

DIGITAL DIMENSION OF MIGRANT SMUGGLING AND ARTIFICIAL INTELLIGENCE: RISKS AND EUROPEAN RESPONSES

*Sebastian GEORGESCU, Ph. D candidate**

Abstract: *The digital transformation of transnational organized crime has significantly changed the way networks involved in migrant smuggling operate. Social media platforms, instant messaging applications and other digital tools are already integrated into various stages of organizing and facilitating illegal border crossings. The rapid development and growing accessibility of generative artificial intelligence, however, introduce a new dimension to the phenomenon.*

The article analyzes the transition from the use of digital tools to the emerging integration of artificial intelligence, distinguishing between already documented practices, developing trends and prospective risks. To this end, an analytical model based on five functions (5F-AI) is proposed: expansion, identification, interaction, concealment and amplification, through which artificial intelligence can amplify the efficiency and scale of the activities carried out by organized crime groups. In parallel, the article examines how AI tools can support law enforcement authorities and border management structures in processing large volumes of information, conducting risk analysis, identifying relevant connections and developing investigative leads.

Particular attention is given to the relationship between migrant smuggling and human trafficking, as well as to the legal and ethical limits on the use of artificial intelligence within the European regulatory framework.

The study argues for the need for an intelligence-led response model, supported by technology and kept under human control, in which artificial intelligence complements, without replacing, professional expertise and human decision-making.

Keywords: *migrant smuggling; illegal migration; AI; organized crime; border management; OSINT; risk analysis.*

DOI **10.56082/annalsarscimilit.2026.3.21**

Introduction

Migrant smuggling, as a form of transnational crime closely linked to the dynamics of illegal migration, is one of the fields in which adaptation to political, technological and operational change is particularly rapid.¹ Networks involved in facilitating illegal border crossings do not operate exclusively through classic hierarchical structures; Paolo Campana

* CAROL I National Defence University, email: sebastian.georgescu13@yahoo.com.

¹ Europol, Criminal Networks in Migrant Smuggling, Europol Spotlight Report, Publications Office of the European Union, Luxembourg, 2023, pp. 2-3, DOI: 10.2813/550319.

highlights the fragmented nature of the activities associated with migrant smuggling, the relative ease with which new actors can become involved, and the frequent presence of small-scale structures with local reach and limited hierarchical development.² European investigations describe a flexible ecosystem made up of organizers, intermediaries, recruiters, transporters, providers of counterfeit documents and other persons who provide logistical, financial or operational support. Europol underlines the adaptable nature of these networks and their capacity to make use of legitimate firms and other lawful commercial activities to support logistics and conceal illegal activities.³

In this context, the digital dimension can no longer be regarded as a secondary element of how groups involved in migrant smuggling operate. Social media platforms are used to promote services, attract migrants and recruit facilitators, while instant messaging applications are frequently used at a later stage, for the exchange of operational information and to move communications away from public channels.⁴ The role of digital technologies has been highlighted by the relevant literature for more than a decade, with research showing that social media platforms can alter the structure of migration networks and access to the information needed for movement.⁵ Recent research on illegal crossings of European borders confirms the existence of genuine digital infrastructures in which migrants, facilitators and other actors exchange information on routes and modes of travel.⁶ In March 2026, on the occasion of the launch of the new European Centre against Migrant Smuggling (ECAMS), Europol underlined that the activities of migrant smuggling networks are increasingly taking place online, confirming the integration of the digital dimension into their *modus operandi*.⁷

The development of generative artificial intelligence may represent the next stage of this transformation: falling costs, reduced technical complexity and the capacity to generate content in multiple languages give

² Paolo Campana, „Human Smuggling: Structure and Mechanisms”, *Crime and Justice*, vol. 49, 2020, pp. 471-519, DOI: 10.1086/708663.

³ Europol, *Tackling Threats, Addressing Challenges - Europol's Response to Migrant Smuggling and Trafficking in Human Beings in 2023 and Onwards*, Luxembourg, 2024, DOI: 10.2813/203212, pp. 3-4, 7-10, 12.

⁴ Europol, *Tackling Threats...*, *op. cit.*, p. 12.

⁵ Rianne Dekker, Godfried Engbersen, „How Social Media Transform Migrant Networks and Facilitate Migration”, *Global Networks*, vol. 14, no. 4, 2014, pp. 401-418, DOI: 10.1111/glob.12040.

⁶ Ismail Oubad, Rassa Ghaffari, „The Digital Infrastructures of Illegal Border Crossings: Solidarity Actors and Networks in the Arabic and Persian Speaking Virtual Spheres”, *Critical Criminology*, vol. 33, 2025, pp. 71-88, DOI: 10.1007/s10612-025-09824-5.

⁷ Europol, „The Grip on Migrant Smuggling Tightens: New Department at Europol to Step Up the Fight”, March 24, 2026.

networks tools that can increase the efficiency of their operations.⁸ Europol shows that AI and other emerging technologies accelerate criminal activities, increasing their speed and reach.⁹ However, a nuanced approach is required: while the use of digital platforms by migrant smuggling networks is already well documented, the use of AI is only beginning to emerge as a distinct trend. UNODC flags, among the emerging challenges, facilitators' use of new information and communication technologies, including documents generated with the help of artificial intelligence.¹⁰

In recent academic literature, the integration of AI into criminal phenomena associated with illegal migration is analyzed explicitly mainly in relation to human trafficking, where the ways in which AI can facilitate the identification and contacting of potential victims, influence them during the recruitment process, and amplify the operational capacity of criminal networks are already being examined.¹¹ This research offers a relevant comparative benchmark, without its findings being automatically transferable to migrant smuggling. Therefore, the question is no longer whether the digital environment is used in migrant smuggling, this reality is already well documented, but rather the extent to which the digital infrastructure already integrated into the activity of these groups creates the conditions for the use of AI at various stages of the facilitation activity and, conversely, how authorities can use these technologies to identify, investigate and dismantle the networks.

