UDC 004.9:343
DOI: 10.63341/naia-chasopis/2.2025.09

Areas of application of artificial intelligence in law enforcement: Trends, challenges and prospects

Andrii Vozniuk*
Doctor of Law, Professor
National Academy of Internal Affairs
03035, 1 Solomianska Sq., Kyiv, Ukraine
https://orcid.org/0000-0002-3352-5626

Oleh Tarasenko
Doctor of Law, Professor
National Academy of Internal Affairs
03035, 1 Solomianska Sq., Kyiv, Ukraine
https://orcid.org/0000-0002-3179-0143

Serhii Skrypnyk
Researcher
National Academy of Internal Affairs
03035, 1 Solomianska Sq., Kyiv, Ukraine
https://orcid.org/0009-0000-6414-7237

Abstract
The escalation of security challenges in the context of digital transformation highlights the need for a systematic review of current practices, risks and the potential for implementing artificial intelligence in law enforcement activities. The aim of this study was to summarise scientific approaches to the application of artificial intelligence in law enforcement, focusing on the stages of its development, key areas of research and insufficiently studied aspects. The use of methods of analysis and synthesis of scientific sources, content analysis, comparative analysis, and classification of existing approaches made it possible to assess the current state of scientific research on trends, challenges, and prospects for the use of artificial intelligence. It has been established that scientific interest in the application of artificial intelligence in law enforcement has increased significantly over the last decade. The rapid development of artificial intelligence technologies has opened up new opportunities for the automation of analytical and operational functions, prompting scientists to study the possibilities and threats of artificial intelligence. Researchers focus primarily on areas such as video analytics, crime prediction, image recognition, and big data processing. At the same time, there is a lack of in-depth interdisciplinary research that takes into account the ethical, legal, and social implications of using such technologies. A disparity in approaches to risk classification and standardisation of implementation practices has been noted. The need for the formalisation of research has been demonstrated, which will contribute to the balanced development of artificial intelligence in law enforcement activities, taking into account security,

Article's History:
Received: 11.02.2025
Revised: 01.05.2025
Accepted: 27.05.2025

Suggest Citation:
Vozniuk, A., Tarasenko, O., & Skrypnyk, S. (2025). Areas of application of artificial intelligence in law enforcement: Trends, challenges and prospects. *Law Journal of the National Academy of Internal Affairs*, 15(2), 9-21. doi: 10.63341/naia-chasopis/2.2025.09.

*Corresponding author

legal, and humanitarian factors. The results obtained can be used by heads of law enforcement agencies, analytical units, and digital transformation specialists to determine priority development directions and consider potential risks

Keywords:
information; digital forensics; combating criminal offences; cybercrime; digitalisation

Introduction

Modern technologies are rapidly changing all spheres of life, and law enforcement is no exception. One of the most promising tools for the digital transformation of law enforcement agencies is Artificial Intelligence (AI). The application of AI in law enforcement covers a wide range of areas – from automated video surveillance and big data analysis to predicting crime in general or its specific manifestations. At the same time, the use of such technologies gives rise to a number of ethical and legal challenges that have required and continue to require careful regulation (Hacker, 2023). In response to these challenges, the European Parliament and the Council of the EU are creating a legal instrument – the EU AI Act[1], which combines the development of innovations with the protection of fundamental rights and societal values. The document, adopted in June 2024, aims to ensure transparent rules for the use of AI technologies, promote innovation, and protect human rights in Europe.

Proper implementation of the adopted legislative acts requires law enforcement agencies to quickly master computational systems and AI models capable of analysing large datasets, learning from them, making necessary decisions, and performing assigned tasks. Europol, using research from its own Innovation Lab, analyses the potential of AI application in terms of technologies that can be effective (e.g., pattern recognition, crime prediction, data analysis); studies practical cases of pilot projects and initiatives for AI application in EU countries; identifies risks and challenges, particularly those related to privacy, ethics, algorithmic discrimination, etc.; formulates recommendations for EU member states on implementing AI without violating human rights and legality; and prepares analytical reports and forecasts (Europol, 2024). The ability to quickly analyse large amounts of information and find correct solutions in critical situations requires a much broader set of tools than traditional forensic data analytics. Therefore, identifying patterns, finding connections, and generating new knowledge from raw data, according to Europol (2024), is an obvious necessity in the era of digital technologies.

Researchers have repeatedly emphasised the broad prospects opened up by the application of AI. According to I. Raji & D. Sholademi (2024), future algorithms are expected to become even more complex, which will expand the possibilities of prediction and its societal perception. The further development of explainable AI will also be of great importance, as noted by A.B. Arrieta *et al*. (2020), helping law enforcement agencies better understand how AI predictions and recommendations are generated and contributing to addressing concerns about AI biases. Its implementation, as indicated by J. McDaniel & K. Peace (2021), significantly increases work efficiency, optimises information collection and analysis processes, prevents criminal offences, and enables more effective detection and investigation.

According to research by K. Huang *et al.* (2021), combining accumulated historical data with real-time data will allow law enforcement agencies to better adapt their strategies, responding to new threats and crime trends. Augmented natural language processing (NLP) plays an important role. As noted by N.C. Dang *et al*. (2020), using sentiment and context analysis with NLP technologies allows for the detection of new threats and the tracking of public sentiment. Indeed, the development of the internet has led to the emergence of blogs, forums, and social networks that provide users with the opportunity to discuss any topic, share their opinions on it, and thereby influence human activity and behaviour. Therefore, the increasing volume of information generated online requires automated computational systems for data analysis, whose algorithms do not always meet the expected accuracy of results.

Thus, the rapid development of AI-based technologies has led to a large number of studies dedicated to the opportunities and challenges of its application. The aim of the study was to systematise and critically review existing scientific literature on the possibilities of using artificial intelligence in law enforcement. The study was based on an analysis of modern scientific research, reports from international organisations, analytical publications, and cases of artificial intelligence implementation in the activities of law enforcement agencies. To achieve a holistic vision of the topic, the review is structured around three key thematic areas, formed in accordance with the stated research objectives. The first area covers the analysis of the possibilities of applying artificial intelligence in open-source intelligence (OSINT) and social media intelligence (SOCMINT). Within this thematic block, technological solutions were investigated that allow for automated

[1] Regulation of the European Parliament and the Council of the European Union No. 2024/1689 "Artificial Intelligence Act". (2024, June). Retrieved from https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng.

monitoring of the digital environment, threat recognition in open sources, and data collection from social media platforms. The second area is devoted to the role of natural language processing (NLP) in threat detection and supporting the activities of law enforcement and judicial bodies. The review considers the application of NLP for analysing textual data, detecting emotional colouring of messages, machine translation, and automated classification and extraction of key information from documents. The third area focuses on reviewing the current state of digital forensics using artificial intelligence technologies. The review included an analysis of practices for processing large datasets, detecting cyber threats, information recovery, analysing digital traces, and evaluating the effectiveness and limitations of these technologies in crime investigation, particularly in conditions of armed conflict. The methodological basis of the review was methods of critical literature analysis, comparison, and content analysis of official reports.

