CADERNOS DE DEREITO ACTUAL
www.cadernosdedereitoactual.es

© *Cadernos de Dereito Actual* Nº 31. Núm. Ordinario (2026), pp. 457-474

·ISSN 2340-860X - ·ISSNe 2386-5229

Legal principles of the use of open intelligence in criminal proceedings in Ukraine and the EU

Anatolii Puhach[1]
Interregional Academy of Personnel Management
Oleksandr Shevchuk[2,*]
National Academy of Internal Affair
Oleh Zrazhevskyy[3]
National University of Water and Environmental Engineering
Alexander Rusnak[4]
National Academy of the Security Service of Ukraine
Viktor Trepak[5]
Security Service of Ukraine National Academy

[1] PhD in Law, Associate Professor, Interregional Academy of Personnel Management, Kyiv, Ukraine.
ORCID: 0009-0007-3283-2142; puhachanatolii@gmail.com

[2] PhD in Juridical Sciences, Associate Professor, Professor of the Department of Operational and Investigative Activities and National Security, National Academy of Internal Affair, Kyiv, Ukraine. ORCID: 0000-0002-5513-6517; sosnaalexandru@gmail.com

[3] PhD in Legal Science, Associate Professor, Department of Constitutional Law and Specialized Disciplines, Educational and Scientific Institute of Law and Humanities, National University of Water and Environmental Engineering (NUWEE), Rivne, Ukraine. ORCID: 0009-0004-7049-0233; zrazhevskyyolog@gmail.com

[4] Doctor of Law, Professor, Associate Professor, Department of Counter Intelligence, National Academy of the Security Service of Ukraine, Kyiv, Ukraine. ORCID: 0009-0000-9129-6086; rusnak9894@gmail.com

[5] Doctor of Law, Professor, Associate Professor, Special Department, the Security Service of Ukraine National Academy, Kyiv, Ukraine. ORCID: 0009-0005-4787-2898; trepak.viktor@gmail.com

Abstract: The growing practical use of OSINT in criminal proceedings, together with fragmented regulation and uneven evidentiary treatment in Ukraine and the EU, called for a clearer legal analysis. This study examined under which conditions OSINT-derived material may be used in criminal proceedings and which legal requirements govern its collection, authenticity, documentation, and judicial assessment. The method combined doctrinal analysis of legislation and case law from Ukraine and EU legal materials, with the United Kingdom and the United States used as comparative reference points because their courts and legal instruments more expressly addressed digital evidence and publicly available online material. The analysis showed that European approaches relied on clearer rules on legality, proportionality, authenticity, and documentation, whereas Ukrainian law treated OSINT mainly through general rules on electronic evidence. On that basis, the article formulated a legal test centered on lawful collection, source identification, preservation of integrity, procedural recording, and judicial review. The novelty of the study lies in restating OSINT issues in conventional evidentiary terms and clarifying where Ukrainian law converges with, and differs from, European approaches. Further research should test these criteria in actual criminal cases.

Keywords: Rule of Law, Criminal Justice, Governance, Corruption, Organized Crime, Human Rights, Legal System

1. Introduction

The increasing use of open-source intelligence (OSINT) in criminal proceedings required clearer legal rules on admissibility, authenticity, and preservation of digital material. In the EU, relevant regulation remained dispersed across data protection, criminal procedure, and security law, so courts often assessed OSINT through general evidentiary principles rather than through a single dedicated procedure[6]. In Ukraine, electronic evidence was governed by the Criminal Procedure Code and related legislation, but OSINT-specific procedural requirements were not stated with sufficient precision[7]. This created uncertainty as to how publicly available online material should be collected, recorded, verified, and assessed in criminal cases[8]. The central legal problem therefore concerned not the technical usefulness of OSINT, but the legal conditions under which such material could be accepted and relied on as evidence in Ukraine and in the broader European legal context[9].

The development of OSINT within criminal proceedings in EU Member States reflects the broader digitalization of evidentiary administration, including the use of open data sources, cybersecurity mechanisms, and inter-agency information exchange. European analytical reports indicate that more than 60% of forensic

[6] MELNYK, D. S.; PARFYLO, O. A.; BUTENKO, O. V.; TYKHONOVA, O. V.; ZAROSYLO, V. O. "Practice of the member states of the european union in the field of anti-corruption regulation", Journal of Financial Crime, v. 29, n. 3, 2022, pp. 853-863. https://doi.org/10.1108/JFC-03-2021-0050

[7] HUBANOVA, T.; SHCHOKIN, R.; HUBANOV, O.; ANTONOV, V.; SLOBODIANIUK, P.; PODOLYAKA, S. "Information technologies in improving crime prevention mechanisms in the border regions of southern Ukraine", Journal of Information Technology Management, v. 13, 2021, pp. 75-90. Available at: https://scispace.com/pdf/information-technologies-in-improving-crime-prevention-5eh5g6z2hh.pdf (accessed on 18 October 2025).

