UDC 343.98:004.8
DOI: 10.63341/naia-chasopis/4.2025.20

Introduction of artificial intelligence and other innovative technologies in the process of investigating criminal offences in the field of official activity

Oleksandr Amelin*
PhD in Law, Associate Professor
Prosecutor General's Office
01001, 13/15 Riznytska Str., Kyiv, Ukraine
Interregional Academy of Personnel Management
03039, 2 Frometivska Str., Kyiv, Ukraine
https://orcid.org/0000-0002-0933-2111

Abstract
The purpose of the study was to analyse the Ukrainian and international experience of using artificial intelligence (AI) in the investigation of official offences and develop recommendations for adapting best practices to the Ukrainian legal system. The research methodology was based on a comparative analysis of the regulation and practice of AI implementation in Ukraine, the USA, Great Britain, Australia, and Brazil, with the examination of technological mechanisms of functioning, legal guarantees in law enforcement activities. The study established the specifics of the Ukrainian approach to the implementation of technologies through the creation of an integrated system "iCase", which provided electronic interaction between the National Anti-Corruption Bureau of Ukraine, the Specialised Anti-Corruption Prosecutor's Office, and the High Anti-Corruption Court, in contrast to the fragmented implementation in other countries. Technological solutions are systematised: machine learning for analysing large amounts of data, explanatory AI, digital forensics with nine phases of evidence processing, and blockchain analytics for tracking virtual assets. Ukrainian cases were analysed: arrest of Tether, Tron, Ethereum cryptocurrencies in Case No. 991/1512/23 of the Supreme Anti-Corruption Court, verdict in case No. 991/3227/24, risk assessment system in public procurement with 21 automatic indicators, and use of open-source intelligence techniques by the National Anti-Corruption Bureau of Ukraine. International experience has demonstrated the effectiveness of AI, in particular, in the cases of Rolls-Royce, Operation Gold Rush, the work of the European Prosecutor's Office, and the use of the Brazilian bot ALICE. Critical challenges were identified: the problem of the "black box" of algorithms, the risks of system bias, legal gaps in relation to digital assets, and the need to harmonise with the EU AI regulation 2024/1689. The results of the study can be used by anti-corruption bodies in the implementation of AI technologies, the judicial system – to form a unified practice for evaluating digital evidence, legislative authorities – in the development of special legislation on AI, and scientific-educational institutions – to train qualified personnel in the field of digital crime investigation

Keywords:
digitalisation; electronic document management; innovative investigative methods; digital evidence; cybercrime; anti-corruption bodies; illegal enrichment

Article's History:
Received: 10.07.2025
Revised: 28.10.2025
Accepted: 25.11.2025

Suggest Citation:
Amelin, O. (2025). Introduction of artificial intelligence and other innovative technologies in the process of investigating criminal offences in the field of official activity. *Law Journal of the National Academy of Internal Affairs*, 15(4), 20-38. doi: 10.63341/naia-chasopis/4.2025.20.

*Corresponding author

Introduction

Official crimes, especially those with a corruption component, pose a threat to national security, economic stability and citizens' trust in state institutions of Ukraine. Their hidden nature, complexity of proof, and often transnational nature require continuous improvement of investigative methods. In this context, the rapid development of artificial intelligence (AI) technologies and other innovative solutions, including machine learning, blockchain analytics, digital forensics, pattern recognition systems, big data analytics, and geographic information systems, opens up new opportunities to effectively combat these offences.

The problem of exploring the use of AI in the investigation of official crimes is due to the need to overcome the systemic limitations and inefficiency inherent in traditional methods of law enforcement. Among the key limitations are the low speed of processing large amounts of documentary information, which is manifested in the need to involve numerous experts to analyse even standard corruption schemes, and the high time costs of establishing factual circumstances that arise due to complex procedures for verifying and comparing information from different sources. This problem manifests itself in the investigation of multi-episode corruption cases, where the number of documents and, accordingly, the time for their processing increases exponentially.

In a comprehensive study of the peculiarities of applying innovative technologies in criminal analysis, M. Mordvyntsev *et al*. (2025) focus on an in-depth analysis of methodologies for using these technologies. The researchers have identified the potential capabilities of recognition systems at the stage of identification and identification of suspects, offering an innovative approach to their technical implementation, providing for an increase in the effectiveness of Investigation at the early stages of criminal proceedings in the Ukrainian reality. These results are supported by the findings of M. Lontai *et al*. (2024), who viewed AI in Forensic Sciences as a revolutionary tool for transforming investigative activities.

In the field of economic crimes, AI demonstrates qualitatively new opportunities for law enforcement activities. D. Chaikovskyi (2023) revealed the potential of AI as a new tool for combating crimes in the Ukrainian economy. The author demonstrated that AI can be used to analyse text and speech information during preventive measures and investigative actions, which is relevant for the investigation of official crimes with an economic component in the context of digitalisation of the Ukrainian economy. International experience, presented in the paper of N. Ansari (2025) on machine learning in the examination of forensic evidence, demonstrated a new era of forensic analysis, where algorithms are able to automate the processes of classifying and analysing digital traces of crimes.

The practical capabilities of AI in investigations were systematised by S. Gulyamov & S. Tatar (2023), who demonstrated: automated detection of fraud, money laundering, and financial crimes with high accuracy; processing of large amounts of multimedia data (images, videos) in real time; automation of routine tasks of data entry and analysis of evidence. Thereby, the authors identified key risks: algorithmic bias, privacy threats, and potential impact on employment in the investigative sector.

Blockchain technologies open up new prospects for tracking financial flows and determining hidden links in corruption schemes. A study by M. Karchevsky (2021) on cryptocurrencies and blockchain technologies in anti-corruption highlighted these opportunities in the Ukrainian context. The author justified the expediency of introducing blockchain technologies in the activities of Ukrainian anti-corruption bodies to increase the transparency and effectiveness of investigations. These results are consistent with the conclusions of the international study authored by D. Zinnbauer (2025) on the use of AI in the fight against corruption at the global level.

The international context for implementing AI technologies in law enforcement is described in detail by C. Rigano (2019) on the use of AI to meet the needs of criminal justice. The author analysed the US experience in the field of public safety and demonstrated specific AI capabilities: identification of individuals and their actions in video footage related to criminal activity, DNA analysis, automated gunshot detection, and crime prediction.

The legal system of Ukraine faces practical challenges in assessing the authenticity of video evidence in criminal proceedings. O. Gura (2020) established that Ukrainian courts do not have clear enough criteria for determining the reliability of digital materials, which creates legal uncertainty in cases of official offences. Judicial practice shows cases when video evidence was rejected due to the inability to confirm its originality or the lack of a proper digital data storage chain. Ethical aspects of the use of AI in Justice are studied in the training programme for judges of the Supreme Anti-Corruption Court. Y. Bernazuk (2025) determined key risks of algorithmic bias and discrimination when using AI in criminal proceedings. The problem of transparency of algorithmic solutions is closely reviewed in the study by S. Nandipati *et al*. (2024) on the role of explanatory AI in criminal investigations, which offers specific mechanisms to address the "black box" problem to ensure fair justice.

The degree of scientific development of the problem demonstrates the active formation of research areas in the field of technological modernisation of law enforcement activities. Therewith, despite a large number of studies of certain aspects of the use of technologies in law enforcement, a comprehensive analysis of the

introduction of AI and other innovative technologies in the investigation of official crimes in the Ukrainian context was practically not conducted. Most of the existing works concentrate on general issues of digitalisation of criminal justice or technical aspects of individual technologies, leaving out the specifics of their application in the field of combating corruption and official offences.

The study aimed to perform a comprehensive analysis of the introduction of AI and innovative technologies in the investigation of official crimes in Ukraine, identify the advantages and challenges of their application, and evaluate the effectiveness of existing technological solutions in the activities of Ukrainian anti-corruption bodies. The following research tasks were set to achieve the goal: examine the legal basis and technological features of the use of AI in the investigation of official crimes; analyse modern innovative technologies and the practice of their implementation in the activities of Ukrainian law enforcement agencies; develop comprehensive recommendations for further development of legislation, ethical standards, and practical application of innovative technologies.

Materials and Methods

The study was conducted in three main stages using a set of complementary scientific methods and analysis of various sources of information. During the initial stage, the legal basis for regulating official crimes and applying innovative technologies in law enforcement activities was reviewed using the comparative legal method and content analysis. The Article analyses Ukrainian legislation, in particular, the Constitution of Ukraine[1] on the principles of the rule of law and the responsibility of officials, Criminal Code of Ukraine[2] with an emphasis on Section XVII "Criminal offences in the sphere of official activity and professional activities related to the provision of Public Services", Criminal Procedure Code of Ukraine[3] with regard to articles 84, 99, 103 on digital evidence. Attention is paid to the breakdown of Law of Ukraine No. 889-VIII "On Public Service"[4] regarding the principles of integrity and responsibility of civil servants, Law of Ukraine No. 1700-VII "On Prevention of Corruption"[5] on preventive mechanisms and system of restrictions, Law of Ukraine No. 1698-VII "On the National Anti-Corruption Bureau of Ukraine"[6] regarding the authority for innovative investigative methods. The Law of Ukraine No. 794-VIII "On the State Bureau of Investigations"[7] was also analysed in terms of competence in the field of official crimes and Law of Ukraine No. 2074-IX "On Virtual Assets"[8] regarding the legal regulation of cryptocurrencies.

In the second stage, international legal acts and their implementation in Ukrainian legislation, in particular, the United Nations Convention against Corruption[9], ratified by Ukraine in 2006, the Criminal Convention on Combating Corruption[10], and the Civil Law Convention on Corruption[11], were considered. Regulation of the European Parliament and Council of the European Union No. 2024/1689 "On Artificial Intelligence"[12] with requirements for high-risk AI systems in law enforcement. The experience of the European Public Prosecutor's Office (2025) was further reviewed. Using the case method and system analysis, the judicial practice of using digital technologies in cases of official crimes is examined. Judgements in Case No. 991/1512/23[13] regarding the seizure of cryptocurrencies Tether (USDT), Tron (TRX), Ethereum (ETH) in the case under Article 368 of the Criminal Code of Ukraine[14], were also analysed.