Big datasets

A significant part of law enforcement work involves information, particularly the analysis of data related to committed criminal offences, individuals suspected of committing them, obtaining evidence, taking measures to prevent criminal activity, and so on. As Y. Lee *et al*. (2024) note, accumulated large sets of static and dynamic data serve as a source for AI. By processing such data, AI assists law enforcement agencies in predictive policing, OSINT or SOCMINT intelligence, NLP, and digital forensics. For crime prediction, AI can use automatic and semi-automatic models: automatic models are capable of independently processing input data, analysing them, and drawing conclusions without human intervention, while semi-automatic models involve humans to solve more complex and unpredictable tasks through interaction with algorithms.

However, given the latest advancements in AI, it is important to be cautious when delegating decision-making to systems whose operating principles are not always fully understood. The main challenge remains the creation of an AI oversight system that ensures algorithmic transparency and allows for human intervention when necessary. The UK Government classifies powerful general-purpose artificial intelligence models that can perform a wide range of tasks and equal or exceed the capabilities of the most advanced models today as Frontier AI. Such models will have improved accuracy, reasoning, planning, memory, and self-correction and will be necessary for creating truly autonomous agents capable of performing more than basic tasks without human supervision (UK Government Office for Science, 2023). As M. Javaid *et al*. (2022) indicate, finding correlations to avoid or predict AI errors is an urgent current need. Given the current significant uncertainty, there is insufficient evidence to rule out the possibility that future Frontier AI, if improperly configured, misused, or insufficiently controlled, could pose an existential threat.

The large and complex datasets operated by law enforcement agencies are difficult to process using traditional tools. Such data require specialised analysis that uses sophisticated mathematical algorithms, machine learning, and trained models (Hardyns, 2024). By processing large and complex datasets in this way, AI can analyse and comprehend this data, and also develop certain predictions. This allows for a high probability of answering key questions: who might commit a criminal offence, when and where, and who will be its victim. This determines the level of risk of committing a particular offence. Obtaining such information is a critically important component of crime prevention. A trained AI model can automatically establish the essence of textual, voice, and visual datasets. AI can identify information about phone numbers, IP addresses, names, etc., without necessarily reviewing the content of the message. AI performs this work significantly faster and more efficiently than a human, who would have to read text, watch video, or listen to audio recordings. This approach also increases the level of protection of personal data from unauthorised access and subsequent illegal use, eliminating the human factor (Europol, 2024).

The European Commission, within the framework of Horisont-ERC grants, started funding the BIGDATPOL project in 2023, which aims to improve crime prevention work on the European continent. The harmonisation of statistical, criminological, economic, legal, and ethical aspects of large datasets should lead to the creation of a new AI model that uses historical data to predict and prevent the growth of crime. By directing their resources to hot spots thanks to the generated predictions of the new trained AI model, the police will have more opportunities to keep crime at a certain level (European Research Council, 2023). The project, which will be implemented until September 2028, aims to: combine knowledge and expertise in the field of protecting large datasets, which are currently fragmented; conduct interdisciplinary research in the study of police work with big data; study, scientifically substantiate, and compare different models of police work with big data.

Identifying patterns in criminal activity, studying connections between different types of data, and forecasting resource needs based on accumulated historical data will require the use of appropriate technological infrastructure (Tarasenko, 2020). That is why, as I. Ben-Israel *et al*. (2020) note, since 2017, more than 30 countries have published national strategies or national plans in the field of AI, with investments in billions of dollars. As of April 2025, there are already more than 1000 AI initiatives from 69 countries, territories, and the EU (OECD.AI, 2021). The creation, operation, and maintenance of such infrastructure requires significant financial expenditure and specialised expertise from law enforcement officers, which can be a

significant limitation, especially for small law enforcement units. Solving this problem can be based on a systemic approach that combines organisational, legislative, financial, and educational measures. The state plays a key role, as public funding through targeted budget programmes for the creation and support of digital analytical infrastructure in law enforcement agencies will allow for the creation of, for example, a single state platform for data analysis (Data-as-a-Service), to which various units can connect – instead of duplicating infrastructure for each of these units separately. Interregional analytical centres can also be created as structural units of a single state platform. To implement such changes, legislation must be amended, namely a Law on the Use of AI in Law Enforcement must be adopted, defining safety and data protection standards; conditions for access to centralised platforms; mechanisms for external and internal control. Legislative regulation will also be needed for the institutionalisation of the role of an independent technological auditor who evaluates the expediency of AI solution procurement and their compliance with standards. Amendments to the Budget Code and local government laws will allow for the financing of AI solutions in the security sector from various sources. Professional training and advanced training for law enforcement officers, including the study of AI, criminal analytics, and cybersecurity topics in the curricula of specialised higher education institutions and advanced training courses, partnership with universities for staff internships in IT or analytics, and the use of online courses and self-education models (in cooperation with Coursera, edX, EUROPOL Academy, etc.) will allow staff to be prepared for the effective use of AI in law enforcement.

In the study of large and complex datasets operated by the Dutch police, four contexts are considered: big data policing directly from a law enforcement agency operating within the state; big data policing from ex-territorial law enforcement agencies (such as Europol, Interpol, and others); big data policing from civilians involved in information collection; big data policing from software applications developed by third-party commercial companies (Schuilenburg & Soudijn, 2023). In the Netherlands, many big data applications are developed and supported directly by police units. For example, the CAS system, developed by the Amsterdam Regional Police Unit in 2014, is used for predictive police surveillance. Police intelligence analysts use the Helios application from the Dutch Police, as well as automatic speech recognition (ASR) software and relevant tools for language analysis. The IT team of the Dutch Police is involved in the development of applications for patrol police. The integration of its own technological teams and developments into the structure of the Dutch Police enhances its operational capacity, ensures rapid adaptation to service needs, and creates synergy between IT and law enforcement practice, which, obviously, provides more control, better data protection, and greater flexibility in innovation implementation. The situation in the Netherlands differs significantly from that in the UK or the USA. In the USA, software products are developed by third-party contractors, such as Palantir. These differences can lead to varying results of big data policing in practice. This is especially relevant when feedback loops occur in algorithms, as new data processed by different algorithms generate different results, prompting police units to react differently. Furthermore, it is notable that the deployment of big data applications leads to significant changes in skills and positions within the police organisation. Research on the Dutch police shows that each police unit includes positions and teams of coders, programmers, data processors, cloud developers, testing specialists, and backend developers. Working with big data and algorithms requires different skills and knowledge than were needed for the risk and actuarial systems previously used by the police for crime analysis.

