UDC 351.74:004(1-87) DOI: https://doi.org/10.32631/pb.2026.3.02

OLHA LUNHOL,
Candidate of Pedagogical Sciences, Associate Professor,
Donetsk State University of Internal Affairs (Kropyvnytskyi),
The Educational and Research Institute for Training Specialists
for Criminal Police Units named after E. O. Didorenko,
Department of Operational and Investigative Activities and Information Security;
https://orcid.org/0000-0001-8128-0072,
e-mail: ordtaib@dnuvs.ukr.education;

OLHA HABORETS,
Doctor of Philosophy, Associate Professor,
Donetsk State University of Internal Affairs (Kropyvnytskyi),
The Educational and Research Institute for Training Specialists
for Criminal Police Units named after E. O. Didorenko,
https://orcid.org/0000-0001-7791-6795,
e-mail: olga-gaborets@ukr.net

INFORMATION AND ANALYTICAL SUPPORT FOR LAW ENFORCEMENT: FOREIGN EXPERIENCE AND DEVELOPMENT TRENDS

The article is devoted to elucidating foreign experience and the leading trends in the development of information and analytical support of law enforcement, as well as to substantiating the directions for its implementation in Ukraine. The relevance of the topic is driven by the digital transformation of the law enforcement sphere, the rapid growth in the volume of data to be processed, the increasing complexity of transnational and organised crime, and Ukraine's European integration course, which requires bringing national approaches closer to the standards of the European Union. The aim of the study is to identify the patterns and trends in the development of information and analytical support of law enforcement agencies in the European Union, the United States of America and the United Kingdom, and to formulate proposals for taking them into account in domestic practice. The methodological basis comprises the comparative legal, formal legal and systemic-structural methods, as well as the methods of analysis, synthesis and generalisation. The article analyses the concept of intelligence-led policing, models of predictive analytics, the institutional and technological solutions of Europol and Interpol, and the mechanisms of information exchange within the European Union. It is established that the key trends are the transition to a proactive, data-driven model of policing, the introduction of artificial intelligence and Big Data technologies, the development of interoperability and cross-border information exchange, and the strengthening of requirements for the protection of personal data and human rights. It is determined that the use of analytical technologies is accompanied by the risks of algorithmic bias and excessive interference with privacy, which requires appropriate legal regulation. It is substantiated that the implementation of foreign experience in Ukraine should take into account the existing infrastructure, the need to train qualified analysts and the security conditions of wartime. The scientific novelty lies in a comprehensive comparative legal generalisation of the leading models and trends in the development of information and analytical support and in identifying the conditions for their adaptation to the domestic legal system. The results obtained may be used for further scholarly research, for improving departmental rule-making, and in the educational process of higher education institutions with specific conditions of study that train police officers.

Keywords: *information and analytical support, law enforcement, criminal analysis, intelligence-led policing, predictive analytics, foreign experience, artificial intelligence, personal data protection.*

Copyright: © 2026 by the authors.
Submitted for possible open access publication under the terms and conditions of the
Creative Commons Attribution (BY) license (https://creativecommons.org/licenses/by/4.0/).

Original article

INTRODUCTION. The effectiveness of law enforcement in modern conditions increasingly depends on the quality, timeliness and completeness of information and analytical support. The digital transformation of social relations, the exponential growth in the volume of data, the spread of cybercrime, and the transnational and organised nature of contemporary crime substantially complicate the tasks facing law enforcement bodies. Under these circumstances, the reactive model of responding to offences already committed is giving way to a proactive approach centred on the analyst, who is capable of transforming disparate datasets into well-founded management decisions.

The scale of these changes can hardly be overestimated. The volume of digital data that may potentially have evidential or orienting significance is growing rapidly, while the sources of such information are becoming ever more diverse – from traditional departmental records to traces in social and communication networks and Internet of Things devices. The ability of a law enforcement agency to detect, within this array, hidden patterns, links and trends is becoming an independent factor in the effectiveness of countering crime. This is precisely why, over recent decades, the world's leading states have been consistently building up systems of information and analytical support, and this problem occupies a prominent place on the agenda of international police cooperation.

The relevance of the study is further reinforced by the fact that the effectiveness of countering crime depends directly on the ability of law enforcement agencies to carry out timely, prompt and reliable analysis of the activities of organised groups and criminal organisations (Honcharuk, 2025). At the same time, Ukraine's course towards membership of the European Union brings to the fore the need to harmonise domestic approaches with European standards, in the system of which the information and analytical component plays a key role. The full-scale armed aggression against Ukraine has additionally sharpened the issues of the security of the information resources of law enforcement agencies and the effective use of analytical tools in the complex conditions of martial law.

Despite considerable attention from scholars, a comprehensive comparative legal understanding of foreign experience and the latest trends in the development of information and analytical support, in conjunction with the possibilities for their implementation in Ukraine, remains insufficiently developed. It is precisely this unresolved part of the general problem that determines the focus of this study: understanding the logic of the development of the relevant systems in the world's leading states makes it possible to avoid erroneous management decisions, to allocate available resources optimally, and to formulate scientifically grounded proposals for improving domestic practice.