[8] KORTUKOVA, T.; KOLOSOVSKYI, Y.; KOROLCHUK, O. L.; SHCHOKIN, R.; VOLKOV, A. S. "Peculiarities of the legal regulation of temporary protection in the european union in the context of the aggressive war of the russian federation against ukraine", International Journal for the Semiotics of Law, v. 36, n. 2, 2023, pp. 667-678. https://doi.org/10.1007/s11196-022-09945-y

[9] ARTEMOV, V.; ISHCHENKO, Y.; RUSNAK, A.; TREPAK, V.; DENYSENKO, M. "The role of American intelligence in shaping foreign policy strategies", Edelweiss Applied Science and Technology, v. 8, n. 5, 2024, pp. 1385–1399. https://doi.org/10.55214/25768484.v8i5.1842

units employ OSINT elements in the investigation of cybercrime, financial offences, and corruption, while only approximately 27% of jurisdictions have formally regulated procedures governing digital verification and evidentiary authentication[10]. At the same time, the expansion of investigative and analytical functions of security agencies has increased the role of OSINT in preventive risk assessment and in enhancing the transparency of investigative processes[11]. These developments substantiate the need for clearer and more unified legal standards governing the incorporation of OSINT-derived materials into criminal proceedings, with the aim of strengthening evidentiary reliability and ensuring regulatory coherence within the European legal framework.

The aim of the study is to identify, through doctrinal and comparative legal analysis, the legal conditions under which OSINT-derived materials may be used in criminal proceedings in Ukraine and the European Union. The objective is to clarify rules on lawful collection, authenticity, preservation, procedural recording, and judicial assessment in order to state more clearly when such material may be admitted and how existing Ukrainian regulation compares with European approaches.

Research objectives: (1) To identify the legal requirements applied to OSINT-derived materials in selected comparative jurisdictions (EU, UK, USA) through analysis of legislation and case law. (2) To determine how Ukrainian criminal procedure and related legislation regulate the collection, recording, and use of OSINT-derived materials. (3) To compare the Ukrainian and European approaches with regard to lawful collection, authenticity, preservation of integrity, and judicial assessment. (4) To identify the main points at which OSINT-derived material may lose evidentiary value because of defects in collection, documentation, or verification. (5) To formulate a concise legal test for the admissibility of OSINT-derived material in criminal proceedings.

The academic novelty of the study lies in the legal restatement of OSINT within the ordinary law of evidence in criminal proceedings. On the basis of comparative analysis, the article clarified the main legal requirements for the use of OSINT-derived material: lawful collection, identifiable source, preservation of integrity, proper procedural recording, and judicial review. It also showed more precisely where Ukrainian regulation approached European standards and where important differences remained. The research hypothesis posited that a clearer statement of the legal requirements governing OSINT-derived material would improve analysis of admissibility, clarify requirements of authenticity and documentation, and assist comparison between the criminal justice systems of Ukraine and the European Union.

2. Literature review

The review of academic sources clarified how current scholarship connected digital investigative practice with established rules of evidence and procedural safeguards. It also showed that much of the literature described operational uses of OSINT more readily than it explained the legal conditions of admissibility. This made it necessary to restate the debate in conventional legal terms: legality of obtaining the material, authenticity of the source, preservation of integrity, and judicial assessment of evidentiary value.

[10] KOPOTUN, I.; NIKITIN, A.; DOMBROVAN, N.; TULINOV, V.; KYSLENKO, D. "Expanding the potential of the preventive and law enforcement function of the security police in combating cybercrime in ukraine and the EU", TEM Journal, v. 9, n. 2, 2020, pp. 460–468. https://doi.org/10.18421/tem92-06

[11] SHCHOKIN, R.; OLIINYK, V.; BONDARENKO, O.; KYSLENKO, D.; KOLOS, O.; TYMOSHENKO, Y. "Sport management in the context of criminal liability for corruption", Retos, v. 48, 2023, pp. 708–719. https://doi.org/10.47197/retos.v48.96768

Within the broader debate on the admissibility of OSINT in criminal proceedings, Van Puyvelde and Tabárez Rienzi[12] conceptualized OSINT as an evolutionary extension of forensic intelligence rather than a distinct evidentiary category. Their analysis demonstrated institutional continuity with traditional evidence-gathering practices, while simultaneously highlighting persistent legal concerns regarding data over-collection, verification reliability, and procedural legitimacy. This position implicitly supported the view that OSINT must be assessed through established evidentiary standards rather than technological innovation alone.