As M. Schuilenburg & M. Soudijn (2023) indicate, there is an "elite of coders" within the Dutch Police who make important decisions during the design and development of big data applications, particularly regarding which data sources to use, which variables to include in the analysis, and how to weigh these variables. These decisions are not neutral and have a significant impact on the final results. To avoid excessive discretion, the following tools should be introduced: approval of documentation for all choices in the development process, namely which data sources, variables, weights, etc., are used; clear limitation of the freedom of decision of technical teams in critical areas (e.g., in criminal intelligence) in internal instructions/regulations; all changes in the architecture or logic of algorithms must be approved by an authorised body; creation of a register of models/algorithms used in the police – with access for supervisory bodies. V.L. Glaser *et al*. (2021) argue that deep learning algorithms have a higher level of uncertainty in the results obtained due to their insufficient transparency (the so-called "black box") and ability to generate their own goals and rules. For example, deep learning algorithms can influence the development of police operations without proper human control. Therefore, fully autonomous solutions, i.e., without any human intervention, are not yet used in law enforcement activities. As of 2023, the use of big data by the Dutch police mainly involved relatively simple applications, such as investigation tools with mostly relatively simple algorithms for frontline police work, or combining large data files to improve access, which meant very limited AI involvement in managing law enforcement activities (Schuilenburg & Soudijn, 2023).

The use of large datasets by law enforcement agencies is not always lawful. The case of the Metropolitan Police of London (MOPAC – Met Police) and the Gang Violence Matrix (GVM), introduced in 2011 after the

London riots, demonstrates how sensitive accumulated data are for society and how erroneous or biased algorithms can affect citizens (Scott-Davis, 2023). MOPAC reports on the GVM, despite numerous mentions of analytics, data systematisation, standardised procedures, and automation, do not contain direct references to the use of Artificial Intelligence (AI) or deep learning algorithms. However, according to data from the Mayor's Office for Policing and Crime (2021), data on stops and arrests of individuals from the GVM are generated as part of an automated process. This means that algorithmic logic and digital automation are applied. The use of GVM in London has drawn criticism regarding transparency and discriminatory risks, as young people were labelled as gang members based on their friendships and connections, often leading to increased negative police attention and increasing the risk of being charged under the doctrine of joint enterprise, which allows several people to be convicted of a crime even if they did not commit the act themselves (Hattenstone, 2025). Despite the matrix being presented as a sophisticated intelligence database on "gangs" and those involved in gang-related violence, names were often entered randomly based on unreliable information (Hattenstone, 2025). Individuals whose personal data were entered into the matrix had no mechanism to challenge their inclusion. Following a legal challenge initiated by the human rights organisation Liberty (2022) on behalf of a young Black man, MOPAC agreed to radically change or completely dismantle the GVM. The lawsuit alleged that the GVM violated human rights, exhibited racial bias, and harmed individuals with no criminal history. According to experts interviewed by Liberty (2022), the system contributed to racial profiling: the vast majority of individuals in the matrix were young Black men, often without conviction or criminal record.

The predictive activity of law enforcement agencies is based on large and complex datasets. Modern mathematical data processing algorithms, combining tools for digital crime mapping, search engines, and pattern matching systems, aim to identify trends and patterns that can be used to predict the likelihood of new crimes being committed and to appropriately deploy law enforcement forces and resources to minimise these risks. Machine learning models that implement this approach are trained based on two main stages: data collection and modelling (prediction). As A. Raja (2023a; 2023b) notes, data collection and preparation is an iterative process and may require several rounds of cleaning, pre-processing, and feature selection to obtain a high-quality dataset. Data must represent the population under study and be properly labelled and documented to ensure reproducibility. Once the data are prepared, the next step is to perform exploratory data analysis (EDA), which is a preliminary, indicative study of the structure and patterns in the data. By analysing and visualising data, EDA can reveal patterns, correlations, and exceptions that provide insight into data relationships and characteristics. Using Python libraries such as Seaborn, Pandas, and Scikit-learn, the best understanding of the data can be achieved for use in a machine learning model. The next stage involves selecting the type of machine learning models, namely: supervised, unsupervised, or reinforcement learning. After choosing one of these types, one proceeds directly to selecting the machine learning model, for example, logistic regression, decision trees, random forests, support vector machines (SVMs), or neural networks. The choice of models and learning type are crucial for building accurate and effective machine learning models. Law enforcement agencies accumulate structured and unstructured data from various sources, such as historical crime data (time, place, type), socio-economic indicators, and can also supplement their datasets with information from other relevant sources, such as social or probation services.

Also important is the analysis of encrypted information sources, such as Dark Web platforms, which are a launchpad for criminals and criminally motivated individuals, as they provide a relatively untraceable and convenient way to carry out a wide range of illegal activities (Sangher *et al*., 2023). Therefore, gaining new opportunities to analyse the Dark Web using AI is an important step in combating crime. Research conducted on the Agora DarkNet Market Archives (2013-2015) dataset, which contained over 109,000 records with manual data division by activity type into cybercrime/non-cybercrime/cannot be determined, using four deep machine learning models, namely RNN (recurrent neural network), CNN (convolutional neural network), LSTM (long short-term memory network), and BERT (bidirectional encoder representations from transformers), showed the best results for BERT – a modern powerful model for natural language processing in classification, search, and translation tasks, which analyses the context of words in a sentence from both left and right. Researchers achieved 96% accuracy in classification by activity type (Sangher *et al.,* 2023).

The predictive activity of law enforcement agencies includes territorial and individual components. Algorithms focused on specific territories identify connections between events, geographical locations, and crime statistics, predicting the likelihood of crimes being committed at a certain time and in specific places. Predictive activity at the individual level uses algorithms aimed at identifying individuals prone to committing crimes (Europol, 2024). The key difference from previous data processing algorithms, for example, processing statistical data and AI-based predictions, is that statistics are a tool for testing hypotheses, while AI is for building prediction functions. AI operates with very complex, multidimensional relationships that cannot be described by simple formulas. Statistical models remain valuable for interpretable analytics, whereas modern AI allows

for processing large unstructured datasets, generating highly accurate predictions, and automating complex processes that were previously inaccessible to classical models. That is why predictive activity at the individual level has gained popularity in EU countries such as the Netherlands (ProKid, CAS), Germany (Precobs, Palantir Gotham), Austria, France, Estonia, and Romania, and other countries are exploring the possibilities of its implementation (Europol, 2024).