During the third stage, a comparative legal method and institutional approach were applied to review the practice of implementing AI technologies in the UK, USA, Brazil, and Australia. In the UK, the case R v. Rolls-Royce PLC on the use of RAVN AI was considered based on the document analysis of P. Yuk (2017). The activities of the National Economic Crime Centre (2025) on the use of machine learning and reports on the activities of law enforcement agencies (UK Government, 2025) were further investigated. In Brazil, the

[1] Constitution of Ukraine. (1996, June). Retrieved from https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.
[2] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text.
[3] Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text.
[4] Law of Ukraine No. 889-VIII "On Public Service". (2015, December). Retrieved from https://zakon.rada.gov.ua/laws/show/889-19#Text.
[5] Law of Ukraine No. 1700-VII "On Prevention of Corruption". (2014, October). Retrieved from https://zakon.rada.gov.ua/laws/show/1700-18.
[6] Law of Ukraine No. 1698-VII "On the National Anti-Corruption Bureau of Ukraine". (2014, October). Retrieved from https://zakon.rada.gov.ua/laws/show/1698-18.
[7] Law of Ukraine No. 794-VIII "On the State Bureau of Investigations". (2015, November). Retrieved from https://zakon.rada.gov.ua/laws/show/794-19#Text.
[8] Law of Ukraine No. 2074-IX "On Virtual Assets". (2022, February). Retrieved from https://zakon.rada.gov.ua/laws/show/2074-20#Text.
[9] United Nations Convention Against Corruption. (2003, October). Retrieved from https://www.unodc.org/documents/brussels/UN_Convention_Against_Corruption.pdf.
[10] Criminal Convention on Combating Corruption. (1999, January). Retrieved from https://rm.coe.int/168007f3f5.
[11] Civil Law Convention on Corruption. (1999, November). Retrieved from https://rm.coe.int/168007f3f6.
[12] Regulation of the European Parliament and Council of the European Union No. 2024/1689 "On Artificial Intelligence". (2024, June). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689.
[13] Judgement of the High Anti-Corruption Court of Ukraine in Case No. 991/1512/23. (2023, June). Retrieved from https://reyestr.court.gov.ua/Review/111590400.
[14] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text.

Law of Brazil No. 12.846 "On Combating Corruption"[1] was considered as a legal basis for the use of technologies in the fight against corruption, technical documentation of the Governance Risk Assessment System (GRAS) for detecting corruption in public procurement (World Bank, 2023). Australia reviewed the activities of the National Economic Crime Centre (2025), which implemented the "Frontier" system for proactive identification of corruption risks in the public sector (Independent Commission against Corruption, 2018). The methodological approach of the study also provided for the development of practical recommendations for improving legal regulation.

Results

Legal basis and classification of official crimes in Ukraine. The investigation of official crimes in Ukraine is a complex legal process based on the fundamental provisions of the Criminal Code of Ukraine[2], in particular, section XVII "Criminal offences in the sphere of official activity and professional activity related to the provision of public services". This section forms the legal basis for countering corruption and official abuse, providing for responsibility for a wide range of acts that undermine the effective and virtuous functioning of the state apparatus and the system of public services. The systematic approach to criminal legal qualification of official crimes reflects the complexity of the problem of corruption in Ukrainian society and the need to use differentiated mechanisms of legal influence. A special feature of the Ukrainian criminal legislation in the field of official crimes is the detailed regulation of various forms of corruption behaviour, which allows law enforcement agencies to apply a differentiated approach to the qualification and investigation of crimes, depending on their specifics. Key articles of the criminal legislation cover the full range of possible official offences, from active forms of abuse of power to passive negligence in the performance of official duties. Table 1 is given to unify the material.

Table 1. Key articles of official crimes under the Criminal Code of Ukraine

Article of the Criminal Code of Ukraine	Name of the crime	The essence of the act
364	Abuse of power or official position	Use of power contrary to the interests of the service
364-1	Abuse of authority (private legal entities)	Abuse in private legal entities
365	Abuse of power by a law enforcement officer	Actions outside the granted authority
366	Official forgery	Entering false information in documents
366-2	Declaring false information	Providing false information in the declaration
367	Official negligence	Improper performance of official duties
368	Obtaining illegal benefits	Bribery by an official
368-5	Illegal enrichment	Acquisition of assets without legal grounds
369	Providing illegal benefits	Offering a bribe to an official

Source: compiled by the author according to the Criminal Code of Ukraine[3]

Corruption acts, such as acceptance of an offer, promise, or receipt of an illegal benefit by an official (Article 368 of the Criminal Code of Ukraine), cover the receipt by an official of an unlawful benefit for themselves or a third person for committing or not committing any action using his or her official position. Illegal enrichment, according to Article 368-5 of the Criminal Code of Ukraine, is defined as the acquisition by an official of assets whose value exceeds his legal income by more than three thousand subsistence minimums for able-bodied persons. Article 369 of the Criminal Code of Ukraine concerns the offer, promise, or provision of undue benefits to an official for committing actions using their official position. These articles create a comprehensive system of criminal and legal counteraction to corruption, covering both active and passive forms of corruption behaviour. The legislative approach to regulating official crimes reflects international standards of anti-corruption policy and accounts for the specifics of the functioning of the Ukrainian state apparatus. Proof of official crimes is often complicated by their latent nature, the presence of complex schemes, and the use of official position to conceal traces, in addition to large volumes of documentation and financial transactions, which requires law enforcement agencies to use special investigative methods and analytical approaches.

The variety of elements of crimes provided for in Section XVII Criminal Code of Ukraine determines the need for law enforcement agencies to apply a wide range of investigative methods and use modern technological solutions. Each Article provides for different objects of criminal encroachment, forms of guilt, and methods of commission, which require a differentiated approach to collecting and evaluating the evidence base. Official forgery requires a detailed analysis of documents and handwriting examinations, while

[1] Law of Brazil No. 12.846 "On Combating Corruption". (2013, August). Retrieved from https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12846.htm.
[2] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text.
[3] Ibidem, 2001.

illegal enrichment requires a deep investigation of financial flows and property declarations using financial analysis methods. AI systems that are implemented to investigate official crimes cannot be universal "boxed" solutions due to the specifics of each type of offence. They should be modular and adaptive, capable of processing various types of data, from text documents and financial transactions to communication records and video materials. This means using specific algorithms to identify patterns specific to each type of crime that affect the foundations of AI systems, the requirements for their development and training.

The Criminal Code of Ukraine defines the main elements of official crimes and establishes criminal sanctions for their commission, but it is not the only regulatory legal act in this area. The comprehensive system of countering official offences includes special laws on Civil Service and Prevention of corruption, bylaws of anti-corruption bodies, and international conventions and standards. Without considering these additional legal sources, the picture of regulating official crimes would be incomplete since they establish preventive mechanisms, procedural aspects, and institutional bases for combating corruption. It is advisable to address the main thematic blocks of normative legal acts and their functional purpose in the investigation process to systematise the legal regulation of official crimes in Ukraine, which are shown in Table 2.

Table 2. Legal basis for regulating official crimes in Ukraine

Theme block	Regulatory act	Key provisions	Importance for the investigation of official crimes
Principles of public service	Law of Ukraine No. 889-VIII	Rule of law, legality, professionalism, integrity, political impartiality	Creates an ethical basis for distinguishing legitimate official activities from official crimes
Preventive mechanisms	Law of Ukraine No. 1700-VII	Declaration of property and income; settlement of conflicts of interest; system of restrictions and prohibitions	Provides early detection of corruption risks and creates an evidence base for investigating illicit enrichment
Disciplinary responsibility	Law of Ukraine No. 889-VIII	Remark, reprimand, warning about incomplete official compliance, dismissal from office	The graded system of penalties allows you to differentiate liability depending on the severity of violations
Financial liability	Law of Ukraine No. 889-VIII	Right of recourse of the state for intentional damage	Creates an additional deterrent and mechanism for compensation of losses from official crimes
Institutional arrangements	Bylaws of the National Agency for the Prevention of Corruption	Methodological recommendations on conflicts of Interest; Code of Ethical Conduct; system of explanations	Provide a unified interpretation of anti-corruption norms and practical tools for law enforcement
International standards	United Nations Convention against Corruption; Criminal Convention on Combating Corruption; Civil Law Convention on Corruption	Global standards for criminalisation of corruption acts; harmonisation with European standards; protection of whistleblowers	Create common international approaches to combating corruption and provide the basis for international legal assistance
Monitoring and control	Participation in GRECO (since 2006)	Regular international monitoring of the anti-corruption system	Provides an external assessment of the effectiveness of the anti-corruption system and recommendations for improvement
Special conditions	Explanation of the National Agency for the Prevention of Corruption on martial law	Simplified declaration procedures for military personnel while maintaining the main mechanisms	Adapt anti-corruption mechanisms to special conditions without losing the effectiveness of control

Source: compiled by the author based on Law of Ukraine No. 889-VIII[1], Law of Ukraine No. 1700-VII[2], United Nations Convention against Corruption[3], Criminal Convention on Combating Corruption[4], Civil Law Convention on Corruption[5], Code of Ethical Conduct for Employees of the National Agency for Corruption Prevention[6]

The analysis of the presented legal framework indicates a multi-level system of regulation of official crimes in Ukraine, covering preventive, repressive, and restorative mechanisms. Civil service and corruption prevention laws play a central role, providing a legal basis for distinguishing between lawful and illegal official behaviour. International standards ensure the harmonisation of the Ukrainian anti-corruption system with European requirements, while departmental acts of the National Agency for the Prevention of Corruption detail practical aspects of law enforcement. The system is characterised by a comprehensive approach – from

[1] Law of Ukraine No. 889-VIII "On Public Service". (2015, December). Retrieved from https://zakon.rada.gov.ua/laws/show/889-19#Text.
[2] Law of Ukraine No. 1700-VII "On Prevention of Corruption". (2014). Retrieved from https://zakon.rada.gov.ua/laws/show/1700-18.
[3] United Nations Convention against Corruption. (2003, October). Retrieved from https://www.unodc.org/documents/brussels/UN_Convention_Against_Corruption.pdf.
[4] Criminal Convention on Combating Corruption. (1999, January). Retrieved from https://rm.coe.int/168007f3f5.
[5] Civil Law Convention on Corruption. (1999, November). Retrieved from https://rm.coe.int/168007f3f6.
[6] Code of Ethical Conduct for Employees of the National Agency for Corruption Prevention. (2019, May). Retrieved from https://nazk.gov.ua/uk/documents/rishennya-vid-17-05-2019-1382-pro-zatverdzhennya-kodeksu-etychnoyi-povedinky-pratsivnykiv-natsionalnogo-agentstva-z-pytan-zapobigannya-koruptsiyi/.

ethical principles of public service to specific monitoring and control procedures, which enable effective counteraction against various forms of official offences. The analysis of the legal basis for the investigation of official crimes in Ukraine shows the complexity and multidimensional nature of this issue, which requires an integrated approach to countering corruption manifestations. The criminal legislation of Ukraine in the field of official crimes is characterised by sufficient detail and coverage of a wide range of corruption acts, which meets international standards of anti-corruption policy. However, the effectiveness of law enforcement largely depends on the quality of the investigation, which is complicated by the latent nature of official crimes and the need to process large amounts of diverse information. The introduction of AI technologies in the process of investigating official crimes should address the specifics of each type of offence and require the creation of specialised modular systems.