PURPOSE AND OBJECTIVES OF THE RESEARCH. The purpose of the article is to identify the patterns and leading trends in the development of information and analytical support of law enforcement on the basis of generalising foreign experience, and to substantiate scientifically sound proposals for its implementation in Ukraine. Achieving this purpose entails addressing the following objectives: 1) to reveal the content and structure of information and analytical support of law enforcement as a scholarly and applied category; 2) to analyse the leading conceptual models (in particular, intelligence-led policing and predictive analytics) and the practice of their implementation in the United Kingdom and the United States of America; 3) to characterise the institutional and technological solutions of the European Union and Interpol in the sphere of information exchange and analytical support; 4) to determine the key technological trends and the related legal and ethical challenges; 5) to formulate proposals for improving the information and analytical support of Ukraine's law enforcement agencies in the light of the experience analysed.

LITERATURE REVIEW. The problem of information and analytical support of law enforcement is interdisciplinary in nature and lies at the intersection of administrative law, management theory, criminalistics and computer science. In domestic scholarship, the theoretical and applied foundations of criminal analysis have been thoroughly elaborated: the work of I. A. Fedchak (2021) and the collective textbook under the general editorship of A. M. Babenko, O. M. Zaiets, V. A. Nekrasov et al. (2020) systematically set out the concept, types and methods of criminal analysis; O. M. Honcharuk (2025) revealed the main components of ensuring the effective activity of the criminal analysis units of the National Police and the structure of the information cycle; the works of O. A. Haborets, O. M. Lunhol and A. O. Voloboiev (2026) substantiated the role of strategic criminal analysis in forecasting and preventing crime; the legal dimensions of the use of AI technologies in this sphere were examined by O. V. Turuta and O. P. Turuta (2022).

Certain applied aspects of the problem are covered in works devoted to ensuring the effective activity of criminal analysis units and the training of analysts (Honcharuk, 2025; Fedchak, 2021), to strategic criminal analysis as a tool for forecasting and preventing crime (Haborets, Lunhol, Voloboiev, 2026), and to the automation of digital evidence collection by means of OSINT in countering organised crime (Nurhaliiev, Lunhol, 2026). The legal features of the use of artificial intelligence technologies by law enforcement actors were studied by I. M. Shopina (2026). At the same time, the vast majority of domestic works focus on individual components of the problem. In foreign scholarship, by contrast, a developed conceptual model of intelligence-led policing has been formed, substantiated by J. H. Ratcliffe (2026), while at the level of the European Union, institutional mechanisms of analytical support have been established, represented by the activities of Europol.

An analysis of the existing body of work shows that, despite considerable attention to individual components of information and analytical support, a comprehensive comparative legal generalisation of foreign experience combined with the identification of the conditions for its implementation in Ukraine – taking into account contemporary challenges such as digital transformation, European integration and the security conditions of wartime – remains insufficiently developed, which determines the need for this study.

METHODOLOGY. The methodological basis of the study is a combination of general scholarly and special legal methods of cognition, applied in accordance with the stated purpose and objectives. The comparative legal method was the leading one and was used to compare the conceptual models, institutional solutions and tools of information and analytical support applied in the United Kingdom, the United States of America and the member states of the European Union, as well as to identify common trends in their development. The application of this very method made it possible but to critically assess the preconditions for their functioning and their potential suitability for the Ukrainian legal system.

The formal legal (dogmatic) method was used in analysing the normative legal acts that govern information and analytical activity, in particular the provisions of Ukrainian legislation, as well as European Union acts in the sphere of data protection and the regulation of AI. The systemic-structural method made it possible to consider information and analytical support as an integral system in which normative, institutional, technological and personnel components interact. The methods of analysis and synthesis were applied to decompose complex phenomena into elements and their subsequent generalisation; the method of generalisation was used to formulate conclusions and proposals; and the logical-semantic method served to clarify the conceptual apparatus, in particular the correlation between the categories of “information support”, “information and analytical support” and “criminal analysis”.

The empirical basis of the study comprises the provisions of the legislation of Ukraine and the European Union, official documents and analytical materials of the European Union Agency for Law Enforcement Cooperation (Europol), and the results of scholarly research by domestic and foreign authors. Given the comparative legal focus of the study, several foundational works published more than five years ago were included because they retain conceptual significance for understanding the genesis of the relevant models. Such a selection of sources ensures the reliability of the results obtained and their correspondence to the current state of scholarly knowledge and practice.

RESULTS AND DISCUSSION. The concept of information and analytical support of law enforcement should be considered in conjunction with related categories. Information support of police services is usually interpreted as a set of methods, measures and means that ensure the creation and functioning of information technologies and their effective use for solving the tasks entrusted to the police. Information and analytical support, by contrast, entails coordinated activity to determine the content, volume and quality of information necessary for preventing crime, as well as measures for the most expedient collection, systematisation, accumulation and processing of such information by means of various methods, techniques and technical tools (Honcharuk, 2025).