A research group from the University of Chicago (Illinois, USA) developed a model capable of predicting probable crime areas a week in advance. The tool has an accuracy of 90%, making it one of the most successful predictive policing systems operated by companies such as PredPol, Azavea, and KeyStats in major cities like Los Angeles and New York. However, even with such high accuracy, this does not mean that the model should be used for prescriptive guidance by law enforcement agencies (Rotaru *et al*., 2022). Instead, this model should be added to the set of tools for urban policy and police strategies to combat crime. A disadvantage of the model is that the prediction algorithm is unable to identify actual areas with the highest crime rates, as only reported cases are analysed by the police. For example, Black communities in the USA conceal crimes that occur in their communities, and this distorts the prediction result. At the same time, as J. Ludwig & S. Mullainathan (2021) note, African Americans constitute only 13% of the US population but account for 26% of those arrested and 33% of those incarcerated in state prisons. Determining how much of this inequality is due to discrimination by the criminal justice system is a complex task. However, there is no doubt that at least part of such inequality has a discriminatory basis. As already noted, such biases negatively affect the accuracy and fairness of statistical models. Several Scandinavian countries have a prediction model where it is possible to predict with a useful level of accuracy whether a newborn infant will be arrested for a crime by the time he or she turns 20 (Berk, 2021). The study describes the application of machine learning algorithms that implement supervised learning, including: random forests, stochastic gradient boosting, and neural networks, including deep learning. These algorithms are trained on historical data about: demographic characteristics, past offences, social conditions, and place of residence. After training, the models can be used to predict the risk of offences, including in the long term, and therefore can predict future potential offences. Potential risks remain constant, namely: bias in training data (e.g., arrests related to racial discrimination), algorithmic opaqueness ("black box"), the danger of over-reliance on model accuracy without contextual analysis.

Conclusions: AI is being increasingly implemented in law enforcement practices, particularly for crime prediction, big data analysis, and processing information from open sources. Modern machine learning models provide high analytical accuracy, but risks remain associated with algorithmic opaqueness, biased training data, and a lack of proper oversight. Practice shows that the effective use of AI requires legislative regulation, institutional supervision, and the training of appropriate personnel. At the same time, excessive automation without human intervention can lead to serious errors and human rights violations.

Open-source intelligence

OSINT or SOCMINT analytics generates datasets from open information sources. For example, by combining information from fixed CCTV cameras and footage from swarming drones, AI can create a comprehensive picture of the current situation in abandoned areas, surveying buildings or other objects (Sholademi, 2024). New AI technologies can recognise people by how they look, walk, speak, write, or type (McDaniel & Pease, 2021).

The introduction of new communication and data transfer technologies, coupled with the impact of global societal problems such as the COVID-19 pandemic, has led to a rapid increase in online services and the expansion of the Internet. Along with the increase in web traffic, the number of cybercrimes has also grown. The use of trained AI models in OSINT (SOCMINT) not only helps detect unidentified threatening information sources or cyber threats, or reconstruct the digital traces of online criminals. AI can assist law enforcement agencies in actively countering crime on social media. For example, the AI bot dAIsy, developed by O_2, is designed to combat fraudsters who attempt to gain access to the personal information of elderly people in Britain. With the help of AI, the bot tries to keep the phone conversation with the fraudster going for as long as possible, during which the fraudster wastes their time and money but never obtains the data or computer access they expect. This way, fraudsters expend resources and are unlikely to target those protected by AI again. The use of AI to create an illusion of "credibility" for criminals, misleading them and preventing crimes from fraudulent call centres, can significantly reduce the workload of law enforcement agencies in certain areas of cybercrime (Hickey, 2025).

AI can reformat unstructured data, conduct targeted searches, perform open-source research, and provide real-time statistics. It is critically important that these processes occur at a speed that surpasses criminals' ability to erase their digital traces. That is why, in accordance with the Digital Services Act (DSA)[1], online

[1] Regulation of the European Parliament and of the Council No. 2022/2065 "On a Single Market For Digital Services and Amending Directive 2000/31/EC (Digital Services Act) (Text with EEA Relevance)". (2022, October). Retrieved from https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng.

service providers and internet providers are obliged to improve monitoring and engage AI to detect and combat terrorist propaganda, disinformation, hate speech, and the dissemination of illegal content. High-speed data analysis, detection of prohibited content, and timely notification of law enforcement agencies about monitoring results will ensure the swift and effective removal of harmful content before its widespread dissemination.

OSINT assists investigators not only in preventive measures but also in the investigation of committed crimes. The fight against human trafficking, drug distribution, and cyber fraud becomes much more effective with the use of open-source intelligence tools. L. Daniel (2024), describing "pig butchering" – social engineering scams that combine elements of trust-building and fake investment opportunities – notes that, according to the FBI's Internet Crime Complaint Center in 2023, these scams caused losses of over $5.6 billion. Erin West, a Deputy District Attorney in Santa Clara County, California, emphasises the devastating impact on victims: "We are seeing losses we were never seen before. This is essentially a massive transfer of billions of dollars of wealth from the middle class not only in the US but in a number of countries". She stresses that anyone with money can become a target. Victims range from young professionals to retirees, lured by the promise of significant financial gain, accompanied by the manipulation of victims' emotions, weaknesses, or vulnerabilities. The fraud begins with a message on WhatsApp, Telegram, or an email with a seemingly innocent offer of crypto investments or even friendship. Cryptocurrencies such as Bitcoin, Ethereum, or Solana differ from traditional currencies like the US dollar, Euro, or Japanese Yen. Cryptocurrency can be moved instantly, without oversight (Vozniuk & Tytko, 2019). This means that fraudsters can covertly transfer currency across borders worldwide and hide their identity (Vozniuk *et al*., 2020). It is claimed that cryptocurrency is completely anonymous, but certain elements can be traced. Each investor's currency has an "address": a unique accumulation of letters and numbers that only one person can own. One person's wallet can contain several unique "addresses". The crypto ecosystem does not give names to these wallets. However, several details are freely available in a universal ledger known as the blockchain. Anyone can see which "addresses" a wallet contains, the amount of currency inside, and the financial transactions that occur between wallets. These facts are publicly available – and this means they can all be used in OSINT.

