UDC 343.98:343.352
DOI: 10.63341/naia-chasopis/2.2026.18

ISSN 2519-4216
E-ISSN 2519-4313

Legal and practical aspects of the application of OSINT methodologies for evidence collection during pre-trial investigation of public office offences

Oleksandr Amelin*
PhD in Law, Associate Professor
Office of the Prosecutor General
01011, 13/15 Riznytska Str., Kyiv, Ukraine
Educational and Scientific Institute of Law of State Tax University
08201, 31 Universytetska Str., Irpin, Ukraine
https://orcid.org/0000-0002-0933-2111

Abstract
The purpose of the study was to examine legal constraints, procedural requirements, and practical challenges arising during the recording, verification, and use of information from open sources in proceedings concerning public office offences. Contextual, legal and regulatory, and problem-oriented analysis methods were employed to achieve the purpose. Given the increasing trend in the number of such offences in 2024-2025, the use of information from open sources is appropriate for the timely identification of criminal schemes, prevention of losses, and strengthening of public trust in state institutions. The study drew on an examination of the regulatory framework and contextual analysis to identify strengths and prospects of evidence collection from open sources, including broad access to relevant information, rapid data acquisition, and the possibility of investigating offences across different segments of state activity, including military, educational, medical, and other domains. The analysis found a number of problems and risks with using open-source information, such as the lack of standard procedures, limited technical skills, and possible ethical issues. Examination of these challenges informed recommendations aimed at improving the effectiveness of using open sources in the investigation of public office offences. Improvement of investigative effectiveness involved transformation across multiple dimensions, particularly regulatory, procedural, institutional, staffing, methodological, technical, ethical, and control-related aspects. The results of the study may be used by legislators to improve the regulatory framework, by law enforcement bodies and investigators to enhance the effectiveness and quality of investigations into public office offences, by researchers for further analysis of methodologies for processing information from open sources, and by educational institutions for the development of training programmes and courses on the use of digital evidence in criminal proceedings

Keywords:
open-source information; personal data; declarations; registers; disinformation; deepfakes; illicit enrichment

Article's History:
Received: 18.12.2025
Revised: 26.03.2026
Accepted: 26.05.2026
Published: 08.07.2026

Suggest Citation:
Amelin, O. (2026). Legal and practical aspects of the application of OSINT methodologies for evidence collection during pre-trial investigation of public office offences. *Law Journal of the National Academy of Internal Affairs*, 16(2), 18-30. doi: 10.63341/naia-chasopis/2.2026.18.

*Corresponding author (*yuamelinoleksandr@gmail.com*)

Introduction

The importance of analysing the legal and practical dimensions of implementing Open Source Intelligence (OSINT) methodologies in the pre-trial investigation of public office offences is underscored by the digitalisation of social interactions and the increasing significance of open information resources in public administration. When someone commits a crime while in public office, they leave digital traces in open state registers, electronic declarations, public procurement systems, social media, and other online platforms. This makes it easier to find them. The lack of clear regulatory recognition of OSINT as a separate tool in the Criminal Procedure Code of Ukraine, the uncertainty surrounding the evaluation of the admissibility and evidentiary value of results derived from open-source analysis, and the potential for infringing on human rights and freedoms necessitate a thorough academic investigation into the legal parameters and practical application of OSINT in the operations of pre-trial investigation entities.

The potential for OSINT methodologies in criminal investigations is evidenced in academic literature, notably the research conducted by S. Bocharov *et al.* (2025). These researchers highlighted the validity of utilising information from open sources, including social media, government registries, mass media, and satellite imagery, for criminal investigations. According to S. Bocharov *et al*., the effectiveness of OSINT methodologies increases through integration with other intelligence disciplines, namely Human Intelligence, Signals Intelligence, and Imagery Intelligence. Drawing on a review of thematic studies, academic literature, and industry reports, R. Sazibur (2025) examined the application of OSINT in threat detection, incident response, and forensic investigations. The researcher concluded that the use of OSINT methodologies improved threat detection, reduced the risk of data breaches, and increased analytical effectiveness. N. Breuer (2025) investigated the use of OSINT technologies to obtain data from an Italian pre-trial detention order and to analyse the Italian business register for the construction of networks representing the "Ndrangheta" group involved in infiltration into the legal business sector. The researcher concluded that OSINT offers several advantages over conventional closed sources, as it functions as a proxy for analysing local network structures. S. Szymoniak & K. Foks (2024) examined the advantages of using OSINT technologies in a case of the Federal Bureau of Investigation involving a woman who participated in mass protests in Philadelphia in 2020 and prepared criminal offences, including phishing attacks. The evidence obtained in that case indicated that the use of OSINT methodologies supports effective verification of the accuracy and reliability of information for objective investigation. O.Yu. Amelin *et al*. (2025) analysed the possibilities for implementing international experience in investigating criminal offences in the sphere of official activity to assess its applicability to the legal system of Ukraine. These researchers said that some analytical tools are okay to use, but their effectiveness depends on things like the independence of investigative bodies, clear jurisdiction, and openness of evidentiary procedures.

Challenges associated with the use of OSINT methodologies in criminal investigations have also been addressed previously, in particular by J. Rajamaki *et al*. (2022). The researchers examined the use of OSINT technologies in the context of investigating cases of child abuse. J. Rajamaki *et al*. concluded that a barrier to the use of the OSINT approach lies in procedures related to data storage for further investigation, since the fact of abuse cannot be documented or examined by anyone other than a law enforcement officer specifically assigned and trained for this purpose. Similar barriers were identified by B.S. Kosokhatko (2025), who focused on the use of OSINT methodologies in the investigation of war crimes committed by the Russian Federation against Ukraine. The researcher identified a gap concerning the procedural status of OSINT specialists in criminal investigations in Ukraine. This gap arises because, despite the importance of expertise required for collecting and analysing open-source data, the Criminal Procedural Code of Ukraine[1] does not recognise the opinion of a specialist as an official source; therefore, this legal inconsistency constrains the use of OSINT methodologies in criminal investigations. Ethical aspects of the use of OSINT technologies were analysed by M. Van der Woude & G. Torres (2024), who considered the use of open sources in journalistic investigations in the Netherlands. Interview results indicated that participants involved in investigations relied to a significant extent on personal judgement and continuous dialogue with colleagues when making decisions regarding confidentiality, which raises concerns about the objectivity of conclusions.

Analysis of previous studies indicates that, despite extensive examination of the potential of OSINT methodologies in criminal investigations, several issues remain unresolved. One such gap is the lack of a systematic account of the specific features of applying OSINT technologies in pre-trial investigations of public office offences. There is also a lack of systematic research on the procedural status of OSINT analysis results as evidence in criminal proceedings in Ukraine, particularly with regard to the requirements of admissibility, relevance, and reliability. In this context, the purpose of the study is to examine the legal and practical problems associated with the use of OSINT methodologies for evidence collection during the pre-trial investigation of public office offences. The objectives of the study are

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

to analyse the legal grounds and procedural possibilities for the use of OSINT methodologies in pre-trial investigations of such offences, to identify key practical challenges and risks associated with the use of OSINT in investigative activities, and to propose directions for improving national legislation and investigative practice with reference to international experience in the use of OSINT methodologies.

