CARLOS IMBROSIO FILHO[1]
Autonomous University of Lisbon, Portugal
ORCID: 0000-0003-0480-4084

DOI : 10.14746/rie.2025.19.8

Artificial Intelligence in European Border Policing: Legal Challenges, Migration Governance, and Security Sector Reform

Introduction

The intersection of artificial intelligence (AI) and law enforcement has become a critical area of research, particularly in the context of migration governance. As the European Union (EU) continues to experience complex and fluctuating migration patterns along its three primary corridors – the Eastern, Central, and Western Mediterranean routes – AI-driven mechanisms are increasingly employed to enhance border security and manage migration flows. National police forces and border agencies across EU Member States are incorporating predictive analytics, biometric surveillance, and automated risk assessment systems into their operational frameworks, thereby redefining the traditional scope of migration control (European Commission, 2023; Frontex, 2022).

These issues necessitate a critical assessment of whether the integration of AI into border policing requires broader Security Sector Reform (SSR). In the EU context, SSR involves recalibrating police governance structures in line with democratic principles, emphasizing human rights compliance, institutional transparency, and civilian oversight. Drawing from established UN and OSCE models, SSR entails reforming legal mandates, enhancing accountability mechanisms, and ensuring inclusive participation in security policy. Yet, the current implementation of AI technologies often bypasses these principles – favoring efficiency over transparency and automation over deliberation.

While AI holds the potential to improve the efficiency of border control strategies, its deployment also raises significant ethical, legal, and operational concerns. Algorithmic bias, data privacy violations, and the risk of discriminatory enforcement have emerged as central challenges in AI-driven policing (Brouwer, 2021, p. 493; Molnar, 2020, p. 43). These issues necessitate a critical assessment of whether the integration of AI into border management requires broader security sector reform (SSR) – particularly in the regulation of police conduct at both national and transnational levels. Without comprehensive legal oversight and specialized training, AI technologies may inadvertently reinforce structural inequalities and undermine fundamental rights, ultimately eroding public trust in law enforcement institutions (European Union Agency for Fundamental Rights [FRA], 2021).

This study examines the implementation of AI in European border policing and its broader implications for migration governance. By analyzing current AI applications in law enforcement across the Mediterranean migration routes, the study explores the extent to which these technologies contribute to security objectives while respecting human rights principles. It also evaluates the existing regulatory frameworks governing AI in border security, identifying key gaps in legal and institutional oversight. Through this critical examination, the study seeks to offer policy recommendations for a balanced approach that aligns technological innovation with safeguards for fundamental rights, transparency, and continuous capacity-building among law enforcement professionals (Europol, 2023; Guild, Carrera, Vosyliūtė, 2022).

Research Aim and Hypotheses

The primary aim of this research is to examine how the adoption of AI in European border policing affects the legal, ethical, and institutional principles underpinning SSR. Specifically, the study explores whether AI-driven mechanisms align with the EU’s commitment to transparency, accountability, and human rights in law enforcement.

The analysis is guided by the following hypotheses:

1. The integration of AI into border policing enhances operational efficiency but undermines transparency and accountability.
2. Algorithmic risk assessment and biometric surveillance in migration management exacerbate the risk of discrimination and human rights violations.
3. Embedding AI governance within SSR frameworks can reconcile technological innovation with democratic oversight and institutional legitimacy.

Methodology and Framework

This research employs a qualitative and interpretative legal methodology grounded in doctrinal analysis, policy review, and critical examination of legal instruments and institutional practices. The study draws upon primary sources such as the EU Artificial Intelligence Act, the General Data Protection Regulation (GDPR), and relevant UN and OSCE frameworks, complemented by secondary sources including academic literature, peer-reviewed studies, and official reports from the European Commission, Frontex, Europol, and the EU Agency for Fundamental Rights (FRA).

The analysis follows a comparative legal approach, contrasting developments within EU Member States with international human rights and security governance standards. Three analytical indicators guide the assessment: (1) transparency in AI deployment, (2) accountability and oversight mechanisms, and (3) compliance with fundamental rights and Security Sector Reform (SSR) principles. While the study relies on extensive documentary and legal evidence, it does not include field-based or quantitative data, which constitutes a methodological limitation in evaluating the empirical outcomes of AI deployment in border policing.

To critically assess the integration of AI in European border policing, this article draws on theories of techno-governance, digital borders, and critical surveillance studies. These theoretical frameworks treat technological systems not as neutral tools, but as embedded within legal, political, and socio-technical infrastructures. As Didier Bigo (Bigo, 2006, pp. 46–68) argues in his work on the “Ban-opticon,” border security regimes increasingly rely on preemptive surveillance and algorithmic categorization, which blur the boundaries between policing, intelligence gathering, and migration management. This process, often termed digital bordering, enacts control over mobility not only through physical barriers but also through data-driven mechanisms such as biometric profiling and predictive risk scoring.

Furthermore, Mireille Hildebrandt (Hildebrandt, 2015, pp. 214–216) introduces the concept of legal techno-regulation, highlighting how automated decision-making can shift normative power from democratic institutions to opaque technological systems. From a legal critique perspective, Elspeth Brouwer (Brouwer, 2021, p. 502) underscores the risks posed by algorithmic opacity and legal ambiguity, contending that AI use in border control must be evaluated not only against data protection standards, but also in relation to the erosion of legal safeguards – such as the right to an effective remedy.

These insights frame the study’s approach to analyzing how AI reconfigures legal authority, operational discretion, and accountability within border enforcement across the EU.

Accordingly, the findings of this research contribute to ongoing debates on AI governance, migration policy, and security sector reform. By bridging technological developments with legal and ethical concerns, the study underscores the urgent need for a coherent, rights-based approach to AI-driven border policing. The broader implications extend beyond the European context, offering critical insights into global discussions on the responsible governance of AI in migration management and law enforcement.

1. The Integration of AI-Driven Technologies in European Border Security

The European Union (EU) faces multifaceted challenges along its Eastern, Central, and Western Mediterranean migration routes, including irregular migration, human trafficking, and smuggling of illicit goods. To address these issues, law enforcement agencies have increasingly turned to AI technologies to enhance border security and streamline migration management.[2] This chapter examines the latest trends and devel-

[2] AI-driven mechanisms are increasingly being integrated into the policing sector to enhance operational efficiency, improve crime prevention strategies, and support evidence-based decision-making. However, ensuring their safe and ethical deployment requires addressing critical concerns such as algorithmic bias, transparency, and accountability (Larson, 2020, pp. 891–914). AI applications in law enforcement, including predictive policing and automated surveillance, must align with fundamental human rights principles to mitigate risks associated with discriminatory profiling and unjustified intrusions on privacy (Mittelstadt et al., 2016, pp. 1–21). Effective governance frameworks, robust oversight mechanisms, and continuous human-in-the-loop monitoring are essential to main-

opments in AI-driven technologies within law enforcement, criminal investigations, and justice systems across these critical borders.

The deployment of AI technologies in border surveillance and control cannot be examined solely in terms of operational efficiency. As Bigo (Bigo, 2006, pp. 46–68) and Galič and Timan (Galič, Timan, 2021, pp. 212–233) have shown, the emergence of algorithmic sovereignty – where machine-driven risk scoring governs human mobility – represents a fundamental transformation in how state authority is exercised. The migration routes under EU scrutiny are not merely physical corridors but are increasingly shaped by digital infrastructures that profile individuals long before physical encounters at the border.

In this digital landscape, border management becomes a field of techno-governance, where law enforcement agencies engage with private tech vendors, data platforms, and biometric solution providers in shaping both policy and practice. Hildebrandt (Hildebrandt, 2015, pp. 214–216) cautions that this creates a new kind of regulatory environment – governed by code, data patterns, and machine learning – where accountability is diffused across actors and layers of automation.