The use of OSINT technologies for further model training requires a careful and responsible approach, taking into account the copyrights on the input data. A notable example is Judge Stephanos Bibas's decision in the case of Thomson Reuters v. Ross Intelligence, one of the first US court cases concerning the use of copyrighted materials for training artificial intelligence[1]. In December 2020, Thomson Reuters, which owns the Westlaw platform, sued the startup Ross Intelligence. It accused Ross Intelligence of illegally using special legal annotations from Westlaw (known as headnotes) to create its own AI-powered legal research system that competes with Westlaw. Ross initially tried to obtain an official licence but was denied, and instead commissioned "memoranda" from LegalEase that contained the same annotations. These texts were then used to train the search tool. This was not a generative AI system – it merely searched for and extracted fragments from existing court decisions, which are not protected by copyright in themselves. The court considered four factors. The first factor was that the court's conclusions apply only to non-generative AI and cannot automatically be applied to cases involving generative AI, as this field is rapidly changing. Regarding the second factor of fair use – the nature of the work – the court decided that Westlaw's headnotes, while copyrighted, did not exhibit a high level of creativity. They were more technical than artistic works, so this factor favoured Ross. However, the court added that this criterion is rarely decisive. The third factor – the amount and substantiality of the use – also favoured Ross, as the end-users of its system did not see the Westlaw headnotes themselves. Crucially, the copies did not become publicly available. But the fourth, most important factor – market impact – decided the case in favour of Thomson Reuters. The court found that Ross's tool effectively created a substitute for the Westlaw product, threatening the company's market, particularly in the area of licensing data for AI training. Despite the public benefit of access to legal information, the court emphasised that this does not override copyright: those who create tools for the public good deserve to be paid. Considering this, the court ruled that Ross's use of Westlaw headnotes was not fair use, and decided in favour of Thomson Reuters (United States District Court for the District of Delaware, 2025). Therefore, the use of OSINT technologies without the owner's consent can have legal consequences, including copyright infringement, which can lead to lawsuits, blocking access to data, or imposing fines.

The application of AI in OSINT and SOCMINT significantly expands the capabilities of law enforcement agencies in threat detection, crime prevention, and the analysis of large streams of open data, including cybercrime. However, the effectiveness of such systems depends on their ability to act faster than criminals, while adhering to ethical and legal norms. Examples such as

[1] Memorandum Opinion of the United States District Court for the District of Delaware No. 1:20-cv-00613-SB "Thomson Reuters Enterprise Centre GmbH et al. v. Ross Intelligence Inc". (2025, February). Retrieved from https://www.ded.uscourts.gov/sites/ded/files/opinions/20-613_5.pdf.

the dAIsy bot demonstrate that AI can not only react but also proactively reduce risks. At the same time, the case of Thomson Reuters v. Ross Intelligence shows that using open data to train AI without proper authorisation can have serious legal consequences, particularly due to copyright infringement.

NLP (natural language processing)

NLP is another area of AI whose use opens up additional opportunities in the fight against crime. The application of NLP allows machines to understand, analyse, interpret, and generate human language in oral or written form (Wickramasekara *et al*., 2025). Among the main tasks of NLP are syntactic and semantic text analysis; speech recognition (converting voice to text); text generation; sentiment analysis; machine translation between languages; and entity extraction from text. To perform these tasks, methods such as tokenisation, normalisation, stemming, lemmatisation, POS-tagging, statistical language modelling, N-gram analysis, regular expressions, etc., are used. These tools form the basis of modern large language models (LLMs), including BERT, RoBERTa, and XLNet, which can be adapted to specific NLP tasks.

At the same time, a paradox arises: the increasing accuracy of calculations and the quality of models like BERT, GPT, and T5 in translation, classification, and question answering are accompanied by an increase in model sizes (billions of parameters), the need for hundreds of gigabytes of text data for training, expensive equipment, and significant energy consumption. Therefore, increasing attention is being paid to the use of quantum computing for representing, processing, and analysing language and overcoming the numerical limitations of modern methodologies. This has formed a new promising field – Quantum Natural Language Processing (QNLP), which uses quantum computers.

In 2023, the National Center for State Courts in the USA conducted an analysis of the use of Natural Language Processing (NLP) technologies in civil case management processes in US courts. Three pilot projects (Proof of Concept) were implemented, which proved the effectiveness of NLP in extracting data from court documents, automatically determining the type of case, and improving the quality control of decisions. The greatest successes were achieved when working with structured documents – over 90% accuracy in data extraction (National Center for State Courts, 2023). NLP also helped identify errors and shortcomings in debt collection case documents, which could prevent hasty or erroneous decisions. Another area of application was sorting cases by complexity level for proper allocation of court resources (National Center for State Courts, 2023). The report highlights NLP's potential for transforming justice by reducing staff workload; implementing ChatBots; automatic document editing; and combining NLP with business intelligence, but notes the need for gradual implementation, quality digital data, and phased testing with quality control.

No less important an aspect of natural language processing application is video information analysis. For instance, the advent of police body cameras, which first appeared in the early 2000s and became an integral part of modern law enforcement practice, provided the opportunity to collect and accumulate large amounts of visual data. While traditional sources, particularly police reports, usually contain basic information about an event, body camera footage documents interactions between police and citizens in much greater detail. This is precisely why software for automated video data analysis using NLP is being developed. Specifically, the TRULEO system scans video recordings and labels statements with tags such as "high professionalism", "de-escalation attempts", and "high composure" (Farooq, 2024).

Another example is the development by Polis Solutions called TrustStat, which analyses police interactions "using the same patterns as human experts" (Polis Solutions, n.d.). These programmes are the first commercial attempts to process body camera footage using natural language processing technologies and are aimed at practical use in a wide range of police units. This indicates that NLP opens up new opportunities for law enforcement and judicial bodies in combating crime and increasing the efficiency of administrative processes. Thanks to NLP, AI systems are capable of recognising, analysing, and generating human language, allowing for automated translation, identification of key text features, and emotional analysis.

Digital forensics

Digital forensics, specialising in the examination of electronic devices, media, and tools, is experiencing the greatest impact from AI. As of 2022, there is a shift of individual AI digital technologies from the implementation of pilot projects to widespread deployment in technological processes and the market launch of mass digital products (Matulienė *et al*., 2022). An example of this is Palantir Technologies, an American company that has progressed from a startup with experience in developing fraud detection software for PayPal to a leading provider of analytical software systems for the security and defence sectors internationally. Palantir collaborates with various police departments in the USA and other countries, creating applications ranging from database management to predictive policing (Palantir technologies…, 2024).