Building on this doctrinal trajectory, Lazarov et al.[13] shifted attention from conceptual definition to regulatory differentiation. Through a comparative assessment of 140 OSINT platforms, they demonstrated the functional heterogeneity of tools and the absence of a unified legal regime governing their use. Importantly, their findings underscored the constraining role of the GDPR and the Budapest Convention, thereby reinforcing the argument that admissibility depends not on analytical capability but on compliance with data protection and jurisdictional safeguards. A different emphasis appeared in the work of Garg et al.[14], who examined OSINT within cybersecurity architectures. Although their review acknowledged OSINT's operational utility in threat detection, it also exposed structural legal vulnerabilities, including the absence of standardized validation procedures and insufficient procedural transparency. This duality illustrated the central tension between technological efficiency and evidentiary reliability, confirming the necessity of translating technical practices into legally verifiable authentication standards. Similarly, Rahman[15] addressed OSINT within cyber-forensic workflows, demonstrating its effectiveness in identifying threat patterns through open-source analysis. Yet the study simultaneously documented risks of redundancy, misinterpretation, and normative ambiguity. These observations reinforced the proposition that effectiveness in detection does not automatically equate to procedural admissibility, thereby strengthening the case for formal evidentiary tests.

From a forensic-network perspective, Breuer[16] reconstructed organized crime structures using open business registers. While confirming the analytical relevance of OSINT-derived networks, the study identified methodological constraints concerning representativeness and node identification. In legal terms, these limitations translate into potential challenges regarding evidentiary sufficiency and judicial assessment of reliability. Turning to institutional practice, Aji et al.[17] validated an OSINT platform for forensic profiling and implemented multi-source identification algorithms. Although the study demonstrated operational feasibility, it

[12] VAN PUYVELDE, D.; TABÁREZ RIENZI, F. "The rise of open-source intelligence", European Journal of International Security, 2025, pp. 1–15. https://doi.org/10.1017/eis.2024.61

[13] LAZAROV, W.; MORAVEC, V.; LOUTOCKÝ, P.; VOSTOUPAL, J.; MARTINASEK, Z. "Comparative analysis of OSINT tools, techniques, and legal aspects", 2025. https://doi.org/10.2139/ssrn.5579220

[14] GARG, P.; SHRIVAS, N.; KALIA, A.; ROY, R.; SHARMA, S.; AGARWAL, G. "OSINT: A Double-Edged Sword", In 2025 First Global Conference on AI Research and Emerging Developments (G-CARED 2025), 2025, pp. 150–157. https://doi.org/10.63169/GCARED2025.p22

[15] RAHMAN, M. D. "The art of open source intelligence (OSINT): Addressing cybercrime, opportunities, and challenges", 2025. https://doi.org/10.2139/ssrn.5281845

[16] BREUER, N. "Investigating the internal structure of mafias using open-source intelligence" (Doctoral dissertation, University of Oxford, 2025a). Available at: https://ora.ox.ac.uk/objects/uuid:77533443-112f-42d6-baba-599b77c17142 (accessed on 18 October 2025).

[17] AJI, M. P.; ASSIDIQ, M. H.; SUGIYANTO, S.; WIJAYA, E. S.; WICAKSONO, A. P. "Design a profiling tool using OSINT (open source intelligence)", In The 1st brawijaya international conference on chemical engineering (bromine) 2024. AIP Publishing, 2025, art. no. 050013. https://doi.org/10.1063/5.0258515

provided limited clarification of procedural safeguards governing authentication and chain of custody. This gap further illustrates the broader pattern in the literature: technical validation frequently precedes legal formalization.

The empirical legal analysis conducted by Pitman and Walsh[18] brought the discussion closer to procedural doctrine. Their examination of OSINT within criminal investigations revealed structural interaction between open sources and evidentiary materials but identified significant risks, including ethical conflicts and insufficient procedural transparency. Their findings directly support the argument that standardized protocols are indispensable for ensuring judicial admissibility.

In a trial-oriented context, Djamadi et al.[19] assessed the admissibility of OSINT-derived electronic artifacts in human trafficking proceedings. While confirming that courts accepted such materials under existing evidentiary rules, they exposed institutional weaknesses in technical expertise and procedural documentation. These findings emphasize that admissibility often depends on the quality of evidentiary administration rather than on the nature of the source itself.

At the meta-analytical level, Chermak et al.[20] documented increasing methodological variability in OSINT repositories and identified deficits in procedural verification and reliability metrics. Their conclusions substantiate the systemic absence of standardized admissibility criteria across jurisdictions.

Finally, Crawford-Holland et al.[21] critically examined the professionalization of OSINT within criminal justice systems. They highlighted the restrictive character of jurisdiction-centered evidentiary procedures while advocating more pluralistic approaches. However, from a procedural standpoint, decentralization does not eliminate the need for legality, authenticity, and proportionality safeguards.

The literature review showed a wide range of analytical approaches to OSINT, but no stable legal account of when such material should be admitted in criminal proceedings. Across jurisdictions, the main unresolved questions concerned lawful collection, authenticity, reliability, preservation of integrity, and proportionality. For Ukraine and the EU, these gaps made comparative doctrinal clarification necessary, particularly because cross-border use of open-source material raised recurring issues of privacy, proof, and procedural fairness.

