitative and quantitative perspectives to examine the evolution and challenges of emerging technologies applied to police intelligence, with particular emphasis on criminal investigations, biometric recognition, and predictive analytics. The qualitative dimension is reflected in the exploratory analysis of scientific publications and the interpretive examination of the findings, whereas the quantitative dimension derives from the use of descriptive statistics to identify patterns, frequencies, and trends within both academic publications and patent records. The research integrates two complementary methodological approaches: a bibliographic analysis of scientific literature and a technological prospecting study of patents.

For the technological prospecting stage, the The Lens platform (thelens.org) was employed. This internationally recognized platform offers extensive coverage of both scientific publications and patent records. As an open-access database, it enabled an integrated analysis of academic advances and innovations protected under intellectual property regimes within the field of public security.

The search strategy involved the formulation of bilingual queries in Portuguese and English, constructed from combinations of strategic descriptors to maximize thematic coverage while minimizing redundancies. The search configurations included: (i) terms related to police intelligence (“police intelligence” OR “inteligência policial”) combined with expressions associated with artificial intelligence (“artificial intelligence” OR AI OR “machine learning” OR “aprendizagem automática”) and investigation (“investigation” OR “investigação”); (ii) terms related to biometric recognition and computer vision (“facial recognition” OR biometrics OR biometria) linked to police intelligence; and (iii) specific combinations addressing predictive analysis in public security (“police intelligence” OR “inteligência policial” OR “law enforcement analytics”) AND (“crime forecasting” OR “data-driven policing” OR “predictive analytics”). This procedure ensured coverage of the principal technological domains relevant to the study.

The selection criteria included: (i) a temporal scope extending from January 2000 to May 2025, designed to capture both the initial wave of security-related innovations catalyzed by the September 11, 2001 attacks and the subsequent maturation of technologies such as deep learning and Big Data; (ii) publications in English and Portuguese; and (iii) two document types, namely scientific articles and patents related to information processing and information capture technologies. For patents, additional filters were applied based on jurisdiction (Brazil, the United States, Europe, and China) to identify inventions of both global and regional relevance.

Data analysis combined descriptive statistics with a systematic comparison between scientific literature and patent records. Descriptive statistics were used to map the temporal distribution of publications, geographic concentrations, and the principal institutional and corporate actors involved, including authors and assignees. The comparative analysis, in turn, enabled the identification of technological convergences, research gaps, and opportunities for the development of new patentable solutions in the field of public security.

### 2.1 Search Strategy

To ensure comprehensive thematic coverage while minimizing redundancies, three bilingual search queries (English/Portuguese) were developed and applied to the titles, abstracts, and keywords of the records:

- a) Query 1 – Artificial Intelligence and Police Investigation  
 (“police intelligence” OR “inteligência policial”) AND (“artificial intelligence” OR AI OR “machine learning” OR “aprendizagem automática”) AND (“investigation” OR “investigação”)
- b) Query 2 – Biometric Recognition  
 (“police intelligence” OR “inteligência policial”) AND (“facial recognition” OR biometrics OR biometria)
- c) Query 3 – Predictive Analytics in Public Security  
 (“police intelligence” OR “inteligência policial” OR “law enforcement analytics”) AND (“crime forecasting” OR “data-driven policing” OR “predictive analytics”)

It is important to note that the selection of descriptors prioritized contemporary terminology that is widely established in the recent scientific literature, such as *machine learning*, *artificial intelligence*, and *predictive analytics*. This methodological choice was intended to ensure conceptual consistency and alignment with the technological frontier of recent years. However, it is acknowledged that, prior to 2010, expressions such as

*data mining, expert systems, and knowledge-based systems* were more commonly used, as were broader and more indirect terms, including *law enforcement, public safety technologies, and pattern recognition*.

As a result, some historically relevant publications may not have been fully captured, representing an inherent limitation of the terminological scope adopted in this study. Nevertheless, this approach proved appropriate for the purpose of mapping recent trends and reflecting the current stage of development and maturation of emerging technologies applied to police intelligence.

### 3 Resultados e Discussão

- a) Query 1 – Artificial Intelligence and Police Investigation  
 (“*police intelligence*” OR “*inteligência policial*”) AND (“*artificial intelligence*” OR AI OR “*machine learning*” OR “*aprendizagem automática*”) AND (“*investigation*” OR “*investigação*”)

The application of Query 1 yielded 31 academic records. Among these, one publication was cited by four distinct patents, resulting in a total of four citations in patent documents. Within the scientific domain, 24 of these publications collectively received 485 citations from other academic works, highlighting their impact and visibility within the scholarly literature. Regarding document types, the dataset comprises one book, one book chapter, 28 journal articles, and one preprint.

