

## **Artificial Intelligence Innovations in Law Enforcement Training: CEPOL Strategy 23-27**



Maria Joao Guia

PhD, research & knowledge
management officer, invited
professor, researcher
CEPOL – European Union for
Law Enforcement Training,
Universidade Autonoma de
Lisboa, Portugal,
Universidade de Coimbra
maria.guia@cepol.europa.eu



Ioan-Cosmin Mihai
PhD, supervisor, associate
professor
CEPOL – European Union for
Law Enforcement Training,
Alexandru Ioan Cuza Police
Academy, Romania
ioan-cosmin.mihai@cepol.
europa.eu





Marzena Kordaczuk-Wąs
PhD, senior training officer, expert

CEPOL – European Union for Law Enforcement Training, Collegium Civitas, Poland marzena.kordaczuk-was@cepol.europa.eu



#### Abstract

Aim: The paper examines the role of artificial intelligence (AI) in law enforcement training and highlights the benefits and challenges associated with its use. AI in training can provide law enforcement officials with real-time, customised feedback on their performance, which can help them improve their skills and knowledge. However, the use of AI in law enforcement training also raises several challenges, such as ethical concerns related to the use of personal data and potential biases in AI algorithms. Therefore, it is crucial to effectively prepare law enforcement personnel to utilise AI to its full potential while minimising potential harm.

**Methodology:** The paper also explores the new digital strategy of the European Union Agency for Law Enforcement Training (CEPOL) and how it incorporates

The manuscript was submitted in English. Received: 24 July 2025. Revised: 30 July 2025. Accepted: 16 August 2025.

AI technology into its training programmes to equip law enforcement authorities with the most up-to-date knowledge and skills. Additionally, the paper underscores the importance of research and science in identifying and developing new AI advancements and best practices.

**Findings:** Finally, this article presents the identified gaps in digital skills and the use of new technologies in law enforcement training.

Value: CEPOL periodically collects data to define strategic training priorities for law enforcement officials, emphasising digital skills and the use of new technologies. The need to increase the knowledge of law enforcement representatives on the rules of responsibility for artificial intelligence in the field of internal security remains a constant priority accompanying the development of technologies used in the work of law enforcement authorities.

**Keywords:** artificial intelligence, law enforcement, training innovations, digital skills, new technologies, training activities, skills gap, CEPOL strategy 23-27

### Artificial Intelligence benefits for law enforcement

Traditional training skills and knowledge dissemination tools are facing the most substantial challenges of the current times: Artificial Intelligence (AI) is shaking the structures of our society in all kinds of actions, including learning. Beyond all the new emerging technologies applied to learning, such as federated learning (Poushter, et al., 2016), allowing "the central server to train an excellent global model (...) avoiding sharing local private data." (Zhu & Jin, 2018). AI appears as the new generation transforming tool, with the introduced concept of the anthropomorphic machine learning by Angelov and Gu (2018), where machines show their capacity to learn as humans do through techniques such as deep learning neural networks, with some ongoing discussed limitations. The European Union as a whole, in its voice of Member States, must be prepared to profit from the benefits of this new tool, exercising its critical spirit to identify the potential harms from this instrument applied to learning and training. Three main challenges have been identified in the EC Communication on Artificial Intelligence for Europe¹ on this matter: the first one relates to "prepar[ing] the

<sup>1</sup> Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Artificial Intelligence for Europe {SWD (2018) 137 final}. Brussels, 25.4.2018 COM (2018) 237 final (2018).

society as a whole" (Lunhol & Torhalo, 2024) into digital skills in a current war time that has been impoverishing the Member States overall societies (increase of inflation rates, consequent cost of life, rise of the interest rates and the difficulty of facing daily economic obligations, etc). Implementing a comprehensive digitalization programme 2021-2027 (URL1) during the current exigent commitment times to allow citizens to extract the best possible potentials of this tool is burdensome (yet not impossible). The second focuses on the changing shape of the working pattern (URL2) that we are used to, obliging us to envisage a complete turn-off of industrialisation. The new "intelligenciation" era is already on the table, and we must quickly evolve and make the best of it while transforming this change into a brand-new professional adaptation without risking our European citizens to jeopardize their acquired social rights. The third one refers to the need to implement Train the Trainers on AI to cascade the quick adaptation needed and hence attract new investments by the new talented experts.