The functional purpose of information and analytical support is to satisfy the information needs of decision-making actors at all levels of management – from the direct performance of operational and service tasks to the formation of a strategy for countering crime. Unlike purely information support, which is focused on creating and maintaining information resources, information and analytical support entails an additional – analytical – superstructure that gives information a new quality and turns it into a basis for action. This is why this category combines a technological component (information systems and tools), a substantive component (methods and techniques of analysis) and a subject component (analysts).

The need for developed information and analytical support is directly conditioned by the transformation of crime itself. Organised and transnational crime, cybercrime, and financial and drug-related crimes are increasingly committed according to complex schemes that span several jurisdictions and require the processing of large arrays of heterogeneous data. Under such conditions, the detection of hidden links between persons, events and financial flows becomes possible only through systematic analytical processing of information, and individual episodes acquire evidential significance only in the context of a broader analytical picture.

The core of information and analytical support is analytical activity, which is predominantly predictive in nature and makes it possible to anticipate the course of phenomena in the future and, consequently, to make adequate management decisions (Haborets, Lunhol, Voloboiev, 2026). In applied terms, this activity is realised through criminal analysis, which is defined as the activity of law enforcement analysts in verifying, evaluating and interpreting information about the unlawful acts of individuals and groups, and in establishing significant links between such information in order to determine the tactical and strategic directions of countering and preventing crime (Fedchak, 2021). Traditionally, operational, tactical and strategic levels of analysis are distinguished, as well as open-source intelligence (OSINT) and multi-source data analysis (Honcharuk, 2025).

In structural terms, information and analytical activity encompasses the successive stages of the intelligence cycle: the collection (acquisition) of information, its primary processing and systematisation, analytical processing, and the use and dissemination of the resulting analytical product (Honcharuk, 2025). The most complex and, at the same time, the most important stage is the analytical one, at which disparate pieces of information are transformed into new knowledge suitable for making a well-founded management decision. This circumstance explains why all modern models of information and analytical support are based on the figure of the professional analyst, rather than merely on a set of technical tools.

The leading conceptual model that shapes the development of information and analytical support in common-law states is intelligence-led policing (ILP), substantiated by J. H. Ratcliffe (2026). Within this model, criminal analytics is regarded as a combination of crime analysis and criminal intelligence, functioning within a management system in which analysts influence decision-makers, and response and long-term prevention measures are based on an evidential foundation. Historically, this model was formed in the United Kingdom in the 1990s and subsequently acquired institutional form in the National Intelligence Model. Its essence lies in reorienting police activity from responding to individual events towards the systematic management of the risks posed by the most dangerous persons and places.

Analytical output is differentiated according to three levels: the strategic, which determines long-term priorities; the tactical, oriented towards specific operations; and the operational, which accompanies current work. A key element of the model is the mechanism of tasking and coordination, which ensures the link between analytical conclusions and the allocation of forces and resources. This approach makes it possible to concentrate limited resources on the most dangerous objects, increasing the effectiveness of countering crime at unchanged or even reduced costs.

In a broader theoretical context, the intelligence-led model is part of the general movement towards evidence-based and data-driven policing, which presupposes that decisions on the allocation of resources and the choice of tactics should be based on the systematic analysis of data rather than on intuition or established practice. The management logic of such an approach lies in increasing effectiveness by concentrating efforts on priority areas, the measurability of results and accountability. It is precisely this logic that has made the relevant models attractive to the law enforcement systems of various states, despite the differences in their legal traditions.

In the United States of America, the field of predictive analytics gained parallel currency; it consists in applying analytical – primarily quantitative – methods to identify likely objects of police intervention with the aim of preventing crimes or solving acts already committed. In the scholarly literature, several groups of predictive methods are distinguished – forecasting places and times of heightened risk of crime, forecasting persons prone to committing offences, and forecasting potential victims. Such forecasting is regarded as a continuous cycle in which the collection and analysis of data are followed by police intervention and offenders' responses, and the results obtained are taken into account in the next iteration. Predictive tools are not a "crystal ball" and are effective only provided that the forecast is followed by well-founded response measures backed by appropriate resources. Notably, the use of predictive and other automated tools was, from the outset, accompanied by debate about their correlation with human rights guarantees, the risks of algorithmic bias and the requirements

of due process. At the same time, artificial intelligence technologies are increasingly being used by offenders themselves, in particular to commit cybercrimes (Shopina, 2026; Miahkikh, Shopina, 2025; Ezzeddine, Bayerl, Gibson, 2023).

The practical embodiment of the data-driven approach has taken the form of such organisational and technological solutions as the COMPSTAT system of managerial accountability based on crime statistics, the fusion centres that became widespread after the events of 11 September 2001, and real-time crime centres. Among the best-known predictive policing software products are the PredPol system (subsequently Geolitica) and similar solutions. At the same time, the practice of their application has revealed substantial divergences in assessments of effectiveness and has brought to the fore the debate about the risks of reproducing the biases present in the source data.