As illustrated in Figure 1, the temporal distribution graph reveals that research on “artificial intelligence and police investigations” remained limited and sporadic between 2002 and 2020, before reaching its highest level in 2020. Until 2019, most years recorded only one publication or none at all, indicating that the topic had yet to achieve widespread penetration within the academic community. Across all years, journal articles represent the dominant publication type, accounting for nearly all records, whereas books, book chapters, and preprints appear only occasionally. The increase to five publications in 2020, almost all of them journal articles, suggests a recent maturation of the field and growing scholarly interest in the topic, likely driven by advances in machine learning technologies and increased investments in security-related applications during this period.

As shown in Figure 2, the country-level analysis reveals a strong concentration of research output in English-speaking nations. The United Kingdom leads with ten publications (32%), followed by the United States with nine (29%). Australia ranks third with three studies (10%), while China accounts for two publications (6%). The remaining countries each contributed a single publication (3% each),

namely Brazil, Canada, Germany, the Netherlands, Norway, and Portugal. The six most prominent institutions among the 31 publications are University College London (United Kingdom), with four articles; Goldsmiths, University of London (United Kingdom), with three; Tsinghua University (China), also with three; the University of Cambridge (United Kingdom), with two; the University of Sydney (Australia), with two; and the Massachusetts Institute of Technology (United States), with two publications. These results indicate a predominance of British institutions, followed by organizations from China, Australia, and the United States.

The concentration of studies in Computer Science, Artificial Intelligence, Engineering, Political Science, Sociology, and Law highlights an interdisciplinary approach shaped by the challenges posed by globalized cybercrime. Technical disciplines contribute algorithms and capabilities for processing large volumes of data across transnational networks, while the social sciences and legal studies address the normative, ethical, and governance dimensions of operating within a borderless digital environment. In this context, artificial intelligence emerges as an essential co-analyst, enabling real-time detection, the mapping of illicit flows, and predictive threat assessment, while integrating sociotechnical insights into police investigations. The prominence of legal research further underscores the need to develop coherent regulatory frameworks and mechanisms for international cooperation capable of balancing innovation, privacy, and accountability in the use of these technologies.

The patent analysis identified two patent applications, organized into one simple patent family and one extended patent family. Among these documents, two contain references to prior patents, and both have been cited in subsequent patent applications, resulting in a total of 117 patent citations. Additionally, one of the patent records includes a citation to non-patent literature (NPL), generating a single resolved NPL citation linked to an academic publication through its Lens ID.

The two patents identified in this study were filed under the jurisdiction of the United States and currently hold expired legal status.

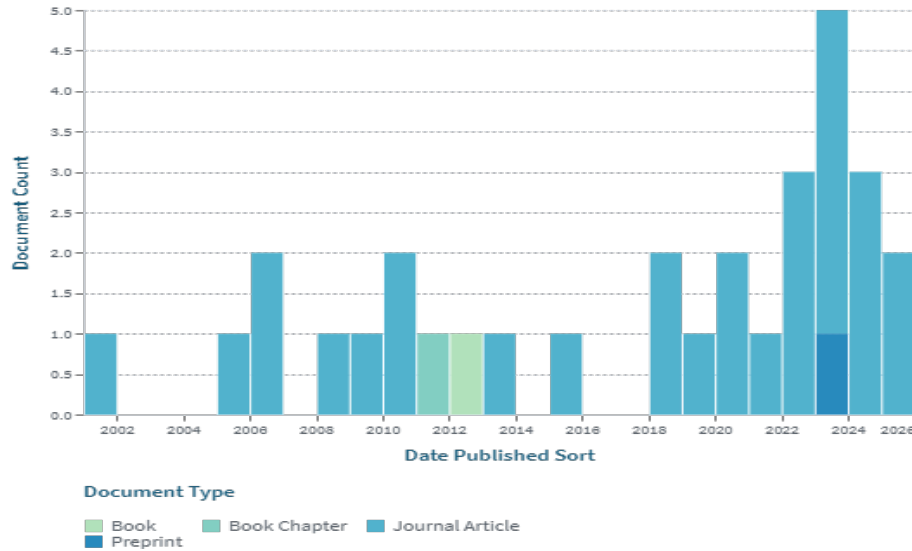
According to the data presented in Figure 4, the limited number of patent records, both expired and filed in the United States, suggests that the field of AI-assisted police intelligence has been explored predominantly within the academic and theoretical domain rather than through the development of proprietary technologies protected by intellectual property rights. Although academic production is relatively significant, comprising 31 publications involving research institutions in the United Kingdom, the United States, China, and Australia, this body of research has not yet translated into a substantial portfolio of

patentable innovations. This disparity between the intensity of conceptual and scholarly discussions and the scarcity of patent activity suggests that the field remains largely grounded in exploratory investigations and regulatory debates, with technological development still at an early stage of maturation.