These conceptual tools are essential for understanding how European AI-based border security mechanisms are reshaping traditional norms of proportionality, necessity, and non-discrimination. The literature also highlights the danger of “surveillance interoperability,” where different datasets – from visa applications, asylum claims, and passenger records – are linked and analyzed through algorithmic processes with minimal transparency. Brouwer (Brouwer, 2020, pp. 150–151; Brouwer, 2021, p. 505) underscores that without clear legal limitations and redress mechanisms, the EU risks institutionalizing a form of automated policing that circumvents constitutional and international human rights standards.

1.1. AI Applications in Border Surveillance and Control

AI technologies have been integrated into various aspects of border surveillance and control to improve efficiency and effectiveness. Automated border control systems, such as biometric identification and facial recognition, facilitate the rapid processing of travelers while maintaining security standards. Additionally, AI-powered surveillance towers and unmanned aerial systems (UAS) equipped with advanced sensors and machine learning algorithms monitor vast and challenging terrains, providing real-time data to border authorities (Frontex, 2020).

Maritime domain awareness has equally benefited from AI integration. Machine-learning models now analyze data from diverse sources – including satellite imagery, radar feeds, and maritime traffic records – to identify and predict irregular migration patterns and potential smuggling activities. However, empirical studies by

taining ethical standards and public trust (Kafteranis, Sachoulidou, Turksen, 2023, pp. 60–66). Additionally, law enforcement agencies must build technological capacity by fostering interdisciplinary collaboration, enhancing officers’ digital literacy, and ensuring compliance with data protection laws (Federal Trade Commission, 2024). A balanced approach that combines AI’s potential with rigorous legal and ethical safeguards can contribute to a more transparent and accountable policing system.

Statewatch (2024) and Molnar (Molnar, 2020, pp. 23–45) demonstrate that such systems frequently produce false positives and contribute to the over-policing of specific migration routes, reflecting biases embedded in historical datasets. These technologies often define “threats” through racialized or nationality-based profiling, leading to disproportionate scrutiny of African and Middle Eastern migrants. Field observations further indicate that predictive systems have, in some instances, prompted the detention of vessels carrying asylum seekers based on misclassified movement patterns (Statewatch, 2024). Although predictive analytics enable law enforcement agencies to act proactively and intercept unauthorized vessels before they reach European shores (RAND Europe, 2021), such efficiency gains come at the cost of transparency and proportionality.

While Dijstelbloem and Meijer (Dijstelbloem, Meijer, 2011, p. 15) interpret the digitalization of European borders as an adaptive response to migration management, this article argues that technological expansion often occurs beyond democratic oversight, thereby undermining the principles of proportionality and accountability that are central to Security Sector Reform (SSR).

1.2. Enhancing Criminal Investigations through AI

AI-driven tools have become instrumental in criminal investigations related to migration and border security. Advanced data analytics and pattern recognition algorithms assist in identifying and dismantling human trafficking and smuggling networks. By analyzing large datasets, including communication records and financial transactions, AI systems can uncover hidden connections between suspects and illicit activities.

For example, the United Kingdom and Germany have entered into a bilateral agreement to share intelligence and operational resources aimed at dismantling human-smuggling networks facilitating dangerous Channel crossings. This cooperation extends to monitoring smuggling-related content on social media platforms and tracing financial transactions to apprehend offenders (*UK and Germany sign…*, 2024).

Nonetheless, the growing reliance on AI-powered predictive analytics and risk assessment tools carries the risk of reproducing bias, disproportionately affecting individuals from particular demographic or national backgrounds. Ensuring transparency, accountability, and fairness in the design and use of such systems is crucial to prevent discrimination and uphold fundamental principles of justice.

Contrary to Vavoula (Vavoula, 2022, p. 51), who considers the EU’s AI Act a sufficient regulatory safeguard, this research contends that the framework remains inadequate, as it fails to resolve the persistent issues of algorithmic opacity and discriminatory outcomes in AI-based border policing.

1.3. Legal and Ethical Considerations

The deployment of AI technologies in border security raises significant legal and ethical concerns. Critics argue that AI-powered surveillance systems may infringe

upon the rights of migrants and asylum seekers, leading to potential violations of privacy and human rights. The European Union's Artificial Intelligence Act, adopted in March 2024 (European Commission, 2021), has been criticized for not adequately addressing these issues, particularly in the context of migration (Platform for International Cooperation on Undocumented Migrants [PICUM], 2024).

Moreover, the deployment of AI in predictive analytics and risk assessment systems may generate biased outcomes that disproportionately impact individuals from specific social or ethnic backgrounds. Upholding transparency, accountability, and fairness in AI applications is therefore essential to prevent discriminatory practices and preserve the integrity of justice.

In contrast to Vavoula (Vavoula, 2022, pp. 457–460), who regards the EU's Artificial Intelligence Act as an adequate legal safeguard, this study argues that the regulation remains incomplete – failing to fully address the operational opacity, systemic bias, and discriminatory potential embedded in AI-driven border policing practices.

1.4. In a Brief

The integration of AI-driven technologies into European border security and migration management presents both opportunities and challenges. While these technologies can enhance the efficiency and effectiveness of law enforcement responses, careful consideration of legal, ethical, and human rights implications is essential. Balancing security objectives with the protection of individual rights will determine the success and legitimacy of AI applications in this sensitive domain.

2. AI-Driven Mechanisms in EU Border Patrol

The increasing deployment of AI in border control has transformed the operational capacity of European Union (EU) agencies, particularly the European Border and Coast Guard Agency (Frontex). Predictive analytics, biometric surveillance, and automated risk assessment mechanisms play crucial roles in enhancing security and managing border crossings. However, the use of these AI-driven technologies raises concerns regarding algorithmic bias, data privacy, and potential discriminatory enforcement (Brouwer, 2020, p. 151; Molnar, 2021 p. 492). This chapter examines these mechanisms, exploring their implementation and impact within the EU's external border governance.[3]

[3] In the international context, several key documents address the balance between the integration of technologies in law enforcement and the safeguarding of fundamental rights. The Universal Declaration of Human Rights (United Nations, 1948) establishes core principles that guide the protection of human dignity and rights, including during police activities. The United Nations Office on Drugs and Crime (UNODC) emphasizes the importance of education and capacity-building in the fight against cybercrime while advocating for the responsible use of technology in policing (United Nations Office..., 2023). The European analysis of AI-driven border control systems, as discussed in "Automating the Fortress: Digital Technologies and European Borders" (Statewatch, 2024), highlights the challenges posed by digital technologies in migration and surveillance, stressing the need

2.1. Predictive Analytics in Border Control

Predictive analytics utilizes AI to process vast datasets, identifying patterns and trends to anticipate potential security threats. Frontex and national border agencies employ predictive modeling to assess migration flows, detect irregular crossings, and allocate resources effectively (Scherer, 2022, p. 68). One prominent example is the EUROSUR (European Border Surveillance System), which integrates data from sensors, satellite imagery, and historical records to generate real-time risk assessments (Carrera, Stefan, 2020, pp. 179–201). While EUROSUR is often highlighted as a technological advancement (Frontex, 2020), field-based research suggests limited accountability mechanisms and minimal transparency regarding how risk scores are calculated (Carrera, Stefan, 2020, p. 192). Tazzioli argues that EUROSUR’s predictive capacity is shaped more by geopolitical priorities than objective security threats, often producing overbroad alerts that justify militarized responses rather than facilitating humanitarian assessments (Tazzoli, 2022, pp. 276–295).

While predictive analytics enhances operational efficiency, scholars argue that reliance on historical migration data can reinforce systemic biases, leading to disproportionate scrutiny of certain nationalities or ethnic groups (Tazzioli, 2022, p. 289). Furthermore, critics highlight that data-driven border policing may contribute to the criminalization of migration rather than fostering humanitarian responses (Galič, Timan, 2021, p. 223).