Innovative technologies and their application in criminal investigations. The use of AI and machine learning to analyse large amounts of data, recognise patterns, predict crimes, and detect anomalies is one of the most promising areas of modern criminal investigation. AI and machine learning algorithms are capable of processing and interpreting large amounts of data, which is important for solving complex criminal schemes (Ansari, 2025). AI can be used to analyse text and speech information during preventive measures and investigative actions (Chaikovskyi, 2023). In Computer Forensics, machine learning algorithms make it much easier to classify digital files and prioritise them for further investigation by analysing metadata, which increases the speed and efficiency of analysing large amounts of digital evidence. AI is also used in the field of public safety for video and image analysis, DNA analysis, shot detection, and crime prediction (Rigano, 2019). These systems are able to overcome human errors, learn complex tasks, and even develop their own complex facial recognition parameters that go beyond what humans can see.

The role of explanatory AI in ensuring transparency and accountability is becoming a priority in the context of criminal justice. The "black box" nature of many AI models creates challenges for accountability and justice in criminal justice. Explanatory AI acts as a critical response to these problems, with the goal of making the initial data of AI systems understandable to humans, thereby providing interpreted conclusions and increasing trust (Nandipati *et al*., 2024). As emphasised by Y. Bernazuk (2025), in the training programme for judges of the High Anti-Corruption Court, opacity, the inability to explain AI decisions, and the risks of bias are key features of the "black box" that create legal and ethical challenges in areas where motivation is needed, such as justice.

Digital forensics, or forensic science, is the applied science of investigating computer-related crimes that focuses on finding, obtaining, storing, analysing, and presenting digital evidence. This industry has evolved significantly with the advent of cybercrime and the development of sophisticated digital investigation models. The digital forensics process includes several steps that must be carefully followed in order for digital evidence to be acceptable in court. A detailed structure of these steps and related tools is presented in Table 3.

Table 3. Digital forensics phases and typical tools

Phase	Description	Key actions / Methods	Typical tools
Identification	Identify and localise potential digital evidence	Search and recognition of evidence; documentation of the storage location	Inspection protocols, scene diagrams, photo recording
Saving	Protecting the integrity of detected data from changes or corruption	Isolation, security, and storage of data; creation of forensic duplicates (images)	FTK Imager (for creating images)
Collecting evidence	Extracting data from devices in compliance with forensic standards	Collecting data from deleted devices using specific methods	The Sleuth Kit
Security of evidence	Providing a controlled and secure environment for storing evidence	Access to a secure environment; ensuring accuracy, authenticity, and accessibility	Specialised repositories, access control systems, accounting logs
Getting data	Seizure of electronically stored information from suspected digital assets	Extraction of electronically stored information; ensuring data integrity when receiving data	FTK Imager
Analysis	Reconstruction and interpretation of digital data to identify relevant information	Data analysis, identification, separation, transformation and modelling; metadata analysis; recovery of deleted files	Sleuth Kit, Xplico (for network analysis), specialised tools for analysing files and registries
Evaluation of evidence	Correlation of the identified data with the circumstances of the case and their legal assessment	Careful assessment of the compliance of data with the scope of the case	Analytical software, case databases
Documentation and reporting	Create a detailed record of all Investigation steps and conclusions	Record all data; prepare an official report for the court	Document management systems, report templates, electronic signature tools
Presentation	Presentation of collected and analysed evidence in court	Generalisation of conclusions and their presentation	Presentation software, data visualisation tools, multimedia equipment

Source: compiled by the author based on open analytical sources (Cyber Writes Team, 2023; What is digital forensics..., 2024)

The emphasis on careful multiphase processes and specialised tools for digital forensics shows that the integrity and chain of digital evidence storage is paramount. Unlike physical evidence, digital evidence has the property of instability and is subject to alteration without leaving visible traces of interference. The legal system's reliance on digital evidence means that any failure in these forensic processes or failure to authenticate evidence can lead to their inadmissibility, effectively undermining the entire investigation. This is important in office crime cases, where digital footprints are often central. This requires continuous training for lawyers and a solid legal framework for regulating digital evidence, as highlighted by the Supreme Court in cases on the authenticity of video evidence (Gura, 2020). The transition from the "investigative type" to the "adversarial" criminal process further increases the importance of irrefutable digital evidence.

Big data analysis platforms allow law enforcement agencies to process and analyse huge amounts of data from various sources to identify suspicious indicators, patterns, correlations, and trends. This is crucial for proactive policing, identifying criminal trends, preventing threats, and solving complex cases. In particular, big data analytics can identify crime trends by analysing historical crime data to identify "hot spots" and predict the locations and times of likely crimes, enabling proactive allocation of resources, reducing response times, and deterring criminal activity. Real-time data analytics help law enforcement agencies to monitor and respond immediately to emerging threats, for example, by analysing social media feeds during public events (The power of big…, 2025). By integrating data from a variety of sources, these platforms help investigators pinpoint patterns, unusual actions, and hidden connections in cases of identity theft, financial fraud, organised crime, and cybercrime.

The ability of Big Data analysts to predict crime hotspots and identify emerging threats demonstrates a fundamental shift from a purely reactive investigation model to a more proactive and preventive approach. For official offences, this means moving from investigating after exposing a corruption scheme to potentially identifying risks or early indicators of corruption before damage is done. This allows for more efficient allocation of limited resources and potentially deters criminal activity by increasing the likelihood of detection. This shift, while promising to improve efficiency and prevention, raises considerable ethical and privacy concerns about potential over-surveillance, algorithmic bias in targeting, and the erosion of civil liberties, which must be carefully balanced with public safety goals, as in the Council on Criminal Justice (2025) report. The success of this approach depends on the quality and representativeness of the data.

Blockchain forensics involves the use of specialised tools and procedures to extract and analyse data from the blockchain, including transactions, addresses, and other data, along with the search for and tracking of individuals and groups involved in illegal activities. These methods are used to investigate financial crimes such as fraud, money laundering, and terrorist financing (Merkle Science, 2025). Methods include address clustering (grouping addresses controlled by a single entity), transaction tracking (tracking the flow of digital assets from origin to destination), and linking to off-network data (such as IP addresses, social media profiles) to create a complete profile of individuals. Despite the transparency of the registry, the pseudo-anonymous nature of cryptocurrency addresses, the lack of a central authority, and the use of mixing services create substantial problems for investigators. Transactions of bitcoin and other virtual currencies are publicly recorded in online blockchain registries, identifying users only by their cryptocurrency address-a long string of letters and numbers – without names, locations, or other personal identification data. The main paradox of the blockchain in criminal investigations is its internal transparency (all transactions are recorded in the public register), combined with the pseudo-anonymity of addresses (no direct connection with personal identification). Although the registry is open, linking a cryptographic address to a real person requires complex "de-anonymisation" techniques and often depends on "off-network data" or collaboration with exchanges.

The proliferation of smart devices and Internet of Things (IoT) technologies creates fundamentally new opportunities for collecting digital evidence in cases of official offences. Smartphones, smartwatches, Global Positioning System (GPS navigation) systems, and other connected devices generate metadata about location, time, and behavioural patterns (U.S. General Services Administration, 2025). Modern cars equipped with advanced telematics systems record almost all driver actions, preserving turn-by-turn navigation, speed, acceleration and detailed data on turning on headlights, opening doors, and fastening seat belts. The most documented case involving the use of GPS tracking in the investigation of official offences is the case of Cunningham v. State Dep't of Labor[1], where Michael Cunningham, director of the New York State Department of Labour, was accused of falsifying timesheets. Investigators installed a GPS device on the employee's personal BMW without a warrant and tracked his movements for a month, finding notable discrepancies between the stated working hours and the actual location. In the

[1] Justia Opinion Summary of the Court of Appeals of NY in Case "Cunningham v. State Dep't of Labor". (2013, June). Retrieved from https://law.justia.com/cases/new-york/court-of-appeals/2013/123.html.

Michigan theft case, police established a link between the perpetrator and the stolen car due to GPS data, door opening records, and mobile phone connections (Solon, 2020). An audit by the North Carolina Department of Motor Vehicles (2017-2020) found systemic abuse of official vehicles totalling more than USD 100,000, including a DMV inspector who made unauthorised commutes worth USD 85,000 over three years, leading to the installation of telematics systems throughout the state fleet (Wood, 2017).

Smart home devices store recordings of voice commands that can be requested by law enforcement agencies under a court order. In a criminal case in Arkansas, prosecutors tried to obtain recordings from an Amazon Echo for a murder investigation (Chin, 2025). A study by O. Trebilcock (2020) shows that these devices can accidentally activate and record conversations even without pronouncing the "activator word". Behavioural biometrics analyses typing patterns and the use of the mouse to identify users even when using other people's accounts, which is important for detecting unauthorised access to confidential information. The United States Government Accountability Office (2020) report documents 100 confirmed cases of time-tracking violations at 24 federal agencies from 2015 to 2019, detected using IoT systems, including access card login systems, video surveillance, and GPS data from government devices.

Drone technologies allow detecting official offences through quality control of materials, when the aerial survey records the use of low-quality or cheaper materials instead of those stated in the tender documentation, which, when compared with the technical specifications, establishes the fact of deception and obtaining illegal benefits by the contractor with the assistance of corrupt officials. The most common types of reports forged in the construction industry include material quality reports (drones with high-resolution cameras can verify the materials actually used), work progress reports (timestamped videos document the real progress of construction), safety compliance reports (aerial monitoring can detect non-compliance with safety standards), and environmental assessments (aerial surveillance can detect unauthorised environmental violations). The U.S. Occupational Safety and Health Administration has introduced protocols for the use of unmanned systems for construction site inspections (Galassi, 2018), and the GSA Inspector General issued a 2023 warning against the use of prohibited drones to photograph construction sites in the port of San Luis, Arizona[1]. Monitoring of the work schedule through the timestamps of drone images, combined with document analysis, reveals systematic forgery of construction progress reports, when drones record the absence of work on the site, but official reports on the progress of work, reports on the completion of construction stages, and reports on the use of materials claim the opposite, indicating official forgery of documents.