As of today, the profession of a Digital Investigator can be recognised – a specialist who employs digital technologies to investigate crimes. E.A. Vincze (2022) notes that the role of a digital investigator is to bring cybercriminals to justice. At the same time, digital forensics is not limited to cybercrimes, as a significant portion of modern offences are committed using

electronic devices, primarily smartphones. In light of the above, digital forensics is used both in the investigation of cybercrimes and any other criminal offences, the commission of which is associated with the use of telephones, computers, electronic storage media, and other electronic devices (e.g., illegal drug trafficking, fraud, theft) or during which these tools were used (they were present during the commission of a criminal act) or on which traces of a criminal offence are stored (audio, photos, videos, documents, etc.).

The Europol (2024) report highlights the following areas of AI use within digital forensics:

1. Analysis of large datasets. This automates certain processes that traditionally took a lot of time. For example, AI can quickly classify, filter, and extract necessary information, replacing the laborious process of manual file sorting (e.g., image classification or hash values).

2. Data recovery. Thanks to AI, several tools have been developed for data recovery and analysis. These tools can recover deleted files, access data from corrupted devices, and restore fragmented information in appropriate formats.

3. Detection of cybercrimes and other offences. It should be noted that one of the main problems of the digital space is the detection of cybercrimes and the proper conduct of investigative (search) actions that are important for investigating cases of this category and their correct resolution (Tarasenko, 2021). Malicious activity, such as hacking or phishing, often leaves barely noticeable traces or is disguised as normal web traffic. AI effectively detects patterns and anomalies in such data. By constantly analysing new data, AI models are able to distinguish between normal network traffic and potential threats, even if attackers use new tactics.

4. Data decryption. AI has also shown great potential in data decryption. Modern encryption methods can complicate the work of investigators, but AI is capable of predicting encryption patterns and accelerating the decryption process by narrowing down possible encryption keys through pattern recognition.

5. Analysis of digital traces across different devices and platforms. This has become critically important, especially with the development of the Internet of Things (IoT). Over the next 15 years, as D. Tosi *et al*. (2024) note, the integration of machine learning and deep learning technologies will enhance the analytical capabilities of big data processing systems, providing more accurate predictions and well-founded conclusions. Another important trend is the growing emphasis on edge and fog computing infrastructures, indicating a shift towards decentralised information processing. This is particularly relevant in the context of the development of the Internet of Things, where the speed of data processing and decision-making is critical, as a person can interact with several devices daily – from smartphones to smart home devices. AI can and will track these interactions, creating a comprehensive digital profile that helps researchers understand the subject's connections and identify additional aspects for further analysis.

In the context of armed conflicts, the collection and analysis of digital traces from electronic devices – smartphones, geopositioning systems, video surveillance, network services – acquires particular importance. Occupation and military actions significantly complicate law enforcement access to crime scenes, suspects, victims, witnesses, and also hinder the conduct of investigative actions (Klosterkamp & Jeffrey, 2024). In such conditions, digital forensics becomes a key tool in investigating war crimes, human rights violations, and crimes against humanity in occupied and de-occupied territories. For digital information to become admissible evidence in court – i.e., confirmation that a certain event occurred or did not occur – a series of procedures must be followed: from verifying the source to authenticating the content (Bohdanova, 2023).

During the Russian-Ukrainian war, both state and private initiatives emerged aimed at collecting and documenting digital evidence. In particular, the Mizhvukhamy Cultural Institute (2023) implemented the Wall Evidence project – an archive of inscriptions left by Russian military personnel during the occupation of Ukrainian territories since February 2022. These inscriptions are not only artefacts of Russian military culture but also potential evidence of war crimes. The WarCrimes project, coordinated by the Office of the Prosecutor General of Ukraine, also operates in Ukraine, allowing citizens to submit digital evidence of crimes committed by occupying forces (Office of the Prosecutor General of Ukraine, n.d.). The collected information can be used in national courts, the International Criminal Court in The Hague, and a future special tribunal. In addition, the Starlight media group, together with the civic network OPORA, implemented the Center for War Crimes Documentation initiative (2025), which allows citizens to submit photos, videos, written testimonies, or other evidence that may have procedural significance through an online form. Modern digital technologies allow for: identifying military personnel and commanders; detecting communication and orders within military structures; determining the location of participants in events; and reconstructing the sequence of criminal actions. The collected digital data (audio, video, geolocation data, metadata) can be analysed, verified, and used as evidence in criminal proceedings – both in Ukrainian courts and in international tribunals.

Digital forensics is actively transforming today under the influence of artificial intelligence technologies. It is no longer limited to combating cybercrime but covers a wide range of offences where digital technology is used or leaves traces. The development of companies such as Palantir Technologies demonstrates a shift from pilot projects to the widespread implementation of analytical solutions in the law enforcement sphere. The emergence of the new profession of digital

investigator testifies to a change in approaches to criminal investigations, where data analytics and the use of AI play a key role. According to the Europol (2024) report, artificial intelligence is already effectively used for analysing large datasets, recovering and decrypting information, detecting cyber threats, and analysing digital traces from various devices. This significantly increases the accuracy, speed, and depth of investigations. The collection of digital evidence becomes critically important in wartime conditions, where traditional investigative methods are limited or impossible. Digital forensics specifically allows for documenting crimes, identifying those involved, and building a basis for prosecution even in complex conditions of armed conflict. Thus, AI becomes not only a supporting tool but a strategic factor in ensuring digital justice.

Conclusions

This article investigated modern technological and analytical approaches to the collection, processing, and use of digital traces in the fight against crime, including through the example of the Russian-Ukrainian war. Despite limitations related to the lack of complete official statistics and access to some court decisions, the authors managed to achieve the set goal – to highlight the transformation of criminal procedural tools under the influence of digitalisation, automation, and the implementation of artificial intelligence. During the research, key areas of application for natural language processing, machine learning, large language models, as well as OSINT and SOCMINT methods in the field of criminal prosecution were analysed. It was demonstrated that the increasing volume of available digital traces in Big Data – textual, visual, and geospatial – stimulates the development of analytical platforms capable of automatically detecting crimes, behavioural patterns, and linguistic markers of offences.

The analysis revealed a trend towards the institutionalisation of digital crime recording systems through national initiatives such as WarCrimes, Wall Evidence, and the Center for War Crimes Documentation. Generalising the results obtained, it can be stated that digital forensics and open-source analytics not only compensate for the complexity of investigations in frontline and de-occupied regions but also form a new evidentiary paradigm – fast, decentralised, and legitimate. Conceptually, all of the above indicates a shift in emphasis in criminal proceedings: from traditional sources of evidence to digital data streams processed using AI/NLP/OSINT mechanisms. This means that the role of the interpreter shifts from a human expert to a complex digital system capable of uncovering the truth even beyond physical access to the crime scene. Promising areas for further research include: adapting legal mechanisms to accept digital evidence from open sources, assessing the risks of data manipulation in social networks, and standardising the evidentiary value of Big Data in international criminal justice.