2.2. Biometric Surveillance at EU Borders

Biometric surveillance has become a cornerstone of EU border security, with AI-driven facial recognition, fingerprint scanning, and iris recognition deployed in major entry points. The Schengen Information System (SIS II) and the Entry/Exit System (EES) integrate biometric data to monitor traveler movements and detect irregular entries (Fuster, 2020, pp. 105–119). These systems aim to enhance identity verification and prevent document fraud. However, multiple empirical studies – including Babuta & Oswald (Babuta, Oswald, 2022, pp. 45–62) and Kuner (Kuner, 2021, pp. 23–39) – document systematic bias and misidentification errors in facial recognition software, particularly affecting darker-skinned individuals and children. For instance, a European Journal of Law and Technology study found that false rejection rates exceeded 20% for African and Middle Eastern travelers at certain checkpoints. These failures not only delay entry but often trigger wrongful detentions or asylum claim rejections (Brouwer, 2021, pp. 341–364).

However, concerns persist regarding biometric data accuracy and the risk of misidentification, particularly among non-European travelers (Kuner, 2021, p. 33). Studies indicate that facial recognition algorithms demonstrate racial and gender-based biases, disproportionately affecting individuals from African and Middle Eastern backgrounds

for balancing security measures with human rights protections. Furthermore, the ongoing critique by the Abolish Frontex group (2023) calls attention to the risks of AI in border surveillance and its implications for the protection of fundamental freedoms.

(Babuta, Oswald, 2022, pp. 45–62). In response, regulatory bodies such as the European Data Protection Supervisor (EDPS) advocate for stronger safeguards to ensure compliance with the General Data Protection Regulation (GDPR) (European Data Protection Supervisor (EDPS), 2021).

While some scholars, such as Kuner (Kuner, 2021, pp. 35–39), argue that biometric technologies at EU borders – when properly regulated – can enhance security while maintaining compliance with privacy norms, empirical findings present a more critical picture. Babuta and Oswald (Babuta, Oswald, 2022, pp. 45–62), for instance, demonstrate that facial recognition systems consistently underperform when processing non-Caucasian facial features, particularly among African and Middle Eastern populations. These discrepancies suggest that reliance on biometric systems can reproduce racial hierarchies within border policing structures. Therefore, the purported neutrality of biometric safeguards, as presented by proponents like Kuner, fails to account for the lived experiences of racialized travelers and the sociotechnical limitations of these tools. A rights-based critique must foreground not just data protection, but also the material consequences of misidentification, such as unlawful detentions and asylum denials.

2.3. Automated Risk Assessment and Decision-Making

Automated risk assessment tools employ AI algorithms to classify travelers based on predefined risk profiles. The Advanced Passenger Information (API) and Passenger Name Record (PNR) systems analyze travel histories, behavioral patterns, and socio-economic indicators to flag potential security threats (Guild, 2020, p. 117). Frontex also utilizes machine learning models to assess asylum applications and detect fraudulent claims (Molnar, 2021, p. 199).

Despite efficiency gains, the opacity of these algorithms raises accountability concerns. Scholars argue that automated decision-making lacks transparency, making it difficult to challenge erroneous classifications or discriminatory risk assessments (Brouwer, 2020, pp. 157–159). Additionally, the over-reliance on predictive profiling risks violating the principle of non-discrimination under EU law (Carrera, Stefan, 2020, p. 189).

Scholars such as Jeandesboz and Vavoula provide contrasting interpretations of automation in border policing. Jeandesboz conceptualizes “smart borders” as efficient governance mechanisms capable of optimizing migration management through data-driven risk detection (Jeandesboz, 2016, pp. 292–309). However, this study aligns with Vavoula’s (Vavoula, 2022, p. 502) critique that such systems tend to reinforce a “logic of automation,” where legal responsibility becomes diffused across algorithms, agencies, and private contractors. This fragmentation undermines both the right to an effective remedy and the principle of accountability enshrined in EU law. Furthermore, as Martins et al. (Martins et al., 2021, pp. 567–589) contend, the digitalization of sovereignty at European borders produces a form of “algorithmic authority” that blurs the distinction between administrative discretion and automated coercion. Consequently, far from enhancing governance neutrality, AI-based risk assessment may entrench new layers of opacity that challenge the very legitimacy of EU border law enforcement.

2.4. Ethical and Legal Implications and Associated Risks

The integration of AI into border control necessitates a balance between security imperatives and fundamental rights.[4] The European Commission’s AI Act proposes risk-based regulations to govern AI applications, aiming to prevent undue surveillance and algorithmic discrimination (European Commission, 2021). Civil society organizations continue to advocate for greater oversight and accountability in AI-driven border enforcement (Galič, Timan, 2021, pp. 212–233; European Data Protection Supervisor [EDPS] & Fundamental Rights Agency [FRA], 2022–2024).

AI-driven mechanisms in EU border control – predictive analytics, biometric surveillance, and automated risk assessment – offer significant security enhancements but also pose critical ethical and legal challenges. While these technologies streamline border operations, their potential for reinforcing biases and infringing on privacy rights necessitates robust regulatory frameworks. Future research should focus on developing more transparent and accountable AI systems that align with EU fundamental rights principles.

While proponents such as Kafteranis, Sachoulidou, and Turksen (Kafteranis, Sachoulidou, Turksen, 2023, pp. 60–66) argue that the EU’s evolving legal framework – particularly through the AI Act – creates sufficient safeguards to balance innovation with rights protection, this study challenges that optimism. The persistent asymmetry between technological capability and legal oversight suggests that the EU’s regulatory approach remains largely reactive rather than preventive. As Taylor, Floridi, and van der Sloot (Taylor, Floridi, van der Sloot, 2017, pp. 60–66) emphasize in their concept of group privacy, data-driven surveillance mechanisms can infringe collective rights even when individual privacy protections appear intact. This tension exposes a critical flaw in the current governance paradigm: the assumption that procedural safeguards alone can neutralize structural biases embedded in algorithmic decision-making. Therefore, rather than merely refining risk-based classifications, the EU must adopt an anticipatory regulatory model – one that embeds human rights impact assessments and transparency obligations at every stage of AI deployment in border management.

3. Findings and Discussion – Risks to Fundamental Rights and Public Trust

3.1. Introduction

AI is increasingly being integrated into law enforcement operations worldwide. While AI-driven policing offers potential benefits such as enhanced surveillance,

[4] The use of AI-powered surveillance in national security must be approached with caution to balance security concerns with fundamental rights. The expansion of such technologies beyond their initial scope, such as their deployment during international events like the Paris Olympic and Paralympic Games, raises concerns about normalization and potential overreach (*Let’s beware of a post-Olympic*…, 2024). Similarly, large-scale AI-driven systems, like the European Border Surveillance System (Eurosur), illustrate how AI is increasingly embedded in transnational security frameworks, requiring careful oversight to prevent undue encroachments on privacy and civil liberties (EDPS, FRA, 2022–2024).

predictive analytics, and automated decision-making, its deployment without proper safeguards poses significant risks to fundamental rights and public trust. This chapter examines these concerns by exploring how AI-driven policing can infringe on civil liberties, exacerbate biases, and erode democratic accountability.