AI can change law enforcement by delivering investigative, crime prevention, and public safety-enhancing tools and tactics (Rademacher, 2020). Some additional advantages of AI in law enforcement are enhanced speed and efficacy, improved awareness, predictive analytics, enhanced investigative methods, increased public security, and cost savings (Hayward & Maas, 2020). On a first reflection, we would name the *improved speed and efficacy*. AI is capable of processing enormous quantities of data and information fast and precisely (Chubb, Cowling & Reed, 2022). This can assist law enforcement authorities in swiftly identifying patterns and trends pertinent to a specific case or investigation.

AI can also automate mundane jobs such as data entry and analysis, allowing law enforcement officials to focus on more challenging duties. Secondly, it would also *improve awareness* since AI can monitor and analyse real-time data from various sources (Zhu, et al, 2021), including surveillance cameras, sensors, and social media. This can aid law enforcement officials in gaining a deeper understanding of a specific place or scenario, allowing them to respond more effectively to emergencies and other occurrences. AI can also be utilised as *predictive analytics*, examining data and forecasting future events. Using

The amount of information Law Enforcement (LE) institutions have to deal with has increased due to the use of the Internet and digital tools. In order to ensure successful investigations and effective crime prevention and to keep up with the increasingly complex and sophisticated methods used by criminals, LE need to acquire a high level of skills in the technological domain while often facing restrictions concerning financial and personal resources. LE institutions are expected to act efficiently in a rapidly changing and evolving technological landscape, and that creates challenges for training as institutions have heavy and long administrative procedures and are mostly running behind the way. We should also be aware that whilst digital technologies clearly generate new opportunities, they also pose new threats and increase certain risk of bias and discrimination.

historical crime data and other criteria, AI can predict the chance of specific types of crimes occurring in a particular place. This can assist law enforcement agencies in distributing their resources more efficiently and concentrating their efforts where they are most needed. In what concerns *enhanced investigative methods*, AI can analyse enormous amounts of data and identify patterns that may not be evident to human investigators (Lotfi & Bouhadi, 2022). This can aid law enforcement authorities in identifying suspects, locating new leads, and solving complicated cases. AI can also evaluate audio and video recordings to assist with suspect identification and evidence collection. Reflecting on the potential increased public security(Gesk & Leyer, 2022), public areas, such as parks, transportation networks, and events, can be monitored with AI to detect potential threats and improve public safety. AI can be used, for instance, to detect suspicious conduct, identify lost or missing individuals, and monitor crowd behaviour to flag potential safety hazards.

Last, but not least, a very relevant current challenge: *cost savings*. By automating mundane activities and lowering the need for human resources, AI can help law enforcement agencies save money. For example, AI can automate data entry and analysis, hence minimising the requirement for human analysts. Moreover, AI can discover where resources might be deployed more efficiently, reducing overall expenses<sup>3</sup>.

So, what is the state of play regarding the European Union Agency for Law Enforcement Training on these new technological challenges? The first point touches on the designed and approved strategy of CEPOL as an innovative hub centre for Law Enforcement Training, after collecting the needs from the EU Member States, that reported a need for some of these technological challenges.

## Artificial Intelligence challenges in the training environment

While the benefits of AI in law enforcement are substantial, significant obstacles must be overcome to ensure that AI is employed relatively and justly. Some issues linked with AI in law enforcement include the following:

• *Bias* - Bias is one of the primary problems with using AI in law enforcement. AI systems are only as objective as the data used to train them; if the data used to prepare the system is biased (Ntoutsi, Fafalios & Gadiraju, et al., 2020), the

<sup>3</sup> We cannot exclude from these reflections the associated risks AI may pose regarding Fundamental rights, data protection, biases, automated biases discrimination and other relevant points.

AI system will also be prejudiced. This can lead to unjust or discriminatory outcomes, especially for underprivileged communities.