Materials and Methods

To achieve the purpose of the study, contextual analysis was applied to identify trends in the commission and investigation of public office offences in 2024 and throughout 2025. The selection of this period reflects changes in law enforcement practice and statistical indicators of such offences under conditions of martial law and institutional transformations of law enforcement and anti-corruption bodies, as evidenced by official statistical data for the respective periods. Materials for the contextual analysis included official reports of the National Anti-Corruption Bureau of Ukraine (2024a; 2024b; 2025a; 2025b) and the Specialised Anti-Corruption Prosecutor's Office for the first half of 2024, the annual report for 2024, and reporting materials for the first half of 2025, which were used to generalise statistical indicators relating to the registration, investigation, and procedural progress of criminal proceedings concerning public office offences. The contextual analysis considered indicators such as the number of initiated pre-trial investigations, notices of suspicion, indictments submitted to court, as well as the amounts of funds recovered for the state and the value of prevented financial losses resulting from the detection of such offences during 2024-2025. Given the digitalisation of the evidentiary base in proceedings concerning public office offences, the methodological approach also encompassed an analysis of regulatory and methodological documents governing the recording, collection, and preservation of electronic (digital) evidence, particularly in the context of OSINT use.

The task of the legal and regulatory analysis consisted in examining the legal grounds for the use of OSINT methodologies in the pre-trial investigation of public office offences. The analysis was based on the following regulations: the Constitution of Ukraine[1], Criminal Code of Ukraine[2], Law of Ukraine No. 2297-VI "On Personal Data Protection"[3], Law of Ukraine No. 2135-XII "On Operational and Investigative Activities"[4]. These legal instruments were examined in terms of their content and key provisions, as well as their role in enabling the use of OSINT methodologies in pre-trial investigations of such offences. The classification of public office offences presented in this study was developed based on the Criminal Code of Ukraine and features the following articles: 364, 364-1, 365, 366, 367, 368, 368-3, 368-5, 369, 369-2, and 370. This framework lists the name of each crime, what it means, and how it relates to the use of OSINT.

The study utilised SWOT analysis to evaluate the practical implications of employing OSINT technologies in the investigation of public office offences. The recognised benefits and obstacles of OSINT utilisation were categorised through thematic grouping and allocated to the classifications S, W, O, and T, reflecting the internal attributes of the technologies, such as functional capabilities and constraints, as well as the external circumstances of their implementation, encompassing legal, institutional, and practical considerations. The results were checked for consistency by comparing them to other sources and doing the analysis again. Legal, technical, and ethical aspects of the use of open sources in the investigation of such offences were examined using the example of a case involving a judge suspected of illicit enrichment and submission of false declarations. In this instance, open digital data, specifically electronic declarations, open property registers, market listings, and related sources, were used as part of the evidentiary base to establish discrepancies between income and assets (Ukrinfopress, 2025).

The study applied a problem-oriented analysis, which involved step-by-step identification of key challenges associated with the use of OSINT technologies in the investigation of public office offences based on previously analysed material. Based on the synthesis of identified challenges, recommendations were developed for improving OSINT strategies, including the identification of responsible actors for implementation and metrics for evaluating effectiveness, with consideration of legal, technical, and ethical constraints associated with the application of such technologies.

Results

Legal basis for the use of OSINT methodologies in pre-trial investigation

In this study, public office offences are defined as criminal offences committed by a public official in the course of, or in connection with, the exercise of official duties, through the use of granted authority or official position (Amelin, 2024). The study indicates that Articles 364-370 of the Criminal Code of Ukraine define, in different ways, practical scenarios for the use of OSINT methodologies in the investigation of public office offences. For offences related to abuse of power and authority

[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] Law of Ukraine No. 2297-VI "On Personal Data Protection". (2010, June). Retrieved from https://zakon.rada.gov.ua/laws/show/2297-17?lang=en#Text.
[4] Law of Ukraine No. 2135-XII "On Operational and Investigative Activities". (1992, February). Retrieved from https://zakon.rada.gov.ua/laws/show/en/2135-12?lang=en#Text.

(Articles 364, 364-1, 365 of the Criminal Code of Ukraine), OSINT is used primarily for the analysis of open data on managerial decisions, public procurement, corporate linkages, and digital traces of official activity. For cases of official forgery and negligence (Articles 366 and 367 of the Criminal Code of Ukraine), open sources are used to check the accuracy of official documents and find differences between public records and what actually happened. Corruption offences related to undue advantage and bribery (Articles 368, 368-3, 369, 369-2 of the Criminal Code of Ukraine) are characterised by the use of OSINT to establish links between benefits, official decisions, and socio-economic relationships of the actors involved. The highest evidentiary relevance of OSINT arises in cases of illicit enrichment (Article 368-5 of the Criminal Code of Ukraine), where open digital sources enable the identification of inconsistencies between income and assets. At the same time, in proceedings under Article 370 of the Criminal Code of Ukraine, the use of OSINT remains limited due to the prohibition of provocation of bribery.

Conclusions regarding the dynamics of public office offences were drawn based on reporting materials of the National Anti-Corruption Bureau of Ukraine (2024b; 2025a) and the Specialised Anti-Corruption Prosecutor's Office. According to data for 2024-2025, during this period detectives of the National Anti-Corruption Bureau of Ukraine, in cooperation with prosecutors of the Specialised Anti-Corruption Prosecutor's Office, notified 115 individuals of suspicion in cases related to high-level corruption and public office offences, and submitted 69 indictments to court concerning 154 individuals out of a total of 370 initiated investigations, which is nearly twice the figure recorded in the first half of 2024. This comparison of quantitative indicators over time demonstrates a substantial increase in the activity of law enforcement bodies in the investigation of public office offences in 2025 compared with the previous year, which may be associated both with an increasing number of offences involving high-ranking officials and with procedural or institutional changes in the operation of the National Anti-Corruption Bureau of Ukraine and the Specialised Anti-Corruption Prosecutor's Office. The reporting period is also characterised by the exposure, for the first time in the history of the National Anti-Corruption Bureau of Ukraine and the Specialised Anti-Corruption Prosecutor's Office, of a sitting Deputy Prime Minister. During the same period, two corruption schemes within the Ministry of Defence were uncovered, with a total value of 733 million hryvnias. The reported data also indicate that in the first half of 2025, the National Anti-Corruption Bureau of Ukraine initiated 370 investigations and submitted 69 indictments to court concerning official offences. These figures emphasise that the problem of public office offences in Ukraine remains unresolved and requires attention already at the stage of investigation. The investigation of public office offences can be strengthened through the use of OSINT methodologies, which, although based on the analysis of open-source data, remain subject to specific legal provisions, as presented in Table 1.