3.2. AI-Driven Policing and Fundamental Rights Violations

AI-driven policing involves the use of algorithms for facial recognition, predictive policing, and automated risk assessments. However, various human rights organizations have raised concerns about the potential for AI to infringe on privacy rights, freedom of expression, and due process. The United Nations High Commissioner for Human Rights (The United Nations High Commissioner for Human Rights, 2021) has warned that AI-powered surveillance systems may enable mass monitoring, leading to an environment of constant surveillance that disproportionately affects marginalized communities. Field reports by PICUM (Platform for International Cooperation on Undocumented Migrants [PICUM], 2024) and Galič & Timan (Galič, Timan, 2021, pp. 231–233) reinforce this concern, showing that AI-based surveillance disproportionately targets undocumented migrants and racialized individuals in frontline EU states such as Greece, Italy, and Hungary. PICUM’s interviews with migrants subjected to AI profiling systems reveal instances of forced fingerprinting, repeated data extraction without consent, and complete lack of access to legal remedies. Similarly, the Human Rights Watch (Human Rights Watch, 2023) highlights the risk of AI-based law enforcement systems reinforcing existing discriminatory practices, particularly against racial and ethnic minorities.

One of the key concerns is the lack of transparency in AI decision-making. The opacity of AI models makes it difficult for individuals to challenge or understand law enforcement decisions that affect them. The United Nations Human Rights Council (United Nations Human Rights Council, 2022) underscores the importance of accountability mechanisms to prevent AI-driven policing from violating the right to privacy in the digital age.

3.3. Algorithmic Bias and Discrimination in Law Enforcement

AI models are often trained on historical crime data, which may reflect systemic biases in law enforcement practices. A study by the “Georgetown Law Journal on Modern Critical Race Perspectives” (Barabas, 2020, pp. 83–96) found that predictive policing tools used in Europe often amplify discriminatory policing patterns, particularly in border zones near marginalized urban communities. Ethnographic data from refugee camps in Lesbos and Lampedusa collected by “El País” (*El ‘Gran Hermano’ de la UE en los campos…*, 2025) further highlight that AI-based “suspicion algorithms” flag non-white male individuals for secondary screening at rates disproportionately higher than other groups – despite no criminal indicators in most cases.

As a result, predictive policing systems risk perpetuating racial profiling and unfair targeting of marginalized communities (Human Rights Watch, 2021). The UN Human Rights Council’s resolution on AI in security and policing (UN Human Rights Coun-

cil, 2021) highlights that AI tools, if not properly regulated, can lead to discriminatory enforcement practices and reinforce social inequalities.

The Interpol & UNICRI (Interpol, UNICRI, 2023) toolkit for responsible AI innovation in law enforcement advocates for bias mitigation strategies, yet acknowledges the limitations of existing regulatory frameworks. Without strict oversight, AI-driven policing tools may contribute to over-policing in certain neighborhoods while neglecting systemic issues that lead to crime. The discriminatory impact of AI in policing undermines public trust and creates a perception of injustice, particularly in communities that already experience over-policing and state surveillance.

Ethical AI initiatives, such as the widely cited *AI4People* framework (Floridi, Cowls, Beltrametti, Chatila, Chazerand, Dignum, Schafer, 2018, pp. 689–707), advocate for principles of fairness, transparency, and accountability in the use of artificial intelligence. However, these frameworks often operate within an abstract normative landscape, insufficiently addressing how algorithmic systems function within structurally unequal societies. When applied to policing and migration contexts, these principles risk becoming symbolic gestures rather than actionable safeguards. For example, AI4People provides few mechanisms to prevent predictive policing models from amplifying racial profiling – a concern echoed in critiques from Human Rights Watch (Human Rights Watch, 2021) and the “Georgetown Law Journal on Modern Critical Race Perspectives” (Barabas, 2020, p. 17). In practice, ethical codes without binding enforcement mechanisms do little to mitigate the real-world risks faced by marginalized populations at European borders. Thus, the current wave of ethical AI literature often underestimates the racialized nature of migration control and fails to disrupt the power asymmetries embedded in AI governance.

3.4. Erosion of Public Trust in Law Enforcement

Public trust in law enforcement is crucial for effective policing. However, the unregulated use of AI in policing can lead to decreased confidence in law enforcement agencies. The European Union’s flawed approach to AI regulation has been criticized for not adequately addressing the risks posed by AI in social security and law enforcement (Human Rights Watch, 2021). This lack of regulatory safeguards contributes to fears of AI being used in ways that undermine human rights rather than protect them.

Furthermore, the secretive nature of AI systems and their potential misuse for mass surveillance erode democratic accountability. The United Nations Human Rights Council (United Nations Human Rights Council, 2021) emphasizes that without clear legal frameworks ensuring transparency and human oversight, AI-driven policing threatens to normalize invasive surveillance practices and arbitrary law enforcement actions.

3.5. Conclusion

The deployment of AI in policing must be accompanied by robust safeguards to prevent violations of fundamental rights and maintain public trust. Current AI-driven

policing strategies risk exacerbating discrimination, infringing on privacy, and eroding democratic accountability. Effective governance frameworks, transparency measures, and human oversight are essential to ensure that AI tools are used ethically and in a manner that upholds human rights. Without such safeguards, AI-driven policing could do more harm than good, ultimately weakening public confidence in law enforcement institutions.

4. Policy Implications and Reform Proposals

The evolution of European border security has been significantly influenced by technological advancements, particularly the integration of AI and automated surveillance systems. While these developments have improved operational efficiency and reinforced security, they have also sparked ethical and legal concerns, particularly regarding human rights, privacy, and transparency. This chapter explores the necessity of a balanced approach – one that aligns security objectives with fundamental rights, ensures accountability, and fosters continuous skill development among border security personnel.

4.1. The Expansion of AI in Border Security

The European Union (EU) has increasingly relied on AI-driven technologies to monitor and manage its external borders. Automated surveillance systems, biometric identification, and predictive analytics have become essential tools for border control agencies, particularly Frontex. However, as AI assumes a larger role, concerns regarding its ethical implications have surfaced. Reports indicate that AI-enabled surveillance often disproportionately affects migrants and refugees, raising concerns about potential human rights violations (Abolish Frontex, 2023). The deployment of such technology in refugee camps, for instance, has been criticized for reinforcing control rather than offering humanitarian solutions.[5]

4.2. Surveillance and Mass Data Collection: A Double-Edged Sword

The increasing use of AI-driven mass surveillance in border management poses a significant challenge in balancing security and privacy.[6] Technologies such as facial

[5] Recent reports describe the expansion of AI surveillance in refugee camps in Greece (*El ‘Gran Hermano’ de la UE en los campos…*, 2025). A *Guardian* editorial warns that proposed EU surveillance measures risk normalizing mass data collection (*The EU wants to scan every message…,* 2025).

[6] The increasing reliance on artificial intelligence for massive data collection and automated processing raises significant ethical and legal concerns, particularly regarding privacy, bias, and systemic discrimination. AI-driven algorithms, when applied to areas such as predictive policing, financial decision-making, and social services, have been shown to reinforce existing inequalities rather than mitigate them. O’Neil (2016) highlights how opaque and unregulated AI models con-

recognition, automated risk assessment, and data analytics enable authorities to predict potential security threats. However, critics argue that these tools promote excessive governmental power and a culture of suspicion, often without sufficient oversight.[7] The proposal to scan all digital communications within the EU further complicates this debate, as it raises concerns about the erosion of privacy under the pretext of security (Fotiadis, 2025, para. 3).

The normalization of AI surveillance, as seen in the use of video analytics during major events such as the Paris Olympic Games, could lead to expanded applications in border control (*Let’s beware of a post-Olympic…*, 2024). Yet, UNESCO (UNESCO, 2023) and UNODC (UNODC, 2023) report that national police forces often lack adequate digital literacy training to correctly interpret the outputs of such systems, leading to overreliance on AI-generated risk assessments without meaningful review. These findings challenge the assumption that surveillance capacity necessarily translates into lawful or proportionate enforcement action. Without proper legal safeguards, such measures may infringe upon civil liberties and create an environment of perpetual surveillance, disproportionately affecting vulnerable populations such as asylum seekers.