- Privacy and civil liberties Using artificial intelligence in law enforcement creates privacy and civil liberties problems. The employment of AI could result in excessive surveillance or the violation of the privacy of persons (Montasari, 2022). Face recognition technology, for instance, can be used to identify persons in real-time, which raises concerns about the possibility of government spying. In addition, using AI in law enforcement can raise issues around the case of profiling and prejudice based on race, ethnicity, religion, or other criteria.
- Transparency and clarity Another obstacle related to artificial intelligence in law enforcement is the need to comprehend how AI systems make choices. AI systems can be complicated and challenging to comprehend, making it difficult to identify how decisions are made. In law enforcement, decisions made by AI systems must be explicable and transparent (Felzmann, Villaronga & Lutz et al, 2019) so that individuals may comprehend their rationale.
- Ethical considerations The employment of artificial intelligence in law enforcement creates a variety of ethical concerns. Concerns exist, for instance, over the use of AI in predictive policing, which could lead to targeting specific populations or individuals based on their past conduct (Vidu, Zbuchea, Mocanu & Pinzaru, 2020). This could negatively influence these areas and result in a loss of trust between law enforcement and the community. In addition, the employment of AI in law enforcement may raise worries about dehumanisation and the loss of human judgment.
- *Technical difficulties* There are also technological obstacles related to law enforcement's usage of AI. For example, AI systems may have trouble on accurately interpreting data from many sources or recognising specific sorts of behaviour. There are also concerns regarding the possibility of AI systems being hacked or manipulated (Celik, et al., 2019).

To address these issues, law enforcement agencies must collaborate closely with AI developers and experts to guarantee that AI systems are designed and used responsibly and effectively. It worths also the mention that the EU-Innovation hub for Internal Security (URL3), hosted at EUROPOL<sup>4</sup> and in which CEPOL is also participating and contributing (among the 13 current members), has evolved as collaborative platforms to foster innovation and address specific challenges, as well as discuss about projects in areas of research, innovation and technologies.

Belügyi Szemle, 2025·9 1901

<sup>4</sup> It has been established by the Council's Standing Committee on Operational Cooperation on Internal Security (COSI) and it focuses on coordinating and collaborating on innovation in internal security.

Anyway, these identified items demand a complete awareness of AI technology and its limitations and a dedication to its ethical and transparent application. In this regard, training courses organised by CEPOL are essential for enhancing the expertise and understanding of law enforcement personnel in this subject.

In addition, appropriate protections and regulations should be implemented to protect the privacy and civil liberties and ensure that AI systems are transparent and explicable. Mindful of this importance, as referred above, CEPOL cooperates actively with the EU Innovation Hub for Internal Security<sup>5</sup> (URL4) led by EUROPOL, as the partner of the AP4AI Project related to responsible use of AI in the EU Internal Security Sector and contribution to discussion on the implementation of the EU AI Act<sup>6</sup>. This initiative is focused on developing a web-based tool for application for practitioners and training awareness sessions on responsible use of AI supported by CEPOL.

Moreover, to ensure proper implementation of AI-based components related to interoperability between EU large-scale information systems following the obligations imposed by regulations<sup>7</sup>, CEPOL Knowledge Centre on Law Enforcement Cooperation, Information Exchange and Interoperability<sup>8</sup> (URL5) provides training activities covering the AI -related issues.

Law enforcement agencies must also connect with the community to sustain public support and address ethical considerations. By following these steps, we can ensure that AI is used responsibly and effectively to improve public safety and law enforcement operations. With appropriate protections and restrictions, we can harness the power of AI to better our societies and secure our communities.

<sup>5</sup> The EU Innovation Hub is a cross-sectorial EU platform and aims to ensure coordination and collaboration between all innovation actors in the wider field of the internal security. The Innovation Hub, being composed of various EU Agencies, European Commission (including JRC), the Council General Secretariat and the Office of the EU Counter Terrorism Coordinator, works to provide the latest innovation updates and effective solutions to support the efforts of internal security actors in the EU and its Member States (MS), including justice, border security, immigration, asylum and law enforcement practitioners.

Regulation (EU) 2024/1689 Of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)

One of them is Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816.