Table 1. Legal grounds for the use of OSINT in pre-trial investigations

Regulation/source	Content/provisions	Role in the use of OSINT
Constitution of Ukraine (Articles 31, 32, 34)	Guarantees of the right to privacy, protection of personal data, secrecy of correspondence, and non-interference in private life; principle of openness of information	Defines the balance between the protection of privacy and the collection of open-source information for evidentiary purposes
Criminal Procedure Code of Ukraine (Articles 87, 89, 94)	Defines the procedure for the collection of evidence, including documents, public sources, and other factual information	Permits the lawful documentation and use of information from open sources as evidence
Law of Ukraine "On Personal Data Protection"	Regulates the procedure for the processing of personal data, including data obtained from open sources; establishes the principles of legality, proportionality, and minimisation	Restricts and directs the use of OSINT in relation to the collection and analysis of personal data
Law of Ukraine "On Operational and Investigative Activities"	Defines the procedure for the application of overt and covert investigative and counterintelligence measures conducted through the use of operational and operational-technical means	Plays an important role in distinguishing between OSINT and covert measures, particularly during the use of specialised software tools

Source: compiled based on Law of Ukraine No. 2135-XII "On Operational and Investigative Activities"[1], Constitution of Ukraine[2], Law of Ukraine No. 2297-VI "On Personal Data Protection"[3]

The presented table demonstrates that the use of OSINT methodologies in pre-trial investigation in Ukraine is grounded in a set of regulations that cover constitutional guarantees, procedural provisions,

[1] Law of Ukraine No. 2135-XII "On Operational and Investigative Activities". (1992, February). Retrieved from https://zakon.rada.gov.ua/laws/show/en/2135-12?lang=en#Text.
[2] Constitution of Ukraine. (1996, June). Retrieved from https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.
[3] Law of Ukraine No. 2297-VI "On Personal Data Protection". (2010, June). Retrieved from https://zakon.rada.gov.ua/laws/show/2297-17?lang=en#Text.

legislation on information, and personal data protection. The Constitution of Ukraine establishes fundamental principles of privacy protection and confidentiality of personal life, while also securing the right of access to open information, which forms the legal basis for the lawful collection of data from open sources. Law of Ukraine No. 2657-XII "On Information"[1] and Law of Ukraine No. 2297-VI "On Personal Data Protection"[2] further specify the framework for the use of open information and personal data. The former regulates access to information and distinguishes between open and restricted information, thereby providing legitimacy for OSINT methodologies when operating with open sources. The Law of Ukraine No. 2297-VI "On Personal Data Protection" emphasises the need to limit the processing of personal data and to comply with the principles of proportionality and minimisation of interference, which is critical for preventing violations of individual rights and ensuring the admissibility of evidence in court.

Practical challenges and risks of applying OSINT methodologies

The conducted SWOT analysis identifies key external and internal factors that influence the effectiveness of applying OSINT methodologies in the pre-trial investigation of public office offences in Ukraine; the results are presented in Table 2. OSINT methodologies in Ukraine have internal strengths, including rapid access to open sources and the ability to collect evidence in a timely manner. Nevertheless, weaknesses are present, including the lack of standardised procedures, limited technical resources, and a shortage of qualified analysts. Opportunities include the use of OSINT for documenting war-related and corruption offences and the development of international cooperation, while threats include the risk of disinformation, violations of privacy, and the potential legal inadmissibility of evidence. Effective use of OSINT therefore requires a combination of technical, methodological, and legal measures that maximise advantages and minimise associated risks.

Table 2. SWOT analysis of the application of OSINT methodologies in the investigation of public office offences in Ukraine

Component	Internal factors	External factors
Strengths	Speed of data collection and verification: the OSINT analysis of declarations and open registers assisted the National Anti-Corruption Bureau of Ukraine in identifying corruption schemes involving illicit enrichment and the embezzlement of assets (for example, cases concerning the illicit enrichment of members of parliament and high-ranking officials, where declaration data differed substantially from actual assets)	Establishment of judicial practice: the Supreme Court of Ukraine confirms the admissibility of electronic evidence when properly documented, which permits the inclusion of OSINT data in cases concerning corruption and public office offences
Weaknesses	Absence of standardised protocols: in several proceedings, detectives of the National Anti-Corruption Bureau of Ukraine encountered situations in which data from open sources were declared inadmissible because of improper documentation, which complicated the advancement of particular proceedings before the High Anti-Corruption Court	Inconsistency in judicial approaches: certain courts impose increased requirements concerning metadata and the methods used for documenting OSINT data, which complicates their use in cases concerning public office offences (for example, cases involving evidence related to embezzlement schemes in the defence sector)
Opportunities	Integration of OSINT into investigative algorithms: in major proceedings, such as the exposure of schemes involving the embezzlement of food supplies for the defence sector or fraud related to land rights during Operation "Clean City" conducted by the National Anti-Corruption Bureau of Ukraine, OSINT enabled the rapid identification of networks of individuals and the connections between them during the early stages of investigations	International harmonisation: the use of the practice of the European Court of Human Rights concerning digital evidence and the positions of the Supreme Court of Ukraine contributes to strengthening the evidentiary value of OSINT in cases concerning public office offences
Threats	Incorrect interpretation of data: without appropriate analytical training, OSINT conclusions may be interpreted incorrectly, which leads to delays in investigations or the exclusion of data from proceedings	Recognition of evidence as inadmissible: strict requirements concerning procedural documentation and privacy rights may result in the rejection of OSINT materials in court, and practice has demonstrated such situations in particular episodes of corruption investigations involving officials participating in large-scale schemes

Source: compiled based on C. Adionyi (2024), S. Lehominova *et al.* (2024), National Anti-Corruption Bureau of Ukraine (2024a; 2024b), A. Yadav *et al.* (2023), M.J. Yuthvek *et al.* (2024)

The analysis provides a basis for conclusions regarding the advantages and prospects of using OSINT technologies in the investigation and prevention of public office offences. According to the press service of the Specialised Anti-Corruption Prosecutor's Office, a judge of one of the courts in Kyiv acquired assets whose value exceeded his lawful income by more than 16 million UAH, while declarations contained inaccurate information regarding owned property and its valuation, which formed the basis for notification of

[1] Law of Ukraine No. 2657-XII "On Information". (1992, October). Retrieved from https://zakon.rada.gov.ua/laws/show/2657-12#Text.
[2] Law of Ukraine No. 2297-VI "On Personal Data Protection". (2010, June). Retrieved from https://zakon.rada.gov.ua/laws/show/2297-17?lang=en#Text.