The study's hypothesis is that the use of artificial intelligence does not lead to the emergence of a distinct phenomenon within illegal migration, nor to a new manifestation of migrant smuggling, but rather amplifies the efficiency, speed and scale of practices already used by organized crime groups involved in organizing and facilitating illegal border crossings. This may extend these groups' capacity to reach persons interested in illegal border crossing, may accelerate communication, reduce language barriers, automate certain activities and increase the level of sophistication of fraudulent or deceptive content, while also facilitating the conduct of activities across multiple geographic and linguistic spaces.

Conversely, the same tools can support law enforcement authorities in making use of large and heterogeneous volumes of information, by identifying patterns, connections and anomalies that are difficult to detect

⁸ OSCE/Bali Process, *New Frontiers: The Use of Generative AI to Facilitate Trafficking in Persons*, Policy Brief, 2024, pp. 6, 11-12.

⁹ Europol, *EU-SOCTA 2025*, Luxembourg, 2025, p. 11.

¹⁰ UNODC, *Legislative and Policy Solutions to Emerging Issues Related to the Smuggling of Migrants*, CTOC/COP/WG.7/2025/3, August 5, 2025.

¹¹ Joel Levesque, „The AI-Enhanced Trafficking Threat: Examining the Technological Evolution of Trafficking in Persons Operations with AI Tools”, *Journal of Human Trafficking*, 2025.

through exclusively traditional methods. The use of AI can thus contribute to guiding risk analysis, prioritizing operationally relevant information and developing investigative leads, without the automatically generated results replacing professional judgment and human decision-making. In this dual use of artificial intelligence, as a multiplier of the capacity of networks involved in migrant smuggling and, at the same time, as a support tool for authorities, one of the main future challenges for border management takes shape.

1. Methodology and Conceptual Distinctions

The study uses a qualitative approach, based on document analysis and comparative analysis, supplemented by a prospective analysis of emerging trends and threats.¹² The main documentary basis consists of assessments and documents produced by Europol, UNODC, Frontex, OSCE, INTERPOL, the European Commission and other EU institutions, supplemented by recent academic literature on migrant smuggling, the digital dimension of migration and the use of new technologies in border management. Recent research on the integration of AI into related criminal activities, particularly human trafficking, is also used as a comparative benchmark for identifying possible developments in migrant smuggling, without automatically transferring conclusions between legally distinct phenomena.

To limit unwarranted extrapolation, information on the use of technology by organized crime groups is analyzed at three levels. The first level covers documented practices, supported by operational information or empirical research, such as the use of social media platforms, instant and encrypted messaging applications, geolocation tools and counterfeit documents. The second level concerns emerging uses of AI, already flagged by authorities and international organizations but still insufficiently documented through public data to be considered widespread practices. The third level concerns prospective risks, namely technically plausible uses resulting from combining AI's current capabilities with already documented modes of operation, without these being presented as already confirmed practices.

This distinction is important because artificial intelligence should not be confused with digitalization in the broad sense. Encrypted messaging, cryptocurrencies, social media platforms and navigation applications are digital tools, but they do not, in themselves, constitute AI systems.¹³ They form part of the digital infrastructure already used in migrant smuggling activities, into which AI-based functions or tools may subsequently be

¹²Glenn A. Bowen, „Document Analysis as a Qualitative Research Method”, *Qualitative Research Journal*, vol. 9, no. 2, 2009, pp. 27-40.

¹³Regulation (EU) 2024/1689 (Artificial Intelligence Act), Art. 3(1).

integrated. The distinction between the broader integration of digital technologies and the use of AI to amplify or automate certain components of these activities is therefore purely analytical in nature and does not imply the existence of legally distinct forms of the offence.

The assessment of emerging trends and threats also takes into account the risk-analysis principles used in the field of European border management, namely the three-component structure of the Common Integrated Risk Analysis Model (CIRAM), without the study seeking to apply this operational methodology in full, but only to adopt its logic of graduated assessment of the threat, vulnerability and impact associated with a security phenomenon.¹⁴

2. Migrant Smuggling and Human Trafficking: Legal Delimitation and Zone of Convergence

The Protocol against the Smuggling of Migrants by Land, Sea and Air, supplementing the United Nations Convention against Transnational Organized Crime, constitutes the main international legal instrument on migrant smuggling. Under Article 3(a) of the Protocol, migrant smuggling involves facilitating the illegal entry of a person into a state party of which that person is not a national or permanent resident, for the purpose of obtaining, directly or indirectly, a financial or other material benefit.¹⁵ Human trafficking has a different legal structure. Under the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, it involves the recruitment, transportation, transfer, harbouring or receipt of a person, through means such as threat, coercion, fraud, deception or abuse of a position of vulnerability, for the purpose of exploitation.¹⁶

This distinction is essential for the present analysis, since the mere fact that a person turns to a group involved in facilitating illegal border crossing does not confer on that person the status of a victim of human trafficking. In migrant smuggling, the initial relationship between the migrant and the facilitator may be consensual in nature, with the migrant seeking illegal entry into another state and the facilitator seeking a financial benefit. In human trafficking, the determining element is exploitation, and the victim's consent is irrelevant where the means set out in the Protocol have been used. This legal delimitation does not, however, mean that a person smuggled illegally is free from vulnerability. Europol highlights the existence of connections between the two phenomena, showing that,

¹⁴Frontex, Common Integrated Risk Analysis Model 2.1 (CIRAM 2.1), Warsaw, 2021.