<sup>8</sup> CEPOL Knowledge Centre on Law Enforcement Cooperation, Information Exchange and Interoperability (CKC INT) brings together professionals from Member States and relevant EU services, as experts in a specific thematic area, to elaborate a holistic multiannual training portfolio, composed of onsite and online activities as well as follow-up activities.

## CEPOL and its Strategy towards digitalisation

The European Union Agency for Law Enforcement Training (CEPOL) plays an essential role in the prevention of serious and organised crime, terrorism, and other emerging security threats by promoting and improving cross-border cooperation through the provision of vocational training. CEPOL is a leading institution that provides high-quality training activities for law enforcement and judicial professionals in various thematic areas (URL6). Through its comprehensive training programmes, CEPOL enables law enforcement officials to acquire the necessary skills, knowledge, and expertise to tackle various forms of criminality, including cybercrime, terrorism, and border management. Moreover, CEPOL's training initiatives are aligned with the EU's overall strategic objectives and policies and aim to enhance the interoperability and effectiveness of law enforcement agencies across the EU.

CEPOL has developed its strategy in November 2022 to enhance its role in promoting law enforcement cooperation and effectiveness across the European Union through law enforcement training. This strategy was built on four main pillars: becoming the EU hub for law enforcement training fostering knowledge, nurturing a common EU law enforcement culture via training, promoting accreditation of law enforcement vocational training, and excelling at governance as a modernised EU Agency trusted by its stakeholders (URL7).

CEPOL's first goal is to become the EU's hub for law enforcement training by utilising its vast network to define, facilitate, monitor, and evaluate the EU Law Enforcement Training Priorities while incorporating research outputs into creative training to improve its effectiveness and efficiency. The agency also seeks to strengthen cooperation with non-EU countries and other external partners, including international organisations, to create a more inclusive and collaborative approach to law enforcement training that will increase security and safety for citizens.

The second goal of fostering a common EU law enforcement culture through training recognises the importance of equipping law enforcement officials with the same competencies, knowledge, skills, and attitudes necessary for cooperation in combating transnational criminality. The agency's multiannual, multi-disciplinary, and multi-layered training portfolio focuses on EU Law Enforcement Training Priorities, providing qualifications and promoting exchange programmes for law enforcement officials. Through its hands-on and interactive approach, CEPOL's training initiatives aim to create a common professional language and culture among law enforcement authorities within and beyond the EU, essential for promoting practical cooperation and coordination in addressing common security challenges.

CEPOL's third goal of promoting law enforcement vocational training accreditation aims to ensure that the highest standards are applied, and trainees are qualified in specific domains with tested and certified competencies. The agency planned and is developing a framework for accreditation of training activities that align with EU Law Enforcement Training Priorities, creating a sectoral qualification framework that will enable CEPOL to take an active role in accrediting training activities. CEPOL will draw from the practical implementation of the EU sectoral qualification framework and training accreditation to study their achievements and lessons learned, ultimately exploring the appropriate ways to implement law enforcement vocational training accreditation to ensure the highest standards are met.

The last goal of excelling at governance as a modernised EU Agency trusted by its stakeholders recognises the importance of upholding and improving the agency's good practices and processes while streamlining workflows and improving its corporate culture. The agency has stepped into modern infrastructure and facilities, ensuring to be fit for purpose and support its training and knowledge-sharing activities. Additionally, CEPOL is working to enhance its corporate governance practices and promote transparency and accountability to build trust with its stakeholders. Ultimately, by improving its governance and infrastructure, CEPOL aims to become a modernised EU Agency trusted and respected by its stakeholders.

CEPOL has acknowledged the significance of digitalisation and AI in boosting the efficacy and productivity of law enforcement training (MB 33/2019/MB). As a result, the agency has incorporated AI technologies into training programmes, such as online classes and virtual reality simulations. CEPOL has also held training activities to enhance knowledge sharing and exchange best practices on digitisation and AI among law enforcement organisations. In addition to collaborating with other agencies, such as EUROPOL or INTER-POL, the agency has developed cooperative efforts on AI training. In addition, CEPOL has underlined the relevance of ethical and human rights issues in using AI in law enforcement and set rules to ensure that its training programmes adhere to these tenets. Overall, CEPOL's involvement in digitalisation and AI demonstrates its dedication to equipping law enforcement authorities across the EU with the most up-to-date knowledge and abilities required to address growing security threats.