suspicion under Article 368-5 and Part 2 of Article 366-2 of the Criminal Code of Ukraine, namely illicit enrichment and declaration of false information (Ukrinfopress, 2025). This case is illustrative, as conventional mechanisms of control over declarations and financial reporting often do not allow the identification of concealed assets or discrepancies between declared data and actual circumstances without the use of additional analytical methods. In this context, OSINT technologies significantly expand investigative capabilities through the systematic collection, verification, and analysis of large volumes of data from public registers, social media, open databases, and other accessible sources, which enables identification of undisclosed assets, establishment of network relationships between individuals and property, and development of digital evidence applicable in criminal proceedings concerning public office offences, which is supported by contemporary OSINT research indicating that the development of methodologies and automated tools increases the efficiency and accuracy of open-source data analysis, making OSINT an important element of modern intelligence practice (Ivkova & Opirskyy, 2025). Legal positions of the Supreme Court of Ukraine (2024; 2025), set out in decisions of 2024-2025 concerning admissibility, relevance, and evaluation of digital evidence and information from open sources in criminal proceedings on public office offences, indicate the gradual development of judicial practice that recognises the evidentiary value of open-source data subject to compliance with procedures of verification and assessment, which expands the prospects for wider use of OSINT in such investigations and strengthens the evidentiary base, increasing the effectiveness of anti-corruption proceedings.

Improvement of the effectiveness of OSINT methodologies in the investigation of public office offences occurs through systematic analysis of problems and risks, followed by the development of procedures and response strategies. One of the key practical challenges is the identification, verification, and proper documentation of reliable information within large volumes of open data, which is essential for establishing facts that may influence the course of criminal proceedings and the legal liability of public officials (National School of Judges of Ukraine, 2025). For example, OSINT data from electronic declarations, property registers, or public procurement systems are used to confirm discrepancies between declared income and actual assets in proceedings concerning illicit enrichment and abuse of power, particularly through integrated analysis of declarations and digital traces, and these approaches are described as key practical elements in the analysis of open sources in legal research and practice. Law enforcement and the judicial system in Ukraine are also improving their skills and knowledge about OSINT. For example, they are holding seminars and webinars for judges and investigators on the best ways to collect, verify, and document digital evidence, including how to present OSINT data as part of electronic evidence in criminal cases. These kinds of projects are meant to make the use of open sources in real investigations of public office crimes, like corruption cases involving abuse of office or illegal enrichment, better. For example, courts need proper recording, validation, and legal justification of OSINT materials for them to be accepted.

Another practical problem is that there is too much open data because new digital tools and platforms are becoming more common. The Ukrainian Helsinki Human Rights Union (2021) says that the digital footprint keeps getting bigger, which makes it harder to analyse OSINT data when looking into crimes committed by public officials. Social media, forums, videos, open databases, and other sources create a constant stream of digital information that police and analysts must sort through, filter, and organise to find signs of crimes, such as abuse of power, overstepping authority, or getting an unfair advantage. When there is so much data, there is a real risk of evidentiary overload, where important information might be missed or misinterpreted because there aren't good ways to process and classify it all. This problem isn't just a problem during war; it also happens in criminal cases involving official actions, where it's important to tell the difference between useful digital traces and wrong or unimportant data. The Ukrainian Helsinki Human Rights Union's report also says that even big government agencies like the National Anti-Corruption Bureau of Ukraine and the Specialised Anti-Corruption Prosecutor's Office have trouble processing a lot of data, especially when it comes in different formats and contexts. To analyse big datasets from open sources, you need systems for storing, sorting, and processing them automatically. This includes software that lets you filter data in a structured way, find the right indicators, and make sense of the results. Without these tools, investigators might miss important digital clues or misread open data, which could lead to wrong conclusions in criminal cases involving public officials.

In addition to the challenges identified, there are also significant constraints on the available resources and competence to analyse open sources, especially due to the need to use more advanced platforms, software, geolocation, and satellite imagery in the process. Training programmes and courses on OSINT are in the initial stages of development in Ukraine, and the level of training varies. International courses and training programmes organised by the Council of Europe have focused on training prosecutors and investigators in the use of open sources in criminal investigations, including war crimes investigations (Council of Europe Office in Ukraine, 2022). Another international training of trainers' programme for academic institutions has aimed to train specialists in OSINT who will train law enforcement agents of Ukraine in the techniques

for verifying and analysing open-source information (Kharkiv National University of Internal Affairs, 2025). Basic online courses, such as the OSINT School on the Diia.Education platform offer training in searching for and verifying open-source data, geolocation, and the use of reverse image search techniques but do not include training on using that data in court proceedings. The difference in the focus of each of these training programmes accounts for the differences in the competence of practitioners in the field of OSINT.

Within the investigation of offences committed by public office, the issue of the protection of personal data of the individuals encountered within the open sources presents a problematic issue. Investigations based on open sources often require the analysis of content published to social media platforms, videos published online, and the geolocation data of the individuals in those videos to determine their involvement in the commission of the offences. Each of these data elements may contain personally-sensitive data about the individuals in those videos, such as their names, places of residence, contact information, photographs of themselves, or data regarding the relationships of those individuals to the members of their own families and their finances. In the lack of rules regarding the ethical use of such data, the information can be used against those individuals without a legal basis for such use, potentially leading to the violation of their human rights and the incorrect interpretation of the actions of the public officials involved in the offences. According to the Ukrainian Helsinki Human Rights Union (2021), while the open sources from which investigation of the public officials can be performed may contain information that is to be useful to the investigation, that information has the potential to be harmful to the rights of those individuals if it is incorrectly processed. For instance, social media platforms can be analysed to reveal the personal data of civilians who have little relation to the offences being investigated. Due to the lack of established standards for documenting open sources of evidence, as well as the analysis of such evidence in criminal cases, many courts and investigators are sceptical of the use of such information within criminal investigations (Radeiko, 2025). Furthermore, as H.-W. Huang *et al.* (2025) state in their publication on issues related to the investigation of public officials, open sources of digital data cannot be documented properly without the inclusion of features to record the metadata of that digital data, to cryptographically secure that data, and to document the digital data and its analysis in the reports of the investigators. Without such proper documentation, the digital data from open sources is often rejected as admissible in the courts, as has happened in the prosecutions of individuals in various international jurisdictions.

Considering the above, it is possible to conclude that the methodology of OSINT can be used in the investigation of offences committed by public office. The selection of the tools to be utilized in the investigation and the implementation of those tools indicates the challenges that might exist in the investigation of these types of crimes, such as the difficulty in accessing and reviewing the data, the need for ethical and impartial handling of the data, and the limited resources available to the police investigation itself. Understanding these challenges enables the development of appropriate responses and supports the planning of further use of OSINT technologies in the investigation of public office offences.