3. Methods and materials

3.1. Research design

The research design was structured as a five-stage doctrinal and procedural framework integrating legal analysis, comparative assessment, and normative modelling. It encompassed: (1) doctrinal examination of EU, UK, and US law to extract admissibility, authenticity, and traceability standards; (2) analysis of Ukrainian legislation to determine the procedural scope of OSINT; (3) comparative legal assessment to evaluate normative convergence and procedural compatibility; (4) procedural reconstruction of the evidentiary pathway to identify regulatory gaps;

[18] PITMAN, L.; WALSH, L. "Policy considerations of open-source intelligence: A study of bellingcat's online investigation patterns (2014-2024)", International Journal of Cybersecurity Intelligence Cybercrime, v. 8, n. 2, 2025. https://doi.org/10.52306/2578-3289.1202

[19] DJAMADI, N.; W. BADU, L.; TOWADI, M. "The use of digital evidence in law enforcement efforts in human trafficking cases", Estudiante Law Journal, v. 7, n. 3, 2025. https://doi.org/10.33756/eslaj.v7i3.33365

[20] CHERMAK, S. M.; FREILICH, J. D.; GREENE-COLOZZI, E.; KLEIN, B. R. "Open-Source research in criminology and criminal justice", Annual Review of Criminology, 2025, pp. 141-170. https://doi.org/10.1146/annurev-criminol-022422-013842

[21] CRAWFORD-HOLLAND, S.; SMITH, P. B.; WILLIAMS, A. "Law's capture of human rights focused open-source investigation", London Review of International Law, v. 33, n. 1, 2025, pp. 93–113. https://doi.org/10.1093/lril/lraf007

and (5) normative synthesis establishing a unified admissibility framework grounded in legality, authentication, traceability, and judicial review. This design ensured systematic alignment between doctrinal inquiry, procedural modelling, and the formalization of a coherent legal framework for OSINT integration.

3.2. Methods

The study was conducted as a doctrinal and comparative legal inquiry. The method was defined in concrete terms as follows: (1) Selection of jurisdictions and legal materials. The analysis covered Ukraine and EU legal instruments, with the United Kingdom and the United States used as comparative reference points. These materials were selected because they contained rules on digital evidence, data protection in criminal matters, or reported judicial treatment of publicly available online material. (2) Selection of cases. Cases were included where a court or other legal source addressed at least one of four questions: whether the material had been lawfully obtained, whether the source could be identified, whether the integrity of the digital copy had been preserved, and how the material affected admissibility or evidentiary weight. (3) Comparative categories. The comparison used four fixed categories derived from criminal procedure doctrine: legality of collection, authenticity, procedural recording and preservation, and judicial assessment. These categories were applied throughout Tables 2–4. (4) Doctrinal reading of legal sources. The selected provisions and decisions were examined to identify the applicable legal rule, the procedural problem before the authority, and the legal consequence for admissibility or evidentiary weight. (5) Comparative synthesis. The findings were then compared across jurisdictions in order to determine where Ukrainian law already contained functionally similar safeguards and where further clarification remained necessary.

Each step was tied to identified legal sources and to the same evidentiary questions. The section therefore described what was compared, why the materials were selected, and how the evaluative labels used in the analysis were derived.

3.3. Sample

The sample presented in Table 1 was limited to categories of openly available digital material that regularly appeared in criminal investigations and that could be linked to identifiable legal questions. Material was included where it had practical relevance to criminal proceedings and where legal discussion concerned at least one of the following matters: lawfulness of access, authenticity of source, preservation of integrity, or judicial assessment of evidentiary value. The table therefore did not classify OSINT tools for technical purposes; it grouped common forms of public digital material according to the legal problems they most often raised in evidentiary practice.

Table 1. OSINT categories and their procedural significance in criminal proceedings.

OSINT category	**Type of digital material**	**Main legal issue**	**Illustrative case**
SOCMINT (Social Media Intelligence)/Stegen[22]	Social media posts, metadata, geolocation	Authentication of authorship, timing, and context	France v. Azimov (2022); R v. Rahman (2020)

[22] STEGEN, J. I. "Leveraging social media intelligence (SOCMINT) in the African intelligence context", Journal of Policing, Intelligence and Counter Terrorism, v. 20, n. 2, 2025, pp. 243–257. https://doi.org/10.1080/18335330.2025.2465529