¹⁵Protocol against the Smuggling of Migrants by Land, Sea and Air, Art. 3(a), New York, 15 November 2000, ratified by Romania through Law No. 565/2002.

¹⁶Protocol to Prevent, Suppress and Punish Trafficking in Persons, Art. 3(a), New York, November 15, 2000.

particularly in the case of long and costly journeys, migrants may end up being exploited to pay off debts accumulated in connection with facilitation services.¹⁷ Specialized literature confirms that the relatively clear legal distinction between the two offences becomes much more difficult to apply in certain concrete situations. Roxane de Massol de Rebetz describes the existence of a “grey zone” at the intersection of migrant smuggling and human trafficking, in which consent, vulnerability, debt, abuse and exploitation may overlap over the course of the same journey, with persons who voluntarily begin their journey later ending up in situations of exploitation.¹⁸ From a border-control perspective, this zone of convergence requires an assessment of the individual context of the journey, since the apparently voluntary nature of the movement or the existence of valid documents does not, in itself, exclude the presence of elements of coercion, deception or exploitation.

More recent research also examines the convergence between the two phenomena in regional contexts in which the same vulnerability factors and the same organized crime structures can connect the facilitation of illegal migration with the exploitation of persons.¹⁹ These findings are also relevant to the analysis of how AI could amplify the risk of a shift from the consensual relationship specific to migrant smuggling toward forms of exploitation specific to human trafficking, since the same tools for personalizing communication and building credibility can be used in both contexts, even though the legal classification of the activity remains different.

3. From Existing Digital Infrastructure to the Integration of AI

The traditional model, based mainly on direct contact with local intermediaries and physical coordination of transport, no longer reflects the full diversity of current modes of operation. The digital environment enables remote coordination, the distribution of tasks among persons located in different states, and the conduct of certain components of the activity without direct contact²⁰. Europol shows that digital tools are used at various stages of migrant smuggling, from promoting routes and prices and communicating with migrants, to providing travel instructions and producing counterfeit documents, with leaders coordinating activities without being present along the route, intermediaries managing recruitment,

¹⁷Europol, Tackling Threats..., *op. cit.*, p. 6.

¹⁸Roxane de Massol de Rebetz, „How Useful Is the Concept of Transit Migration...”, *European Journal on Criminal Policy and Research*, vol. 27, 2021, pp. 48-49.

¹⁹Concepción Anguita-Olmedo, „The Convergence of Trafficking and Migrant Smuggling in West Africa: Migration Pressure Factors and Criminal Actors”, *Social Sciences*, vol. 14, no. 8, 2025, art. 447.

²⁰Europol, *Criminal Networks in Migrant Smuggling*, *op. cit.*, pp. 3, 5.

logistics and payments, and other persons providing transport, supplying false documents or offering other forms of specialized support.²¹ A 2025 qualitative study shows that facilitators actively use social media platforms to communicate with migrants, while the use of encrypted communications represents a growing difficulty for law enforcement authorities.²² Networks also run sophisticated, professional online campaigns to recruit drivers to carry out transport, providing information on working conditions, pay, vehicle insurance and the support promised in the event of detection by the authorities.²³

Earlier research has also shown that the online environment facilitates the identification of and contact with facilitators and allows migrants to compare information on costs, routes, destinations and reputations, effectively turning the decision to use a facilitator into an informed process, supported by reviews and recommendations similar to those found in legitimate e-commerce.²⁴ Contacting persons interested in the facilitation of illegal border crossing is no longer confined to the communities or geographic locations in which intermediaries operate, and different components of the activity can be coordinated remotely and distributed among persons with distinct roles, thereby extending the geographic range in which networks can effectively operate.

This change is also recognized at the European institutional level. In 2024, Europol and the European Commission supported the development of a European network of experts capable of making more effective use of information obtained from the online environment, a direction given concrete form through DigiNeX, the network of digital investigators aimed at monitoring open sources and detecting and analyzing online activities associated with migrant smuggling.²⁵ Within the first joint actions carried out by DigiNeX in October 2025, investigations focused on identifying suspects' digital fingerprints, mapping the links between the persons involved, and locating points relevant to investigations; the results presented by Europol in December 2025 included 160 social media accounts associated with migrant smuggling activities, which were assessed and

²¹Europol, *Criminal Networks in Migrant Smuggling*, *op. cit.*, pp. 2-6.

²²Özlem Özdemir, Bülent Baykal, Elif Başak Sarıoğlu, „The Use of Social Media in Irregular Migration and Migrant Smuggling: A Qualitative Study in Türkiye”, *Journal of Borderlands Studies*, vol. 40, no. 6, 2025, pp. 1497-1519.

²³ Europol, *Tackling Threats...*, *op. cit.*, p. 12.

²⁴ Parisa Diba, Georgios Papanicolaou, Georgios A. Antonopoulos, „The Digital Routes of Human Smuggling? Evidence from the UK”, *Crime Prevention and Community Safety*, vol. 21, 2019, pp. 159-175.

²⁵ Europol, „New Network to Target Migrant Smugglers in the Digital Domain”, May 3, 2024.

referred to the platforms concerned for appropriate action to be taken.²⁶ INTERPOL identifies a similar trend, showing that social networks facilitate contact and the exchange of information between migrants and facilitators, while instant messaging applications and real-time geolocation technologies simplify the planning and execution of journeys.²⁷

As a result, combating migrant smuggling can no longer be addressed solely in relation to the physical border; from an investigative perspective, part of the relevant activity takes place before the migrant actually reaches the border, in the digital environment where services are promoted, negotiated and coordinated. Overall, these developments show that the integration of artificial intelligence into migrant smuggling does not start from an environment devoid of technological infrastructure. Social media platforms, encrypted communications, navigation tools, digital payment services and information flows are already present in various components of the criminal activity, and AI can be integrated into this already existing infrastructure, contributing to the amplification or automation of functions previously performed by digital means.