These caveats are not merely of theoretical significance. Empirical assessments of the effectiveness of predictive systems vary extremely widely, and certain implemented solutions have demonstrated extremely low predictive accuracy, which has cast doubt on the expediency of their further use (Lee, Bradford, Posch, 2024). The main methodological flaw of predictive policing is that algorithms are trained on historical data about recorded crime, which itself reflects previous response practices. As a result, existing distortions may not only be reproduced but also amplified, forming a vicious circle of excessive attention to certain territories or population groups. This is precisely why the scholarly debate increasingly advances the thesis that an analytical tool is not value-neutral and requires critical human control.

In the European Union, information and analytical support of law enforcement develops primarily in the plane of supranational coordination and information exchange. The central role is played by Europol, which provides the member states with specialised systems for collecting, storing, analysing and linking criminally relevant information. The principal reference system is the Europol Information System, which contains more than 1.6 million objects, while the secure exchange of operational and strategic information is carried out through the SIENA (Secure Information Exchange Network Application) network, introduced in 2009, to which more than 3,000 law enforcement authorities are now connected[1]. Strategic planning is based on the EU Serious and Organised Crime Threat Assessment (EU-SOCTA), on the basis of which crime-fighting priorities are determined within the EMPACT platform[2].

Europol provides analytical support to the member states by means of a specialised analysis system and thematic analytical projects, within which the agency's experts process large and complex arrays of data, including directly on the territory of the member states. The implementation of the defined priorities takes place in the format of four-year EU policy cycles. The next EMPACT cycle is designed for 2026–2029. At the same time, the practice of the functioning of these systems reveals the problem of the uneven contributions of the member states: a significant proportion of the objects in the information systems is formed by a limited number of them, which brings to the fore the task of improving the quality and volume of structured information exchanged by the participants in the cooperation.

Information exchange within the EU is also ensured by the Schengen Information System and by the mechanisms introduced on the basis of the so-called Prüm Decisions, which enable the automated exchange of data on DNA profiles, dactyloscopic (fingerprint) information and vehicle registration. At the global level, an analogous function is performed by Interpol, whose secure I-24/7 network ensures round-the-clock cross-border information exchange and access to international databases. Tellingly, Europol has joined the joint investigation team investigating the international crimes committed in Ukraine, providing its analytical potential, which attests to the practical significance of such mechanisms for our state as well.

A key trend in the development of the European information-exchange architecture is the development of interoperability among large-scale information systems. The introduction of the principles of interoperability is intended to ensure the coordinated operation of individual pan-European databases and to eliminate the situation in which key information about a person – regarding suspects, financial flows or movements – is stored in fragmented systems and not linked to other relevant data. For law enforcement agencies, this means a transition to an integrated information environment in which data become accessible in compliance with established protection guarantees.

[1] Europol. (2024, April 12). *More than 3 000 law enforcement authorities now connected to Europol*. https://www.europol.europa.eu/media-press/newsroom/news/more-3-000-law-enforcement-authorities-now-connected-to-europol.

[2] Europol. (2025). *The changing DNA of serious and organised crime*. https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.

A separate and increasingly significant area of information and analytical activity is open-source intelligence (OSINT) and social media analysis. Specialized web analytics tools make it possible to obtain information relevant to investigations from publicly accessible Internet sources, in particular, regarding a person's circle of contacts, the identification of their accounts in various social networks, or the establishment of the device from which access to the network was carried out (Honcharuk, 2025; Nurhaliiev, Lunhol, 2026; Basysta et al., 2024). Closely connected with this area is the problem of electronic (digital) traces, the volume and diversity of which are growing rapidly along with the spread of mobile devices, means of communication and the Internet of Things.

The technological toolkit of modern analytics also encompasses geographic information systems and methods of spatial analysis, which make it possible to identify crime hot spots and to identify locations at heightened risk, as well as network analysis platforms that visualise the links between persons, events and objects. Solutions based on machine learning and Big Data, capable of processing volumes of information that exceed the possibilities of traditional analysis, are increasingly being introduced (Apostolakis et al., 2022). It is precisely the convergence of these technologies – Big Data, AI, biometrics and geoanalytics – that defines the technological dimension of modern information and analytical support.

The effectiveness of applying any analytical technologies depends critically on the quality and integration of the source data. The fragmentation of departmental records, the inconsistency of formats and problems with the completeness and reliability of data substantially reduce the analytical potential of even the most sophisticated tools. Therefore, one of the cross-cutting tasks of the development of information and analytical support is to ensure the integration of data from many sources on the basis of common standards, which makes it possible to develop a comprehensive analytical picture and improve the quality of management decisions.

No less important is the final stage of the analytical cycle – the preparation and dissemination of analytical products. Operational, tactical, strategic and administrative analytical products must be objective, timely and comprehensible to the addressee, as well as suitable for direct use in decision-making. The standardisation of the form and content of such products, as foreign experience attests, is a necessary condition for their effectiveness and a basis for evaluating the quality of analytical work.

