STATE OF SCIENTIFIC RESEARCH ON THE ADMINISTRATIVE AND LEGAL REGULATION OF OSINT FUNCTIONING IN ENSURING PUBLIC ORDER AND SECURITY IN THE WORKS OF FOREIGN SCHOLARS: LESSONS FOR UKRAINE

Byba Roman

DOI: https://doi.org/10.61345/1339-7915.2025.4.2

Annotation. The article provides a comprehensive analysis of scientific research devoted to the administrative and legal regulation of OSINT functioning in the field of public order and security. It examines the approaches of foreign scholars who study the use of open-source information, the impact of digital technologies on law enforcement activities, and the ethical, legal, and procedural challenges associated with OSINT operations conducted by public authorities. The findings show that researchers emphasize the need for professional standards, digital competencies, reliable methodologies, and effective procedures for assessing the accuracy of open-source data. Particular attention is given to issues of privacy protection, risks of profiling, transparency of OSINT practices, and the growing influence of artificial intelligence on intelligence-gathering processes. It is argued that AI-based OSINT strengthens analytical capabilities but also intensifies legal risks, which requires harmonized international standards and robust oversight mechanisms. The study notes that Ukrainian legal scholarship lacks comprehensive research on the administrative and legal foundations of OSINT, which highlights the relevance and scientific novelty of further studies in this area. Based on the analysis of foreign literature, the article formulates recommendations for the development of Ukrainian doctrine, including the definition of OSINT actors, procedural requirements for their work, ethical principles, privacy guarantees, and models of independent oversight in the field of public order and security.

Key words: OSINT, public security, public order, administrative regulation, open-source information, ethics, artificial intelligence, privacy, law enforcement.

1. Introduction.

The need to study the administrative and legal regulation of OSINT use in ensuring public order and security is driven by the growing importance of open-source information in the activities of state authorities. Contemporary security challenges–such as information operations, coordination of unlawful actions through open networks, the spread of extremist content, and digital threats–require public authorities to rapidly obtain and verify data from accessible sources. However, the scale of such use has surpassed existing regulatory frameworks, creating a range of practical and theoretical problems.

First, active engagement with open sources requires clearly defined limits for officials, since even publicly available information can affect an individual's private life. The absence of established procedures for collecting, analysing, and applying such data in the work of law enforcement bodies creates risks for personal rights and calls into question the integrity and transparency of authorised units. This highlights the need to clarify the requirements for OSINT use, establish clear criteria of admissibility, and introduce safeguards for the protection of individuals.

Second, there is a significant gap between practice and regulation. State bodies increasingly employ open-source intelligence methods, yet do so without unified standards, through diverse approaches, and without harmonised procedures. This hinders institutional cooperation, causes duplication of functions or, conversely, gaps in operational activity, and raises concerns about proper oversight of OSINT-derived results. Unified approaches and clear rules are essential for strengthening effectiveness and ensuring accountability.

Third, the modernisation of public order and security systems further reinforces the relevance of OSINT. The use of open-source data enables timely identification of threats, forecasting of hazardous situations, and prevention of offences. However, these advantages can be realised only if supported by legal certainty, standardised procedures, and proper oversight of the actions of responsible authorities.

Therefore, the chosen topic possesses clear scientific and practical significance and requires systematic and comprehensive research.

2. Analysis of scientific publications.

Issues related to the functioning of OSINT in the field of public order and security have already attracted considerable attention from foreign scholars, who examine both the theoretical foundations and the practical challenges of using open-source information in the activities of public authorities. Various dimensions of open-source intelligence–its role in contemporary security models, organisational and procedural principles of its application, ethical and human-rights limitations, as well as the impact of digital technologies and artificial intelligence on OSINT practices–have been explored, in particular, by O. Larsen, D. Van Puyvelde, E. Millett, H. Bean, Q. Eijkman, L. Fereidooni, A. Mahmood, A. Asnawi, N. Soni and others. Their works form an essential theoretical basis for understanding the role of OSINT within law enforcement and other bodies responsible for maintaining public safety and order. In contrast, Ukrainian administrative-legal scholarship lacks comprehensive research specifically devoted to the regulation of OSINT functioning in the sphere of public order and security, which underscores the need for focused and systematic academic study of this topic.

3. The purpose of the work.

The purpose of this scientific study is to examine the achievements of foreign legal scholarship, to summarise the prevailing academic views, and to develop a coherent theoretical and practical foundation for defining the administrative and legal principles of OSINT functioning in the sphere of ensuring public order and security in Ukraine.

4. Review and discussion.

In contemporary academic literature, there is a marked increase in attention to the study of the possibilities and consequences of using open-source information in the activities of bodies responsible for maintaining public order and security. Foreign and Ukrainian scholars examine both the theoretical foundations of OSINT and the practical models of its application in the work of law enforcement agencies and institutions within the security and defence sector.