4. Artificial Intelligence in the Dynamics of Migrant Smuggling: The 5F-AI Model

To systematize the ways in which artificial intelligence can alter the activity of networks involved in migrant smuggling, the article proposes an analytical model based on five functions (5F-AI): expansion, identification, interaction, concealment and amplification. These functions do not necessarily represent sequential stages; rather, they may overlap and occur at different points in the criminal activity, depending on the network's technical resources and level of sophistication.

The model is analytical rather than exhaustive or purely descriptive: its purpose is not to document individual cases of AI use, but to provide a common conceptual framework applicable both to threat analysis and to the construction of coherent institutional responses. Each of the five functions is examined below with reference to its level of available documentation, confirmed practice, emerging trend or prospective risk, so as to avoid presenting technical possibilities as established facts.

4.1. Expansion - Extending Reach in the Digital Environment

The first function concerns the extension of reach. Generative AI can rapidly produce content in the form of text, images, audio and video, and the development of multilingual capabilities allows communication to be

²⁶ Europol, „Firm Stand against Migrant Smuggling: Global Alliance Convened in Brussels”, December 12, 2025.

²⁷ INTERPOL, Project CCISOM: New Technologies - Cyber Challenges in Smuggling of Migrants and Human Trafficking.

adapted to different linguistic and cultural groups.²⁸ By reducing these barriers, AI tools can significantly extend the capacity of groups involved in migrant smuggling to reach persons and communities that were previously harder to access. In the field of human trafficking, OSCE already warns that AI can amplify the phenomenon's reach and complexity, which calls for coordinated responses at the national, regional and international levels. Automatically transferring these conclusions to migrant smuggling would, however, be unwarranted. The possibilities offered by these technologies are nonetheless also relevant in this field, and Europol explicitly shows that AI applications can create new opportunities for attracting persons interested in illegal border crossing, including through disinformation campaigns and the use of deepfake technology, which can lead a larger number of people to turn to facilitators²⁹. Consequently, automated, multilingual and personalized content generation can extend the reach of groups involved in migrant smuggling and their capacity to reach broader categories of persons.

4.2. Identification - Identifying and Selecting Target Groups

The second function concerns the identification and selection of categories of persons online, without necessarily involving the construction of an individual profile for each person. In the field of human trafficking, OSCE describes, as an emerging risk, the possibility of automating the identification of potential victims through the use of AI agents configured to browse social networks and initiate interactions, as well as the possibility of scaling up such activities.³⁰ By functional analogy, in migrant smuggling, analysis of the language used, participation in certain online communities, interest in certain routes, and other publicly available information could enable groups to target their messages toward categories of persons more likely to be interested in the facilitation of illegal border crossing. Such a scenario must currently be treated as an emerging risk, not as a systematically documented practice in migrant smuggling. The technological relevance of this possibility is, however, confirmed by developments observed in other criminal activities carried out in the digital environment: Europol shows that the use of generative AI enables the personalization of messages and the targeting of a very large number of people at high speed.³¹ The difference from conventional digital promotion therefore lies in the ability to select and prioritize communities, languages, themes and categories of interest, and subsequently to adapt messages accordingly.

²⁸ OSCE/Bali Process, New Frontiers..., *op. cit.*, pp. 6, 11-12, 16-19.

²⁹ Europol, Tackling Threats..., *op. cit.*, p. 13.

³⁰ OSCE/Bali Process, *op. cit.*, pp. 13, 16-17.

³¹ Europol, IOCTA 2026, Luxembourg, 2026, p. 17.

4.3. Interaction - Building Credibility Online

The relationship between migrant and facilitator is strongly influenced by the level of trust between the two parties. In the absence of formal mechanisms to guarantee that agreements will be honoured, the relationship is marked by uncertainty and an information imbalance, which increases the importance of trust and reputation in choosing a facilitator.³² Generative AI can influence precisely this dimension of the relationship: conversational assistants, machine translation adapted to cultural context, the generation of images and video materials, and voice synthesis and cloning can contribute to building digital identities and seemingly credible interactions, including between persons who do not speak the same language.³³ Deepfake technologies and synthetic identities can amplify the potential for deception. Europol assessments of biometric system vulnerabilities highlight the possibility of using them to present a person under a different identity or to avoid identification, including in remote verification processes.³⁴ In the specific field of migrant smuggling, Europol explicitly identifies the possibility that AI applications may be used to attract persons interested in illegal border crossing, showing that disinformation and deepfakes can help mobilize migrants in an irregular situation and increase demand for the services offered by facilitators.³⁵ This assessment does not demonstrate the existence of systematic use of deepfakes in migrant smuggling, but it shifts the analysis from a purely abstract technical possibility to an operational risk explicitly identified by Europol. Within the 5F-AI model, the Interaction function thus denotes the use of AI to strengthen the credibility of a message, personalize interaction, and lower the trust barriers between the facilitator and the targeted person, regardless of whether the means used consist of machine translation, visual content generation or voice synthesis.

4.4. Concealment - Hindering Detection of Digital Activity

The fourth function concerns the capacity to adapt digital content in an environment in which authorities and online platforms identify and remove accounts or materials associated with the promotion of migrant smuggling activities. Generative AI enables the large-scale production of synthetic content and the automation of activities that previously required human intervention, which can facilitate the repeated alteration of wording,

³² Paolo Campana, Loraine Gelsthorpe, „Choosing a Smuggler: Decision-making Amongst Migrants Smuggled to Europe”, *European Journal on Criminal Policy and Research*, vol. 27, 2021, pp. 9-13.