Improvement of the use of OSINT methodologies in pre-trial investigation of public office offences

The analysis of legal foundations and judicial practice and the SWOT assessment of the application of OSINT methodologies in pre-trial investigation of public office offences in Ukraine indicate the potential of this set of tools, while also identifying several systemic issues that reduce the effectiveness of its practical use. Key challenges include the absence of unified standards for the collection and documentation of OSINT data, risks of legal inadmissibility of digital evidence, a shortage of qualified analysts, overload of investigators with large volumes of open data, and risks related to violations of privacy and personal data protection. Recommendations aimed at addressing these challenges are systematised in Table 3.

Table 3. Support for the use of OSINT methodologies in the pre-trial investigation of public office offences

Area	Recommendation	Responsible entities	Performance metrics
Regulatory	Development of official methodological guidelines on OSINT	OPG, MIA, National Anti-Corruption Bureau of Ukraine	Existence of an approved document; number of proceedings referring to it
Procedural	Standardisation of requirements for documenting OSINT evidence	OPG, Supreme Court	Reduction in cases where evidence is declared inadmissible
Institutional	Establishment of specialised OSINT units	NABU, SBI, SSU	Number of units established; number of investigations conducted
Human resources	Systematic OSINT training for investigators	MIA, international partners	Number of trained specialists; assessment results
Methodological	Implementation of data verification standards	Law enforcement agencies	Share of verified data; reduction in erroneous conclusions
Technical	Procurement and deployment of analytical platforms	MIA, MDT	Data processing time; number of automated processes

Table 3, Continued

Area	Recommendation	Responsible entities	Performance metrics
Ethical	Development of an OSINT code of ethics	Ukrainian Parliament Commissioner for Human Rights	Number of complaints regarding privacy violations
Oversight	Prosecutorial supervision and judicial control over OSINT	Prosecutor's Office, courts	Quality of judicial reasoning regarding OSINT evidence

Note: MIA – Ministry of Internal Affairs; MDT – Ministry of Digital Transformation of Ukraine; OPG – Office of the Prosecutor General; SBI – State Bureau of Investigation; SSU – Security Service of Ukraine
Source: developed by the researcher

The analysis affirms that enhancing the application of OSINT methodologies in the pre-trial investigation of public office offences in Ukraine necessitates a holistic and systematic approach that addresses the legal, organisational, methodological, technical, and ethical aspects of investigative practices. There needs to be progress on both the legal and procedural fronts. The lack of specific rules in the Criminal Procedure Code of Ukraine and other laws about how to use OSINT makes it unclear whether such evidence is acceptable in court. It is therefore appropriate to develop and adopt unified departmental methodological guidelines for investigators and prosecutors. These guidelines should set the legal limits on how to gather information from open sources, what makes it valid as evidence, and what metadata needs to be recorded, including the source, time of acquisition, publication context, and preservation. Standardisation like this helps create consistent law enforcement practices and lowers the chance that digital evidence will be thrown out of court.

One important area is making law enforcement agencies better at open-source analysis. In practice, the use of OSINT is often assigned directly to investigators, who simultaneously conduct procedural actions and analytical processing of data, which leads to overload and reduced quality of analysis. Institutionalisation of OSINT analytics through the establishment of specialised units or inter-agency groups represents an effective approach, as research has indicated that the development and formalisation of OSINT methodologies increases the accuracy of collection and analysis of open data and establishes OSINT as a key element of modern intelligence and decision-making in the field of national security (Ivkova & Opirskyy, 2025). Within such a model, the investigator retains procedural responsibility for the use of information, while the analyst is responsible for its technical and analytical processing, which contributes to improving the quality of the evidentiary base in proceedings concerning public office offences.

The methodological dimension of the use of OSINT methodologies is also significant, as open sources are characterised by high levels of informational noise, disinformation, and manipulation. Minimisation of these risks requires the implementation of standardised approaches to assessing the reliability of information, including multi-level verification of data, analysis of the context of dissemination, and critical evaluation of sources; such approaches were described in international OSINT research as a critical component of fact verification and reduction of errors when working with open data, particularly within models of multi-dimensional truth verification and integration of contextual information (Wang *et al*., 2022). The documentation of the logic of the analytical conclusions that are made, the tools used in the analysis, and the methods of verifying the results of that analysis will become a mandatory element of OSINT investigations in order to ensure the transparency of the investigation's analytical processes.

The technical support of the OSINT analysis will be a priority task due to the growing volume of digital information and the increasing number of open digital platforms from which that information can be obtained, but which cannot be manually processed; automated software analysis tools will improve the accuracy of investigations into corrupt and professional connections, as well as reduce the amount of time that is required for those investigations to be performed. The implementation of secure systems for the storage of OSINT data with controlled access also remains important because such systems will contribute to the preservation of the confidentiality and integrity of information.

A separate set of recommendations concerns compliance with standards for the protection of personal data and the privacy of individuals whose information appears in open sources. Although OSINT methodologies rely on the analysis of publicly available information, this does not remove the obligation to adhere to the principles of legality, proportionality, and the minimisation of interference in private life. The use of open-source data without appropriate ethical and procedural safeguards may lead to unjustified interference with the rights of individuals who are not subjects of criminal proceedings and may call into question the legitimacy of the obtained evidence. For this reason, the development of internal ethical standards for the application of OSINT and the mandatory assessment of risks to human rights during large-scale digital investigations remain important, similarly to international ethical codes and practices that require respect for privacy, legality, and the minimisation of harm during work with open-source data, which is widely discussed

in academic research on OSINT and human rights, particularly in studies that examine the ethical limitations of OSINT and the necessity of regulation for the protection of human rights during the use of open-source data by E. Millett (2023).

Thus, the improvement of the use of OSINT methodologies in the pre-trial investigation of public office offences in Ukraine should occur through the combination of regulatory governance, institutional strengthening, methodological standardisation, technical modernisation, and adherence to ethical principles. The implementation of such a comprehensive approach will increase the effectiveness of the identification and documentation of official offences, ensure the admissibility of digital evidence in court, and strengthen public trust in the activities of law enforcement agencies under conditions of the digitalisation of criminal justice.

Discussion

The study examined the prospects for the use of data from open sources during the pre-trial investigation of public office offences. These prospects were identified through the analysis of the annual report of the National Anti-Corruption Bureau of Ukraine and the SWOT analysis. The conclusions regarding the application of OSINT methodologies in investigations received full or partial support in previous research, including the study conducted by J. Rajamaki & K. Tiitta (2024). After examining international financial organisations, J. Rajamaki & K. Tiitta concluded that the use of information from open sources was advisable for the timely identification and prevention of threats. A similar position appears in the present study, which emphasises that investigations conducted by the National Anti-Corruption Bureau of Ukraine exposed schemes within the Ministry of Defence amounting to 733 million hryvnias. The analysis nevertheless considered the different research focuses, because the study conducted by J. Rajamaki & K. Tiitta concentrated exclusively on the financial sector, whereas the present study examined public office offences that may produce not only financial consequences, but also broader forms of impact.