A generalisation of the experience analysed makes it possible to distinguish a number of leading trends in the development of information and analytical support. The first and most significant trend is the transition to a proactive, data-driven model of law enforcement, in which analytics is transformed from an auxiliary function into the basis for making management decisions. The second is the intensive introduction of Big Data and AI technologies. The third is the development of interoperability and cross-border information exchange, driven by the transnational nature of contemporary crime. The fourth is the expansion of the application of open-source intelligence and social media analysis. The fifth trend, which has a counterbalancing character, is the strengthening of requirements for the protection of personal data, ensuring the transparency and accountability of algorithms, and observing human rights.

It is precisely this last trend that determines the limits of the permissible use of analytical technologies. In European Union law, the processing of personal data is governed by the General Data Protection Regulation[1], while the specifics of such processing by competent authorities for the purposes of preventing, investigating and detecting criminal offences are defined by a separate Directive[2]. The adoption of the Artificial Intelligence Act[3] introduced a risk-based approach to the regulation of the relevant systems, in particular

[1] EUR-Lex. (n.d.). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.

[2] EUR-Lex. (n.d.). *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*. https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng.

[3] EUR-Lex. (n.d.). *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)*. https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng.

substantial restrictions on remote biometric identification and certain forms of predictive policing. The scholarly literature emphasises that the use of biometric identification and predictive tools is capable of causing discrimination and excessive interference with privacy, while excessive trust in the conclusions of automated systems gives rise to the risk of "automation bias".

The regulatory approach of the European Union is based on the classification of AI systems according to their level of risk – from prohibited practices to high-risk systems, which include many of the tools applied in the law enforcement sphere and subject to strict requirements regarding transparency, human oversight and risk management. This approach reflects the aspiration to reconcile the effectiveness of analytical technologies with fundamental rights – the right to privacy, non-discrimination and the presumption of innocence. In scholarly and human rights circles, it is emphasised that remote biometric identification in public places poses a particular threat to individual autonomy and therefore requires the strictest safeguards.

A striking example of the contradictory nature of technological progress is facial recognition technology and other means of biometric identification. On the one hand, they substantially expand the possibilities of identifying persons and solving crimes; on the other, they are associated with the risks of false identification, differing accuracy for particular demographic groups and mass surveillance (Johnson et al., 2022). In a number of states, the use of such technologies has already become the subject of litigation and public debate, and certain jurisdictions have introduced moratoriums or restrictions. This confirms that the introduction of the latest analytical tools cannot take place outside the bounds of appropriate legal regulation and public control.

Comparative analysis proves that the vector of development is shifting from response to anticipation, but that this is accompanied by a strengthening of the requirements of proportionality. A distinction is drawn between place-based approaches (identifying territories of heightened risk) and person-based approaches (assessing the probability of a particular person's involvement in criminal activity). It is precisely the latter that provoke the sharpest debates from the standpoint of human rights. This gives rise to the need for a clear normative definition of the grounds, limits and guarantees for the application of predictive tools, which is a common challenge both for states with developed systems and for states that are only building up the relevant practice.

Ensuring a balance between effectiveness and human rights requires not only substantive legal restrictions but also procedural guarantees. These include assessing the impact on data protection before the introduction of new analytical systems, ensuring the principle of purpose limitation in data processing, keeping records of the tools applied, and independent oversight of the activities of law enforcement agencies in the sphere of personal data processing. Such mechanisms make it possible to detect and minimise the risks of abuse in a timely manner, and to maintain public trust in law enforcement agencies, without which effective countering of crime is impossible.

In Ukraine, the institutional and technological foundations of information and analytical support are at the stage of formation. The powers of the police in the sphere of information and analytical support are enshrined in the Law of Ukraine "On the National Police"[1], according to which the police carry out information and analytical activity solely to implement the powers defined by law, form registers and databases that are part of the unified information system of the Ministry of Internal Affairs, and may create their own databases. The practical instrument for implementing these powers is the information and communication system "Information Portal of the National Police of Ukraine"[2], which is a functional subsystem of the unified information system of the Ministry of Internal Affairs.

The formation of the information resources of the police and the maintenance of the relevant registers and databases within the unified information system of the Ministry of Internal Affairs constitute the normative basis of domestic information and analytical support. At the same time, the effectiveness of this system is determined not only by the availability of the relevant records but also by the ability to process the accumulated information analytically, which requires the development of the methodological, technological and personnel components.

Bringing domestic legal regulation closer to the standards of the European Union entails, in particular, the development of legislation on personal data protection in accordance with the requirements imposed on data processing in the

[1] Verkhovna Rada of Ukraine. (2015, July 2). *On the National Police* (Law No. 580-VIII). https://zakon.rada.gov.ua/laws/show/580-19.

[2] Ministry of Internal Affairs of Ukraine. (2017, August 3). *On Approval of the Regulation on the Information and Communication System "Information Portal of the National Police of Ukraine"* (Order No. 676). https://zakon.rada.gov.ua/laws/show/z1059-17.

law enforcement sphere, as well as the elaboration of the principles for applying AI technologies in the light of the risk-based approach. The formation of clear legal grounds, limits and guarantees for the use of analytical tools is a necessary precondition for both the effectiveness and the legitimacy of information and analytical support of law enforcement.