³³ OSCE/Bali Process, *op. cit.*, pp. 13, 16-19.

³⁴ Europol, *Biometric Vulnerabilities...*, *op. cit.*, pp. 39-41.

³⁵ Europol, *Tackling Threats...*, *op. cit.*, p. 13.

images or the style of messages.³⁶ In the case of other criminal activities carried out in the digital environment, the accessibility of these technologies is already associated with additional difficulties in identifying content and the persons generating it. In the case of migrant smuggling, the use of AI for this purpose must currently be treated as an emerging risk, not as a systematically documented practice. From an operational standpoint, the ability to rapidly generate variants of the same content can reduce the effectiveness of mechanisms based solely on the recognition of known terms, images or patterns. The relevance of this challenge is also recognized at the political level. The action plan adopted by the G7 interior and security ministers in October 2024 calls for cooperation with social media platforms to monitor and remove content promoting migrant-smuggling-related services and explicitly recommends the use of new technologies, including AI tools, for the rapid removal of online activities through which facilitators promote illegal migration.³⁷ Within the 5F-AI model, Concealment does not denote the achievement of anonymity, but rather the potential capacity to rapidly adapt digital presence and content in order to hinder identification and sustain online activity.

4.5. Amplification - Scaling and Automating Activities

The final function concerns the possibility of expanding the volume and pace of activities carried out with the support of AI. Its effect does not necessarily stem from the emergence of entirely new criminal methods, but from the capacity to automate, reproduce and rapidly adapt practices that already exist, reducing the time and resources needed to carry them out. Operationally, generative tools can enable the simultaneous management of a larger number of interactions, the rapid production and adaptation of content in multiple languages, the synthesis of large volumes of information, and the automation of repetitive communication tasks.³⁸ Through these mechanisms, activities that previously required more extensive human involvement can be carried out with significantly greater capacity and speed. In its 2026 analysis of cybercrime, Europol notes that the growing accessibility of AI tools lowers barriers to entry and allows criminals to expand their activities more effectively, increasing their speed, efficiency and reach.³⁹ Within the 5F-AI model, the Amplification function thus denotes AI's capacity to extend and accelerate practices that already exist, not to generate fundamentally new forms of criminality.

³⁶ Europol, „Firm Stand against Migrant Smuggling”, December 12, 2025.

³⁷ G7 Interior and Security Ministers, Action Plan to Prevent and Counter the Smuggling of Migrants, October 2024.

³⁸ OSCE/Bali Process, *op. cit.*, pp. 11-12, 16-19.

³⁹ Europol, IOCTA 2026, Luxembourg, 2026, p. 14.

The five functions of the 5F-AI model should not be interpreted in isolation: expanding reach facilitates the identification of larger target groups; identification supports the personalization of interaction; interaction strengthens the credibility needed to sustain the activity; concealment protects the continuity of digital presence; and amplification links all of these functions into a cycle that can sustain and expand itself over time, as the network accumulates operational experience in using AI tools.

5. Document Fraud and Digital Identity

Document fraud has long been one of the tools used to facilitate illegal migration, and its digital dimension is becoming increasingly evident. In 2026, Europol documented the existence of an online platform supplying forged identity and administrative documents, in both physical and digital formats, used to facilitate migrant smuggling, evade border checks and support secondary movements within the European Union.⁴⁰ The development of generative AI adds a new dimension to this problem: current tools allow the production and manipulation of highly realistic images, including the generation of synthetic faces, the alteration of a person's features, or the creation of deepfakes, technologies that can be used to present a person under a false identity and to compromise biometric verification processes.⁴¹

This development calls for further reflection on how border authorities cooperate with structures specialized in combating document fraud, given that generative technologies lower the technical skill threshold needed to produce high-quality forged documents. The implication for border management therefore goes beyond the simple verification of a travel document's authenticity. As digital identities and materials become increasingly difficult to distinguish from authentic ones, verification of the document presented must be cross-checked with other relevant elements of the journey and with information available in authorized systems. Europol recommends an integrated approach to the biometric identification process, from the initial registration of data to identity verification, in order to reduce exploitable vulnerabilities.⁴² This development calls for more rigorous checks, but does not justify automatically interpreting every discrepancy as an indication of fraud.

⁴⁰ Europol, „Fake Document Factory Dismantled in Spain: Around 800 IDs Seized”, 4 June 2026.

⁴¹ Europol, Biometric Vulnerabilities: Ensuring Future Law Enforcement Preparedness, Europol Innovation Lab Observatory Report, Luxembourg, 2025, DOI: 10.2813/8081090, pp. 39-41.

⁴² Europol, Biometric Vulnerabilities..., *op. cit.*, pp. 10-11, 55.

6. Using Artificial Intelligence to Combat Migrant Smuggling: From Information Overload to Stronger Analytical Capacity

The same technologies that can amplify migrant smuggling activities can, conversely, provide important tools for law enforcement authorities. One of the current problems facing investigations is not a lack of information, but the volume, diversity and speed at which it must be analyzed. A cross-border investigation may involve processing a considerable volume of messages, data extracted from electronic devices, images, transactions, and information concerning persons, locations and the relationships between them. Europol shows that AI can support the analysis of such data volumes by classifying and filtering information, identifying patterns and connections, extracting relevant elements, and automatically translating communications into multiple languages.⁴³ The applicability of these technologies to border management is no longer purely theoretical. EU-funded research projects have already tested the use of AI in maritime surveillance: COMPASS2020 used AI-assisted surveillance systems to improve operational situational awareness, EFFECTOR focused on supporting decision-making in maritime surveillance, and PROMENADE developed automated solutions for vessel tracking and anomaly detection.⁴⁴

Risk analysis is of particular importance. Frontex anticipates the strengthening of intelligence-led activities and risk profiling in border management, alongside the expanding use of biometrics and AI.⁴⁵ The use of such tools can facilitate the aggregation and prioritization of indicators, but the distinction between identifying a risk and formulating a conclusion about the person assessed must be maintained. Europol draws attention to the risk of excessive reliance on the results produced by automated systems and to the possibility of unwarranted suspicions arising when these tools are used outside the purpose for which they were designed.⁴⁶ Such a process does not transfer decision-making authority to automated systems, but rather uses AI to manage information volume and support analytical work.