Monitoring of social networks is already actively used to identify official offences through the analysis of inconsistencies in the lifestyle of officials with their documented income. In Ukraine, the National Agency on Corruption Prevention (2025) performs "lifestyle monitoring" of public figures. According to the results of such monitoring, the National Agency on Corruption Prevention (2024) revealed signs of acquisition of unjustified assets in the amount of UAH 4.85 million by the former acting head of the Kharkiv Centre for Recruitment and Social Support. The National Agency for the Prevention of Corruption also monitors disinformation campaigns on social networks, analysing more than 109 thousand messages on Telegram, Facebook, and X/Twitter. Specific ways to spot misconduct on social media include documenting bribery when Instagram photos and Facebook posts show a luxurious lifestyle that doesn't match an official's official income, suggesting they're getting illegal benefits from contractors or other interested parties. In case of official negligence, social networks can record the presence of a civil servant in places where they should not be during working hours, or document their activities that contradict the performance of professional duties, for example, photos from entertainment events during critical situations that required their personal control.

The legal basis for the use of digital evidence in Ukraine is regulated by the Criminal Procedure Code of Ukraine[2], specifically, articles 84, 99, 103. Ukraine has signed the Budapest Convention on Cybercrime, which creates an international legal framework for cooperation in the field of digital investigations. Recent legislative initiatives pose risks of political interference in law enforcement activities. The integration of AI and innovative technologies in the investigation of official offences opens up new opportunities for fighting corruption, but requires careful legal regulation and the development of mechanisms to protect citizens' rights.

Cases and prospects of using innovative technologies in the investigation of official crimes in Ukraine. The legal basis for the use of digital technologies in pre-trial investigations is laid down in Law of Ukraine No. 1698-VII[3], which defines the powers

[1] Alert Memorandum: PBS Allowed the Use of a Drone from a Prohibited Source to Photograph Construction at a Land Port of Entry in San Luis, Arizona. (2025, March). Retrieved from https://www.gsaig.gov/sites/default/files/audit-reports/A220036-5%20Alert%20Memorandum.pdf.

[2] Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text.

[3] Law of Ukraine No. 1698-VII "On the National Anti-Corruption Bureau of Ukraine". (2014, October). Retrieved from https://zakon.rada.gov.ua/laws/show/1698-18.

of the National Anti-Corruption Bureau of Ukraine to apply innovative investigative methods. Similar powers of the State Bureau of Investigation are regulated by Law of Ukraine No. 794-VIII[1]. The use of OSINT methods (intelligence from open sources) in criminal proceedings is based on the general principles of collecting evidence, enshrined in articles 93, 99 of the Criminal Procedure Code of Ukraine[2], which allow the use of information from open sources as an evidence base, provided that the requirements for the admissibility of evidence are met. The National Anti-Corruption Bureau (2021) actively implements innovations in pre-trial investigation, including the translation of criminal proceedings into electronic format, the use of procedural interview methods, and standardisation of pre-trial investigation.

One of the most important initiatives is the "iCase" pre-trial investigation information and telecommunications system. The legal basis for the functioning of the "iCase" system is established by Article 106-1 of the Criminal Procedure Code of Ukraine and Order of the National Anti-Corruption Bureau of Ukraine No. 175/390/57/72 "On the Information and Telecommunications System for Pre-Trial Investigation "iCase"[3]. The detailed procedure for the functioning of the system is defined by the regulation on the information and telecommunications system of pre-trial investigation "iCase". This system, developed with the support of the EU Anti-Corruption Initiative, optimises the pre-trial investigation of anti-corruption bodies, is integrated with the Unified Register of pre-trial investigations and judicial systems, allowing the National Anti-Corruption Bureau of Ukraine, the Specialised Anti-Corruption Prosecutor's office, and the High Anti-Corruption Court to interact online. "iCase" reduces time, optimises resource usage, and promotes effective digital adoption in Justice (National Anti-Corruption Bureau, 2025).

The State Bureau of Investigation (2025) demonstrates the practical application of digital technologies through the active seizure of documents and electronic media as evidence of illegal operations, which confirms the effectiveness of using digital traces in cases of official crimes. For example, in the case of embezzlement of state property by the heads of Ukrproftur and the Federation of Trade Unions, the state Bureau of Investigation seized electronic information carriers confirming fictitious real estate purchase and sale agreements.

Ukrainian judicial practice is already facing criminal proceedings related to the use of cryptocurrencies and other innovative technologies in the field of official offences, which demonstrates both new opportunities for criminals and new challenges for law enforcement agencies in the use of AI and digital technologies for investigation. This suggests that while operational efficiency is improved by the introduction of AI and digital tools in the investigation of official offences, the deep legal certainty and consistency required for a full-fledged digital criminal justice system using AI technologies are still under development, the lack of a clear legal status of virtual assets and regulation of the use of AI creates gaps and difficulties for investigators and prosecutors in the use of innovative technologies, potentially hindering asset recovery and successful sentences in cases of official offences involving new digital forms of illegal profits. This highlights the urgent need for comprehensive legislative reform that addresses the unique characteristics of digital evidence, virtual assets, and AI's ability to counter official crimes.

The use of AI in these criminal proceedings was conducted through the use of a specialised blockchain-analytical platform Chainalysis Reactor, which operates on the basis of machine learning algorithms for automated cluster analysis of cryptocurrency addresses, deterministic tracking of transaction chains and identification of abnormal patterns of movement of digital assets (Internal Revenue Service, 2023). Technical implementation includes the use of heuristic algorithms to group addresses of a single owner, assign risk scores through multi-layered neural networks, and automatically deanonymise pseudonymous blockchain operations. Ukrainian detectives of the National Anti-Corruption Bureau of Ukraine, prosecutors of the Specialised Anti-Corruption Prosecutor's office, and other law enforcement agencies have received certified training in cryptocurrency forensic science within the framework of the programme of international cooperation with the Criminal Investigation Department of the US Internal Revenue Service, which ensured professional competence in applying these technological solutions in pre-trial investigations. The practice of the Supreme Anti-Corruption Court regarding the seizure of virtual assets in cases of official crimes is of major scientific interest, particularly the case when the court granted the prosecutor's request for the arrest of USDT, TRX, ETH belonging to a suspect and located in a multi-currency crypto wallet, criminal proceedings were conducted under Part 4 of Article 368 of the Criminal Code of Ukraine[4], the sanction of which provides for a mandatory additional penalty in the form of confiscation of property. The

[1] Law of Ukraine No. 794-VIII "On the State Bureau of Investigations". (2015, November). Retrieved from https://zakon.rada.gov.ua/laws/show/794-19#Text.
[2] Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text.
[3] Order of the National Anti-Corruption Bureau of Ukraine No. 175/390/57/72 "On the Information and Telecommunications System for Pre-Trial Investigation "iCase". (2021, December). Retrieved from https://zakon.rada.gov.ua/laws/show/v0390886-21#Text.
[4] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text.

court considered sufficient grounds to believe that virtual assets belong to the suspect and are the subject of possible confiscation of property as a form of punishment, the use of seizure of virtual assets complies with the principle of reasonableness and does not create negative consequences for third parties, and the degree of interference with the rights of the suspect is proportionate to the task of criminal proceedings and justifies the needs of pre-trial Investigation[1]. In Judgment in Case No. 991/3227/24[2], the accused – a people's deputy of Ukraine – offered and transferred illegal benefits in the form of cryptocurrency (0.39 BTC, equivalent to ≈10036 USD) to an official for assistance in allocating budget funds. The court found him guilty under Part 4 of Article 369 of the Criminal Code of Ukraine, sentenced him to 8 years in prison, confiscation of all property, and deprivation of the right to hold public office for 3 years. In addition, the court applied a special confiscation of cryptocurrency and the hardware wallet "LedgerNano S Plus" as physical evidence.

The criminal proceedings against Yuriy Shchyhol, former head of the State Service for Special Communications and Information Protection of Ukraine, set a precedent for Ukrainian law enforcement practice. On 30 November 2023, the High Anti-Corruption Court issued a ruling to seize crypto assets with a total value of USD 1,476,963, including USDT 1,201,285, BTC 6.9, and TRX 331 (The court seized…, 2023). Identification and quantification of these virtual assets became possible as a result of the use of the cryptanalytic platform Chainalysis Reactor, which was accessed by Ukrainian law enforcement agencies in the framework of bilateral cooperation with the Criminal Investigation Department of the US Internal Revenue Service. The technological process included automated analysis of blockchain transaction graphs, the use of heuristic algorithms for address clustering, and machine learning to detect attempts to obfuscate financial flows.

The Supreme Anti-Corruption Court is increasingly considering cases where the evidence base includes analysis of blockchain data. The National Anti-Corruption Bureau of Ukraine, under the procedural guidance of prosecutors of the Specialised Anti-Corruption Prosecutor's office, actively investigates corruption crimes using virtual assets, and the relevant materials are submitted to the court. The National Anti-Corruption Bureau of Ukraine systematically trains its detectives in methods of investigating crimes with cryptocurrencies and reports on cases related to bribes or false declarations of digital assets.

One of the most promising initiatives is a joint project of the Ministry of Digital Transformation and the EU Anti-Corruption Initiative in Ukraine. A special IT module was developed to monitor the Prozorro Portal that uses 21 automatic risk indicators to detect potentially corrupt purchases (EU Anti-Corruption Initiative, 2025). The algorithm-based system analyses purchases and signals anomalies, which helps regulatory and law enforcement agencies focus on the most suspicious tenders. This experience demonstrates Ukraine's gradual integration into global trends in the use of AI in criminal proceedings, going beyond the simple digitalisation of document flow. The legal regulation of the use of AI in Ukraine is characterised by considerable gaps. According to lawyer A. Klyan (2022), Ukrainian legislation does not contain a legal definition of AI, and liability for its misuse is not regulated. The main programme document in this area remains the concept of AI development in Ukraine, approved by Resolution of the Cabinet of Ministers of Ukraine No. 1556-r "On Approval of the Concept for the Development of Artificial Intelligence in Ukraine"[3]. The document defines the absence or imperfection of legal regulation of AI as one of the key problems that need to be solved. K. Tokarieva & N. Savliva (2021) note that AI activities are not regulated by Ukrainian legal acts. This situation creates legal uncertainty about the use of AI technologies in law enforcement and legal proceedings.

However, court cases involving cryptocurrencies and video evidence reveal fundamental legal challenges in adapting existing rules of evidence to innovative technologies for investigating official offences (for example, the definition of "physical evidence", the originality of digital files, the use of AI to analyse evidence), to the unique nature of digital and virtual assets. Courts are forced to interpret traditional laws in new contexts of AI and blockchain analytics applications, which sometimes lead to inconsistent decisions or rely on broad interpretations to ensure confiscation (Gura, 2020). The Ukrainian experience demonstrates pragmatic, step-by-step digitalisation of criminal proceedings with the introduction of AI elements and innovative technologies in the investigation of official offences, while using OSINT methods and analytical tools for detecting official crimes.