4.3. Ensuring Transparency and Ethical Oversight

A key challenge in integrating AI into border security is ensuring transparency and accountability. The transformation of Frontex into a more autonomous and technologically equipped agency has raised alarms about the lack of oversight mechanisms.[8] The absence of robust governance structures exacerbates concerns about algorithmic biases, wrongful detentions, and excessive use of force. Implementing comprehensive regulatory frameworks that mandate transparency in AI deployment is essential to mitigate these risks. Beyond that, it’s also important to remark that the EDPS and FRA (European Data Protection Supervisor [EDPS] & Fundamental Rights Agency [FRA], 2022–2024) jointly stress that the deployment of AI in border control must be accompanied by binding transparency requirements and regular rights-impact assessments.

Furthermore, ethical AI deployment should involve a human-in-the-loop approach, where AI serves as an assistive tool rather than an autonomous decision-maker. This approach ensures that human rights considerations remain at the forefront of security operations, preventing automated systems from making unilateral determinations about individuals’ migration status or security risks.

---

tribute to structural injustices, disproportionately affecting marginalized communities. Similarly, Muhammad (2019) explores how historical biases embedded in data have long shaped discriminatory policies, and the integration of AI risks exacerbating these disparities rather than resolving them.

[7] See: Euronews (*Mass surveillance*…, 2023) for a journalistic overview of the EU’s technological border initiatives.

[8] Refer to *El País* for a in-depth approach to Frontex’s Agency main challenges in regards to newly launched technologies and oversight measures (*Frontex será nuestra tumba*…, 2024).

4.4. Investing in Skill Development and Ethical Training

Technological advancements must be complemented by continuous skill development and ethical training for border security personnel. AI should not replace human judgment but rather enhance decision-making processes. Specialized training programs can equip officers with the necessary knowledge to interpret AI-generated data responsibly and identify potential biases in automated systems.

Moreover, fostering a culture of ethical responsibility within border agencies can help counteract the risks associated with AI misuse. Education and training should emphasize the fundamental principles of human dignity, proportionality, and necessity in border security operations.

4.5. Toward a Human-Centered Security Model

A sustainable and ethical border security strategy must integrate technological innovation with a commitment to human rights and legal safeguards. AI-driven surveillance should be subject to continuous evaluation, ensuring that security measures do not override fundamental freedoms. Policymakers must engage in ongoing dialogue with civil society organizations, legal experts, and technology developers to create a border security model that upholds democratic values.

By prioritizing transparency, oversight, and skill development, European border security can harness the benefits of AI while mitigating its risks. Striking this balance is imperative to avoid the unchecked expansion of surveillance capabilities and to protect the rights of those affected by border control policies.

4.6. Reframing AI Deployment: International Standards, Securitization Theory, and the Avoidance of Automation Bias

The deployment of AI in border security intersects with key debates in international security, human rights law, and critical theory – particularly securitization theory, which emphasizes how issues become framed as existential threats requiring extraordinary measures. In the context of European border management, AI technologies risk reinforcing securitized narratives that treat migration as a threat, legitimizing invasive technologies without sufficient public scrutiny or democratic accountability. This framing has been criticized by scholars such as Didier Bigo and Elspeth Guild, who argue that the construction of migration as a “security problem” enables exceptional policing practices, including data-intensive surveillance and automated decision-making at borders.

Current international legal standards, however, offer an alternative paradigm – one rooted in human security and the protection of individual rights. The Universal Declaration of Human Rights – UDHR (United Nations, 1948), the International Covenant on Civil and Political Rights – ICCPR (United Nations, 1966), and the UN Guiding Principles on Business and Human Rights all affirm the importance of privacy,

non-discrimination, and dignity in state and institutional practices. Moreover, UNESCO’s 2021 Recommendation on the Ethics of Artificial Intelligence calls on states to adopt a human-centered approach to AI governance, emphasizing the need for algorithmic transparency, fairness, and inclusivity, particularly in high-risk applications such as law enforcement and migration governance.

Similarly, the Council of Europe’s Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+) and the EU General Data Protection Regulation (GDPR) (Council of Europe, 2018; European Data Protection Supervisor (EDPS), 2021) provide binding standards that prohibit disproportionate data collection, require informed consent, and mandate mechanisms for individuals to challenge automated decisions that affect their rights. These instruments underscore the need to embed “algorithmic due process” and the right to explanation within all AI-based border enforcement systems.

To reframe AI deployment within border security while avoiding automation bias, EU institutions and Member States must shift from a reactive security-first model to a rights-preserving risk management model. This would entail the following reforms:

1. **Preemptive Human Rights Impact Assessments (HRIAs):** Before AI technologies are deployed at borders, independent HRIAs should evaluate whether they align with the principles of necessity, proportionality, and non-discrimination, as required under international human rights law.
2. Human-in-the-Loop Design: AI applications in border policing should always be accompanied by meaningful human oversight. This principle is affirmed in the “UN Human Rights Council’s Resolution A/HRC/48/31” (United Nations Human Rights Council, 2021), which warns against autonomous systems making unreviewable decisions in policing and border control.
3. **Bias Auditing and Transparency Mandates:** Drawing from the OECD Principles on AI (OECD, 2019) and the Interpol-UNICRI Toolkit for Responsible AI Innovation in Law Enforcement (Interpol, UNICRI, 2023), systems should be periodically audited for discriminatory outcomes. Public authorities must disclose algorithmic logic and ensure that independent auditors can access the underlying data.
4. **Security Sector Reform (SSR) Alignment:** The responsible use of AI in border security must form part of broader SSR frameworks, as outlined in *UN Security Council Resolutions 2151 and 2553* (United Nations Security Council, 2014; United Nations Security Council, 2020). These resolutions advocate for transparent, accountable, and rights-compliant policing institutions, including reforms in training, oversight, and public trust building.
5. **Regional and Civil Society Engagement:** A truly balanced AI strategy should involve dialogue with civil society, privacy advocates, and refugee organizations. This participatory approach is essential to prevent the legitimization of surveillance infrastructures that disproportionately target racialized or vulnerable populations.

While UN and OSCE frameworks conceptualize Security Sector Reform (SSR) as a process rooted in democratic accountability and human rights protection, the European Union’s approach to AI in border security still privileges operational efficiency over institutional transformation. As Bryden and Hänggi (Bryden, Hänggi, 2005) observe, SSR must prioritize human-centred governance rather than mere technical

modernization. Yet, EU strategies often frame AI deployment as an innovation-driven upgrade rather than a reform of governance structures, neglecting the participatory and oversight mechanisms vital for sustainable legitimacy.

Reframing AI deployment within European border security therefore requires embedding technological innovation in binding legal and ethical frameworks that place human dignity above algorithmic expediency. Grounding AI in international human rights standards would not only enhance the legitimacy and accountability of border operations but also strengthen the democratic rule of law that underpins the EU’s normative order.

4.7. Security Sector Reform and the Future of Ethical Border Policing

The responsible use of AI in European border security must be embedded within broader frameworks of Security Sector Reform (SSR), a concept rooted in democratic transitions and promoted by institutions such as the United Nations (UN) and the Organization for Security and Co-operation in Europe (OSCE). SSR prioritizes the transformation of security institutions – including police forces – into structures that are effective, accountable, rights-compliant, and subject to democratic oversight.

Within the EU, applying SSR principles to AI deployment in border control would involve adapting existing police governance frameworks to:

– Establish legally binding transparency obligations around algorithmic use in policing decisions;
– Create independent oversight bodies to audit AI-based enforcement tools;
– Ensure public participation in security technology procurement and deployment decisions;
– Mandate training programs to develop ethical and rights-based AI literacy among law enforcement personnel;
– Align border control strategies with international human rights standards, including the UN Universal Declaration of Human Rights, ICCPR, and GDPR.