The expanding use of biometrics also raises questions regarding the interoperability of existing European systems, such as EURODAC and the Entry/Exit System (EES), with any AI-assisted analysis tools developed at the national level, so that data correlation complies with both the technical

⁴³ Europol, AI and Policing: The Benefits and Challenges of Artificial Intelligence for Law Enforcement, Europol Innovation Lab, Luxembourg, 2024, DOI: 10.2813/0321023, pp. 11-12, 16-21.

⁴⁴ European Commission - CORDIS, Counteracting Migrant Smuggling: A Multifaceted Approach to Fight Migrant Smuggling, Results Pack, 22 November 2024.

⁴⁵ Frontex, Strategic Risk Analysis Report 2024, Warsaw, 2024, pp. 27, 47-48.

⁴⁶ Europol, AI Bias in Law Enforcement - A Practical Guide, Europol Innovation Lab, 2025, pp. 18-19, 25.

requirements of interoperability and the legal limits on the purpose for which each dataset was originally collected.

This technical interoperability cannot, however, replace genuine institutional cooperation: AI-assisted analysis tools produce operational value only to the extent that the structures using them have a clear mandate, common working procedures, and functional channels for exchanging results with the other institutions involved in the decision-making chain, from the initial detection of a risk to the concrete measure applied by the competent authority.

These functions can be integrated into a possible operational cycle for the use of AI in support of combating migrant smuggling, structured around five stages: (1) Detection - identifying relevant signals within a large volume of information; (2) Correlation - establishing links between apparently disparate pieces of information; (3) Prioritization - directing resources toward information with high operational value; (4) Intervention - the decision on and application of measures by the competent authorities, in accordance with the law; (5) Learning and Adaptation - incorporating operational results to improve analysis and reduce errors. This cycle allows each intervention to feed subsequent rounds of analysis, without the final decision ever being automatically delegated to the system.

7. Legal Limits on the Use of Artificial Intelligence in Border Management

Regulation (EU) 2024/1689 on artificial intelligence establishes a framework directly relevant to the use of such systems in the field of migration, asylum and border management. Certain systems intended to assess the risks posed by persons entering the territory of a member state, to assist in the examination of applications for asylum, visas or residence, and to detect, recognize or identify persons in this context are classified as high-risk systems.⁴⁷ The Regulation pays particular attention to the accuracy, non-discriminatory nature and transparency of these systems, given the impact their use may have on the rights of the persons concerned. At the same time, high-risk systems must be designed so that they can be effectively overseen by natural persons, and the results they produce must be capable of being interpreted and, where necessary, disregarded, modified or reversed. The Regulation also draws attention to the risk of automatic or excessive reliance on the results generated by these systems.⁴⁸ From a border-management perspective, the implication is clear: the output of an AI system can guide analysis or trigger additional checks, but it cannot substitute for the legal conditions required for taking a decision or measure concerning the person assessed. The use of the technology must therefore be

⁴⁷ Regulation (EU) 2024/1689, Art. 6(2), Annex III(7) and Recital (60).

⁴⁸ Regulation (EU) 2024/1689, Art. 14(1) and (4)(b)-(d).

assessed both in terms of operational efficiency and in terms of the possibility of verifying and justifying the result obtained.

The Regulation also imposes specific governance obligations on operators of high-risk systems, including conducting a fundamental-rights impact assessment before deployment, keeping activity logs that allow the traceability of AI-assisted decisions, and establishing effective human-oversight mechanisms capable of identifying and correcting the system's systemic errors.

For national authorities with responsibilities in border management, these requirements are not merely additional administrative constraints, but a mandatory framework for any future strategy for integrating artificial intelligence. The design of decision-support tools must include, from the design stage onward, mechanisms for human oversight, documentation and verification of results, not merely the technical component of data analysis.

8. Relevance for Romania Following Full Integration into the Schengen Area

The analysis of how AI can influence migrant smuggling cannot be separated from the specific context in which Romania exercises its responsibilities as a member state with an external border of the Schengen area, a context that heightens the stakes of the accuracy and timeliness of the information available to national authorities.

Romania's full integration into the Schengen area also changes the context in which illegal migration and migrant smuggling must be analyzed. As of 1 January 2025, checks on persons at Romania's internal land borders were eliminated.⁴⁹ This change does not diminish the importance of combating cross-border crime; rather, it increases the importance of risk analysis, information exchange, police cooperation and activities carried out at the external border and within the territory. Data from the Romanian Border Police for 2025 show a decrease of approximately 78% in the number of persons detected during illegal crossings compared with the previous year, while 188 migrant smuggling offences were recorded during the same period.⁵⁰ A decrease in detections cannot automatically be equated with the disappearance of the threat, particularly since significant recruitment, communication and coordination activities already take place in the digital environment. In this context, AI's relevance for Romania must primarily be assessed in relation to the capacity to make use of available information: integrating analysis of the digital environment with operational analysis, the investigation of migrant smuggling and international cooperation can enable the early identification of connections that cannot be

⁴⁹ Council of the European Union, „Schengen: Council decides to lift land border controls with Bulgaria and Romania”, December 12, 2024.