An important component of information and analytical support is international information exchange. Ukraine is a participant in the system of international police cooperation, and interaction with Interpol and Europol opens access to international information resources and analytical products. The deepening of such cooperation – in particular, through accession to the relevant channels of secure information exchange and participation in joint analytical projects – is one of the promising directions for bringing domestic practice closer to European standards.

At the same time, the level of technological support for analytical work in Ukraine remains uneven. As research attests, the most widespread tool of the everyday activity of the bodies of the National Police is still general-purpose office software, and only in certain units are specialised analytical products used, in particular IBM i2 Analyst's Notebook, Maltego, Palantir, ArcGIS and others (Honcharuk, 2025; Strukov, Uzlov, Gnusov, 2021). This contrasts substantially with the practice of leading states, where the use of specialised analytical platforms is the standard. An additional barrier is the shortage of qualified analysts: the effectiveness of criminal analysis depends directly on the level of professional training of specialists, which requires the formation of a system of competences oriented towards modern methods of analytical activity (Honcharuk, 2025; Voloboiev, Lunhol, Haborets, 2022). The corresponding priorities – the introduction of modern analytical technologies and the development of international cooperation – are consistent with the Strategy for the Development of the National Police of Ukraine for 2026–2030[1].

The problem acquires additional significance in the context of Ukraine's European integration and the full-scale armed aggression. Association with the European Union entails the gradual approximation of national legislation and practice to European standards, including in the sphere of data protection and police cooperation. A practical manifestation of such interaction was the involvement of Europol in investigating the international crimes committed in Ukraine. At the same time, the conditions of martial law impose heightened requirements on the security of information resources, the resilience of information infrastructure and cybersecurity, which makes the issues of information and analytical support strategically significant for the effective functioning of the system of the Ministry of Internal Affairs.

A comparison of domestic and foreign practice clearly demonstrates that the decisive factor in the effectiveness of information and analytical support is human capital. The training of a criminal analysis specialist entails the formation of a broad range of competences – from a command of the methods of crime analysis, statistics and geographic information systems to the skills of analytical writing and the preparation of analytical products (Honcharuk, 2025). The absence of systematic training of analysts negates the advantages of even the most modern software, whereas investment in the personnel component yields a long-term effect.

In light of the above and taking into account Ukraine's European integration course, we propose several directions for improving information and analytical support for law enforcement. First, it is necessary to ensure the gradual institutionalisation of the intelligence-led model by standardising analytical products (operational, tactical and strategic) and consolidating their place in the system of management decision-making. Second, it is expedient to expand the application of specialised analytical software and to build up the relevant information infrastructure on the basis of common data formats, which is a precondition for compatibility with European systems. Third, the development of a system of professional training and advanced training of analysts on the basis of scientifically grounded competence models acquires critical importance. Fourth, the introduction of analytical technologies should be accompanied by the harmonisation of national legislation with European Union law in the sphere of personal data protection and the regulation of AI, as well as by the introduction of effective guarantees of the observance of human rights and the transparency and accountability of algorithms. Additional measures include the formation of specialised analytical units and the consolidation of the methodological foundations of their activity, the introduction of data-quality standards, the deepening of cooperation with Europol on a contractual basis, and the creation of mechanisms of ethical control over the application of analytical technologies.

[1] National Police of Ukraine. (2026). *Strategy for the Development of the National Police of Ukraine for 2026–2030*. https://npu.gov.ua/static-objects/npu/sites/1/uploaded-files/strategiia-rozvitku-nacionalnoyi-policiyi-ukrayini-na-2026-2030-roki.pdf.

The implementation of these directions should be carried out in the light of the security conditions of wartime, which impose heightened requirements on the security of information resources.

To summarise, one can note the formation of a paradigm of information and analytical support that is common to the leading states and that combines an intelligence-led model of decision-making, intensive technologisation and supranational cooperation with a simultaneous strengthening of human rights guarantees. It is precisely within this paradigm that the prospects for the development of the relevant system in Ukraine should be conceptualised. At the same time, the mechanical copying of foreign solutions without taking into account the national legal, institutional and security context may prove ineffective or even counterproductive. Therefore, the borrowing of best practice should be accompanied by its critical adaptation, a phased introduction and the mandatory provision of legal guarantees, which corresponds both to the interests of effective countering of crime and to the requirements of the protection of human rights.

CONCLUSIONS. Information and analytical support of law enforcement is an integral system of normative, institutional, technological and personnel components, the core of which is analytical activity of a predictive nature, realised primarily through criminal analysis. Comparative analysis of foreign experience has demonstrated the existence of two interconnected conceptual models – intelligence-led policing, which was formed in the United Kingdom, and predictive analytics, which was developed in the United States of America – as well as developed supranational mechanisms of information exchange and analytical support, represented by the systems of Europol and Interpol.