The importance of research and the dynamism in acquiring new goals in AI cannot be overstated. AI is an emerging technology that is rapidly changing the landscape of law enforcement. Research and science are essential in identifying and developing AI's latest advancements and best practices. Through

research, new applications of AI can be identified, and existing models can be optimised to enhance their effectiveness and efficiency. Additionally, science is essential in ensuring that the development and deployment of AI in law enforcement are aligned with ethical and human rights principles and are consistent with data protection regulations. Research and science dynamism also promote innovation and agility in law enforcement, enabling law enforcement officials to adapt to emerging security challenges and stay ahead of criminals using AI for illegal purposes. Therefore, investment in research and science is essential for law enforcement agencies to effectively use AI in addressing the latest security challenges.

## The identified gaps in digital skills and the use of new technologies in law enforcement training

Training activities are aimed at achieving a specific change. This means that their universal goal is to move from a clear state of knowledge and skills among a particular group of people to a state defined as better, improved and more helpful in achieving predetermined goals. In the life of an organization, training activity, therefore, means striving to achieve a different - and better - desired state of its functioning (Trutkowski, 2016). Therefore, collecting the necessary information about their needs is essential to prepare a training offer that meets the needs of law enforcement officials dealing with a specific problem. Then, analyse their opinions and translate them into an offer covering the identified aspects. According to the literature, the training needs assessment process is the first step in planning an effective training programme.

This process usually focuses on the training recipients' current and desired knowledge, skills and attitudes and provides clear guidance on what skills gaps should be filled and what the profile of future trainees should be. Over the years, training needs have been defined in various ways. According to McGehee and Thayer, for example, training needs arise from underdeveloped skills, insufficient knowledge, or inappropriate attitudes of employees (McGehee & Thayer, 1961). In turn, training needs defined by Mager and Pipe are the identified differences between the current performance of employees and the results that the organization expects from them (Mager & Pipe, 1979). And according to Cascio, the need for training is the need to improve human performance, which some appropriate type of training can best meet.

The many available studies on training need to use a variety of terminologies, including training needs analysis, training needs assessment, training needs

measurement and identification. The needs assessment process emphasises the current knowledge, skills or attitudes at the individual, group or organizational level to determine the future course of action. In the analysis of training needs, attention is paid to aspects of work that are vulnerable to failure or ineffectiveness of the workforce and the possibility of improving them through training (URL8).

CEPOL periodically collects and focuses data on defining strategic-level training priorities for law enforcement officials to achieve the training needs. European Union Strategic Training Needs Assessment aims at identifying those EU-level training priorities in the area of internal security and its external aspects to help build the capacity of law enforcement officials, while seeking to avoid duplication of efforts and achieve better coordination.

Among the eight identified core capabilities gaps identified in the published European Union Strategic Training Needs Assessment (EU-STNA) (URL9), the highest priority has been given to the need for digital skills and the use of new technologies. Technological innovations continue to change the law enforcement landscape, and the related training needs have been revealed by identifying the core capability challenges across the European law enforcement community. Despite the investments already made in improving digital skills and the use of new technologies among law enforcement officials, the EU-STNA process has identified several specific areas where further efforts are required, both in terms of building professionals' capacity to use advanced technology and deepening their understanding of how technology is utilised for criminal purposes. Based on the need for enhanced skills in today's law enforcement professions, the main categories identified during the EU-STNA analysis and consultations include law enforcement's advanced cybersecurity knowledge regarding how to use online surfaces, such as open source intelligence (OSINT), the dark web, and social media, as well as other methods (e.g. artificial intelligence, extensive data analysis, methodologies applied to quantitative and qualitative analysis of information, etc.) for investigation. The European Counter-Terrorism Centre (ECTC) observed that using AI should be prioritised. The Fundamental Rights Agency (FRA) noted that all training activities addressing AI and big data should reference data protection and other fundamental rights, particularly non-discrimination and access to an effective remedy. As indicated by Europol, there is a gap in generic training on topics related to mass data, data protection, machine learning, and law enforcement cooperation and EU cooperation tools.