Acknowledgements

Special thanks to the Defence Forces of Ukraine for the opportunity to study and adapt advanced AI technologies under the conditions of Russian military aggression.

Funding

The study was not funded.

Conflict of Interest

None.

References

[1] Arrieta, A.B., *et al*. (2020). Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities, and challenges toward responsible AI. *Information Fusion*, 58, 82-115. doi: 10.1016/j.inffus.2019.12.012.

[2] Ben-Israel, I., Matania, E., & Friedman, L. (Eds.). (2020). *The national initiative for secured intelligent systems to empower the national security and techno-scientific resilience: A National strategy for Israel. Special report to the Prime Minister.* Retrieved from https://www.researchgate.net/publication/361844383.

[3] Berk, R.A. (2021). Predictive policing: Artificial intelligence, predictive policing, and risk assessment for law enforcement. *Annual Review of Criminology*, 4, 209-237. doi: 10.1146/annurev-criminol-051520-012342.

[4] Bohdanova, T. (2023). *How Ukrainians use crowdsourcing to document the war. Exposing the Invisible.* Retrieved from https://exposingtheinvisible.org/en/articles/crowdsourcing-evidence-ukraine-war/.

[5] Center for War Crimes Documentation. (2025). *Submit evidence on war crimes in Ukraine.* Retrieved from https://warcrimescenter.org/en/.

[6] Dang, N.C., Moreno-García, M.N., & De la Prieta, F. (2020). Sentiment analysis based on deep learning: A comparative study. *Electronics*, 9(3), article number 483. doi: 10.3390/electronics9030483.

[7] Daniel, L. (2024). *The alarming "Pig Butchering" cyber scam costing victims billions – are you at risk?* Retrieved from https://www.forbes.com/sites/larsdaniel/2024/10/30/this-halloween-beware-the-pig-butcher/.

[8] European Research Council. (2023). *Towards an evidence-based model for big data policing: Evaluating the statistical-methodological, criminological and legal and ethical conditions.* doi: 10.3030/101088156.

[9] Europol. (2024). *AI and policing: The benefits and challenges of artificial intelligence for law enforcement*. doi: 10.2813/0321023.

[10] Farooq, U. (2024). *Police departments are turning to AI to sift through millions of hours of unreviewed body-cam footage*. Retrieved from https://www.propublica.org/article/police-body-cameras-video-ai-law-enforcement.
[11] Glaser, V.L., Pollock, N., & D'Adderio, L. (2021). The biography of an algorithm: Performing algorithmic technologies in organizations. *Organization Theory*, 2(2). doi: 10.1177/26317877211004609.
[12] Hacker, P. (2023). The European AI liability directives – critique of a half-hearted approach and lessons for the future. *Computer Law & Security Review*, 51, 105871. doi: 10.1016/j.clsr.2023.105871.
[13] Hardyns, W. (2024). *Big data policing in Europa*. Retrieved from http://hdl.handle.net/1854/LU-01JCZD1HKATKKX7R10QFEN7HXS.
[14] Hattenstone, S. (2025). *Deletion of "gang matrix" database will destroy evidence against police, say campaigners*. Retrieved from https://www.theguardian.com/uk-news/2025/feb/02/deletion-of-gang-matrix-database-will-destroy-evidence-against-police-say-campaigners.
[15] Hickey, S. (2025). *"Dear, did you say pastry?": Meet the "AI granny" driving scammers up the wall*. Retrieved from https://www.theguardian.com/money/2025/feb/04/ai-granny-scammers-phone-fraud.
[16] Huang, K., Hu, Z., & Ma, H. (2021). Big data and predictive policing: A review and research agenda. *IEEE Access*, 9, 131536-131548. doi: 10.1109/ACCESS.2021.3114481.
[17] Javaid, M., Haleem, A., Singh, R.P., & Suman, R. (2022). Artificial intelligence applications for Industry 4.0: A literature-based study. *Journal of Industrial Integration and Management,* 7(1), 83-111. doi: 10.1142/S2424862221300040.
[18] Klosterkamp, S., & Jeffrey, A. (2024). The intimate geopolitics of evidence gathering in war crime investigation in Ukraine. *Political Geography Open Research*, 3, article number 100008. doi: 10.1016/j.jpgor.2024.100008.
[19] Lee, Y., Bradford, B., & Posch, K. (2024). The effectiveness of big data-driven predictive policing: Systematic review. *Justice Evaluation Journal*, 7(2), 127-160. doi: 10.1080/24751979.2024.2371781.
[20] Liberty. (2022). *Met to overhaul "racist" Gangs Matrix after landmark legal challenge*. Retrieved from https://surli.cc/whsazj.
[21] Ludwig, J., & Mullainathan, S. (2021). Fragile algorithms and fallible decision-makers: Lessons from the justice system. *NBER Working Paper No. w29267*. doi: 10.2139/ssrn.3926948.
[22] Matulienė, S., Shevchuk, V., & Baltrūnienė, Yu. (2022). Artificial intelligence in law enforcement and justice bodies: Domestic and European experience. *Theory and Practice of Forensic Science and Criminalistics*, 4(29), 12-46. doi: 10.32353/khrife.4.2022.02.
[23] Mayor's Office for Policing and Crime. (2021). *Review of the metropolitan police service gangs violence matrix – update*. London: Greater London Authority.
[24] McDaniel, J., & Pease, K. (Eds.). (2021). *Predictive policing and artificial intelligence (1st ed.)*. London: Routledge. doi: 10.4324/9780429265365.
[25] Mizhvukhamy Cultural Institute. (2023). *Wall Evidence: An open archive of the inscriptions of the Russian occupiers in Ukraine.* Retrieved from https://wallevidence.mizhvukhamy.com/.
[26] National Center for State Courts. (2023). *Use of natural language processing (NLP) in civil case processing: Proof of concept projects*. Williamsburg, VA: National Center for State Courts.
[27] OECD.AI. (2021). Database of national AI policies [Data set]. Powered by EC/OECD. *National AI Policies & Strategies*. Retrieved from https://oecd.ai/en/dashboards/overview.
[28] Office of the Prosecutor General of Ukraine. (n.d.). *WarCrimes.gov.ua.* Retrieved from https://warcrimes.gov.ua/.
[29] Palantir technologies: A leader in data analytics innovation. (2024). Retrieved from https://jejefinance.com/palantir-technologies/?utm.
[30] Polis Solutions. (n.d.). *TrustStat™: The world's first multimodal AI system for the analysis of body-worn camera video.* Retrieved from https://www.polis-solutions.ai/services/truststat.
[31] Raja, A. (2023a). *Model selection and training: Choosing the right model for your data*. Retrieved from https://alizahidraja.medium.com/model-selection-and-training-choosing-the-right-model-for-your-data-b44958d1b4be.
[32] Raja, A. (2023b). *The machine learning process: From data collection to model deployment*. Retrieved from https://alizahidraja.medium.com/the-machine-learning-process-from-data-collection-to-model-deployment-afbf1bdf8729.
[33] Raji, I., & Sholademi, D.B. (2024). Predictive policing: The role of AI in crime prevention. *International Journal of Computer Applications Technology and Research*, 13(10), 66-78. doi: 10.7753/IJCATR1310.1006.
[34] Rotaru, V., Huang, Y., Li, T., Evans, J., & Chattopadhyay, I. (2022). Event-level prediction of urban crime reveals a signature of enforcement bias in US cities. *Nature Human Behaviour*, 6, 1056-1068. doi: 10.1038/s41562-022-01372-0.