V. Bilous *et al.* (2024) supported the argument presented in this study that the use of information from open sources contributes to situational awareness and strategic planning. The present study considers this issue, in particular, through the case of a judge whose actual assets substantially exceeded declared income. Despite the similarities between the current study and the research of V. Bilous *et al.*, the research of the authors exclusively examined the use of OSINT methodologies within military contexts. In contrast, public office offences may emerge in a variety of contexts. The research of Z. Avrahami *et al*. (2025) investigated the use of OSINT methodologies in the context of cybersecurity threats to organisations. The researchers analysed the experiences of both public and private companies to determine that the use of OSINT methodologies enabled those organisations to identify and respond to cyber threats in a timely manner. Although there are similarities between the study of Z. Avrahami *et al.* and the present study, such similarities are only partial due to the different focuses of the two studies. Whereas Z. Avrahami *et al.* studied public and private organisations, the present study focused on public organisations. Furthermore, the argument of the present study that OSINT technologies can be applied to various sectors is supported by the study conducted by V. Scuro (2025). V. Scuro found that the use of information from open sources enables organisations to identify the individuals who have committed offences in the digital space, such as trafficking in cultural heritage. Though similar to the present study, the research of V. Scuro relates to the private sector only, whereas the majority of public office offences occur within the public sector. Nevertheless, the ability of OSINT methodologies to assist in the identification of and response to criminal activity was recognised in the comparison of the research of the present study to previous research studies on the topic.

Further analysis shows that, even though OSINT methods have a lot of benefits, using data from open sources also comes with a lot of risks and problems. The study of how OSINT methods are used in investigations of public office crimes found that it was hard to quickly and fairly analyse large amounts of open-source data. Similar conclusions appear in the study conducted by D. Van Puyvelde & F. Tabarez Rienzi (2025), who examined the widespread perception of OSINT technologies as a revolutionary approach to criminal investigations. The researchers noted that the exponential growth of data transforms the scale of intelligence activities and encourages both state and non-state actors to seek strategies for integrating OSINT methodologies and improving digital literacy. In the present study, this issue appears through the argument that one of the principal practical problems associated with the use of information from open sources is the high risk of disinformation, including the emergence of deepfakes. The study also argued that the possibility of falsifying information creates risks for individuals and legal entities that are not connected with the commission of public office offences. Issues concerning the protection of confidentiality during criminal investigations also appear in the study conducted by M. Konieczny & P. Wiecej (2025), who emphasised that the use of information from open sources involves a high risk of the unauthorised acquisition and misuse of personal data on the Internet. Unlike M. Konieczny & P. Wiecej, who opposed the use of OSINT methodologies in criminal investigations categorically, the present study supports a more moderate application of this technology. The idea of moderate application also appeared in the study conducted by G.P. Ramadhany (2024), who emphasised the potential of research based on open sources while stressing the

integration of such intelligence tools into the practice of law enforcement agencies. The proposed approaches to integration included the development of policies governing the application of OSINT methodologies, the training and retraining of specialists, and the strengthening of the material and technical resources available for investigations, strategies and recommendations that received full or partial reflection in the present study. The ethical application of OSINT methodologies also received attention in the study conducted by A. Koenig (2024), who emphasised that, regardless of the type of source used during an investigation, information should be collected and analysed in accordance with the principles of accuracy and respect for the dignity of the involved parties. This position fully corresponds with the recommendation presented in the present study concerning the development of a code of ethics for OSINT, the implementation of which could fall under the responsibility of the Commissioner for Human Rights of the Verkhovna Rada of Ukraine. Thus, the emphasis placed in the present study on adherence to ethical standards during the use of open-source data received strong support in previous research concerning the application of OSINT methodologies.

The present study also examined the importance of interdisciplinary cooperation for the effective application of OSINT methodologies in investigations of public office offences. The effectiveness of such cooperation received more detailed consideration during the development of recommendations aimed at improving the effectiveness of the use of information from open sources. The importance of interdisciplinary cooperation during criminal investigations also received support in previous research, particularly in the study conducted by A. Mukhopadhyay *et al.* (2024), who examined interdisciplinary cooperation in the context of the continuously increasing volume of information. According to the researchers, the growing volume of data and the complexity of investigative tasks indicate the need to expand and accelerate OSINT investigations, including through crowdsourcing practices involving experts. Such an approach may improve the effectiveness of investigations within the national context, where distinctions exist between specialists and experts who possess different powers concerning the collection and interpretation of obtained data. The importance of interdisciplinary cooperation also appears in the study conducted by A. Karakikes & K. Kotis (2025), who analysed the prospects for the application of artificial intelligence tools in the analysis of open sources for the protection of state borders. The researchers assert that the execution of these strategies necessitates interdisciplinary collaboration among experts in machine learning, natural language processing, and computer vision. The comparison between the current study and the research by A. Karakikes & K. Kotis revealed only partial alignment, as the studies examined distinct forms of interdisciplinary cooperation: the current study focused on collaboration among law enforcement agencies, while their research concentrated on cooperation within the realm of computer technologies.

The identified correspondences underscore the significance of the current study and highlight the imperative for a more thorough investigation of the proposed issue. The present study contributes to academic discourse by delineating public office offences as a distinct category characterised by unique traits necessitating specialised investigative methodologies.

Conclusions

The study found that there was a trend toward more public office crimes. In the first half of 2025, the National Anti-Corruption Bureau of Ukraine informed 115 people of their suspicions in cases of high-level corruption. This is twice as many as the number reported in the previous reporting period. The timely exposure of public office offences helps to prevent losses and strengthens public trust in state authorities. The investigation of public office offences benefits from the analysis of open-source information, a practice that has proven both advisable and effective across various contexts. In Ukraine, the use of OSINT technologies in the pre-trial investigation of public office offences is regulated by a range of regulations that grant data from open sources the status of admissible evidence, provided that such data are properly documented and impartially verified for authenticity.

The application of OSINT methodologies in the investigation of public office offences guarantees broad access to open sources and rapid data collection. The prospects of OSINT technologies include their use in the investigation of public office offences across different sectors, including the military, educational, and medical sectors, together with the development of a digital evidence base. The analysis of the prospects for the application of OSINT methodologies also considered their weaknesses, including the lack of standardised procedures and trained analysts, together with insufficient material and technical resources. The threats associated with the application of OSINT methodologies include disinformation, fake content, and violations of privacy. From a practical perspective, the obstacles to the application of OSINT technologies in criminal investigations include difficulties related to the identification and processing of reliable information within extensive volumes of open-source data, the overload of open-source information and the impossibility of its rapid processing, resource and competency limitations, and the necessity of adhering to the ethical principles of anonymity and confidentiality during investigations.