Although the OECD (OECD, 2019) and Interpol-UNICRI (Interpol, UNICRI, 2023) guidelines emphasize transparency and human oversight as foundations of responsible AI, their implementation across EU border institutions remains inconsistent. As Stahl, Timmermans, and Flick (Stahl, Timmermans, Flick, 2021, pp. 439–457) argue, ethical commitments risk becoming purely declaratory when not supported by enforceable accountability mechanisms. This deficiency underscores the urgent need for mandatory bias auditing, independent supervision, and public transparency to ensure that algorithmic decision-making aligns with democratic and human-rights-based governance.

However, current AI practices within systems such as EUROSUR, PNR, and biometric surveillance programs continue to operate with limited transparency, ambiguous legal mandates, and minimal civil society engagement. This contradicts core SSR principles, which require policing and security institutions to be not only effective but also democratically accountable and judicially reviewable. Bridging this gap between

technological advancement and governance reform is essential to restore public trust and uphold the legitimacy of EU law enforcement. Embedding SSR principles into EU border AI strategies will ensure that innovation strengthens – rather than undermines – the rule of law, human dignity, and democratic oversight.

Conclusion

This study diverges from dominant narratives that assume technological neutrality or ethical harmonization through soft governance. While ethical AI literature such as Floridi et al. (Floridi, Cowls, Beltrametti, Chatila, Chazerand, Dignum, Schafer, 2018, pp. 689–707) and the OECD AI Principles (OECD, 2019) envision AI as a tool to be responsibly steered, our findings align more closely with critical perspectives such as those advanced by Human Rights Watch (Human Rights Watch, 2023) and Brouwer (Brouwer, 2021, p. 344), which highlight the systemic biases, surveillance overreach, and erosion of rights in current AI applications at EU borders. By centering the discussion on human mobility, securitization, and algorithmic discrimination, this article disputes the assumption that ethical design alone can safeguard against structural injustice. Instead, it calls for enforceable legal reforms and independent oversight to address the deeper political dynamics of AI use in migration governance. The goal is not just responsible AI, but accountable and decolonized border technologies that prioritize human dignity over efficiency metrics.

Furthermore, the integration of AI into border policing across the European Union represents a critical juncture for law enforcement innovation, migration governance, and human rights protection. While AI-driven tools such as predictive analytics, biometric surveillance, and automated risk assessment promise improved operational efficiency, their uncritical deployment raises pressing concerns about algorithmic bias, legal accountability, and the erosion of fundamental rights.

Despite efforts such as the European Commission’s Artificial Intelligence Act (European Commission, 2021) to create a harmonized regulatory framework, the current legal architecture remains insufficient to address the complex ethical, operational, and structural risks posed by AI in border management. As highlighted by Europol (Europol, 2020; Europol, 2024) and academic literature (Brantingham, Valesik, Mohler, 2018, pp. 85–92; Christin, Rosenblat, Boyd, 2020, pp. 1–14; Ferguson, 2017, pp. 1109–1189), there is a growing consensus that legal safeguards and ethical oversight must keep pace with technological innovation.

To that end, this article proposes a set of evidence-based policy reforms to ensure AI is deployed responsibly and inclusively in European border security:

1. **Mandatory Human-in-the-Loop Systems**:

AI tools used in migration control and border policing must never operate autonomously in decision-making that affects individual rights. Human operators with appropriate legal training and ethical awareness should retain ultimate responsibility for reviewing and validating AI-generated outputs. This model is supported by the UN

Human Rights Council’s 2021 resolution on AI in law enforcement (United Nations Human Rights Council, 2021), which warns against “black box” decision-making.

2. Creation of an Independent EU Oversight Authority:

An independent, supranational regulatory body should be established to oversee the development, deployment, and evaluation of AI technologies used in border policing. This authority must be empowered to audit algorithms, investigate complaints of misuse, and ensure compliance with the General Data Protection Regulation (GDPR) (European Data Protection Supervisor (EDPS), 2021), the EU Charter of Fundamental Rights (European Union, 2012), and Convention 108+ (Council of Europe, 2018). Transparency reports should be made public regularly.

3. EU-Wide Standards for Algorithmic Bias Auditing:

All AI systems deployed at borders must be subject to routine anti-bias audits conducted by independent experts. These audits should examine training datasets, performance across demographics, and the potential for systemic discrimination. Inspired by the Interpol-UNICRI Toolkit for Responsible AI Innovation in Law Enforcement (Interpol, UNICRI, 2023), such audits must also include actionable mitigation plans and consequences for non-compliance.

4. Integration into Security Sector Reform (SSR) Frameworks:

The responsible adoption of AI in border enforcement must be part of broader EU efforts toward democratic security sector reform. This includes training law enforcement officers in ethical AI use, embedding transparency and accountability mechanisms, and prioritizing community engagement. AI deployment should enhance – not replace – lawful policing grounded in fundamental rights.

5. Continuous Public and Civil Society Engagement:

Ethical AI deployment requires active dialogue with civil society organizations, refugee advocacy groups, data protection authorities, and legal experts. Public consultations and participatory policymaking must be institutionalized to prevent the technocratic expansion of surveillance powers under the guise of border security.

In conclusion, the future of European border policing depends not only on technological capability but on the Union’s commitment to uphold democratic values and human dignity. The responsible integration of AI must be informed by clear legal standards, robust institutional oversight, and an unwavering dedication to transparency and accountability. By aligning innovation with human rights, the EU can lead globally in crafting a just and secure digital border governance model.

The findings of this research confirm the first two hypotheses: AI technologies have enhanced the operational capabilities of EU border agencies but have simultaneously eroded transparency and increased risks of algorithmic discrimination. The third hy-

pothesis is partially validated, suggesting that embedding AI regulation within Security Sector Reform frameworks can restore elements of oversight and accountability, though such reforms remain unevenly implemented across EU Member States. Overall, the study underscores that technological innovation alone cannot ensure lawful and ethical border governance without parallel legal and institutional transformation.

Bibliography

Abolish Frontex (2023), *AI in border control and surveillance: Current and future implications*, November 18, https://abolishfrontex.org/blog/2023/11/18/ai-in-border-control-and-surveillance-current-and-future-implications/, 13.06.2025.

Babuta A., Oswald M. (2022), *AI and border security: Challenges of biometric recognition systems*, „European Journal of Law and Technology”, 13(1).

Barabas Ch. (2020), *Beyond bias: Re-imagining ethical AI in criminal law*, “Georgetown Law Journal on Modern Critical Race Perspectives”, 12(2).

Bigo D. (2006), *Security, exception, ban and surveillance*, in: *Theorizing Surveillance: The Panopticon and Beyond*, ed. D. Lyon, Willan, London.

Brantingham P. J., Valasik M., Mohler G. O. (2018), *Does predictive policing lead to biased arrests?*, “Social Science & Medicine”, 198.

Brouwer E. (2020), *Artificial intelligence and border control: A threat to fundamental rights?*, “European Public Law”, 26(2).

Brouwer E. (2021), *Artificial intelligence and migration control: A legal perspective on the use of AI in border management*, “European Journal of Migration and Law”, 23(2).

Bryden A., Hänggi H. (2005), *Reforming and Reconstructing the Security Sector*, in: “Security Governance in Post-Conflict Peacebuilding”, Geneva Centre for the Democratic Control of Armed Forces (DCAF), Geneva, https://www.dcaf.ch/sites/default/files/publications/documents/YB2005.pdf, 18.10.2025.

Carrera S., Stefan M. (2020), *Access to biometric data in the EU: Balancing security and privacy*, “Journal of European Migration Studies”, 8(3).

Christin A., Rosenblat A., Boyd D. (2020), *The limitations of machine learning in criminal justice*, “Big Data & Society”, 7(1).

Council of Europe (2018), *Convention 108+ for the protection of individuals with regard to the processing of personal data*, https://www.coe.int/en/web/data-protection/convention108, 10.10.2025.

Dijstelbloem H., Meijer A. (2011), *Migration and the New Technological Borders of Europe*, Palgrave Macmillan, London.