⁵⁰ Romanian Border Police, „Annual Report of the Border Police for 2025”, March 3, 2026.

revealed solely through physical border control. For Romania, the challenge lies not only in adapting the control apparatus, but also in strengthening analytical capacity, so that available information can be effectively correlated and used in a context in which cross-border crime is increasingly connected to the digital environment.

Romania's particular position, as a state located on the European Union's external border and along active transit routes, combined with the elimination of systematic checks at internal borders, requires a rebalancing of the relationship between physical control and intelligence analysis, through the progressive strengthening of the latter's role. Other states that have recently undergone a similar process of eliminating systematic checks at internal borders offer useful benchmarks for anticipating possible developments: their experience shows that the absence of systematic physical control does not reduce pressure from illegal migration, but only its immediate visibility, shifting the centre of gravity of detection from the border toward intelligence-based risk analysis and cross-border operational cooperation.

In this context, strengthening national capacity to analyze the digital environment, in conjunction with tools already developed at the European level, such as the DigiNeX network or projects like COMPASS2020, EFFECTOR and PROMENADE, can serve as a concrete means by which Romania can compensate, at the intelligence level, for the reduced physical visibility of the illegal-migration phenomenon resulting from its Schengen status.

This direction, in turn, requires clear inter-institutional coordination among the structures responsible for border management, combating organized crime and international cooperation, so that information originating from the digital environment can be coherently integrated into the decision-making process, without remaining fragmented among institutions that, at present, largely act independently of one another.

CONCLUSIONS

The increasingly extensive integration of digital technologies into migrant smuggling activities is already well documented, whereas the use of artificial intelligence in this context is still emerging. This distinction is essential for interpreting the phenomenon: technological possibility must not be conflated with the existence of widespread and consistently documented use.

The analysis carried out supports the hypothesis that artificial intelligence does not generate a distinct form of the offence of migrant smuggling, but can amplify and automate practices that already exist. The proposed analytical model highlights precisely the functions in relation to which this influence may become relevant, from extending reach and

personalizing interactions to adapting digital presence and increasing the volume of activities.

The three-level distinction, documented practices, emerging trends and prospective risks, used throughout the study remains relevant for future research in this field as well: as more operational data on the actual use of AI by migrant smuggling networks become available, some of the risks discussed here as emerging may be confirmed as widespread practices or, conversely, shown not to have materialised at scale.

This same transformation, however, also offers authorities the opportunity to make more effective use of large and heterogeneous volumes of information. The value of AI thus derives mainly from its capacity to support analysis when the volume and complexity of information make it difficult to quickly identify relevant elements. At the same time, the use of these tools in border management cannot be separated from legal limits, the protection of fundamental rights, and the need to verify automatically generated results. Technology can flag an anomaly, a connection or a risk, but its significance must be established by reference to context and the information available.

For Romania, full integration into the Schengen area makes this development all the more relevant. The reduced role of systematic control at internal borders, coupled with the persistence of risks associated with cross-border crime, increases the importance of risk analysis, international cooperation and the use of information from the digital environment. In these circumstances, the main challenge is not the adoption of artificial intelligence as an end in itself, but its integration into a border-management model capable of harnessing the technological advantages without turning algorithmic assessment into a substitute for professional analysis and legal accountability.

A relevant direction for future research lies in the empirical validation of the model through qualitative methods that complement documentary analysis, for example through interviews or focus groups with practitioners in border management, the fight against cross-border crime, particularly migrant smuggling, and European cooperation, who, through their direct operational experience, can validate, refine or challenge the functions proposed by the 5F-AI model and their practical relevance to the specific Romanian context.

Such empirical validation would also make it possible to transform the 5F-AI model from an analytical framework into a foundation for building a national inter-agency strategy in response to the digital and technological dimension of migrant smuggling, adapted to Romania's particular characteristics as a state on the external border of the Schengen area. In our view, this perspective opens up a natural direction for continuing the present research.

Ultimately, the effectiveness of using artificial intelligence in border management will depend on institutions' ability to turn technological advantage into genuine operational advantage, without diminishing human oversight, legal accountability or the protection of fundamental rights.



BIBLIOGRAPHY:

1. Scholarly Works and Articles

- ANGUITA-OLMEDO, Concepción, „The Convergence of Trafficking and Migrant Smuggling in West Africa: Migration Pressure Factors and Criminal Actors”, *Social Sciences*, vol. 14, no. 8, 2025, art. 447, DOI: 10.3390/socsci14080447.
- BOWEN, Glenn A., „Document Analysis as a Qualitative Research Method”, *Qualitative Research Journal*, vol. 9, no. 2, 2009, pp. 27-40, DOI: 10.3316/QRJ0902027.
- CAMPANA, Paolo, „Human Smuggling: Structure and Mechanisms”, *Crime and Justice*, vol. 49, 2020, pp. 471-519, DOI: 10.1086/708663.
- CAMPANA, Paolo; GELSTHORPE, Loraine, „Choosing a Smuggler: Decision-making Amongst Migrants Smuggled to Europe”, *European Journal on Criminal Policy and Research*, vol. 27, 2021, DOI: 10.1007/s10610-020-09459-y.
- DE MASSOL DE REBETZ, Roxane, „How Useful Is the Concept of Transit Migration in an Intra-Schengen Mobility Context? Diving into the Migrant Smuggling and Human Trafficking Nexus in Search for Answers”, *European Journal on Criminal Policy and Research*, vol. 27, 2021, pp. 41-63, DOI: 10.1007/s10610-020-09467-y.
- DEKKER, Rianne; ENGBERSEN, Godfried, „How Social Media Transform Migrant Networks and Facilitate Migration”, *Global Networks*, vol. 14, no. 4, 2014, pp. 401-418, DOI: 10.1111/glob.12040.
- DIBA, Parisa; PAPANICOLAOU, Georgios; ANTONOPOULOS, Georgios A., „The Digital Routes of Human Smuggling? Evidence from the UK”, *Crime Prevention and Community Safety*, vol. 21, 2019, pp. 159-175, DOI: 10.1057/s41300-019-00060-y.
- LEVESQUE, Joel, „The AI-Enhanced Trafficking Threat: Examining the Technological Evolution of Trafficking in Persons Operations with AI Tools”, *Journal of Human Trafficking*, 2025, DOI: 10.1080/23322705.2025.2572911.