The identified problems require changes across several areas, namely the regulatory, procedural, institutional, personnel, methodological, technical, ethical, and supervisory dimensions. Changes in these areas

include the development of official methodological recommendations concerning the application of OSINT technologies, the unification of requirements for the documentation of evidence obtained from open sources, the establishment of specialised OSINT units and the organisation of systematic training programmes, the implementation of unified standards for the verification of obtained data, the development of a code for the ethical use of OSINT approaches, and the provision of prosecutorial supervision and judicial oversight regarding their application. The study proposed that such state institutions as the Office of the Prosecutor General, the Ministry of Internal Affairs of Ukraine, the Ministry of Digital Transformation of Ukraine, the National Anti-Corruption Bureau of Ukraine, the Supreme Court of Ukraine, the State Bureau of Investigation of Ukraine, and the Security Service of Ukraine should bear responsibility for the implementation of these recommendations. The study also developed metrics for evaluating the effectiveness of the proposed strategies, including the reduction in cases where evidence is declared inadmissible, the number of established units, the number of trained specialists, the proportion of verified data, the time required for data processing, the proportion of automated processes, and the number of complaints concerning violations of privacy.

Future studies should cover a broader sample of cases, incorporating materials from open sources beginning in 2020. The expansion of the sample will assist in tracing the dynamics of public office offences, the use of information from open sources during their investigation, and strategies aimed at increasing the effectiveness of such application.

Acknowledgements

None.

Funding

The study was not funded.

Conflict of Interest

None.

References

[1] Adionyi, C. (2024). Harnessing OSINT to enhance the investigation of economic crimes. *Journal of Anti-Corruption Law*, 8, 159-174.

[2] Amelin, O.Yu. (2024). Certain aspects of the appointment and replacement of a prosecutor in criminal proceedings on crimes in the sphere of official activities. *Rule of Law*, 56, 143-154. doi: 10.18524/2411-2054.2024.56.315691.

[3] Amelin, O.Yu., Pyniaha, R., Zaloznyi, R., Dmytrova, O., & Kryvoshlykov, S. (2025). Investigation of criminal offences in the field of official activity: Analysis of international experience and the possibility of its application in Ukraine. *International Annals of Criminology*, 63(4), 768-790. doi: 10.1017/cri.2025.10110.

[4] Avrahami, Z., Zwilling, M., & Hajaj, C. (2025). Leveraging OSINT for advanced proactive cybersecurity: Strategies and solutions. *IEEE Access*, 13, 154229-154250. doi: 10.1109/ACCESS.2025.3603868.

[5] Bilous, V., Bodnenko, D., Khokhlov, O., Lokaziuk, O., & Stadnik, I. (2024). Open source intelligence for war crime documentation. *CEUR Workshop Proceedings*, 3654, 368-375.

[6] Bocharov, S., Tyshchuk, V., & Bielai, S. (2025). Use of OSINT in operational and investigative activities: Tools and legal aspects. *State Security*, 1(5), 25-30. doi: 10.33405/2786-8613/2025/1/5/336692.

[7] Breuer, N. (2025). Testing the reliability of OSINT network data for investigating organized crime infiltration of legal-market businesses. *Global Crime*. doi: 10.1080/17440572.2025.2567277.

[8] Council of Europe Office in Ukraine. (2022). *The Council of Europe supports training on OSINT tools for prosecutors and investigators of Ukraine*. Retrieved from https://surl.li/zlwjwh.

[9] Huang, H.-W., Shih, C.-H., Li, C.-Yu., & Teng, H.-Yu. (2025). A blockchain-based framework for OSINT evidence collection and identification. *Future Internet*, 17(12), article number 551. doi: 10.3390/fi17120551.

[10] Ivkova, V.S., & Opirskyy, I.R. (2025). Research of existing OSINT tools and approaches in the context of personal and state information security. *Computer Systems and Networks*, 7(1), 143-159. doi: 10.23939/csn2025.01.143.

[11] Karakikes, A., & Kotis, K. (2025). AI-assisted OSINT/SOCMINT for sefeguarding boarders: A systematic review. *Information*, 16(12), article number 1095. doi: 10.3390/info16121095.

[12] Kharkiv National University of Internal Affairs. (2025). *EUAM experts launch OSINT training course for KhNUIA representatives*. Retrieved from https://univd.edu.ua/en/news/22784.

[13] Koenig, A. (2024). Ethical considerations for open-source investigations into international crimes. *AJIL Unbound*, 118, 45-50. doi: 10.1017/aju.2024.2.

[14] Konieczny, M., & Wiecej, P. (2025). Anti-OSINT methods ensuring protection of personal data in the context of cybercrime. *Annuals of the Administration and Law*, 1(25), 127-144. doi: 10.5604/01.3001.0055.1100.

[15] Kosokhatko, B.S. (2025). Problems of using open-source intelligence in the investigation of crimes committed within the framework of an international armed conflict. *Uzhhorod National University Herald. Series Law*, 3(88), 277-284. doi: 10.24144/2307-3322.2025.88.3.41.