OSINT category	**Type of digital material**	**Main legal issue**	**Illustrative case**
CyberINT (Cyber Infrastructure Intelligence)/Zunino[23]	IP data, DNS records, server information	Attribution of online activity to a person or device	U.S. v. Hutchins (2017)
GeoINT (Geospatial Intelligence)/Novikarany[24]	Satellite imagery, coordinates	Proof of location, presence, or destruction	ICC v. Al-Werfalli (2021); Ukraine v. Russia (2022)
Web Evidence & Forensic Tools/Cantelli-Forti et al.[25]	Archived webpages, screenshots, metadata	Authenticity and preservation of web content	R v. Robson (2019)
Fusion Intelligence/Data Correlation Systems/Dragomir and Morari[26]	Relational data, transaction links	Linking transactions or actors through public data	U.S. v. Cartwright (2021)
FinINT/CorpINT (Financial & Corporate Intelligence)/Hadiq and Mahdi[27]	Corporate registries, financial records	Tracing ownership structures and financial flows	U.S. v. Manafort (2018)
VisualINT (Visual Forensic Intelligence)/Colley and Dylan[28]	Images, videos	Visual identification and geolocation	MH17 JIT (2020)
DarkWeb OSINT (Darknet Intelligence)/Bollikonda and Kiran[29]	Darknet communications, transaction logs	Attribution of darknet communications and transactions	U.S. v. Ulbricht (2015)
Legal & Regulatory OSINT Monitoring/Agalliu and Agalliu[30]	Court decisions, public legal records	Use of public legal records to establish relevant facts	Big Brother Watch v. UK (2021)
Hybrid Graph Intelligence (Integrative OSINT Analytics)/Ayobami[31]	Network diagrams, relational mapping	Proof of relationships between actors	R v. Rahman (2020)
SIGINT-OSINT (Signals Intelligence Integration)/Rangappa et al.[32]	Telecommunication metadata, location data	Verification of movement and device location	U.S. v. Chatrie (2020)

[23] ZUNINO, G. "Digital forensics in corporate simulations: A study of tool efficacy and analysis techniques". (Doctoral dissertation, Politecnico di Torino, 2025). Available at: https://webthesis.biblio.polito.it/35242/ (accessed on 18 October 2025).

[24] NOVIKARANY, R. "Geoint as a driver of national security", International Journal of Scientific Multidisciplinary Research, v. 3, n. 2, 2025, pp. 237–250. https://doi.org/10.55927/ijsmr.v3i2.66

[25] CANTELLI-FORTI, A.; LONGO, G.; LUPIA, F.; RUSSO, E. "WEFT: A consistent and tamper-proof methodology for acquisition of automatically verifiable forensic web evidence", International Journal of Information Security, v. 24, n. 2, 2025. https://doi.org/10.1007/s10207-025-00991-8

[26] DRAGOMIR, A. N.; MORARI, B. A. "The global fight against crime on the dark web. Legal responses and technological innovations", Legea şi Viaţa, v. S, 2025, pp. 83-93. Available at: https://ibn.idsi.md/vizualizare_articol/230518 (accessed on 18 October 2025).

[27] HADIQ, D.; MAHDI, I. "The role of occrp's soft power in framing president joko widodo leadership on corruption", INJECT (Interdisciplinary Journal of Communication), v. 10, n. 1, 2025, pp. 385–406. https://doi.org/10.18326/inject.v10i1.4395

[28] COLLEY, T.; DYLAN, H. "The war on open-source intelligence", The Washington Quarterly, v. 48, n. 3, 2025, pp. 147–162. https://doi.org/10.1080/0163660x.2025.2554477

[29] BOLLIKONDA, V. B.; KIRAN, K. V. D. "Unveiling the hidden: Exploring challenges in dark web investigation using measurement sensors", Journal of Cybersecurity and Information Management, v. 15, n. 1, 2025. https://doi.org/10.54216/jcim.150113

[30] AGALLIU, P.; AGALLIU, T. "Proposing a human-rights-based approach in open-source intelligence", In Lecture notes in networks and systems. Cham: Springer Nature Switzerland, 2025, pp. 48–54. https://doi.org/10.1007/978-3-031-95200-5_6

[31] AYOBAMI, U. "Automated metadata extraction and correlation techniques for digital evidence analysis in cybercrime investigations", International Journal of Research Publication and Reviews, v. 6, n. 6, 2025, pp. 101–124. https://doi.org/10.55248/gengpi.6.0625.2177

[32] RANGAPPA, P.; MUSCAT, A.; SANCHEZ LARA, A.; MOTLICEK, P.; ANTONOPOULOU, M.; FOURFOURIS, I.; ... KOSTKA, K. "Detecting criminal networks via non-content communication data analysis techniques from the TRACY project", In Lecture notes of the institute for computer sciences, social informatics and telecommunications engineering. Cham: Springer Nature Switzerland, 2025, pp. 340–353. https://doi.org/10.1007/978-3-031-89363-6_20

OSINT category	Type of digital material	Main legal issue	Illustrative case
IMINT-OSINT (Imagery Intelligence)/Yazici[33]	High-resolution aerial or satellite images	Spatial identification of objects and events	ICC v. Al-Werfalli (2021)
HUMINT-OSINT (Human Intelligence Correlation)/Mulya et al.[34]	Public biographical and identity data	Confirmation of identity or affiliation	U.S. v. Holmes (2021)
OSINT-AI (Artificial Intelligence-Driven OSINT)/Hawa et al.[35]	Automated analytical outputs, pattern detection	Whether automated output requires independent verification	Europol AI Taskforce Report (2023)
OSINT-Blockchain/CryptoINT/Suh and Kim[36]	Cryptocurrency transactions, wallet identifiers	Tracing digital financial flows	U.S. v. Sterlingov (2022)
OSINT-Threat Intelligence (ThreatINT)/Santos et al.[37]	Indicators of compromise, digital signatures	Attribution of cyber incidents	State v. Davis (2020)

Source: created by the authors.