International experience in using AI in the fight against official crimes. International experience demonstrates effective solutions along with systemic restrictions on the introduction of AI and innovative technologies in the fight against crime, in particular, official offences. Law enforcement agen-

[1] Judgement of the High Anti-Corruption Court of Ukraine in Case No. 991/1512/23. (2023, June). Retrieved from https://reyestr.court.gov.ua/Review/111590400.
[2] Judgment of the Appeal Chamber of the High Anti-Corruption Court in Case No. 991/3227/24. (2024, December). Retrieved from https://opendatabot.ua/court/124014613-06c66175453c19e31fcf50d87ff6e93a.
[3] Resolution of the Cabinet of Ministers of Ukraine No. 1556-r "On Approval of the Concept for the Development of Artificial Intelligence in Ukraine". (2020, December). Retrieved from https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text.

cies in the world's leading countries are actively implementing AI to investigate corruption and financial crimes, achieving concrete results.

The Rolls-Royce PLC case was the first AI-based criminal case precedent in the world, where the UK's Serious Fraud Office (SFO) used the RAVN Applied Cognitive Engine system to analyse 30 million documents 2,000 times faster than human lawyers, resulting in a GBP 671 million settlement for bribery in seven countries (Yuk, 2017). In 2025, the U.S. Department of Justice conducted Operation Gold Rush, the largest medical fraud case in history at USD 10.6 billion, using data analytics to charge 324 people and prevent USD 4.41 billion in fraudulent Medicare payments (UK Government, 2025).

The U.S. Securities and Exchange Commission (SEC) also demonstrates the successful application of AI through the Electronic Data Processing (EPS) initiative, which uses machine learning algorithms to automatically detect potential accounting and disclosure violations in public companies' financial statements (Gratton, 2024). This system analyses large amounts of financial data and identifies anomalies that indicate manipulation of reports or concealment of information from investors. In particular, the system detects anomalies in the distribution of digits (for example, an insufficient share of the digit "4" in the data), indicates deliberate rounding of indicators to achieve the target values of earnings per share. For example, in the case of Gentex Corporation (2023), SEC algorithms discovered manipulations with employee bonuses that allowed the company to artificially lower costs and raise EPS, which led to the imposition of a fine of USD 4 million (Silver Law Group, 2023). The European Public Prosecutor's office (2025) uses digital technology in 2,700+ active investigations, freeing EUR 849 million of assets, and the UK's National Crime Agency has identified 10,700+ previously unknown accounts using machine learning. The National Economic Crime Centre (2025) in Australia has launched the "Frontier" system for proactive detection of corruption.

Despite the benefits, international experience also highlights the risks and challenges of AI, including generating fabricated information and algorithmic bias. In the UK, there have been cases where lawyers have filed "completely fictitious references to court cases" generated by AI. This led to contempt of court charges, fines, and referrals to regulatory authorities. These incidents highlight the serious consequences of AI "hallucinations" and the need for human verification of AI-generated results (Fake cases, real..., 2025).

A positive example of the systematic implementation of AI in the fight against corruption is demonstrated by Brazil through GRAS, developed within the framework of Law of Brazil No. 12.846 "On Combating Corruption"[1]. GRAS uses an AI-based bot called ALICE to automatically analyse public procurement and identify corruption risks in the public sector (World Bank, 2023). The system analysed 190,923 public procurement procedures and identified more than 850 suppliers with signs of collusion, unfair competition, and other corrupt practices. The key achievement was a radical reduction in audit time – from more than 400 days to 8 days, due to automated analysis of contracts, supplier history, price anomalies, and patterns of bidders' behaviour. ALICE uses machine learning algorithms to detect atypical price fluctuations, suspicious relationships between bidders, repeated winning patterns of the same suppliers, and anomalies in technical specifications that may indicate that tenders are tailored to a specific bidder. In turn, the Brazilian experience outlined the challenges of adapting AI systems to the specifics of the local legal environment, regional features of procurement, and the need for constant updating of algorithms to identify new corruption schemes that evolve in response to increased control. The role of the prosecutor in the procedural management of the investigation of official crimes using innovative technologies is of particular importance in the context of adapting international practices. O. Amelin (2024) systematised the international experience of the United States, Brazil, Bulgaria, and Hungary regarding the specifics of the prosecutor's procedural guidance in the investigation of official crimes. The author determined that the Brazilian AI-ACT system provides automation of monitoring of public procurement and audit of public expenditures, which drastically increases the transparency and effectiveness of procedural guidance by prosecutors of anti-corruption investigations. In addition, the study identified critical challenges of implementing such technologies, manifested in the insufficient training of personnel to work with automated systems and the risk of "information overload" due to large amounts of data, which can lead to ignoring critical signals.

For Ukraine, these international risks are becoming more relevant in the context of reforming the judicial system and the institutional fight against corruption. The problem of the "black box" can undermine public confidence in the newly created anti-corruption bodies, algorithmic bias can lead to discrimination in conditions of political instability, and mass surveillance – pose threats to the formation of democratic institutions. A summary of international experience in using AI and data analytics in the fight against official crimes is presented in Table 4, which systematises the most revealing cases by jurisdiction, type of technology application, and results obtained.

[1] Law of Brazil No. 12.846 "On Combating Corruption". (2013, August). Retrieved from https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12846.htm.

Table 4. International cases of using technologies in the investigation of official crimes

Jurisdiction/organisation	Case type	Technology used	Challenges/risks	Outcome
United Kingdom (SFO)	Rolls-Royce PLC case	AI robot (RAVN) for Document Analysis	Need to verify AI results	Save 80% of expenses; work 2,000 times faster than human lawyers; GBP 671 million settlement
United Kingdom	Submission of "fake" court precedents	Generative AI	AI hallucinations, loss of trust in justice	Contempt of court charges, fines; highlighting the risks of AI "hallucinations"
USA (SEC)	Detection of accounting violations and disclosure of information	AI (EPS initiative)	Possible false positives	Successful identification of potential violations; demonstration of AI capabilities in financial supervision
USA (DOJ)	Operation Gold Rush	Data analytics	Dependence on the quality of source data	USD 10.6 billion case; charges 324 people; prevention of USD 4.41 billion fraudulent payments
European Prosecutor's Office	Cross-border investigations of financial crimes	Digital technologies and data analytics	Coordination between jurisdictions, different legal systems	2,700+ active investigations; EUR 849 million of frozen assets
Brazil (GRAS)	Detection of corruption in the public sector	AI for analysing public data (ALICE bot)	The need to adapt to local conditions	Identification of 850 + suppliers with signs of collusion; reduction of audits from 400 + days to 8 days; analysis of 190,923 procurement procedures
Australia (National Economic Crime Centre)	Proactive detection of corruption	Frontier System	Ethical issues of preventive surveillance	Automated detection of corruption risks in the public sector

Source: compiled by the author based on Law of Brazil No. 12.846[1], Independent Commission against Corruption (2018), Sophos (2018), Silver Law Group (2023), World Bank (2023), C. O'Connor (2023), P. Gratton (2024), Fake cases, real consequences: The AI crisis facing UK law firms (2025)

The analysis of the presented cases shows that successful implementations demonstrate the potential of AI with thoughtful integration and sufficient data, but negative examples serve as warnings about challenges to the integrity of the legal process. For Ukraine, this means not only striving for the introduction of technologies but also learning from international mistakes, prioritising ethical frameworks, ensuring data quality, and investing in training lawyers to critically evaluate AI results. Global experience highlights that "man in the loop" is not just a surveillance mechanism, but a guarantee of justice in the AI era.

Recommendations for improving the legal regulation of the use of AI and innovative technologies in the investigation of official crimes. To fully utilise the advantages of AI technologies in the investigation of official crimes, Ukraine needs a systematic approach to eliminating the identified legal gaps and improving practical application, based on the analysis of the successful experience of implementing the "iCase" system and the identified shortcomings in the legal regulation of digital evidence. The primary requirement is to ensure the entry into force of the adopted, but not yet put into effect, Law of Ukraine No. 2074-IX "On Virtual Assets"[2] after the end of martial law. The analysis of the judicial practice of the Supreme Anti-Corruption Court showed legal uncertainty regarding the seizure and confiscation of cryptocurrencies in cases of official crimes.

In particular, in the case of the seizure of virtual assets, USDT, TRX, ETH, the court was forced to interpret the traditional norms of Article 368 of the Criminal Code of Ukraine in the context of digital assets without a clear legislative framework[3]. This creates risks of inconsistent enforcement and complicates the work of investigators and prosecutors. The Criminal Procedure Code[4] of Ukraine needs to be supplemented with special norms on the collection, evaluation, and use of evidence obtained using AI technologies. Article 98 of the Criminal Procedure Code of Ukraine defines general requirements for physical evidence, and Article 99 regulates documents (including electronic ones), but neither of them regulates the specifics of digital evidence obtained using AI technologies. This leads to problems with determining the originality of electronic files and the results of AI analysis, in particular, the authenticity of electronic files, the permissibility of algorithmic analysis of large data sets, verification of machine learning results, and the establishment of a storage chain for digital evidence generated by automated systems.

An analysis of the activities of the National Anti-Corruption Bureau of Ukraine demonstrated that the active use of intelligence from open sources, but

[1] Law of Brazil No. 12.846 "On Combating Corruption". (2013, August). Retrieved from https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12846.htm.
[2] Law of Ukraine No. 2074-IX "On Virtual Assets". (2022, February). Retrieved from https://zakon.rada.gov.ua/laws/show/2074-20#Text.
[3] Judgement of the High Anti-Corruption Court of Ukraine in Case No. 991/1512/23. (2023, June). Retrieved from https://reyestr.court.gov.ua/Review/111590400.
[4] Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text.

the Law of Ukraine No. 1698-VII "On the National Anti-Corruption Bureau of Ukraine"[1] does not contain a detailed regulation of OSINT methods. This creates legal uncertainty about the admissibility of information obtained from social networks, public registers, and other open sources as evidence. It is recommended to provide for a separate section or special articles in this law on the regulation of OSINT methods that will regulate the procedures for collecting, verifying, and processing data from open sources.