b) Query 2 – Biometric Recognition (“*police intelligence*” OR “*inteligência policial*”) AND (“*facial recognition*” OR *biometrics* OR *biometria*)

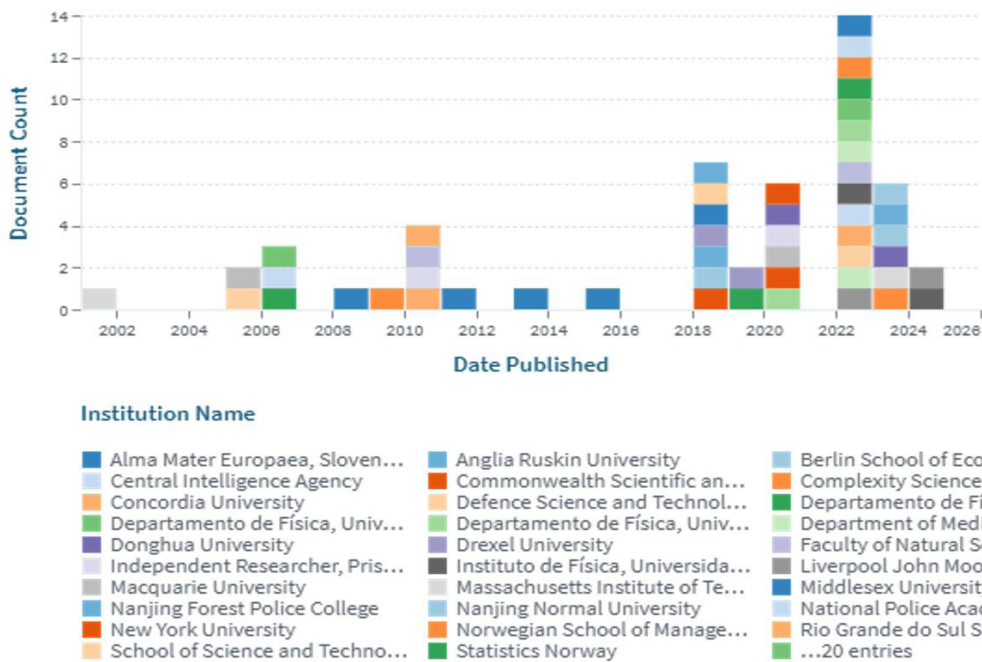
The second query, focused on biometric recognition in police intelligence, yielded 25 academic publications.

**Figure 1** – Number of publications over time (2000–2025): artificial intelligence applied to police investigations



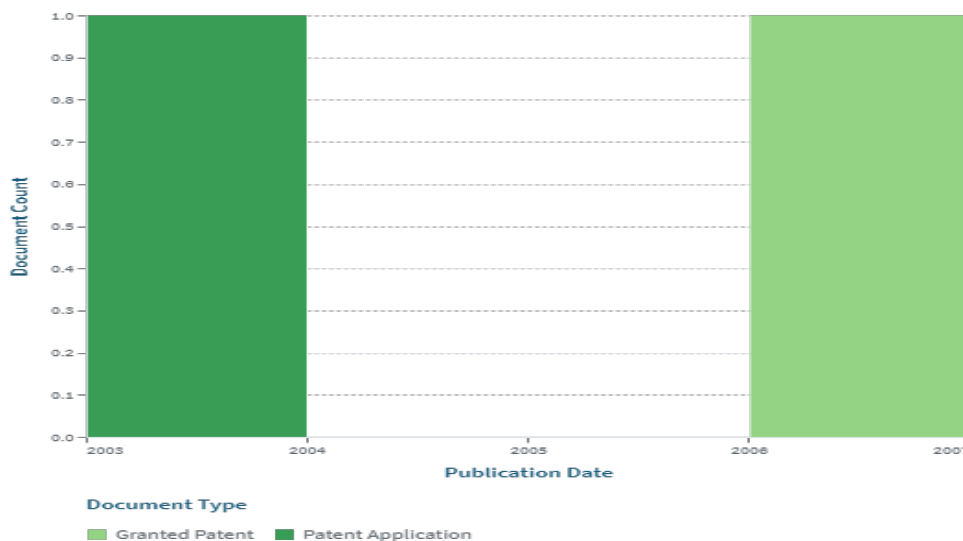
Source: The Lens (2025)