3.4. Instruments

The study relied on standard legal research instruments. The main tool was doctrinal interpretation of criminal procedure legislation, data protection rules, and related judicial decisions governing electronic evidence. Comparative legal analysis was then used to examine how selected EU materials and Ukrainian law addressed four recurring questions: lawful collection, authenticity of source, procedural recording and preservation, and judicial assessment. Case-law analysis served to identify how courts treated these questions in practice and what legal consequences followed for admissibility or evidentiary weight.

4. Results

The comparative legal analysis presented in Table 2 formed the first part of the study. It examined legal instruments and decisions from selected European and comparative jurisdictions in order to identify the legal conditions under which publicly available online material may be used in criminal proceedings. The jurisdictions were selected because they offered clearer legal discussion of digital evidence, authenticity, privacy, and documentation than could be found in a single Ukrainian source base. The analysis therefore focused on concrete legal requirements rather than on technical models of OSINT use.

[33] YAZICI, T. "Standardizing space technologies as admissible evidence: Legal and ethical frameworks for U.S. courts and the international criminal court", University of Miami International and Comparative Law Review, v. 32, n. 2, 2025, p. 180. Available at: https://repository.law.miami.edu/umiclr/vol32/iss2/4/ (accessed on 18 October 2025).

[34] MULYA, A.; PURWANTO, S. A.; DAMAYANTI, A.; POLIMPUNG, H. Y.; PRAMADI, Y. R.; PUTRO, P. A. W. "The security intelligence gathering debate between human intelligence (humint) versus technological intelligence (techint)", Greenation International Journal of Law and Social Sciences, v. 3, n. 2, 2025, pp. 572–588. https://doi.org/10.38035/gijlss.v3i2.497

[35] HAWA, M. R.; OWDA, M.; OWDA, A. Y. "Enhancing digital investigation: The role of generative AI (ChatGPT) in evidence identification and analysis in digital forensics", In 2025 12th International Conference on Information Technology (ICIT). 2025, pp. 19-26. https://doi.org/10.1109/ICIT64950.2025.11049120

[36] SUH, B. W.; KIM, W.-W. "Leveraging open source intelligence (OSINT) for cryptocurrency crime investigation using tools and techniques", In 2025 9th international conference on cryptography, security and privacy (CSP). 2025, pp. 12–16. https://doi.org/10.1109/CSP66295.2025.00010

[37] SANTOS, P.; ABREU, R.; REIS, M. J. C. S., SERÔDIO, C.; BRANCO, F. "A systematic review of cyber threat intelligence: The effectiveness of technologies, strategies, and collaborations in combating modern threats", Sensors, v. 25, n. 14, 2025, p. 4272. https://doi.org/10.3390/s25144272

Table 2. Legal analysis of regulatory provisions for the use of OSINT technologies in criminal proceedings in developed jurisdictions.

Legal instrument	Core procedural requirements	Scope of OSINT use	Illustrative case
Directive (EU) 2016/680	Lawfulness, purpose limitation, proportionality, traceability of data processing in criminal matters	Use of publicly available data for investigation and prosecution, subject to accountability safeguards	France v. Azimov (2022)
Regulation (EU) 2016/679 (GDPR)	Legal basis for processing, data minimization, integrity and confidentiality, protection of special categories of data	Processing of open personal data where necessary for legal claims or security purposes	U.S. v. Hutchins (2017–2019)
Data Protection Act 2018 (UK), Part 3	Necessity, proportionality, documentation of source, law enforcement processing standards	Use of open digital materials by competent authorities	R v. Rahman (2020); R v. Robson (2019)
Budapest Convention on Cybercrime	Preservation of computer data, access to stored data, cross-border cooperation	Collection and preservation of digital traces, including from open sources	U.S. v. Ulbricht (2015)
European Convention on Human Rights (Arts. 6, 8)	Fair trial guarantees, privacy protection, proportionality review of surveillance measures	Judicial assessment of admissibility and balance between security and privacy	Big Brother Watch v. UK (2021)
Europol Regulation (EU) 2016/794	Mandate to collect and analyse information, documented processing chain, inter-agency cooperation	Analytical use of open-source data in cross-border investigations	Europol Cybercrime Report (2022)
U.S. Federal Rules of Evidence + Fourth Amendment jurisprudence	Authentication (Rule 901), chain of custody, absence of reasonable expectation of privacy	Admission of publicly obtained digital materials without warrant, subject to evidentiary verification	U.S. v. Sterlingov (2022); U.S. v. Hutchins (2017–2019)

Source: created by the authors.