[35] Sangher, K.S., Singh, A., Pandey, H.M., & Kumar, V. (2023). Towards safe cyber practices: Developing a proactive cyber-threat intelligence system for dark web forum content by identifying cybercrimes. *Information*, 14(6), article number 349. doi: 10.3390/info14060349.

[36] Schuilenburg, M., & Soudijn, M. (2023). Big data policing: The use of big data and algorithms by the Netherlands Police. *Policing: A Journal of Policy and Practice*, 17(5), article number paad061. doi: 10.1093/police/paad061.

[37] Scott-Davis, S. (2023). *The gangs matrix, where are we now?* Retrieved from https://www.stop-watch.org/news-opinion/the-gangs-matrix-where-are-we-now/.

[38] Sholademi, D.B. (2024). Drones and AI in urban security: Monitoring and mitigating threats. *International Research Journal of Modernization in Engineering Technology and Science*, 6(10), 195-214. doi: 10.56726/IRJMETS61992.

[39] Tarasenko, O. (2020). The application of the science and technology achievements in law enforcement activities. *Legal Science*, 6(108), 424-432. doi: 10.32844/2222-5374-2020-108-6-1.50.

[40] Tarasenko, O. (2021). Features of conducting a search during the investigation of crimes related to illegal content on the internet, with signs of organized crime. *Scientific Bulletin of Public and Private Law*, 5(2), 154-157. doi: 10.32844/2618-1258.2021.5.2.26.

[41] Tosi, D., Kokaj, R., & Roccetti, M. (2024). 15 years of big data: A systematic literature review. *Journal of Big Data*, 11, article number 73. doi: 10.1186/s40537-024-00914-9.

[42] UK Government Office for Science. (2023). *Future risks of frontier AI*. Retrieved from https://assets.publishing.service.gov.uk/media/653bc393d10f3500139a6ac5/future-risks-of-frontier-ai-annex-a.pdf.

[43] Vincze, E.A. (2016). Challenges in digital forensics. *Police Practice and Research*, 17(2), 183-194. doi: 10.1080/15614263.2015.1128163.

[44] Vozniuk, A., & Tytko, A. (2019). Cryptocurrency: Present-day challenges and prospects of development. *Economic Annals-XXI*, 176(3-4), 49-55. doi: 10.21003/ea.V176-05.

[45] Vozniuk, A., Savchenko, A., Tarasevych, T., Dudorov, O., & Klymenko, O. (2020). Electronic money and payments as means of committing crimes. *Academic Journal of Interdisciplinary Studies*, 9(4), 150-159. doi: 10.36941/ajis-2020-0069.

[46] Wickramasekara, A., Breitinger, F., & Scanlon, M. (2025). Exploring the potential of large language models for improving digital forensic investigation efficiency. *Forensic Science International: Digital Investigation*, 52, article number 301859. doi: 10.1016/j.fsidi.2024.301859.

Напрями застосування штучного інтелекту в правоохоронній діяльності: тенденції, виклики та перспективи

Андрій Вознюк
Доктор юридичних наук, професор
Національна академія внутрішніх справ
03035, пл. Солом'янська, 1, м. Київ, Україна
https://orcid.org/0000-0002-3352-5626

Олег Тарасенко
Доктор юридичних наук, професор
Національна академія внутрішніх справ
03035, пл. Солом'янська, 1, м. Київ, Україна
https://orcid.org/0000-0002-3179-0143

Сергій Скрипник
Науковий співробітник
Національна академія внутрішніх справ
03035, пл. Солом'янська, 1, м. Київ, Україна
https://orcid.org/0009-0000-6414-7237

Анотація
Загострення безпекових викликів в умовах цифрової трансформації актуалізує необхідність систематизованого огляду сучасних практик, ризиків і потенціалу впровадження штучного інтелекту в діяльність правоохоронних органів. Метою роботи було узагальнення наукових підходів щодо застосування штучного інтелекту в правоохоронній сфері з фокусом на етапи його розвитку, ключові напрями досліджень і недостатньо вивчені аспекти. Використання методів аналізу й синтезу наукових джерел, контент-аналізу, порівняльного аналізу, класифікації наявних підходів надало можливість оцінити поточний стан наукових досліджень щодо тенденцій, викликів і перспектив залучення штучного інтелекту. Встановлено, що науковий інтерес до застосування штучного інтелекту в правоохоронній сфері суттєво посилився впродовж останнього десятиліття. Стрімкий розвиток технологій штучного інтелекту відкрив нові можливості для автоматизації аналітичних і оперативних функцій, що спонукало науковців до вивчення можливостей та загроз штучного інтелекту. Основну увагу дослідники зосереджують на таких напрямах, як відеоаналітика, прогнозування злочинності, розпізнавання образів й обробка великих даних. Водночас спостерігається брак ґрунтовних міждисциплінарних досліджень, що враховували б етичні, правові та соціальні наслідки використання таких технологій. Констатовано розрізненість у підходах до класифікації ризиків і стандартизації практик упровадження. Засвідчено потребу у формалізації досліджень, що сприятиме збалансованому розвитку штучного інтелекту в правоохоронній діяльності з огляду на безпекові, правові й гуманітарні чинники. Отримані результати можуть бути використані керівниками правоохоронних органів, аналітичними підрозділами та фахівцями із цифрової трансформації для визначення пріоритетних напрямів розвитку й урахування можливих ризиків

Ключові слова:
інформація; цифрова криміналістика; протидія кримінальним правопорушенням; кіберзлочини; цифровізація