**Figure 2** – Distribution of academic publications by country in research on artificial intelligence and police intelligence (2000-2025)



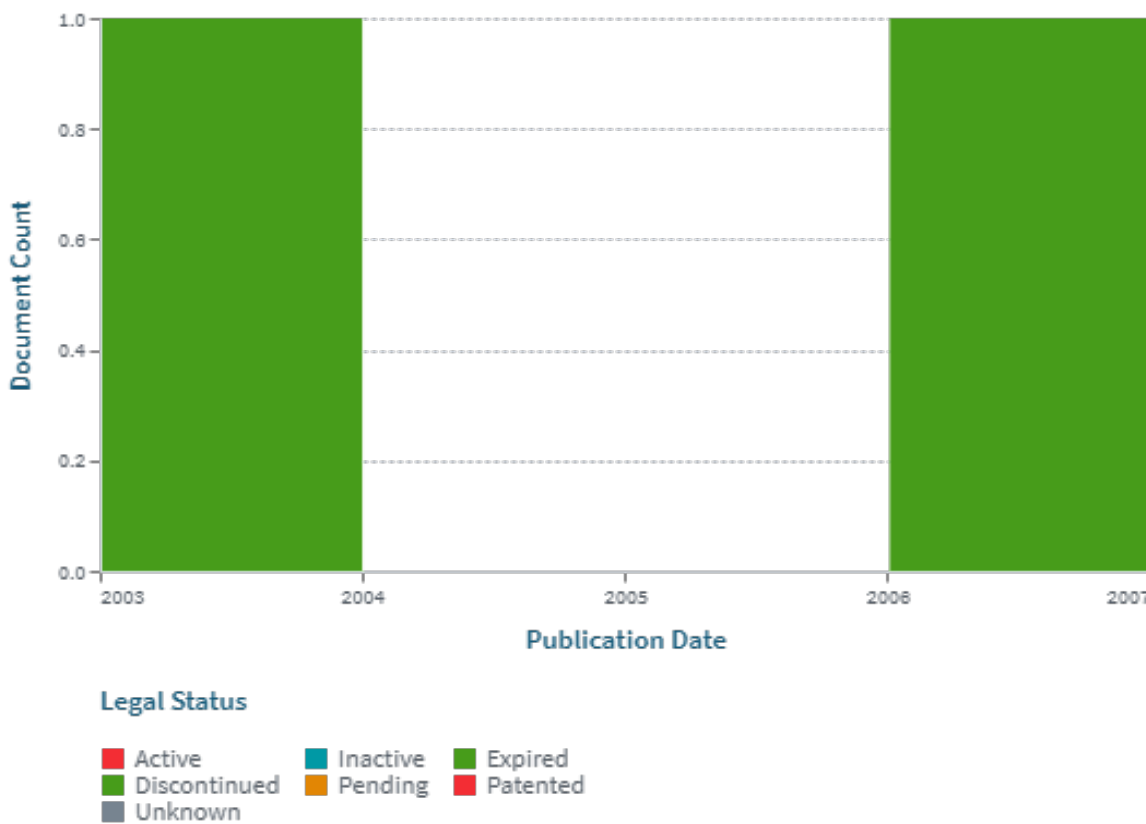
Source: The Lens (2025)

**Figure 3** – Number of Patent Applications in Artificial Intelligence and Police Intelligence (2000-2025)



Source: The Lens (2025)

**Figure 4** – Legal status of patent applications in artificial intelligence and police intelligence (2000-2025)



Source: The Lens (2025)

None of these studies appeared in patent citations, nor did they cite patent documents, indicating the absence of a direct interface with the domain of protected technological innovations. Within the scientific literature, however, 20 of these publications were cited by other academic works, accumulating a total of 519 scholarly citations. These findings underscore the relevance of facial recognition and biometric technologies in the specialized literature, even though their translation into patentable technological developments remains limited, as illustrated in Figure 5.

As illustrated in Figure 6, research on biometric recognition in police intelligence is concentrated in English-speaking countries, with seven publications (28%) originating from the United States and five (20%) from the United Kingdom. Australia ranks third with two publications (8%), while Canada, Israel, India, and Portugal each contributed one study (4% each). This distribution highlights the predominance of regions with substantial investments in security technologies and points to opportunities for expanding academic contributions from other geographic contexts.