El ‘Gran Hermano’ de la UE en los campos de refugiados en Grecia: Cámaras con inteligencia artificial, concertinas y normas draconianas, “El País”, 25.01.2025, https://elpais.com/internacional/2025-01-25/el-gran-hermano-de-la-ue-en-los-campos-de-refugiados-en-grecia-camaras-con-inteligencia-artificial-concertinas-y-normas-draconianas.html, 15.07.2025.

European Commission (2021), P*roposal for a regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*, COM(2021) 206 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206, 11.10.2025.

European Commission (2023), *The EU in 2023: General report on the activities of the European Union*, Publications Office of the European Union, https://op.europa.eu/webpub/com/general-report-2023/en/, 18.10.2025.

European Data Protection Supervisor (EDPS) & EU Agency for Fundamental Rights (FRA) (2022–2024), *Joint Reports on Artificial Intelligence in Border Management*, Brussels.

European Data Protection Supervisor (EDPS) (2021), *General Data Protection Regulation (GDPR)*, https://www.edps.europa.eu/data-protection/our-work/subjects/general-data-protection-regulation_en, 07.06.2025.

European Union (2012), *Charter of Fundamental Rights of the European Union*, Official Journal of the European Union, C 326/391, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT, 10.04.2025.

European Union (2016), *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)*, “Official Journal of the European Union”, L 119, 4.5.2016, https://eur-lex.europa.eu/eli/reg/2016/679/oj, 10.04.2025.

European Union Agency for Fundamental Rights (FRA) (2021), *Fundamental Rights Report 2021*, Publications Office of the European Union, https://fra.europa.eu/en/publication/2021/fundamental-rights-report-2021, 10.04.2025.

Europol (2020), *Malicious uses and abuses of artificial intelligence*, November 19, https://www.europol.europa.eu/publications-events/publications/malicious-uses-and-abuses-of-artificial-intelligence, 10.04.2025.

Europol (2024), *AI and policing: The benefits and challenges of artificial intelligence for law enforcement*, https://www.europol.europa.eu/publication-events/main-reports/ai-and-policing, 21.06.2025.

Federal Trade Commission (2024), *Building tech capacity in law enforcement agencies. U.S. Federal Trade Commission*, https://www.ftc.gov/system/files/ftc_gov/pdf/ot.techcapacityreport.pdf, 21.06.2025.

Ferguson A. G. (2017), *Policing predictive policing*, “Washington University Law Review”, 94(5).

Floridi L., Cowls J., Beltrametti M., Chatila R., Chazerand P., Dignum V., Schafer B. (2018), *AI4People: An ethical framework for a good AI society*, “Minds and Machines”, 28.

Fotiadis A. (2025), *The EU wants to scan every message sent in Europe. Will that really make us safer?*, “The Guardian”, https://www.theguardian.com/commentisfree/2025/jan/24/eu-digital-surveillance-child-protection, 14.10.2025.

Frontex (2020), *Frontex AI Research Study 2020 – Executive Summary*, https://www.frontex.europa.eu/assets/Publications/Research/Frontex_AI_Research_Study_2020_executive_summary.pdf, 21.06.2025.

Frontex (2022), *Risk analysis for 2022: Migration trends and border security developments*, Frontex Publications, https://www.frontex.europa.eu/publications/risk-analysis-for-2022-2023-RfJIVQ, 21.06.2025.

Frontex será nuestra tumba, “El País”, 21.10.2024, https://elpais.com/opinion/2024-10-21/frontex-sera-nuestra-tumba.html, 10.06.2025.

Fuster G. (2020), *The expansion of biometric technologies in EU border control*, “Computer Law & Security Review”, 36.

Galič M., Timan T. (2021), *Surveillance at the EU’s borders: AI, human rights, and accountability*, “Surveillance & Society”, 19(4).

Guild E. (2020), *The use of automated decision-making in border control: Legal challenges*, “European Migration and Asylum Law Review”, 7(2).

Guild E., Carrera S., Vosyliūtė L. (2022), *The use of artificial intelligence in migration and border control: A human rights perspective*, “CEPS Research Paper”, no. 2022/06, https://www.ceps.eu/publications/, 10.06.2025.

Hildebrandt M. (2015), *Smart technologies and the end(s) of law: Novel entanglements of law and technology*, Edward Elgar Publishing, Cheltenham.

Human Rights Watch (2021), *How the EU’s flawed artificial intelligence regulation endangers the social safety net: Questions and answers*, November 10, https://www.hrw.org/news/2021/11/10/how-eus-flawed-artificial-intelligence-regulation-endangers-social-safety-net, 30.06.2025.

Human Rights Watch (2023), *EU: Artificial intelligence regulation should protect people’s rights*, July 12, https://www.hrw.org/news/2023/07/12/eu-artificial-intelligence-regulation-should-protect-peoples-rights, 23.06.2025.

Interpol, UNICRI (2023), *Toolkit for responsible AI innovation in law enforcement*, https://unicri.org/Publication/Toolkit-for-Responsible-AI-Innovation-in-Law-Enforcement-UNICRI-INTERPOL, 23.07.2025.

Jeandesboz J. (2016), *Smartening border security in the European Union: An associational inquiry*, “Security Dialogue”, 47(4).

Kafteranis D., Sachoulidou A., Turksen U. (2023), *Artificial intelligence in law enforcement settings*, “EUCRIM” 2023(1), https://doi.org/10.30709/eucrim-2023-006, 15.10.2025.

Kuner C. (2021), *Data protection implications of biometric border controls in Europe*, „International Data Privacy Law”, 11(1).

Larson J. (2020), *Addressing bias and transparency in predictive algorithms for criminal justice*, “Law and Society Review”, 54(4).

Let’s beware of a post-Olympic drift in the use of AI-powered video surveillance, “Le Monde”, 26.08.2024, https://www.lemonde.fr/en/opinion/article/2024/09/26/let-s-beware-of-a-post-olympic-drift-in-the-use-of-ai-powered-video-surveillance_6727335_23.html, 21.06.2025.

Martins O. et al. (2021), *Border security and the digitalisation of sovereignty: Insights from EU borderwork*, “European Security”, 30(4).

Mass surveillance, automated suspicion, extreme power: How tech is shaping the EU’s borders, Euronews, 06.04.2023, https://www.euronews.com/next/2023/04/06/mass-surveillance-automated-suspicion-extreme-power-how-tech-is-shaping-the-eus-borders, 23.07.2025.

Mittelstadt B. D., Allo P., Taddeo M., Wachter S., Floridi L. (2016), *The ethics of algorithms: Mapping the debate*, “Big Data & Society”, 3(2).

Molnar P. (2020), *Technology on the margins: AI and border control practices in Europe*, “Journal of Human Rights and Digital Technologies”, 2(1).

Molnar P. (2021), *Technological borders: AI-driven risk assessment in migration governance*, “AI & Society”, 36(2).

Muhammad K. G. (2019), *The condemnation of blackness: Race, crime, and the making of modern urban America*, Harvard University Press, Harvard.

O’Neil C. (2016), *Weapons of math destruction: How big data increases inequality and threatens democracy*, Crown Publishing Group, New York.

OECD (2019), *OECD Principles on Artificial Intelligence*, https://www.oecd.org/en/topics/ai-principles.html, 15.07.2025.

Platform for International Cooperation on Undocumented Migrants (PICUM) (2024), *A dangerous precedent: How the EU AI Act fails migrants and people on the move*, March 13, https://picum.org/blog/a-dangerous-precedent-how-the-eu-ai-act-fails-migrants-and-people-on-the-move/, 15.10.2025.

RAND Europe (2021), *Artificial intelligence-based capabilities for the European Border and Coast Guard: Final report*, https://www.rand.org/randeurope/research/projects/2021/european-border-coast-guard-artificial-intelligence.html, 05.08.2025.