[16] Lehominova, S., Shchavinsky, Yu.V., Rabchun, D., Zaporozhchenko, M., & Budzynskyi, O. (2024). The threats of OSINT tools and ways to mitigate the consequences of their application for the organization. *Cybersecurity Education Science Technique*, 1(25), 294-303. doi: 10.28925/2663-4023.2024.25.294303.
[17] Millett, E. (2023). *Open-source intelligence, armed conflict, and the rights to privacy and data protection*. doi: 10.58866/HQKE7327.
[18] Mukhopadhyay, A., Venkatagiri, S., & Luther, K. (2024). OSINT research studios: A flexible crowdsourcing framework to scale up open source intelligence investigations. *Proceedings of the American Association for Computing Machinery. Human-Computer Interaction*, 8(CSCW1), article number 105. doi: 10.1145/3637382.
[19] National Anti-Corruption Bureau of Ukraine. (2024a). *Steadfastness and efficiency: NABU and SAPO results in the first half of 2024*. Retrieved from https://surli.cc/hyntnx.
[20] National Anti-Corruption Bureau of Ukraine. (2024b). *The results of the first half of 2024 indicate that NABU and SAPO are reaching new heights in eradicating corruption: The latest high-profile cases involve former and current top officials committing corruption crimes here and now*. Retrieved from https://surl.li/chtjpa.
[21] National Anti-Corruption Bureau of Ukraine. (2025a). *The first half of 2025 was marked by a number of high-profile relations for NABU and SAPO, particularly in the defence, land, and medical sectors. As in previous periods, the emphasis was on exposing high-level corruption taking place in the context of full-scale aggression by the Russian Federation*. Retrieved from https://reports.nabu.gov.ua/investigations/.
[22] National Anti-Corruption Bureau of Ukraine. (2025b). *Report. II half of 2024*. Retrieved from https://nabu.gov.ua/site/assets/files/48751/zvit_2024_ii_ukr-1.pdf.
[23] National School of Judges of Ukraine. (2025). *Application of OSINT in judicial practice: From legal foundations to practical cases*. Retrieved from https://surl.li/ybbduc.
[24] Radeiko, R.I. (2025). Theoretical and legal framework for the admissibility of OSINT evidence from social networks: Procedural requirements and methodological approaches (case study No. 990/232/24). *Scientific Notes of Lviv University of Business and Law*, 45, 110-116. doi: 10.5281/zenodo.15648855.
[25] Rajamaki, J., Lahti, I., & Parviainen, J. (2022). OSINT on the dark web: Child abuse material investigations. *Information & Security*, 53(1), 21-32. doi: 10.11610/isij.5302.
[26] Rajamaki, J., & Tiitta, K. (2024). Implementation of OSINT for improving an international finance sector organization's cybersecurity. *International Conference on Cyber Warfare and Security*, 19(1), 612-616. doi: 10.34190/iccws.19.1.1977.
[27] Ramadhany, G.P. (2024). Open-source intelligence (OSINT) tools for law enforcement. *Endless: International Journal of Future Studies*, 7(3), 21-33.
[28] Sazibur, R. (2025). *The art of open source intelligence (OSINT): Addressing cybercrime, opportunities, and challenges*. doi: 10.2139/ssrn.5281845.
[29] Scuro, V. (2025). Open-source intelligence (OSINT) for researchers and practitioners. In E. Smith & S. Austin (Eds.), *Researching a rigged game: Digital approaches to tracing the illicit trade in cultural objects* (pp. 11-28). Cham: Springer. doi: 10.1007/978-3-032-02014-7_2.
[30] Supreme Court of Ukraine. (2024). *Supreme Court Judges discussed with experts the issue of admissibility of electronic evidence obtained from open sources*. Retrieved from https://supreme.court.gov.ua/supreme/pres-centr/news/1282146/.
[31] Supreme Court of Ukraine. (2025). *OSINT as evidence in the investigation of war crimes: Representatives of the Supreme Court participated in a thematic seminar*. Retrieved from https://supreme.court.gov.ua/supreme/pres-centr/news/1883443/.
[32] Szymoniak, S., & Foks, K. (2024). Open source intelligence opportunities and challenges – a review. *Advances in Science and Technology Research Journal*, 18(3), 123-139. doi: 10.12913/22998624/186036.
[33] Ukrinfopress. (2025). *Judge with millions in assets: SAPO exposed illegal; enrichment of over UAH 16 million*. Retrieved from https://ukrinfopress.com/2025/09/suddya-z-milyonnym-maynom-sap-vykryla-nezakonne-zbahachennya-na-ponad-16-mln-hrn-ukrinfopres.
[34] Ukrainian Helsinki Human Rights Union. (2021). *War and justice: How investigators can effectively use OSINT and what to do with "court" decisions in uncontrolled territories*. Retrieved from https://helsinki.org.ua/articles/viyna-ta-pravosuddia-iak-slidchym-efektyvno-vykorystovuvaty-osint-ta-shcho-robyty-iz-rishenniamy-sudiv-na-nepidkontrolnykh-terytoriiakh.
[35] Van Puyvelde, D., & Tabarez Rienzi, F. (2025). The rise of open-source intelligence. *European Journal of International Security*, 10(4), 530-544. doi: 10.1017/eis.2024.61.
[36] Van der Woude, M., & Torres, G. (2024). The ethics of open source investigations: Navigating privacy challenges in a gray zone information landscape. *Sage Journals*, 26(10), 2184-2202. doi: 10.1177/14648849241274104.
[37] Wang, H., Li, Ya., Huang, Zh., & Dou, Y. (2022). IMCI: Integrate multi-view contextual information for fact extraction and verification. *arXiv*. doi: 10.48550/arXiv.2208.14001.

[38] Yadav, A., Kumar, A., & Singh, V. (2023). Open-source intelligence: A comprehensive review of the current state, applications and future perspectives in cyber security. *Artificial Intelligence Review*, 56, 12407-12438. doi: 10.1007/s10462-023-10454-y.
[39] Yuthvek, M.J., Adheena, S., Charithra, Y., & Kalaiselvi, K. (2024). Analyzing business crimes by implementing OSINT architecture. *Indian Journal of Natural Sciences*, 15(83), 72456-72464.

Правові та практичні аспекти застосування OSINT-методик для збору доказів під час досудового розслідування службових злочинів

Олександр Амелін
Кандидат юридичних наук, доцент
Офіс Генерального прокурора
01011, вул. Різницька, 13/15, м. Київ, Україна
Навчально-науковий інститут права Державного податкового університету
08201, вул. Університетська, 31, м. Ірпінь, Україна
https://orcid.org/0000-0002-0933-2111

Анотація
Мета дослідження полягала у вивченні правових обмежень, процедурних вимог і практичних проблем, що виникають під час фіксації, перевірки та використання відомостей з відкритих джерел у провадженнях про службові злочини. Для досягнення мети використовувалися методи контекстуального, нормативно-правового та проблемно-орієнтованого аналізу. З огляду на тенденцію до збільшення кількості службових злочинів у 2024–2025 роках, було зроблено висновок про доцільність використання інформації з відкритих джерел для своєчасного виявлення злочинних схем, уникнення збитків і підвищення рівня суспільної довіри до державних інститутів. На підставі дослідження нормативно-правової бази та контекстуального аналізу визначено позитивні аспекти й перспективи пошуку доказів у відкритих джерелах, зокрема широкий доступ до релевантної інформації та її швидкий збір, а також можливість розслідування злочинів у різних сегментах державної діяльності – військовому, освітньому, медичному тощо. Як недоліки й загрози використання відкритих джерел інформації виокремлено недостатність стандартизованих процедур, слабку матеріально-технічну базу, а також потенційне порушення етичних норм. Вивчення проблемних аспектів дало змогу розробити рекомендації щодо підвищення ефективності використання відкритих джерел у розслідуванні службових злочинів. Підвищення ефективності розслідування передбачає трансформаційні процеси в різних напрямах, зокрема нормативному, процесуальному, інституційному, кадровому, методичному, технічному, етичному, а також у напрямі контролю. Результати дослідження можуть бути використані законодавцями для вдосконалення нормативно-правової бази, правоохоронними органами й слідчими – для підвищення ефективності та якості розслідування службових злочинів, науковцями – для подальшого аналізу методик опрацювання інформації з відкритих джерел, а освітніми установами – для розробки навчальних програм і тренінгів із застосуванням цифрових доказів у практиці кримінального провадження

Ключові слова:
відкриті джерела інформації; персональні дані; декларації; реєстри; дезінформація; діпфейки; незаконне збагачення