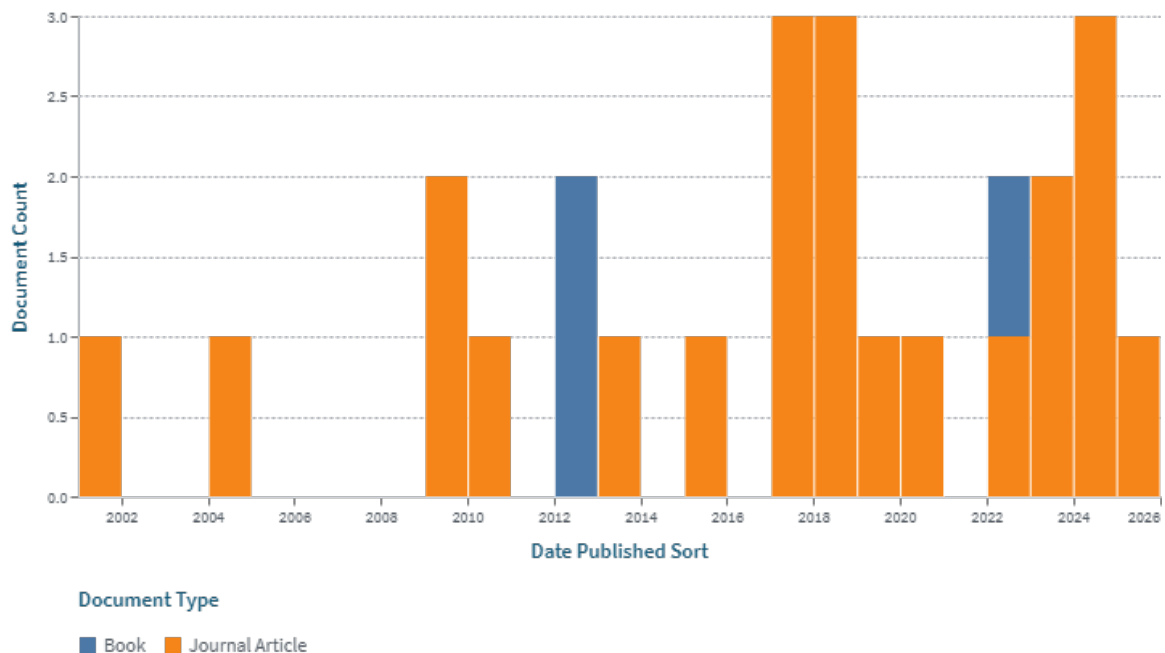
As illustrated in Figure 6, the analysis of the fields of study represented in the 25 publications on biometric recognition in police intelligence reveals a clear predominance of the social sciences. Sociology appears most frequently, with six occurrences, followed by Computer Science, Law, Law Enforcement, and Political Economy, each with three occurrences. Technical and strategic fields, including Artificial Intelligence, National Security, Political Science, and Terrorism Studies, each

account for two occurrences. The long tail of topics represented by a single occurrence, ranging from Bioethics to Paleontology and International Treaties, highlights the profoundly interdisciplinary nature of the field, encompassing normative and ethical perspectives alongside diverse quantitative and qualitative methodologies.

This configuration suggests that, although technological development plays an important role, understanding the social, legal, and political dimensions of these technologies remains essential. Sociology and Law occupy a leading position in the research agenda, indicating a strong emphasis on social dynamics, governance, and the ethical implications of police use of biometric technologies. At the same time, the presence of fields such as Computer Science, Artificial Intelligence, and National Security demonstrates a growing effort to integrate robust technical solutions with a deeper understanding of the social and legal frameworks that govern their application.

The patent prospecting analysis on biometric recognition in police intelligence identified eight patent records, organized into four simple patent families derived from a common priority document and four extended patent families grouping applications with similar technical content. Among these records, seven cite prior patents, and all eight have subsequently been cited by later patent applications, generating a total of 294 patent citations. In addition, four patent records reference non-patent literature (NPL), resulting in 82 NPL citations, of which 22 were successfully resolved and linked to academic publications through their respective Lens IDs, as illustrated in Figure 7.

**Figure 5** – Number of publications over time (2000–2025): biometric recognition in police intelligence



Source: The Lens (2025)



As presented in Figure 7, the eight patents related to biometric recognition in police intelligence exhibit a highly coherent technological profile when their predominant CPC classifications are examined. The G10L group, particularly subclasses 17/00, 25/27, 25/51, and 25/78, highlights a strong emphasis on voice processing techniques and vocal biometric pattern recognition. In parallel, the H04M2203 and H04M3 series indicate the integration of these solutions into telecommunications terminals and networks, pointing to systems that combine audio capture, voice-based authentication, and secure data transmission.