It is established that the leading trends in the development of information and analytical support are the transition to a proactive, data-driven model of policing, the introduction of Big Data and AI technologies, the development of interoperability and cross-border information exchange, the expansion of the application of open-source intelligence, and the strengthening of requirements for the protection of personal data and human rights. It is proved that technological development is inextricably linked with legal and ethical challenges, in particular the risks of algorithmic bias and excessive interference with privacy, which gives rise to the need for appropriate legal regulation and the preservation of critical human control.

It is substantiated that the implementation of foreign experience in Ukraine should be based on the standardisation of analytical products, the expansion of the application of specialised software, the development of a system for training analysts and the harmonisation of legislation with European Union law, subject to the preservation of the security priorities of wartime. The authors' personal contribution lies in carrying out a comprehensive comparative legal generalisation of foreign experience and in formulating the corresponding proposals. Promising directions for further scholarly research are the study of the legal foundations for applying AI in the activities of Ukraine's law enforcement agencies and the development of mechanisms for ensuring the compatibility of national information systems with those of the European Union.

REFERENCES

1. Apostolakis, K. C., Dimitriou, N., Margetis, G., Ntoa, S., Tzovaras, D., & Stephanidis, C. (2022). DARLENE – Improving situational awareness of European law enforcement agents through a combination of augmented reality and artificial intelligence solutions. *Open Research Europe, 1*. https://doi.org/10.12688/openreseurope.13715.2.

2. Babenko, A. M., Zaiets, O. M., Nekrasov, V. A. et al. (2020). *Fundamentals of criminal analysis* (O. Ye. Korystin, Ed.). Kyiv.

3. Basysta, I., Havrylyuk, L., Hutnyk, A., & Khytra, A. (2024). Use of digital data from open sources during the investigation of criminal offenses: certain aspects. *Scientific and Information Bulletin of Ivano-Frankivsk University named after King Danylo Halytsky, 17*, 227–243. https://doi.org/10.33098/2078-6670.2024.17.29.227-243.

4. Ezzeddine, Ya., Bayerl, P. S., & Gibson, H. (2023, May 31). *Citizen perspectives on necessary safeguards to the use of AI by law enforcement agencies*. arXiv. https://doi.org/10.48550/arXiv.2306.01786.

5. Fedchak, I. A. (2021). *Fundamentals of criminal analysis*. Lviv State University of Internal Affairs.

6. Haborets, O. A., Lunhol, O. M., & Voloboiev, A. O. (2026). Strategic crime analysis as an instrument for crime prediction and prevention. *Central Ukrainian Journal of Law and Public Management, 2*(14), 47–54. https://doi.org/10.32782/cuj-2026-2-6.

7. Honcharuk, O. M. (2025). Main components of ensuring effective activity of criminal analysis units of the National Police of Ukraine. *Uzhhorod National University Herald. Series: Law, 88*(2), 355–363. https://doi.org/10.24144/2307-3322.2025.88.2.48.

8. Johnson, T. L., Johnson, N. N., McCurdy, D., & Olajide, M. S. (2022). Facial recognition systems in policing and racial disparities in arrests. *Government Information Quarterly, 39*(4). https://doi.org/10.1016/j.giq.2022.101753.

9. Lee, Y., Bradford, B., & Posch, K. (2024). The effectiveness of big data-driven predictive policing: systematic review. *Justice Evaluation Journal, 7*(2), 127–160. https://doi.org/10.1080/24751979.2024.2371781.

10. Miahkikh, S. V., & Shopina, Yu. O. (2025, October 15). *Problems of using artificial intelligence to commit cybercrimes* [Round table presentation abstract]. Scientific and practical round table "Cybersecurity in action: rrom personal to national protection", Kyiv, Ukraine.

11. Nurhaliiev, E., & Lunhol, O. (2026, April 2). *Automation of digital evidence collection using OSINT methods in countering organized crime* [Conference presentation abstract]. All-Ukrainian scientific and practical conference "Current issues of the National Police activity as a subject of countering organized crime", Kropyvnytskyi, Ukraine.

12. Ratcliffe, J. H. (2026). *Intelligence-led policing* (3rd ed.). Routledge.

13. Shopina, I. M. (2026). The use of artificial intelligence technologies by law enforcement subjects: peculiarities of legal regulation. *Central Ukrainian Journal of Law and Public Management, 1*, 126–132. https://doi.org/10.32782/cuj-2026-1-16.

14. Strukov, V. M., Uzlov, D. Yu., & Gnusov, Yu. V. (2021). Instrumental intelligent platforms for criminal analysis. *Law and Safety, 4*(83), 64–79. https://doi.org/10.32631/pb.2021.4.07.

15. Turuta, O., & Turuta, O. (2022). Artificial intelligence through the prism of fundamental human rights. *Uzhhorod National University Herald. Series: Law, 71*, 49–54. https://doi.org/10.24144/2307-3322.2022.71.7.