In research on the administrative and legal regulation of OSINT functioning in the sphere of ensuring public order and security, it is particularly important to comprehensively analyse the works of both foreign and national scholars. This need stems from the fact that OSINT has developed as a global phenomenon, and its regulatory frameworks differ across states. Such diversity makes it possible to identify common trends, discrepancies, and gaps in legal regulation, as well as to take into account the positive experiences of other countries for the development of OSINT practices in Ukraine. This scholarly approach allows for a holistic understanding of the formation and application of OSINT in the activities of public authorities and enables an assessment of how researchers interpret its role in safeguarding public security and order, as well as the extent of state involvement in these processes.

It is important to analyse studies that explore OSINT in a broad sense–as a technological, informational, and organisational tool that enhances the capacity of the state to counter threats to public order and security. Such research makes it possible to identify general patterns of open-source information use and to outline the characteristics of OSINT that directly influence its application by public authorities.

Separate attention should be devoted to scholarly works examining OSINT within the context of law enforcement, as this sector most actively integrates open-source capabilities into practices aimed at preventing, detecting, and responding to threats to public security and order. The analysis of such works helps determine how OSINT transforms state response mechanisms, what advantages and risks arise in its use, and what administrative and legal implications it generates for relevant actors.

Equally important are the contributions of authors who study the ethical requirements for OSINT use and the activities of actors working with open information. This includes examining administrative procedures, limits of permissible interference with private life, transparency of officials' actions, and the necessity of establishing rules to prevent abuses. Considerable attention is also paid to issues of liability for violations of established requirements, as this is essential for maintaining a balance between security needs and human rights protection.

A systematic review of academic sources helps determine how scholars define the role of OSINT in the work of public authorities, what risks they identify, what proposals they make regarding requirements for actors engaged in open-source data collection and analysis, and how they describe mechanisms for responding to violations. Thus, the coverage of diverse scholarly sources–from technological features of OSINT to ethical and legal principles of its application–creates a coherent foundation for the further theoretical and regulatory comprehension of OSINT in the field of public order and security.

Among foreign researchers, a significant contribution was made by O. Larsen, who conducted an empirical study of the use of open-source information by law enforcement agencies and demonstrated that the effectiveness of OSINT operations depends directly on personnel training and procedural clarity [1]. The author emphasises that the absence of established methodologies complicates data interpretation and decreases the reliability of operational conclusions. Many organisations face barriers in implementing effective OSINT methods and fail to adapt quickly to technological changes. Larsen highlights the need to shift the professional culture from long-term training to practical investigation activity to enhance the status and full utilisation of OSINT tools [1].

An important contribution was also made by D. Van Puyvelde, who traced the evolution of OSINT and emphasised the changing nature of threats in the digital environment [2]. The author argues that open-source information has become a full-fledged intelligence tool but requires proper regulation due to risks associated with the large volume of personal data users voluntarily publish online. Van Puyvelde's work is structured around four themes: the definition of OSINT and its distinction from investigations and general open-source information; the expanding use of OSINT by governmental, non-governmental, and law enforcement bodies; the need for digital literacy training instead of creating new organisations; and key OSINT challenges such as information overload, reliability, ethics, and regulatory limits [2].

In the work of E. Millett, attention is given to the relationship between OSINT and human rights, particularly privacy and data protection [3]. The study analyses conditions under which the use of open information by state authorities may violate international standards and stresses the need for clearly defined limits for such activities.

Ethical issues in OSINT use are also highlighted by other foreign scholars [4]. For example, H. Bean emphasises that collecting and processing publicly available information creates tension between state security needs and human rights guarantees. Mass aggregation and profiling of open data may affect privacy and personal autonomy even when the information is formally public [5].

In her study, Quirine Eijkman notes that state-level OSINT use generates new risks for citizens' privacy, as individuals may be unaware that their online activity becomes an object of systematic monitoring [6]. Existing accountability mechanisms were designed for traditional intelligence methods and are poorly suited to the realities of digital platforms. Eijkman concludes that the state's role in regulating OSINT must be reconsidered, highlighting the need for transparency rules, independent oversight, and effective remedies for individuals subject to open-source monitoring [6].

L. Fereidooni identifies several important conclusions regarding the use of OSINT in international law enforcement cooperation [7]. OSINT enables rapid acquisition of data significant for combating transnational crime and enhances cooperation in areas such as money laundering, terrorism financing, and cybercrime. However, the use of open data raises legal and ethical challenges, particularly due to data protection requirements such as those under the GDPR and unresolved issues regarding the admissibility of OSINT-derived evidence in court. Fereidooni also notes that technological progress, including artificial intelligence and big-data analytics, increases OSINT capabilities but requires internationally harmonised rules that balance security needs with human rights [7].

Research on OSINT application in policing has been conducted by A. Mahmood, A. Asnawi and their colleagues, who performed a systematic review of OSINT tools and assessed their suitability for various types of operational activity [8]. Scholars stress the absence of universal OSINT tools and call for the development of unified standards for their formal application.

In recent years, foreign authors have also paid considerable attention to the integration of artificial intelligence into OSINT activities [9; 10]. For example, Nitin Soni's study on AI-driven OSINT for cybercrime investigations demonstrates that combining AI with open-source intelligence significantly enhances forensic accuracy, speed, and proactivity, although such technologies also pose ethical, legal, and organisational challenges [11].