The G06F21/31–577 classes, associated with security arrangements in data processing, underscore concerns related to encryption, identity protection, and access control mechanisms within police intelligence systems. Meanwhile, the G07C9/257–38 and G08B29/24 classifications reflect applications in suspect monitoring and crime prevention activities.

Finally, the presence of H04L63 classifications, related to secure communication networks, together with remote sensing and positioning codes such as G01S3/784 and G01S5/16, suggests investments in resilient technological architectures and geospatial target positioning capabilities. Collectively, these classifications outline a technological framework that integrates vocal biometrics, information security, and advanced surveillance systems within a unified intelligence environment.

- c) Query 3 – Predictive Analytics in Public Security (“*police intelligence*” OR “*inteligência policial*” OR “*law enforcement analytics*”) AND (“*crime forecasting*” OR “*data-driven policing*” OR “*predictive analytics*”)

As illustrated in Figure 8, the search focused on predictive analytics and data-driven policing within the field of police intelligence yielded seven academic publications between 2000 and 2025. None of these studies were cited by patent documents, nor did they reference patented technologies, indicating a predominantly theoretical orientation rather than the development of protected technological innovations. Within the academic domain, five of these publications were cited by subsequent scholarly works, accumulating a total of 174 academic citations.

This distribution suggests a meaningful level of interest in crime prediction models and data-driven policing tools, but with limited translation into patentable innovations. The findings reinforce the notion that the debate remains largely situated within the conceptual, strategic, and policy-oriented spheres rather than in the domain of proprietary technological development.

Figure 9 presents the institutional distribution of research on police intelligence driven by predictive analytics,

involving seven academic and research organizations. Most studies originate from the United States (2), the United Kingdom (1), and Portugal (1). Notable contributors include John Jay College of Criminal Justice and Rutgers University in the United States, Universidade Nova de Lisboa and the University of Lisbon in Portugal, and the University of London in the United Kingdom. The presence of Eticas Research and Consulting (Spain) suggests a multidisciplinary and international interest in the topic, encompassing both technical-scientific approaches and regulatory perspectives on data-driven policing. Despite the relatively small number of publications, this geographical distribution indicates that the academic debate surrounding crime prediction and data-driven police intelligence extends across diverse national and institutional contexts.

As demonstrated in Figure 10, the patent search did not identify any patent records within the specific scope of the query related to police intelligence driven by predictive analytics and data-driven policing. Consequently, the patent analysis reveals that biometric recognition stands out with eight patent records, compared with only two patents related to artificial intelligence applied to police investigations and none associated with predictive analytics. This imbalance suggests that biometric solutions, such as facial and voice recognition technologies, have already reached a level of technical maturity sufficient to generate protected inventions. In contrast, the other areas, despite their substantial scientific output, remain at a more exploratory stage and have yet to translate into patentable or commercially viable technologies.

Figure 11 summarizes the academic production across the three thematic areas analyzed. Research on artificial intelligence and police investigations leads with 31 publications between 2000 and 2025, followed by biometric recognition with 25 publications and predictive analytics with 7 publications. Collectively, these studies form a significant interdisciplinary research core, with strong representation from Computer Science, Artificial Intelligence, Sociology, Political Science, and Law. They also engage with technical domains such as Human–Computer Interaction (HCI), Big Data, and Machine Learning, while simultaneously addressing social dimensions related to Governance, Ethics, and Security.