Article 106-1 of the Criminal Procedure Code of Ukraine[2], introduced by the Law of Ukraine No. 1498-IX "On Amendments to the Criminal Procedure Code of Ukraine Regarding the Introduction of an Information and Telecommunications System for Pre-trial Investigation"[3], created the legal basis for electronic pre-trial investigation. However, it is necessary to extend these provisions to other law enforcement agencies, in particular, the State Bureau of Investigation, whose activities are regulated by the Law of Ukraine No. 794-VIII[4]. It is recommended to amend Part 1 of Article 7 of this law by supplementing paragraph 7 with provisions on the powers of the state Bureau of Investigation in the use of innovative investigation technologies, in particular: the use of AI systems for analysing large amounts of data, the application of blockchain analytics for tracking virtual assets, the introduction of digital forensics and OSINT techniques, the creation and use of specialised information and telecommunications systems for electronic document management and interaction with other law enforcement agencies. Articles 93-94 of the Criminal Procedure Code of Ukraine, which regulate the collection of evidence, need to be supplemented with provisions on the use of machine learning algorithms, big data analytics and automated anomaly detection systems. This should be noted in the context of Article 87 of the Criminal Procedure Code of Ukraine on the admissibility of evidence, since the results of AI analysis must meet the criteria of belonging, admissibility, and reliability. Considering Ukraine's European integration aspirations and the need for cooperation with European partners in the field of anti-corruption, it is recommended to harmonise Ukrainian legislation with the Regulation of the EU "On Artificial Intelligence"[5]. Of paramount importance is the implementation of provisions on the classification of AI systems as "high-risk" in law enforcement activities, which requires mandatory risk assessment, ensuring transparency of algorithms and human supervision over automated solutions. This involves making changes to the law of Ukraine No. 2657-XII "On Information"[6] and Law of Ukraine No. 80/94-VR[7] regarding the use of AI in law enforcement activities. Article 6 of the "iCase" System Regulation provides for the use of a comprehensive information security system, but it is necessary to strengthen the requirements of the Law of Ukraine No. 2297-VI "On the Protection of Personal Data"[8] regarding the processing of personal data in AI systems. This is important for ensuring the constitutional rights of citizens enshrined in Article 32 of the Constitution of Ukraine[9]. It is recommended to amend the regulations on the National Academy of Internal Affairs and other departmental acts on the mandatory inclusion of courses on digital investigation technologies in the training programmes of investigators, detectives, and prosecutors. These recommendations are based on the legal gaps identified during the study and the successful experience of introducing innovative technologies by Ukrainian anti-corruption bodies, which will create a comprehensive system of legal regulation of the use of AI in the investigation of official crimes.

Thus, the digital transformation of criminal justice is not a one-time project, but an ongoing, complex adaptive challenge. Failure to address any of these interrelated pillars (legal, ethical, human, cooperation) will undermine the effectiveness and legitimacy of AI applications, potentially leading to a system that is effective but unfair, or technologically advanced but legally vulnerable. The ultimate goal is to create a justice system that is not only smarter but also fair and accountable in the digital age.

Discussion

The results of the study demonstrate a comprehensive picture of the introduction of AI and innovative technologies in the investigation of official crimes, which largely correlates with international trends in the digital transformation of law enforcement activities. The identified

[1] Law of Ukraine No. 1698-VII "On the National Anti-Corruption Bureau of Ukraine". (2014, October). Retrieved from https://zakon.rada.gov.ua/laws/show/1698-18.
[2] Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text.
[3] Law of Ukraine No. 1498-IX "On Amendments to the Criminal Procedure Code of Ukraine Regarding the Introduction of an Information and Telecommunications System for Pre-trial Investigation". (2021, June). Retrieved from https://zakon.rada.gov.ua/laws/show/1498-20.
[4] Law of Ukraine No. 794-VIII "On the State Bureau of Investigations". (2015, November). Retrieved from https://zakon.rada.gov.ua/laws/show/794-19#Text.
[5] Regulation of the European Parliament and Council of the European Union No. 2024/1689 "On Artificial Intelligence". (2024, June). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689.
[6] Law of Ukraine No. 2657-XII "On Information". (1992, October). Retrieved from https://zakon.rada.gov.ua/laws/show/2657-12#Text.
[7] Law of Ukraine No. 80/94-VR "On the Protection of Information in Information and Communication Systems". (1994, July). Retrieved from https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.
[8] Law of Ukraine No. 2297-VI "On the Protection of Personal Data". (2010, June). Retrieved from https://zakon.rada.gov.ua/laws/show/2297-17#Text.
[9] Constitution of Ukraine. (1996, June). Retrieved from https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.

specificity of the Ukrainian approach is the gradual implementation of technological solutions through the development of Integrated Information and telecommunications systems and the development of integrated systems, such as "iCase", which differs from the experience of other countries in the more centralised and coordinated nature of digitalisation. In contrast to the fragmented implementation of technologies in many countries, the Ukrainian model is characterised by a systematic approach to integrating various technological solutions into a single anti-corruption ecosystem.

The analysis of the legal basis of official crimes has shown detailed regulation of various forms of corruption behaviour in the Criminal Code of Ukraine, which creates a solid basis for the use of innovative investigative technologies. Compared to the study by R.S. Faqir (2023), which examines general aspects of digital criminal investigations in the AI era, this paper offers a more specific approach to the specific category of crimes and the national context. The results of the analysis confirm the conclusions of K. Blount (2024) on the need to account for the principles of good legal procedure when using AI to prevent crimes. The conducted investigation revealed that the variety of elements of crimes in the field of official activity requires a differentiated approach to the use of AI technologies since each type of offence has specific features of the evidence base and investigation methods.

A study by O. Amelin (2025) on the search of a person in criminal proceedings for obtaining illegal benefits indicates a critical dependence of the admissibility of evidence on compliance with procedural norms. The author determined that procedural violations during the search of a person led to the recognition of inadmissible both directly obtained evidence and derived materials (expert opinions, physical evidence). Compared to traditional methods, innovative digital forensics technologies provide a higher level of procedural discipline through automated recording of evidence by continuous video recording and cryptographic protection of the data storage chain. Analysis of the judicial practice of the Supreme Anti-Corruption Court conducted by O. Amelin (2025) confirms the objective tendency of courts to prioritise video recording over paper protocols when assessing the reliability of evidence. The results of the study indicate that digital technologies do not replace the physical search of a person to identify material objects of illegal benefit, but supplement it with the analysis of electronic communications, financial transactions, and metadata using AI.

The technological solutions identified, in particular, the use of machine learning to analyse large amounts of data and recognise financial anomalies in banking transactions, atypical patterns in public procurement, and suspicious links between officials and contractors, are consistent with the findings of P. Gund *et al*. (2023), which demonstrate the effectiveness of machine learning algorithms in uncovering hidden corruption schemes through analysis of transactional data and social networks. The evolutionary approach to the development of technologies for crime prevention and detection is systematised by O. Apene *et al*. (2024), presenting the transformation from traditional methods to modern AI solutions. The success of the "iCase" system is due to both its technical characteristics and carefully developed procedures for interaction between the National Anti-Corruption Bureau of Ukraine, the Specialised Anti-Corruption Prosecutor's Office, and the High Anti-Corruption Court.

Of particular importance is the highlighted problem of the "black box" in AI systems, which creates challenges for accountability and justice in criminal justice. The results confirm the critical importance of explanatory AI, which is consistent with the conclusions of international experts on the need for transparency of algorithmic solutions. Compared to the work of Y. Leheza *et al*. (2022), which examines international legal standards for the use of AI in criminal proceedings, this study suggests specific mechanisms for solving transparency problems through the introduction of explanatory AI technologies. The legal aspects of AI criminal liability in the context of general crime theory are analysed in detail by C. Kan (2024), expanding the understanding of the fundamental principles of AI application in justice. The problem of the "black box" is particularly acute in cases of official offences since the lack of transparency of algorithmic decisions can undermine public confidence in anti-corruption bodies. Spatial analysis of corruption networks has received a new development due to the paper of M. Swayne (2021), who demonstrated the effectiveness of GIS technologies for mapping complex criminal structures, which is particularly relevant for the investigation of multi-episode official crimes.

The analysis of digital forensics has revealed the critical importance of ensuring the integrity and storage chain of digital evidence, which is especially important for official offences using virtual assets. The results expand the understanding of the problems presented by S. Yadav *et al*. (2023), on the evolution of AI in forensic science and criminal investigations, adding a specific context for official crime and cryptocurrency operations. Biometric identification technologies, particularly keyboard dynamics analysis, are discussed in detail in the study by P. Teh *et al*. (2013), opening up new opportunities for establishing the authorship of digital documents in cases of official offences. The international legal context of cybercrime and the use of AI in this area is presented in the paper of C. Velasco (2022), which analyses the activities of international organisations in the field of criminal justice. Traditional approaches to ensuring the integrity of evidence need to be radically rethought in the context of digital and virtual assets. Ukrainian law enforcement agencies face

special challenges in the field of international legal assistance in the investigation of crimes using virtual assets.

The international experience analysed in the study demonstrates both remarkable successes and critical challenges in implementing AI in law enforcement. The results confirm the conclusions of M. Gupta *et al*. (2025) regarding the ability of AI to revolutionise the speed of evidence processing and the accuracy of analysing large amounts of data in criminal investigations, while demonstrating the need to consider specific national contexts. The practical experience of using AI by government agencies to detect offences is described in detail by A. Bandy *et al*. (2024), pointing to the effectiveness of technological solutions in American law enforcement practice. Current opportunities and challenges of implementing AI in global anti-corruption activities are systematised in the study by S. So (2025), which provides a broad perspective for understanding trends in this area. Compared to the publication of D. Dunsin *et al*. (2024), which presents a comprehensive analysis of the role of AI in modern digital forensic science, this study focuses on a specific category of crimes. The UK's experience in implementing AI displays the ability to achieve significant resource savings, but highlights the importance of careful quality control.

The technical aspects of digital forensics are further covered by S. Kim *et al*. (2020), exploring the features of IoT Device Analysis, which is relevant for the investigation of modern official crimes using "smart" technologies. The methodological foundations of pre-trial investigation are systematised in the work authored by Yu. Belousov *et al*. (2020), which creates the basis for the introduction of innovative technologies in domestic practice. The specified problems of algorithmic bias and the problems of fairness of AI systems are consistent with international studies on the ethical aspects of the use of AI in justice. The results complement the findings of M. Arjamand *et al*. (2024) on the role of AI in forensic analysis with specific proposals for implementing bias audits. The problem of algorithmic bias can have particularly serious consequences in cases of official offences since such cases often have political overtones. Biased algorithms can lead to unfair targeting of certain categories of employees, which undermines the principles of equality before the law.