Scherer A. (2022), *Predictive analytics and AI in EU border security: Implications for policy*, “European Journal of Security Studies”, 10(1).

Stahl B. C., Timmermans J., Flic C. (2021), *Ethics of emerging technologies: Balancing benefits and risks in the use of AI for criminal justice*, “AI & Society”, 36(3).

Statewatch (2024), *Automating the fortress: Digital technologies and European borders*, https://www.statewatch.org/analyses/2024/automating-the-fortress-digital-technologies-and-european-borders/, 15.04.2025.

Taylor L., Floridi L., van der Sloot B. (eds.) (2017), *Group Privacy: New Challenges of Data Technologies*, Springer, Cham.

Tazzioli M. (2022), *Algorithmic border control and the politics of migration risk scoring*, „Journal of Borderlands Studies”, 37(3).

The EU wants to scan every message sent in Europe. Will that really make us safer?, “The Guardian”, 24.01.2025, https://www.theguardian.com/commentisfree/2025/jan/24/eu-digital-surveillance-child-protection, 15.04.2025.

UK and Germany sign deal against people smugglers as Europe struggles to halt Channel crossings, Associated Press, 15.122024, https://apnews.com/article/59779cfb09f3571d4fbd1f49a1dd4cd2, 20.04.2025.

UNESCO (2023), *AI and digital transformation competencies for civil servants: Competency framework* [PDF], https://sdgs.un.org/sites/default/files/2023-05/B44%20-%20Tan%20-%20AI%20and%20Digital%20Transformation%20Competencies%20Framework.pdf, 25.04.2025.

UNESCO (2023), *Artificial intelligence and digital transformation (UNESCO report)*, https://unesdoc.unesco.org/ark:/48223/pf0000383325.locale=en, 15.10.2025.

United Nations (1948), *Universal Declaration of Human Rights*, https://www.un.org/en/about-us/universal-declaration-of-human-rights, 15.02.2025.

United Nations (1966), *International Covenant on Civil and Political Rights (ICCPR)*, https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights, 15.02.2025.

United Nations Educational, Scientific and Cultural Organization (2021), *Recommendation on the ethics of artificial intelligence*, https://unesdoc.unesco.org/ark:/48223/pf0000380455, 15.02.2025.

United Nations High Commissioner for Human Rights (2021), *The use of artificial intelligence and autonomous systems in state-controlled operations* (A/HRC/47/23), https://undocs.org/en/A/HRC/47/23, 10.03.2025.

United Nations Human Rights Council (2021), *Resolution on the use of artificial intelligence in security and policing* (A/HRC/48/31), https://undocs.org/en/A/HRC/48/31, 15.02.2015.

United Nations Human Rights Council (2022), *Right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights* (A/HRC/51/17), https://undocs.org/en/A/HRC/51/17, 15.02.2025.

United Nations Office on Drugs and Crime (UNODC) (2023), *Education and capacity-building in the fight against cybercrime*, https://www.unodc.org/unodc/en/frontpage/2017/April/e4j_countering-cybercrime-creating-prosperity.html, 15.10.2025.

United Nations Security Council (2014), *Resolution 2151 (2014) on security sector reform: Challenges and opportunities*, https://docs.un.org/en/S/RES/2151(2014), 15.10.2025.

United Nations Security Council (2020), *Resolution 2553 (2020) on security sector reform*, https://peacekeeping.un.org/sites/default/files/s_res_2553_2020-en.pdf, 15.02.2025.

Vavoula N. (2021), *Artificial Intelligence (AI) at Schengen borders: Automated processing, algorithmic profiling and facial recognition in the era of techno-solutionism*, “European Journal of Migration and Law”, 23(4), https://doi.org/10.1163/15718166-12340159, 15.02.2025.

Vavoula N. (2022), *Immigration and privacy in the law of the European Union: The case of information systems (1st ed.)*, Brill/Nijhoff, https://doi.org/10.1163/9789004520000_001, 15.02.2025.

Vavoula N. (2022), *Unpacking the EU proposal for an AI Act: Implications for AI systems used in the context of migration, asylum and border control management*, https://orbilu.uni.lu/profile?uid=50076071, 15.02.2025.

Summary

This article aims to critically assess how artificial intelligence (AI) technologies are reshaping European border policing and to evaluate whether their deployment requires a broader framework of Security Sector Reform (SSR) within the European Union (EU). Using a qualitative legal research grounded in doctrinal and policy analysis, the study examines how AI-driven predictive analytics, biometric surveillance, and automated risk assessments influence law enforcement practices along the EU’s key migration routes. The research is guided by three hypotheses: first, that AI enhances border management efficiency but weakens transparency and accountability; second, that algorithmic systems increase the risk of discriminatory enforcement and human rights violations; and third, that embedding AI governance within SSR frameworks can mitigate such risks by reinforcing democratic oversight and institutional responsibility. By linking AI innovation to fundamental rights protection, the study contributes to ongoing debates on ethical governance and the human-rights-based regulation of border technologies in the EU.

Key words: Artificial intelligence, security sector reform, migration governance, law enforcement, European Union borders, technological surveillance, human rights

Sztuczna inteligencja w europejskiej policji granicznej: wyzwania prawne, zarządzanie migracją i reforma sektora bezpieczeństwa

Streszczenie

Artykuł ma na celu krytyczną ocenę sposobu, w jaki technologie oparte na sztucznej inteligencji (AI) przekształcają europejskie praktyki policyjne w zakresie ochrony granic oraz analizę, czy ich wdrażanie wymaga szerszych ram Reformy Sektora Bezpieczeństwa (SSR) w Unii Europejskiej (UE). W oparciu o jakościowe badanie prawa, obejmujące analizę doktrynalną i polityczno-prawną, artykuł analizuje, w jaki sposób systemy analityki predykcyjnej, nadzoru biometrycznego i automatycznej oceny ryzyka wpływają na działania organów ścigania wzdłuż kluczowych szlaków migracyjnych UE. Badanie opiera się na trzech hipotezach: po pierwsze, że integracja AI zwiększa efektywność zarządzania granicami, ale jednocześnie osłabia przejrzystość i odpowiedzialność instytucjonalną; po drugie, że algorytmiczne systemy decyzyjne nasilają ryzyko dyskryminacji i naruszeń praw człowieka; oraz po trzecie, że wdrożenie zasad SSR w zarządzaniu AI może ograniczyć te zagrożenia poprzez wzmocnienie nadzoru demokratycznego i odpowiedzialności instytucjonalnej. Łącząc innowacje technologiczne z ochroną praw podstawowych, artykuł wnosi wkład w debatę nad etycznym zarządzaniem i prawnymi ramami wdrażania sztucznej inteligencji w polityce granicznej UE.

Słowa kluczowe: sztuczna inteligencja, reforma sektora bezpieczeństwa, zarządzanie migracjami, egzekwowanie prawa, granice Unii Europejskiej, nadzór technologiczny, prawa człowieka

Author Contributions

Conceptualization (Konceptualizacja): Carlos Imbrosio Filho

Data curation (Zestawienie danych): Carlos Imbrosio Filho

Formal analysis (Analiza formalna): Carlos Imbrosio Filho

Writing – original draft (Piśmiennictwo – oryginalny projekt): Carlos Imbrosio Filho

Writing – review & editing (Piśmiennictwo – sprawdzenie i edytowanie): Carlos Imbrosio Filho

Competing interests: The authors have declared that no competing interests exist (Sprzeczne interesy: Autor oświadczył, że nie istnieją żadne sprzeczne interesy): Carlos Imbrosio Filho

Article submitted: 04.02.2025; article accepted: 21.03.2025.
Data przekazania tekstu: 04.02.2024; data zaakceptowania tekstu: 21.03.2025.