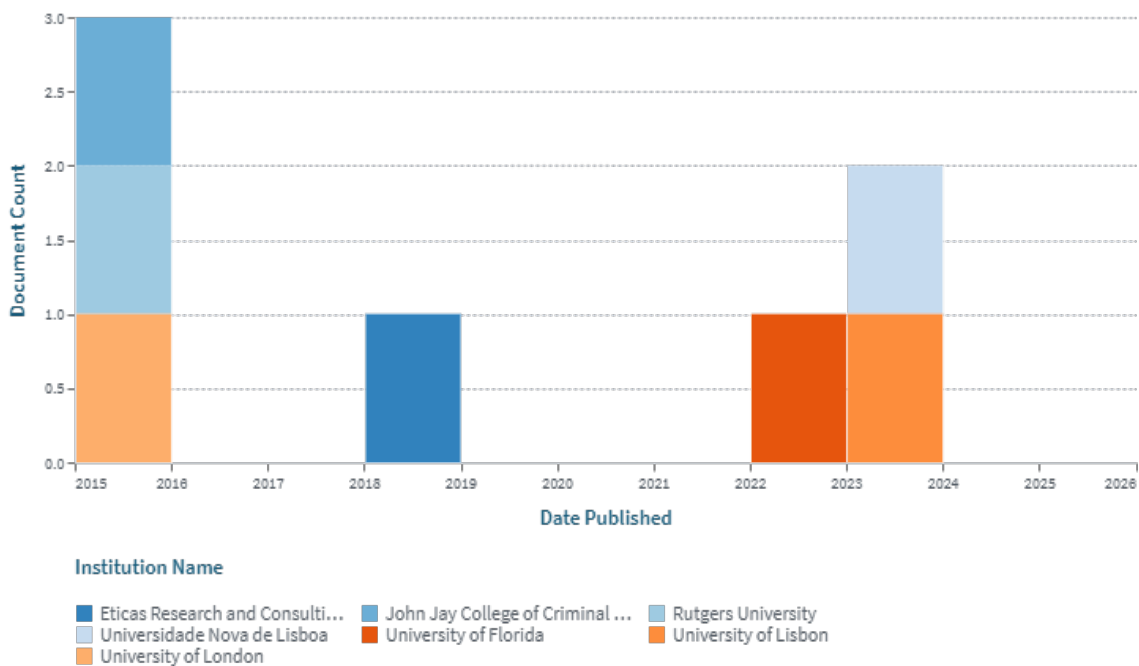
The diversity of disciplines involved demonstrates a solid scientific foundation for debate and knowledge generation. However, it also highlights the need to transform this knowledge into validated prototypes and applied studies capable of strengthening the integration between theory and practice. Overall, the findings indicate that, although research on advanced artificial intelligence techniques and data analytics in policing contexts has achieved considerable conceptual maturity, particularly regarding algorithms, network analysis, and data mining approaches, it remains predominantly theoretical in nature.

**Figure 8** – Number of publications over time (2000–2025): predictive analytics in public security



Source: The Lens (2025)

**Figure 9** – Distribution of academic publications by country in research on predictive analytics in public security (2000-2025)



Source: The Lens (2025)

### 3.1 Limitations and Methodological Considerations

Although this study employed bilingual search strategies and combined queries to maximize thematic coverage, it is important to acknowledge that the selection of descriptors prioritized contemporary terminology, such as *machine learning*, *artificial intelligence*, and *predictive analytics*, which are widely used in recent scientific and technological literature. This methodological choice was intended to ensure conceptual consistency and alignment with the current research frontier in police intelligence. However, prior to 2010, expressions such as *data mining*, *expert systems*, and *knowledge-based systems* were more commonly employed, alongside broader and more indirect terms such as *law enforcement*, *public safety technologies*, *criminal investigation tools*, and *pattern recognition*.

The deliberate exclusion of these terms may have limited the identification of historical studies and technological innovations that did not employ the more recent terminology associated with artificial intelligence. Nevertheless, this limitation does not undermine the objectives of the study, since the analytical focus was directed toward emerging trends and the contemporary stage of development and consolidation of technologies applied to police intelligence. Future investigations may broaden the terminological scope adopted here in order to capture the semantic and technical evolution of the field from its earliest formulations to the present day.

## 4 Final Considerations

Despite the significant growth in academic research on artificial intelligence, biometric recognition, and predictive analytics in police intelligence, the field still lacks empirical studies examining the incorporation of these technologies into real-world operations, comparative assessments of institutional performance, and systematic analyses of algorithmic bias across different contexts. There is also a shortage of research investigating knowledge transfer processes among academia, industry, and security agencies, as well as important gaps regarding the regulatory, ethical, and organizational factors that constrain the adoption of patentable innovations.

Future studies should therefore explore longitudinal case studies of law enforcement agencies that implement artificial intelligence and biometric systems, assessing indicators related to crime reduction effectiveness, social acceptance, and impacts on fundamental rights. Comparative cross-jurisdictional investigations may help clarify how legal and cultural variables influence data protection

practices and technological governance frameworks. In addition, further analysis of the patent ecosystem is recommended to identify barriers to commercialization and to develop guidelines that facilitate the transformation of theoretical insights into practical, secure, and socially responsible solutions for public security.