Practical cases of using cryptocurrencies in official crimes demonstrate new challenges for law enforcement agencies and the need to adapt traditional investigative methods. Compared to the theoretical developments of A. Sahu *et al*. (2024) on the application of AI in forensic science, this paper offers specific examples of judicial practice and mechanisms for seizing virtual assets. An analysis of judicial practice revealed the complexity of procedures for identifying and seizing virtual assets, which requires the coordination of the efforts of various law enforcement agencies. The case of USDT arrest through interaction with Tether demonstrates both the possibilities and limitations of modern approaches to working with virtual assets.

The study demonstrates that the successful implementation of AI in the investigation of official crimes requires not only technological solutions but also a comprehensive approach to legal regulation, ethical standards, and organisational changes. The Ukrainian model of introducing innovative technologies is characterised by a high level of institutional coordination and international cooperation, which distinguishes it from the experience of other countries. Thereby, the identified legal gaps and challenges of digital transformation require further research and systemic solutions to ensure the effectiveness and fairness of justice in the digital age.

Conclusions

The study established that the introduction of AI and innovative technologies in the investigation of official crimes in Ukraine is characterised by a systematic approach to the digitalisation of law enforcement activities. A comprehensive analysis of the legal framework showed that the regulation of official crimes in Ukraine is based on an extensive system of normative legal acts, including the Criminal Code of Ukraine, legislation on civil service, prevention of corruption and international conventions, which creates a sufficient legal framework for the application of technological solutions, accounting for the specifics of each type of offence.

The study revealed the specifics of the Ukrainian approach to the introduction of technologies, which consists in the gradual creation of Integrated Information and telecommunications systems, as opposed to fragmented implementation in other countries. The main technological solutions were systematised: machine learning systems for analysing large amounts of data, pattern recognition technologies for identifying individuals, blockchain analytics for tracking virtual assets, digital forensics methods for ensuring the integrity of electronic evidence, and explanatory AI to overcome the problem of opacity of algorithmic solutions.

It was established that the variety of elements of crimes in the sphere of official activity determines the need for a differentiated approach to the application of technological solutions since each type of offence has specific features of the evidence base and investigation methods. Official forgery requires a detailed review of documents, illegal enrichment – an in-depth examination of financial flows, and abuse of power can involve an analysis of communication records and video materials. The analysis of Ukrainian practice demonstrated the effectiveness of the "iCase" system as an example of successful integration of digital technologies into the activities of anti-corruption bodies. The system provided electronic interaction between the National Anti-Corruption Bureau of Ukraine, the Specialised Anti-Corruption Prosecutor's office, and the High Anti-Corruption Court, optimised the use of resources, and

improved the quality of pre-trial investigations. The active use of OSINT methods and electronic document management by law enforcement agencies was revealed.

The study determined that there are legal gaps in regulating the use of technologies in criminal proceedings. The analysis of judicial practice showed legal uncertainty regarding the procedures for the seizure and confiscation of virtual assets, insufficient regulation of the use of AI results as evidence, and the lack of detailed standards for the OSINT-methods application in the investigation of official crimes. A comparative analysis of international experience has demonstrated the effectiveness of a centralised approach to technology implementation in comparison with fragmented solutions. Successful cases in the UK, USA, Brazil, and Australia pointed to the opportunities to increase the s peed of document processing, improve the detection of financial anomalies, and reduce false positives in systems. International revealed the risks of generating false information by AI systems and the importance of human control over technological solutions. The paper substantiated the need for a comprehensive legislative reform to ensure the effective use of technologies in the investigation of official crimes. The following are necessary: the entry into force of the Law of Ukraine No. 2074-IX "On Virtual Assets", amendments to the Criminal Procedure Code of Ukraine with provisions on the use of AI results as evidence, the development of standards for the application of OSINT methodologies, and the harmonisation of Ukrainian legislation with international standards for AI regulation.

Prospects for further research include quantitative analysis of the effectiveness of implementing specific AI decisions in Ukrainian anti-corruption bodies, development of a methodology for assessing the ethical risks of algorithmic systems in criminal proceedings, research on the impact of automation on the quality of court decisions in cases of criminal offences in the field of official activity, and comparative analysis of the adaptation of European standards for AI regulation to the Ukrainian legal field.

Acknowledgements

None.

Funding

This study was not funded.

Conflict of Interest

None.

References

[1] Amelin, O. (2024). Features of the prosecutor's procedural guidance during the investigation of criminal offences in the field of official activity. *Scientific Journal of the National Academy of Internal Affairs*, 29(4), 9-21. doi: 10.56215/naia-herald/4.2024.09.

[2] Amelin, O. (2025). Search of a person as a way of collecting evidence in the pre-trial investigation of accepting an offer, promise or receiving of an illegal benefit by an official. *Constitutional State*, 58, 220-231. doi: 10.18524/2411-2054.2025.58.331008.

[3] Ansari, N. (2025). *Machine learning in forensic evidence examination: A new era*. Boca Raton: CRC Press. doi: 10.4324/9781003449164.

[4] Apene, O.Z., Blamah, N.V., & Aimufua, G.I. (2024). Advancements in crime prevention and detection: From traditional approaches to artificial intelligence solutions. *European Journal of Applied Science, Engineering and Technology*, 2(2), 285-297. doi: 10.59324/ejaset.2024.2(2).20.

[5] Arjamand, M., Saleem, A., Basit, A., Iftikhar, S., Sharif, M., Cholistani, M.S., Farhan, M., Shumail, Khan, B.A., Ali, Z., Shahid, B., & Hasnain, M. (2024). The role of artificial intelligence in forensic science: Transforming investigations through technology. In O. Czenczer, G. Kovács & B. Mészáros (Eds.), *Ludovika international law enforcement research symposium conference proceedings* (pp. 136-146). Budapest: Hungarian Association of Police Science.

[6] Bandy, A.B., Haffner, E., & Suárez, M.C. (2024). *The US government is using AI to detect potential wrongdoing, and companies should too*. Retrieved from https://surl.li/rbxfml.

[7] Belousov, Yu.L., Venger, V.M., Gryga, R.M., Gyulmagomedov, D.O., Derkach, S.A., Krapivin, Ye.O., & Yavorska, V.V. (2020). *Standards for pre-trial investigation*. Retrieved from https://drive.google.com/file/d/101KaZ6eL4UiLB4TB3hcE3y3Qe0ju_WAp/view.

[8] Bernazuk, Y. (2025). *Artificial intelligence in justice: Risks of algorithmic bias and discrimination*. Retrieved from https://court.gov.ua/storage/portal/supreme/prezentacii_2025/125_AI_Algorithmic_Bias_Discrimination_Risks_bernaziuk.pdf.

[9] Blount, K. (2024). Using artificial intelligence to prevent crime: Implications for due process and criminal justice. *AI & Society*, 39(1), 359-368. doi: 10.1007/s00146-022-01513-z.

[10] Chaikovskyi, D. (2023). Artificial intelligence as a new tool for combating crimes in the economic sphere. *Young Scientist's Tribune*, 6, 335-342. doi: 10.32782/yuv.v6.2023.41.

[11] Chin, C. (2025). *Is your smart speaker a snitch? Exploring the legal and privacy dangers of voice-activated devices*. Retrieved from https://surl.li/tryjjg.

[12] Council on Criminal Justice. (2025). *DOJ Report on AI in criminal justice: Key takeaways*. Retrieved from https://counciloncj.org/doj-report-on-ai-in-criminal-justice-key-takeaways/.
[13] Cyber Writes Team. (2023). *What is digital forensics? Tools, types, phases & history*. Retrieved from https://cybersecuritynews.com/what-is-digital-forensics/.
[14] Dunsin, D., Ghanem, M.C., Ouazzane, K., & Vassilev, V. (2024). A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. *Forensic Science International: Digital Investigation*, 48, article number 301675. doi: 10.1016/j.fsidi.2023.301675.
[15] EU Anti-Corruption Initiative. (2025). Corruption risks in public procurement – Ukraine's agency for restoration is developing a risk management, monitoring, and efficiency evaluation system with the support of EUACI. Retrieved from https://surl.li/vppmww.
[16] European Public Prosecutor's Office. (2025). *2024 Annual Report: EPPO leading the charge against EU fraud*. Retrieved from https://surl.li/srnazr.
[17] Fake cases, real consequences: The AI crisis facing UK law firms. (2025). Retrieved from https://vinciworks.com/blog/fake-cases-real-consequences-the-ai-crisis-facing-uk-law-firms/.
[18] Faqir, R.S. (2023). Digital criminal investigations in the era of artificial intelligence: A comprehensive overview. *International Journal of Cyber Criminology*, 17(2), 77-94. doi: 10.5281/zenodo.4766706.
[19] Galassi, T. (2018). *OSHA's use of unmanned aircraft systems in inspections*. Retrieved from https://www.osha.gov/memos/2018-05-18/oshas-use-unmanned-aircraft-systems-inspections.
[20] Gratton, P. (2024). *Understanding the SEC*. Retrieved from https://www.investopedia.com/articles/investing/112914/understanding-sec.asp.
[21] Gulyamov, S., & Tatar, S. (2023). The role of artificial intelligence in investigations. *Journal of Law & Artificial Intellegence*, 2(1), 16-22.
[22] Gund, P., Patil, S., & Phalke, V. (2023). Investigating crime: A role of artificial intelligence in criminal justice. *The Online Journal of Distance Education and e-Learning*, 11(2), 1520-1526.
[23] Gupta, M., Sood, R.P., & Singh, R. (2025). Artificial intelligence in criminal investigation: Transforming law enforcement and forensic analysis. In B.N., Mukherjee, R. Uduwerage-Perera, M. Mathew & S. Kumar Tripathi (Eds.), *Rethinking the police for a better future: Navigating policing challenges with accountability and trust* (pp. 311-323). Cham: Springer. doi: 10.1007/978-3-031-83173-7_21.
[24] Gura, O. (2020). *Video evidence in criminal proceedings: The view of the Supreme Court*. Retrieved from https://femida.ua/news/videodokazy-u-kryminalnomu-sudochynstvi-poglyad-verhovnogo-sudu/.
[25] Independent Commission against Corruption. (2018). *Sights firmly set on the engine-room of corruption*. Retrieved from https://www.icac.nsw.gov.au/newsletter/issue52/strategic.html.
[26] Internal Revenue Service. (2023). *IRS-CI delivers cyber training, blockchain analysis tools to Ukrainian investigators*. Retrieved from https://www.irs.gov/compliance/criminal-investigation/irs-ci-delivers-cyber-training-blockchain-analysis-tools-to-ukrainian-investigators.
[27] Kan, C.H. (2024). Criminal liability of artificial intelligence from the perspective of criminal law: An evaluation in the context of the general theory of crime and fundamental principles. *International Journal of Eurasia Social Sciences*, 15(55), 276-313. doi: 10.35826/ijoess.4434.
[28] Karchevsky, M. (2021). *Cryptocurrencies and blockchain technologies: Innovations in combating corruption*. Retrieved from https://justtalk.com.ua/post/kriptovalyuti-ta-tehnologii-blockchain-innovatsii-u-protidii-koruptsii.
[29] Kim, S., Park, M., Lee, S., & Kim, J. (2020). Smart home forensics – data analysis of IoT devices. *Electronics*, 9(8), article number 1215. doi: 10.3390/electronics9081215.
[30] Klyan, A. (2022). *Legal regulation of artificial intelligence in Ukraine and worldwide*. Retrieved from https://golaw.ua/ua/insights/publication/pravove-regulyuvannya-shtuchnogo-intelektu-v-ukrayini-ta-sviti/.
[31] Leheza, Y., Len, V., Shkuta, O., Titarenko, O., & Cherniak, N. (2022). Foreign experience and international legal standards for the application of artificial intelligence in criminal proceedings. *Revista de la Universidad del Zulia*, 13(36), 276-287. doi: 10.46925//rdluz.36.18.
[32] Lontai, M., Pamjav, H., & Petrétei, D. (2024). Artificial intelligence in forensic sciences revolution or invasion? Part I. *Belügyi Szemle*, 72(4), 701-715. doi: 10.38146/BSZ-AJIA.2024.v72.i4.pp701-715.
[33] Merkle Science. (2025). *Securing the blockchain: How tracker simplifies blockchain forensics for law enforcement agencies*. Retrieved from https://surl.lu/pumdxr.
[34] Mordvyntsev, M.V., Pashniev, D.V., & Nakonechnyi, V.S. (2025). Specifics of using video analysis technologies and facial recognition software in criminal analysis. *Communities & Collections*, 96(1), 90-103. doi: 10.32631/pb.2025.1.08.
[35] Nandipati, S.K., Balaji, J., & Krishna, K. (2024). The role of explainable AI in criminal investigations: Unveiling the black box for justice. doi: 10.13140/RG.2.2.36685.24804.