The legal analysis presented in Table 2 showed that open-source material was not treated as a separate category of proof, but was usually assessed through ordinary rules on legality, privacy, authenticity, documentation, and evidentiary reliability. In the European legal materials, lawful processing and proportionality remained central. In the United Kingdom, emphasis was placed on source identification, integrity, and documented handling. In the United States, courts focused on authentication and on whether publicly accessible material attracted a reasonable expectation of privacy. These findings provided the comparative baseline for examining Ukrainian legislation and judicial practice in Table 3.

Table 3. Regulatory framework for the use of OSINT-derived materials in criminal proceedings in Ukraine.

Legal act	Core procedural provisions	Procedural scope of application	Illustrative case
Criminal Procedure Code of Ukraine (2012, as amended)	Definition of electronic evidence (Arts. 84, 99, 100); procedure for collection (Art. 93);	Admission, collection, and examination of digital materials obtained from open	Case No. 127/1531/20 (VAKS, 2022)

Legal act	Core procedural provisions	Procedural scope of application	Illustrative case
	involvement of experts (Art. 242)	sources	
Law of Ukraine "On Information"	Principles of openness and accessibility of information; use of publicly available data	Use of open-source information to establish publicly verifiable facts	Case No. 640/10523/19 (KAS, 2021)
Law "On Electronic Documents and Electronic Document Management"	Legal validity, identification, authenticity of electronic documents	Authentication and evidentiary recognition of digital files and screenshots	Case No. 761/12456/20 (2021)
Law "On Personal Data Protection"	Legal grounds for processing personal data; proportionality and liability	Limits on processing open personal data in investigative activities	Case No. 420/2143/21 (2022)
MIA Order No. 1050 (Pre-Trial Investigation Instruction)	Procedural use of information from open sources in investigative practice	Inclusion of open-source materials in case files	Case No. 757/34561/21-k (2023)
SBU Order No. 123 (Information and Analytical Activity)	Collection and analysis of open information within criminal proceedings	Use of open-source intelligence in security-related investigations	Case No. 991/4153/22 (2023)
Law "On National Security of Ukraine"	Information and analytical support for national security based on open data	Analytical use of open information in evidentiary activities of security bodies	Case No. 640/3217/22 (2023)

Source: created by the authors.

The legal analysis presented in Table 3 showed that Ukrainian regulation of OSINT-derived material remained dispersed across several legislative and subordinate acts. No single provision stated a separate procedure for OSINT. Instead, admissibility depended on general rules governing electronic evidence, information law, personal data protection, and investigative procedure. Judicial practice indicated that open-source material could be used in criminal proceedings, but the requirements for recording the source, preserving integrity, and explaining authenticity were not stated with the same clarity as in the comparative materials. This made direct comparison with European approaches necessary.

Table 4. Comparative assessment of procedural regulation of osint in developed jurisdictions and Ukraine.

Comparison criterion	Developed jurisdictions (EU, UK, USA)	Ukraine	Comparative assessment
Regulatory framework	Comprehensive combination of data protection law, criminal procedure rules, and judicial standards	Regulation dispersed across CPC, sectoral laws, and departmental acts	More explicit rules vs. fragmented regulation
Procedural admissibility	Explicit reliance on legality, proportionality, authentication, and documentation standards	Admission under general rules on electronic evidence	Express criteria vs. use of general evidence rules
Personal data protection	Strong emphasis on necessity, minimization, and proportionality	General data protection rules without specific OSINT procedure	Shared safeguards, different procedural detail

Comparison criterion	Developed jurisdictions (EU, UK, USA)	Ukraine	Comparative assessment
Traceability and authenticity	Formalized chain of custody and documentation of source	Authenticity mainly ensured through expert examination	Documented handling vs. case-by-case proof
Institutional regulation	Law enforcement mandates expressly include analytical use of open data	Use of open data permitted through general investigative mandates	Express mandate vs. indirect authorization
Judicial practice	Established case law confirming admissibility of open-source materials	Emerging practice without consistent doctrinal qualification	Stable case law vs. developing practice
Regulatory coherence	Coordination between procedural, data protection, and security law	Limited coordination between branches of law	Higher coordination vs. normative dispersion
Procedural compatibility	Standardized requirements for collection, storage, and evaluation	No unified procedural protocol for OSINT handling	Clearer handling rules vs. partial regulation
Evidentiary status	OSINT accepted as digital evidence if verification standards are met	Recognized as electronic evidence after evidentiary assessment	Comparable function, different legal clarity

Source: created by the authors.

The comparative assessment presented in Table 4 showed that the main difference between the examined jurisdictions concerned the level of legal specificity rather than the existence of wholly different principles. Across the comparison, the same basic legal questions recurred: lawful collection, authenticity, preservation, and judicial assessment. The comparative jurisdictions addressed these matters more expressly, while Ukrainian law usually resolved them through general provisions and case-by-case interpretation. The table therefore showed not absolute incompatibility, but a difference in legal clarity and procedural articulation.