A synthesis of foreign research shows that OSINT plays an important role in modern security systems, yet its effectiveness depends on personnel qualification, unified procedures, and digital competence. Scholars emphasise risks associated with methodological gaps, data overload, and potential violations of privacy and autonomy through large-scale data collection and profiling. They argue for the establishment of transparent rules, independent oversight, complaint mechanisms, and internationally consistent standards that align security objectives with human rights protection.

5. Conclusions.

Summarising the above, the following conclusions can be drawn. First, it is advisable to conduct comprehensive research aimed at defining the administrative and legal status of actors who apply OSINT in the field of public order and security, including their powers, limitations, and operational standards. A separate research direction should focus on issues of professional training, digital literacy, and procedural requirements for the collection, analysis, and use of open-source information, including the algorithmisation of OSINT procedures in the internal regulations of the Ministry of Internal Affairs, the National Police, the State Bureau of Investigation, and other competent bodies.

Second, there is a need to develop a scientific approach to establishing administrative and legal safeguards for privacy protection when using OSINT, including cases involving elements of artificial intelligence. Promising avenues of research include models of transparency, independent oversight, documentation of OSINT operations, and procedures for appealing decisions made by public authorities, as well as the adaptation of European standards (such as GDPR-based approaches) to Ukrainian legislation in the sphere of public order and security.

References:

1. Larsen, O.H. A quantitative study of the law enforcement in using open source intelligence (OSINT) // Journal of Policing, Intelligence and Counter Terrorism. 2023. Vol. 18, № 3. P. 255–270. URL: https://www.sciencedirect.com/science/article/pii/S2666281723001348?utm_source=chatgpt.com [In English].

2. Van Puyvelde, D. The rise of open-source intelligence // European Journal of International Security. 2022. Vol. 7, № 2. P. 203–220. URL: https://www.cambridge.org/core/journals/european-journal-of-international-security/article/rise-of-opensource-intelligence/21122432399ECB8078BF0D89A76D0586?utm_source=chatgpt.com [In English].

3. Millett, E. Open-Source Intelligence, Armed Conflict, and the Rights to Privacy and Data Protection. Security and Human Rights Monitor. 2023. 22 p. URL: https://www.shrmonitor.org/assets/uploads/2023/05/article-Millett.pdf [In English].

4. Digital Forensics and Social Media: Ethics, Challenges and Opportunities; Birkbeck, University of London: London, UK, 2019; Available online. URL: https://www.bbk.ac.uk/news/digital-forensics-and-social-media-ethics-challenges-and-opportunities/ [In English].

5. Bean H. Is open source intelligence an ethical issue? // In: Maret S. (ed.) Government Secrecy (Research in Social Problems and Public Policy, Vol. 19). Bingley: Emerald, 2011. P. 385–402. [In English].

6. Eijkman Q., Weggemans D. Open source intelligence and privacy dilemmas: Is it time to reassess state accountability? // Security and Human Rights. 2013. Vol. 23, No. 4. URL: https://brill.com/view/journals/shrs/23/4/article-p285_5.xml?language=en&srsltid=AfmBOooJ-c12aIiW8_qsxXyP-asGciHEehfR2UK2gyxnsfIRVn4SnW85&utm_source=chatgpt.com [In English].

7. Fereidooni L.Fereidooni, L. Open Source Intelligence (OSINT) and its Role in Enhancing International Law Enforcement Cooperation. SSRN. 2025. 18 p. DOI: 10.2139/ssrn.5501559. [In English].

8. Mahmood, A., Asnawi, A., Azzahra, L. Open-Source Intelligence (OSINT) Tools for Law Enforcement: A Systematic Literature Review // Endless: Journal of Future Studies. 2024. Vol. 1, № 3. P. 45–60 URL: https://endless-journal.com/index.php/endless/article/view/308. [In English].

9. João Evangelista, Renato Jose Sassi, Marcio Romero Systematic Literature Review to Investigate the Application of Open Source Intelligence (OSINT) with Artificial Intelligence. URL: https://www.researchgate.net/publication/341229263_Systematic_Literature_Review_to_Investigate_the_Application_of_Open_Source_Intelligence_OSINT_with_Artificial_Intelligence [In English].

10. Biodoumoye George Bokolo Artificial Intelligence in Social Media Forensics: A Comprehensive Survey and Analysis. URL: https://www.mdpi.com/2079-9292/13/9/1671 [In English].

11. Enhancing Law Enforcement with OSINTSingh, H. Enhancing Law Enforcement with Open-Source Intelligence (OSINT) // In: Advances in Digital Policing. Singapore: Springer, 2025. P. 67–89. DOI: 10.1007/978-981-96-7505-0_5. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5501559https://www.researchgate.net/publication/391482255_Enhancing_Digital_Forensics_with_AI-Driven_OSINT_A_Proactive_Approach_to_Cybercrime_Investigation [In English].

Roman Byba,
Head of the Legal Department of LLC «ATB-Market»,
Dnipro, Ukraine
ORCID: 0009-0009-3246-5682