Shortly, the collected complex identified needs under the "Digital skills and use of new technologies" has focused on numerous objective topics primarily related to the fight of criminal activities.

**Table 1.** Detailed list of training needs

Digital skills and use of new technologies			
1	Cybersecurity fundamentals for EU officials' everyday use (cyber hygiene, cybersecurity guidelines, secure exchange of information, physical security)		
2	Raising awareness of the most important cyber-threats (e-mail-based attacks, web-based attacks, DDoS attacks, social media scams). Understanding cybersecurity challenges from modern technologies, like AI or 5G		
3	Better, modern and validated tools and training materials for tackling activities related to disinformation and fake news that is considered as crime or could lead to criminality are supported by advanced digital technologies		
4	Digital investigation: OSINT, dark net, cyber threat intelligence (CTI) knowledge management, decryption, use of AI, big data analysis, quantitative and qualitative analysis methods, internet of things, advanced use of camera systems, drones, exoskeletons and speech processors, big data analysis for prediction of criminal behaviour, cryptocurrencies		
5	Digital forensics		
6	Victims' protection		
7	Fundamental rights and data protection		

Note. Created by the authors.

# Operational Training Needs Analysis (OTNA) on Digital skills and use of new technologies

Considering the priority security topics defined by the EU-STNA, CEPOL also focuses on understanding the urgency level of training to be delivered regarding the Operational Training Needs Analysis. Furthermore, the freshest analysis also highlights the needs regarding emerging threats, where several activities are related to new technologies and tools.

While all topics related to cybersecurity fundamentals for EU law enforcement official's everyday use and awareness-raising passed the relevancy rate, the following thematic areas were given the highest score:

- · Phishing attacks, malware attacks, ransomware removable media
- Cybersecurity fundamentals for construction of secure systems for EU agencies, law enforcement agencies (tools used, identifying cybersecurity, ways of understanding: specific threats, new ways of operations)
- On-line safety and advice, social media crime prevention campaigning, new social media (TikTok, online video games e.g. Roblox)
- In-depth understanding of the cybersecurity threats for artificial intelligence, 5G and other new technologies
- Cyber hygiene, passwords and authentication, mobile device security, working remotely, public Wi-Fi, cloud security, physical security.

Among the identified Operational Training Needs regarding the use of technologies, among which AI is at the core, at least two were identified: big data analysis, e.g. prediction of criminal behaviour with extensive data analysis and the use of AI, including risks and fundamental rights, especially on face recognition systems, as observed in the table below.

**Table 2.** OTNA on Digital skills and the use of new technologies

Fő téma	Subtopic	Relevance
	Open-Source Intelligence (OSINT)	80%
	Mobile devices for investigation	78%
	Cyberattacks (Ransomware, DDOS, Botnets)	78%
	Encryption, Anonymization techniques (VPN, Spoof calls, Sim boxes)	77%
	Software/tools developed to identify dark web crimes	75%
	Darknet, what is dark web, how to use dark web	74%
	Digital fingerprints and metadata to identify persons and devices	74%
Digital in-	Raw data analysis	72%
vestigations	Big data analysis, e.g. prediction of criminal behaviour with big data analysis	71%
	Analysis techniques/tools for many types of data (normalization, correlation, and fusion) including technical data from different domains	70%
	Information technology as a knowledge management enabler	65%
	Cloud platforms	64%
	Use of Artificial Intelligence, including AI risks towards fundamental rights, especially on face recognition systems	63%
	Internet of Things	63%
	Lawful interception	62%

Note. Created by the authors.

#### **Conclusions**

Using AI in la enforcement can significantly enhance speed, efficacy, awareness, predictive analytics, investigative methods, public security, and cost savings. However, significant challenges are associated with its implementation, including bias, privacy and civil liberties, transparency and clarity, ethical considerations, and technical difficulties. To ensure the responsible and effective use of AI, law enforcement agencies must collaborate closely with AI developers and experts, develop and implement appropriate regulations and protections, and engage with the community to address ethical considerations. Training courses, such as those organised by CEPOL, are essential for enhancing

the expertise and understanding of law enforcement personnel in this subject. By taking these steps, we can harness the power of AI to improve public safety and law enforcement operations while ensuring the protection of privacy, civil liberties, and human rights.