## 5 Future Perspectives

The survey of academic publications and patents related to artificial intelligence, biometrics, and crime prediction highlights the need for practical validation of these technologies in real-world policing environments. Future research should include field studies designed to assess indicators such as accuracy, processing speed, and interoperability among systems, while also examining algorithmic biases and their implications for the presumption of innocence. Further investigation is also needed into recidivism risk assessment algorithms, particularly regarding false-positive and false-negative rates, as well as into multimodal biometric fusion approaches that combine voice, facial, and gesture recognition in order to develop more stable and reliable solutions.

At the same time, the gap between extensive conceptual debate and the limited generation of patentable innovations underscores the importance of integrating technological and regulatory analyses. Future studies should compare regulatory frameworks across jurisdictions, develop algorithmic auditing guidelines for electronic evidence (e-evidence), and investigate governance models capable of ensuring transparency and continuous human oversight. Such efforts may contribute to the improvement of biometric recognition algorithms, data analysis pipelines, and explainable artificial intelligence (XAI) platforms, thereby enhancing the robustness, transparency, and reliability of police intelligence operations.

## Acknowledgments

This study was supported by the Coordination for the Improvement of Higher Education Personnel (CAPES), Brazil, Finance Code 001.

## References

BARBOSA, R. A. Os Estados Unidos pós 11 de setembro de 2001: implicações para a ordem mundial e para o Brasil. *Revista Brasileira de Política Internacional*, Marília, v. 45, n. 1, p. 72-91, 2002. DOI: 10.1590/S0034-73292002000100003.

GALDON CLAVELL, G. Exploring the ethical, organisational and technological challenges of crime mapping: a critical approach to urban safety technologies. **Ethics and Information Technology**, v. 20, p. 265-277, 2018. Disponível em: <https://doi.org/10.1007/s10676-018-9477-1>. Acesso em: 13 jun. 2025.

NISSAN, E. An overview of data mining for combating crime. **Applied Artificial Intelligence**, v. 26, n. 8, p. 760-786, 2012. DOI: 10.1080/08839514.2012.713309.

OATLEY, G.; EWART, B.; ZELEZNIKOW, J. Decision support systems for police: lessons from the application of data mining techniques to “soft” forensic evidence. **Artificial Intelligence and Law**, Dordrecht, v. 14, p. 35-100, 2006. DOI: 10.1007/s10506-006-9023-z.

PAZ, Fernando Eduardo Ramos. Consolidação da análise de vínculos no Centro de Inteligência da PMDF. **Revista Ciência & Polícia**, Brasília, DF, v. 8, n. 1, p. 148-170, 2022. ISSN 2316-8765. Disponível em: <https://www.lens.org/lens/scholar/article/036-802-918-571-87X/main>. Acesso em: 15 jun. 2025.

REJAS DE LA PEÑA, A. F. *et al.* Las aplicaciones de inteligencia artificial: herramientas esenciales para fortalecer la lucha contra la criminalidad. **Arandu UTIC**, v. 12, n. 2, p. 670-691, 2025. DOI: 10.69639/arandu.v12i2.949.

SACHOULIDOU, Athina. Going beyond the “common suspects”: to be presumed innocent in the era of algorithms, big data and artificial intelligence. **Artificial Intelligence and Law**. Springer, 2023. Disponível em: <https://doi.org/10.1007/s10506-023-09347-w>. Acesso em: 12 jun. 2025.

SOARES, J. C.; PACÍFICO, A. M. C. P. As consequências dos atentados de 11 de setembro de 2001 para a economia brasileira. **Brazilian Journal of International Relations**, Marília, SP, v. 12, n. 1, p. 45-60, 2023. DOI: 10.36311/2237-7743.2023.v12n1.p45-60.

THE LENS. **Página de busca**. 2025. Disponível em: <https://about.lens.org/>. Acesso em: 12 jun. 2025.

## About the Authors

---

### Andreia Rodrigues Ferreira Baro

*E-mail:* andreiabaro@hotmail.com

ORCID: <https://orcid.org/0000-0002-7592-0800>

Master's Degree in Intellectual Property and Technology Transfer for Innovation, Federal University of Alagoas.

Professional Address: 41 Rua 3, Cidade Universitária, Maceió, Alagoas, Brazil. ZIP Code: 57073-088.

---

### João Paulo Albuquerque Souza

*E-mail:* joaoalbuquerque Souza@gmail.com

ORCID: <https://orcid.org/0009-0004-2645-6951>

Postgraduate Specialization (Lato Sensu) in Information Security, Focus College (Cascavel, Paraná, Brazil).

Professional Address: 1,113 Dr. Sebastião Correia da Rocha Avenue, Block 3, Apartment 401, Tabuleiro do Martins, Maceió, Alagoas, Brazil. ZIP Code: 57061-410.