16. Voloboiev, A., Lunhol, O., & Haborets, O. (2022). Digital competence development of future legal specialists: practical aspects. *Bulletin of Science and Education, 5*(5), 193–204. https://doi.org/10.52058/2786-6165-2022-5(5)-193-204.

Received: 1 July 2026

Received in revised form: 15 August 2026

Accepted in revised form: 24 August 2026

Published: 12 October 2026

ОЛЬГА ЛУНГОЛ,
кандидат педагогічних наук, доцент,
Донецький державний університет внутрішніх справ (м. Кропивницький),
Навчально-науковий інститут підготовки фахівців
для підрозділів кримінальної поліції імені Е. О. Дідоренка,
кафедра оперативно-розшукової діяльності та інформаційної безпеки;
ORCID: https://orcid.org/0000-0001-8128-0072,
e-mail: ordtaib@dnuvs.ukr.education;

ОЛЬГА ГАБОРЕЦЬ,
доктор філософії за спеціальністю «Освітні, педагогічні науки», доцент,
Донецький державний університет внутрішніх справ (м. Кропивницький),
Навчально-науковий інститут підготовки фахівців
для підрозділів кримінальної поліції імені Е. О. Дідоренка,
кафедра оперативно-розшукової діяльності та інформаційної безпеки;
ORCID: https://orcid.org/0000-0001-7791-6795,
e-mail: olga-gaborets@ukr.net

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ: ЗАРУБІЖНИЙ ДОСВІД І ТЕНДЕНЦІЇ РОЗВИТКУ

Статтю присвячено з'ясуванню зарубіжного досвіду та провідних тенденцій розвитку інформаційно-аналітичного забезпечення правоохоронної діяльності, а також обґрунтуванню напрямів його імплементації в Україні. Актуальність теми зумовлена цифровою трансформацією правоохоронної сфери, стрімким зростанням обсягів даних, що підлягають опрацюванню, ускладненням транснаціональної та організованої злочинності й курсом України на європейську інтеграцію, який потребує наближення національних підходів до стандартів Європейського Союзу. Метою роботи є виявлення закономірностей і тенденцій розвитку інформаційно-аналітичного забезпечення правоохоронних органів у державах Європейського Союзу, Сполучених Штатах Америки та Великій Британії і формулювання пропозицій щодо їх урахування у вітчизняній практиці. Методологічну основу становлять порівняльно-правовий, формально-юридичний, системно-структурний методи, а також аналіз, синтез і узагальнення. Проаналізовано концепцію поліцейської

діяльності, керованої аналітикою (*Intelligence-Led Policing*), моделі предиктивної аналітики, інституційні та технологічні рішення Європолу й Інтерполу, а також механізми обміну інформацією в межах Європейського Союзу. Установлено, що ключовими тенденціями є перехід до проактивної, керованої даними моделі поліцейської діяльності, впровадження технологій штучного інтелекту та великих даних (*Big Data*), розвиток інтероперабельності й транскордонного обміну інформацією, а також посилення вимог щодо захисту персональних даних і прав людини. Визначено, що застосування аналітичних технологій супроводжується ризиками алгоритмічної упередженості та надмірного втручання у приватність, що потребує належного правового регулювання. Обґрунтовано, що імплементація зарубіжного досвіду в Україні має відбуватися з урахуванням наявної інфраструктури, потреби в підготовці кваліфікованих аналітиків і безпекових умов воєнного часу. Наукова новизна полягає в комплексному порівняльно-правовому узагальненні провідних моделей і тенденцій розвитку інформаційно-аналітичного забезпечення та визначенні умов їх адаптації до вітчизняної правової системи. Одержані результати можуть бути використані для подальших наукових досліджень, удосконалення відомчої нормотворчості, а також в освітньому процесі закладів вищої освіти зі специфічними умовами навчання, що здійснюють підготовку поліцейських.

Ключові слова: *інформаційно-аналітичне забезпечення, правоохоронна діяльність, кримінальний аналіз, поліцейська діяльність, керована аналітикою, предиктивна аналітика, зарубіжний досвід, штучний інтелект, захист персональних даних.*

Цитування (ДСТУ 8302:2015): Lunhol O., Haborets O. Information and Analytical Support for Law Enforcement: Foreign Experience and Development Trends. *Law and Safety*. 2026. No. 3 (102). Pp. 17–27. DOI: https://doi.org/10.32631/pb.2026.3.02.

Citation (APA): Lunhol, O., & Haborets, O. (2026). Information and Analytical Support for Law Enforcement: Foreign Experience and Development Trends. *Law and Safety, 3*(102), 17–27. https://doi.org/10.32631/pb.2026.3.02.

Acknowledgements: None.
Funding: This research did not receive any external funding.
Author contributions: The author confirms sole responsibility for this work. The author approves this work and takes responsibility for its integrity.
Conflict of interest: The author declares no conflict of interest.
The use of artificial intelligence technologies: In this manuscript, the author(s) did not use artificial intelligence tools. The author(s) takes responsibility for the originality, accuracy, authenticity, and integrity of the manuscript, understanding that further detection of the use of artificial intelligence is grounds for retraction of the published article.