The EU-STNA highlights the importance of deepening cooperation with the private and academic sectors. Public-private partnerships create an opportunity to combine the competencies of multiple actors and generate new solutions and services relevant to many areas of law enforcement, especially when it comes to the increased use of the machine simulation of human intelligence processes, e.g. artificial intelligence. In addition, closer cooperation must be developed with academia and relevant research institutes regarding training, research and innovation. The EU-STNA has identified several areas where law enforcement officials need further training to use new technologies effectively. While some training on new technologies is already available, it is essential to continuously update and develop training programmes to keep up with rapid technological advancements. For instance, new training programmes should be designed to cover topics such as using new technology learning tools and concepts using artificial intelligence and cryptocurrencies. Additionally, the training programmes should focus on the emergency response of law enforcement and how emerging tools can be used to prevent and fight new criminal trends. A fresh update on training will ensure that law enforcement officials have the necessary knowledge and skills to effectively use new technologies to combat crimes while mitigating any potential adverse effects that may arise.

As AI becomes more integrated into all areas, law enforcement representatives must deeply understand the rules of responsibility accompanying this technology in internal security. This understanding can only be acquired through proper training, essential for raising the competencies necessary to implement AI-based tools and components in the policing domain and their proper use by end-users. However, more is needed for training activities to support the responsible use of AI tools in the EU internal security sector based on the principles of accountability. There must also be a focus on enhancing awareness of the ethical implications of AI and ensuring that its use does not violate fundamental rights. The European Union Agency for Law Enforcement Training (CEPOL) plays a crucial role in shaping this awareness at the EU level through its training programmes and initiatives. CEPOL can ensure that law enforcement officials are equipped to utilise this technology responsibly and effectively by providing training that covers both the technical and ethical aspects of AI.

#### References

- Angelov, P. & Gu, X. (2018). Towards Anthropomorphic Machine Learning. The Expanding Frontier of Artificial Intelligence. *Computer*, *51*(9), 28-36. https://doi.org/10.1109/MC.2018.3620973
- Celik I. et al. (2022). The Promises and Challenges of Artificial Intelligence for Teachers: A Systematic Review of Research. TechTrends, 66, 616–630. https://doi.org/10.1007/s11528-022-00715-v
- Chubb, J., Cowling, P. & Reed, D. (2022). Speeding up to keep up: exploring the use of AI in the research process. AI & Soc 37, 1439–1457. https://doi.org/10.1007/s00146-021-01259-0
- Felzmann, H., Villaronga, E. F. & Lutz, C. et al. (2020). Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns. *Big Data & Society, 6*(1), 1-14. https://doi.org/10.1177/2053951719860542
- Gesk, T. S. & Leyer, M. (2022). Artificial intelligence in public services: When and why citizens accept its usage. *Government Information Quarterly*, 39(3), 101704. https://doi.org/10.1016/j.giq.2022.101704
- Hayward, K. J. & Maas, M. M. (2020). Artificial intelligence and crime. A primer for criminologists. *Crime Media Culture*, 17(2), 209-233. https://www.doi:10.1177/1741659020917434
- Lotfi, I. & El Bouhadi, A. (2022). Artificial Intelligence Methods: Toward a New Decision-Making Tool. *Applied Artificial Intelligence*, *36*(1), e1992141. https://doi.org/10.1080/08839514.2021.1992141
- Lunhol, O. & Torhalo, P. (2024). Artificial Intelligence in Law Enforcement: current state and development prospects. Proceedings of Socratic Lectures, 10, 120-124. https://doi.org/10.55295/PSL.2024.II12
- Mager, R. F. & Pipe, P. (1979). *Analyzing performance problems*. Lake Publishing. https://hpt-manualaaly.weebly.com/mager-and-pipes-model.html
- McGehee, W., & Thayer, P. (1961). Training in business and industry. Wiley.
- Montasari, R. (2022). Artificial Intelligence and National Security. Springer.
- Ntoutsi, E., Fafalios, P. & Gadiraju U. et al. (2020). Bias in data-driven artificial intelligence systems An introductory survey. *WIREs Data Mining Knowl Discov*, 10(6), 1356. https://doi.org/10.1002/widm.1356
- Poushter, J. et al. (2016). Smartphone ownership and internet usage continues to climb emerging economies. *Pew Research Center*, 22, 1-44.
- Rademacher, T. (2020). Artificial Intelligence and Law Enforcement. In T. Wischmeyer, & T. Rademacher (Eds.), *Regulating Artificial Intelligence* (pp. 225-254). Springer. https://doi.org/10.1007/978-3-030-32361-5
- Trutkowski, C. (2016). Training needs analysis and national training strategies Toolkit. Centre of Expertise for Local Government Reform. Council of Europe.
- Vidu, C., Zbuchea, A., Mocanu, R. & Pinzaru, F. (2020). *Artificial Intelligence and the Ethical Use of Knowledge*. Strategica.