[36] National Agency on Corruption Prevention. (2024). *More than 40% of posts about corruption and anti-corruption are disinformation – results of social media monitoring in August*. Retrieved from https://surl.li/wczkye.
[37] National Agency on Corruption Prevention. (2025). *Lifestyle monitoring: 4.85 million UAH may be confiscated from the former acting head of the Kharkiv Territorial Centre for Recruitment and Social Support*. Retrieved from https://surl.li/knpdjm.
[38] National Anti-Corruption Bureau. (2021). *NABU implements innovations to increase the efficiency of pre-trial investigation*. Retrieved from https://surl.li/petzeo.
[39] National Anti-Corruption Bureau. (2025). *Digitalisation of criminal justice: Integration of iCase and the electronic court*. Retrieved from https://surl.li/blypsg.
[40] National Economic Crime Centre. (2025). *A world leading cross system operational response to economic crime*. Retrieved from https://surl.lu/dvspzg.
[41] O'Connor, C. (2023). *DOJ signals increased emphasis on data analytics to prosecute FCPA global corruption*. Retrieved from https://surl.li/hpzoaf.
[42] Rigano, C. (2019). *Using artificial intelligence to address criminal justice needs*. Retrieved from https://www.ojp.gov/pdffiles1/nij/252038.pdf.
[43] Sahu, A., Tripathy, P., & Shahi, S. (2024). AI applications in forensic science: Transforming crime scene analysis and investigation. *African Journal of Biological Sciences*, 6(11), 1871-1879. doi: 10.48047/AFJBS.6.11.2024.1871-1879.
[44] Silver Law Group. (2023). *What to know about The SEC's "EPS Initiative"*. Retrieved from https://www.secwhistleblowerlawyers.net/what-to-know-about-the-secs-eps-initiative/.
[45] So, S.J. (2025). *Artificial intelligence in anticorruption: Opportunities and challenges*. Retrieved from https://surl.lt/jgbjax.
[46] Solon, O. (2020). *Insecure wheels: Police turn to car data to destroy suspects' alibis*. Retrieved from https://www.nbcnews.com/tech/tech-news/snitches-wheels-police-turn-car-data-destroy-suspects-alibis-n1251939.
[47] Sophos. (2018). *Serious fraud office trialling AI for data-heavy cases*. Retrieved from https://news.sophos.com/en-us/2018/09/05/serious-fraud-office-trialling-ai-for-data-heavy-cases/.
[48] State Bureau of Investigations. (2025). *The State Bureau of Investigation exposed the leaders of "Ukrproftur" and the Federation of Trade Unions in a scheme to misappropriate state property*. Retrieved from https://surl.li/ryjcoa.
[49] Swayne, M. (2021). *GIS technology helps map out how America's mafia networks were "connected"*. Retrieved from https://surl.li/vzyhcb .
[50] Teh, P.S., Teoh, A.B., & Yue, S. (2013). A survey of keystroke dynamics biometrics. *Scientific World Journal*, 2013, article number 408280. doi: 10.1155/2013/408280.
[51] The court seized cryptocurrency found in the possession of the former head of the State Special Communications Service. (2023). Retrieved from https://surl.lt/opwhyc.
[52] The power of big data analytics platforms for police departments. (2025). Retrieved from https://www.cognyte.com/blog/big-data-analytics-platform/.
[53] Tokarieva, K., & Savliva, N. (2021). Peculiarities of legal regulation of artificial intelligence in Ukraine. *Scientific Works of Kyiv Aviation Institute. Series Law Journal "Air and Space Law"*, 3(60), 148-153. doi: 10.18372/2307-9061.60.15967.
[54] Trebilcock, O. (2020). *Are Alexa and Google Assistant spying on us?* Retrieved from https://www.which.co.uk/news/article/are-alexa-and-google-assistant-spying-on-us-aW8TJ6N0wdf8.
[55] U.S. General Services Administration. (2025). *GSA Fleet telematics*. Retrieved from https://surl.li/uejezo.
[56] UK Government. (2025). *FOI Log*. Retrieved from https://surl.li/xtehig.
[57] United States Government Accountability Office. (2020). *Time and attendance: Agencies generally compiled data on misconduct, and reported using various internal controls for monitoring*. Retrieved from https://www.gao.gov/assets/710/709146.pdf.
[58] Velasco, C. (2022). Cybercrime and Artificial Intelligence. An overview of the work of international organizations on criminal justice and the international applicable instruments. *ERA Forum*, 23, 109-126. doi: 10.1007/s12027-022-00702-z.
[59] What is digital forensics? Phases of digital forensics in cybersecurity. (2024). Retrieved from https://www.eccouncil.org/cybersecurity-exchange/computer-forensics/what-is-digital-forensics/.
[60] Wood, B. (2017). *North carolina department of transportation division of motor vehicles license and theft bureau: Investigative report*. Retrieved from https://surl.li/urqomr.
[61] World Bank. (2023). *Governance Risk Assessment System (GRAS): Advanced data analytics for detecting fraud, corruption, and collusion in public expenditures*. Retrieved from https://surl.li/bikbsa.

[62] Yadav, S., Yadav, S., Verma, P., Ojha, S., & Mishra, S. (2023). Artificial intelligence: An advanced evolution in forensic and criminal investigation. *Current Forensic Science*, 1(1), article number e190822207706. doi: 10.2174/2666484401666220819111603.
[63] Yuk, P. (2017). *Rolls-Royce reaches £671m agreement to settle corruption probes*. Retrieved from https://www.ft.com/content/04ace079-e3c2-347a-98dc-ec735ea51dbc.
[64] Zinnbauer, D. (2025). *Artificial intelligence in anti corruption – a timely update on AI technology*. Retrieved from https://surl.li/nizaig.

Упровадження штучного інтелекту й інших інноваційних технологій у процес розслідування кримінальних правопорушень у сфері службової діяльності

Олександр Амелін
Кандидат юридичних наук, доцент
Офіс Генерального прокурора
01001, вул. Різницька, 13/15, м. Київ, Україна
Міжрегіональна Академія управління персоналом
03039, вул. Фрометівська, 2, м. Київ, Україна
https://orcid.org/0000-0002-0933-2111

Анотація
Метою дослідження був аналіз українського та міжнародного досвіду використання штучного інтелекту в розслідуванні службових правопорушень, розроблення рекомендацій щодо адаптації найкращих практик до української правової системи. Методологія дослідження ґрунтувалася на порівняльному аналізі регулювання та практики впровадження штучного інтелекту в Україні, США, Великій Британії, Австралії та Бразилії з вивченням технологічних механізмів функціонування, правових гарантій у правоохоронній діяльності. Окреслено специфіку українського підходу до впровадження технологій через створення інтегрованої системи «іКейс», що забезпечила електронну взаємодію між Національним антикорупційним бюро України, Спеціалізованою антикорупційною прокуратурою та Вищим антикорупційним судом, на відміну від фрагментарного впровадження в інших країнах. Систематизовано технологічні рішення: машинне навчання для аналізу великих обсягів даних, пояснювальний штучний інтелект, цифрову криміналістику з дев'ятьма фазами обробки доказів, блокчейн-аналітику для відстеження віртуальних активів. Проаналізовано українські кейси: арешт криптовалют Tether, Tron, Ethereum у справі № 991/1512/23 Вищого антикорупційного суду, вирок у справі № 991/3227/24, систему оцінювання ризиків у державних закупівлях з 21 автоматичним індикатором, використання методик розвідки з відкритих джерел Національним антикорупційним бюро України. Міжнародний досвід продемонстрував ефективність штучного інтелекту, зокрема у справах Rolls-Royce, Operation Gold Rush, у роботі Європейської прокуратури та використанні бразильського бота ALICE. Виявлено критичні виклики: проблему «чорної скриньки» алгоритмів, ризики упередженості систем, правові прогалини щодо цифрових активів, необхідність гармонізації з Регламентом ЄС про штучний інтелект 2024/1689. Результати дослідження можуть бути використані антикорупційними органами під час упровадження технологій штучного інтелекту, судовою системою – для формування єдиної практики оцінювання цифрових доказів, органами законодавчої влади – під час розроблення спеціального законодавства про штучний інтелект, науково-освітніми установами – для підготовки кваліфікованих кадрів у сфері цифрового розслідування злочинів

Ключові слова:
цифровізація; електронний документообіг; інноваційні методи розслідування; цифрові докази; кіберзлочинність; антикорупційні органи; незаконне збагачення