- OUBAD, Ismail; GHAFARI, Rassa, „The Digital Infrastructures of Illegal Border Crossings: Solidarity Actors and Networks in the Arabic and Persian Speaking Virtual Spheres”, *Critical Criminology*, vol. 33, 2025, pp. 71-88, DOI: 10.1007/s10612-025-09824-5.
- ÖZDEMİR, Özlem; BAYKAL, Bülent; SARIOĞLU, Elif Başak, „The Use of Social Media in Irregular Migration and Migrant Smuggling: A Qualitative Study in Türkiye”, *Journal of Borderlands Studies*, vol. 40, no. 6, 2025, pp. 1497-1519, DOI: 10.1080/08865655.2025.2504880.

2. Documents and Reports of International Organizations and Institutions

- European Border and Coast Guard Agency (Frontex), *Common Integrated Risk Analysis Model 2.1 (CIRAM 2.1)*, Warsaw, 2021.
- European Border and Coast Guard Agency (Frontex), *Strategic Risk Analysis Report 2024*, Warsaw, 2024.
- Europol, *Criminal Networks in Migrant Smuggling*, Europol Spotlight Report, Luxembourg, 2023, DOI: 10.2813/550319.
- Europol, *Tackling Threats, Addressing Challenges - Europol's Response to Migrant Smuggling and Trafficking in Human Beings in 2023 and Onwards*, Luxembourg, 2024, DOI: 10.2813/203212.
- Europol, *AI and Policing: The Benefits and Challenges of Artificial Intelligence for Law Enforcement*, Europol Innovation Lab, Luxembourg, 2024, DOI: 10.2813/0321023.
- Europol, *The Changing DNA of Serious and Organised Crime - EU-SOCTA 2025*, Luxembourg, 2025.
- Europol, *Biometric Vulnerabilities: Ensuring Future Law Enforcement Preparedness*, Europol Innovation Lab Observatory Report, Luxembourg, 2025, DOI: 10.2813/8081090.
- Europol, *AI Bias in Law Enforcement - A Practical Guide*, Europol Innovation Lab, 2025.
- Europol, *IOCTA 2026 - The Evolving Threat Landscape: How Encryption, Proxies and AI Are Expanding Cybercrime*, Luxembourg, 2026.
- G7 Interior and Security Ministers, *Action Plan to Prevent and Counter the Smuggling of Migrants*, Mirabella Eclano, 2-4 October 2024.
- INTERPOL, *Project CCISOM: New Technologies - Cyber Challenges in Smuggling of Migrants and Human Trafficking*.
- OSCE Office of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings; Regional Support Office of the Bali Process, *New Frontiers: The Use of Generative Artificial Intelligence to Facilitate Trafficking in Persons*, Policy Brief, 2024, ISBN 978-3-903128-81-1.
- United Nations Office on Drugs and Crime (UNODC), *Trafficking in Persons & Smuggling of Migrants - Module 11*:

Differences and Commonalities, Education for Justice
University Module Series.

United Nations Office on Drugs and Crime (UNODC), Legislative and
Policy Solutions to Emerging Issues Related to the Smuggling
of Migrants, document CTOC/COP/WG.7/2025/3, 5 August
2025.

3. Institutional Documents and Communications

Council of the European Union, „Schengen: Council Decides to Lift Land
Border Controls with Bulgaria and Romania”, 12 December
2024.

European Commission - CORDIS, Counteracting Migrant Smuggling: A
Multifaceted Approach to Fight Migrant Smuggling, Results
Pack, 22 November 2024.

Europol, „New Network to Target Migrant Smugglers in the Digital
Domain”, 3 May 2024.

Europol, „Firm Stand against Migrant Smuggling: Global Alliance
Convened in Brussels”, 12 December 2025.

Europol, „The Grip on Migrant Smuggling Tightens: New Department at
Europol to Step Up the Fight”, 24 March 2026.

Europol, „Fake Document Factory Dismantled in Spain: Around 800 IDs
Seized”, 4 June 2026.

Romanian Border Police, „Annual Report of the Romanian Border Police
for 2025”, 3 March 2026.

4. Legal Instruments and International Legal Acts

Protocol against the Smuggling of Migrants by Land, Sea and Air,
supplementing the United Nations Convention against
Transnational Organized Crime, New York, 15 November 2000,
ratified by Romania through Law No. 565/2002.

Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially
Women and Children, New York, 15 November 2000, ratified
by Romania through Law No. 565/2002.

Regulation (EU) 2024/1689 of the European Parliament and of the Council
of 13 June 2024 laying down harmonised rules on artificial
intelligence (Artificial Intelligence Act).

Directive (EU) 2024/1712 of the European Parliament and of the Council of
13 June 2024 amending Directive 2011/36/EU on preventing and
combating trafficking in human beings.