- Zhu L. et al., (2021). Adding power of artificial intelligence to situational awareness of large interconnections dominated by inverter-based resources. *High Volt*, 6(6), 924-937. https://doi.org/10.1049/hve2.12157
- Zhu, H. & Jin, Y. (2019). Multi-objective Evolutionary Federated Learning. In *IEEE Transactions on Neural Networks and Learning Systems*, 31(4), 1310-1322.

#### Online links in the article

- URL1: Digital Education Action Plan. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?u-ri=CELEX:52018DC0022&from=EN
- URL2: *Tthe New Skills Agenda for Europe*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0381&from=EN
- URL3: EU Innovation Hub for Internal Security Europol. https://www.europol.europa.eu/operations-services-innovation/innovation-lab/eu-innovation-hub-for-internal-security
- URL4: EU Innovation Hub for Internal Security Europol. https://www.europol.europa.eu/operations-services-innovation/innovation-lab/eu-innovation-hub-for-internal-security
- URL5: CEPOL Knowledge Centre. https://www.cepol.europa.eu/training-education/cepol-know-ledge-centres
- URL6: Quality management standards, available online at. https://www.cepol.europa.eu/about-cepol/agency/quality-management-standards
- URL7: CEPOL New Strategy 2023-2027, available online at. https://www.cepol.europa.eu/newsroom/news/management-board-adopts-new-cepol-strategy
- URL8: Necessity of Training and Identification of Training Needs. https://www.researchgate.net/publication/305033478
- URL9: European Union strategic training needs assessment 2022-2025 European Union Strategic Training Needs Assessment 2022-2025 CEPOL. europa.eu

### Law and regulation

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and repealing Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU)

Regulations 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) Decision No. 33/2019/MB of the Governing Board amending Decision No. 23/2019/MB on the CEPOL Single Programming Document 2020-2022 Adopted by the Governing Board on 19 December 2019.

#### Reference of the article according to APA regulation

Guia, J. M., Mihai, I-C., & Kordaczuk-Was, M. (2025). Artificial Intelligence Innovations in Law Enforcement Training: CEPOL Strategy 23-27. *Belügyi Szemle*, 73(9), 1897–1912. https://doi.org/10.38146/BSZ-AJIA.2025.v73.i9.pp1897-1912

#### **Statements**

#### Conflict of interest

The authors have declared no conflict of interest.

#### **Funding**

The authors received no financial support for the research, authorship, and/or publication of this article.

#### **Ethics**

The data will be made available on request.

#### Open access

This article is an Open Access publication published under the terms of the Creative Commons Attribution 4.0 International License (CC BY NC-ND 2.0) (https://creativecommons.org/licenses/by-nc-nd/2.0/), in the sense that it may be freely used, shared and republished in any medium, provided that the original author and the place of publication, as well as a link to the CC License, are credited.

#### Corresponding author

The corresponding author of this article is Marzena Kordaczuk-Wąs, who can be contacted at marzena.kordaczuk-was@cepol.europa.eu.