Table 5. Structured procedural model of OSINT Use in criminal proceedings.

Stage	Procedural action	Responsible subject	Legal risk identified	Procedural consequence
1	Opening of criminal proceedings	Investigator	—	Opening of criminal proceedings
2	Collection of public online material	Investigator	Collection without clear legal record	Need to record source and method
3	Capture of open-source material	Investigator/analytical unit	Missing or incomplete metadata	Need to prove authenticity
4	Receipt of captured material	Investigator	Unclear origin or altered copy	Need to verify integrity
5	Storage of collected material	Evidence storage unit	Insufficient record of handling	Weak proof of continuity
6	Review of collected material	Investigator/analyst	Unclear method of assessment	Limited evidentiary value
7	Decision on admissibility	Investigator/prosecutor	Gaps in source, integrity, or record	Need for further verification

Stage	Procedural action	Responsible subject	Legal risk identified	Procedural consequence
8	Attachment to case file	Investigator/prosecutor	Material still insufficiently verified	Conditional use in the record
9	Judicial assessment	Court	Doubt as to reliability or legality	Assessment of admissibility and weight

Source: created by the authors.

Table 5 summarized the points at which OSINT-derived material most often encountered legal difficulty in criminal proceedings. The sequence began with lawful initiation of the investigation and continued through collection, recording, preservation, verification, and court assessment. At each stage, the relevant issue was legal: whether the source could be identified, whether the copy remained intact, whether the record of handling was sufficient, and whether the court could evaluate reliability. Read in this way, the table served as a legal checklist of potential defects affecting admissibility or evidentiary weight rather than as a technical process model.

Table 6. Structured procedural framework for the use of OSINT in criminal proceedings.

Stage	Procedural action	Responsible subject	Safeguard mechanism	Procedural outcome
1	Opening of criminal investigation	Investigator	Formal initiation under CPC	Opening of proceedings
2	Request to collect open-source material	Investigator	Written authorization and record of purpose	Lawful start of collection
3	Capture of public online material	Authorized analytical unit	Record of URL, date, time, and method	Identifiable source
4	Receipt of material with source data	Evidence repository	Preservation of origin and integrity	Traceable digital record
5	Storage and integrity check	Evidence repository	Hash value or equivalent preservation measure	Proof that the copy remained intact
6	Review of relevance and context	Investigator/Analyst	Recorded method of assessment	Context for evidentiary use
7	Request for expert or additional verification	Authorized expert/analytical body	Independent check of authenticity where needed	Further proof of reliability
8	Result of verification	Expert/system report	Written record of findings	Confirmed or contested authenticity
9	Preparation of evidence file	Investigator/Prosecutor	Consolidated procedural record	Material ready for submission
10	Judicial review of admissibility	Court	Review of legality, authenticity, and reliability	Decision on admissibility
11	Identification of defect	Court/Prosecutor	Court or prosecutor notes deficiency	Need for clarification
12	Additional verification	Investigator/Expert	Supplementary proof of source or integrity	Defect cured or confirmed

Stage	Procedural action	Responsible subject	Safeguard mechanism	Procedural outcome
13	Final record of handling	Investigator/Prosecutor	Complete chain-of-custody record	Material ready for final assessment
14	Final judicial assessment	Court	Court evaluates admissibility and weight	Use or exclusion in the evidentiary record

Source: created by the authors.

Table 6 restated the same sequence as a set of minimum legal safeguards for the use of OSINT-derived material in criminal proceedings. Its purpose was not to propose a new technical architecture, but to show in conventional legal terms what a prosecutor or court must be able to establish: lawful collection, identifiable source, recorded method of capture, preservation of integrity, verification where needed, and judicial review before reliance on the material. The table therefore translated dispersed legal requirements into a more readable evidentiary sequence without changing the underlying legal sources.

The study identified differences in the degree of legal clarity with which OSINT-derived materials were regulated in Ukraine and in the examined European materials. In the EU, relevant standards were expressed more clearly through data protection and criminal justice instruments, especially with regard to legality, proportionality, and accountability. In Ukraine, the same issues were addressed mainly through general rules and subordinate acts, which left greater room for inconsistent practice. Tables 5 and 6 therefore restated the findings as a legal checklist of admissibility requirements: lawful collection, source identification, preservation of integrity, procedural recording, and judicial assessment. On that basis, the research hypothesis was confirmed.

The legal implications of the study lay in clarifying the minimum evidentiary conditions under which OSINT-derived material may be relied on in criminal proceedings. The proposed restatement may assist courts, investigators, and prosecutors in distinguishing between questions of admissibility and questions of evidentiary weight. It may also serve as a reference point for legislative clarification and for closer alignment between Ukrainian practice and European standards on digital evidence.

5. Discussion

The discussion assessed whether the literature addressed OSINT in the terms expected by criminal procedure doctrine. The central question was whether prior studies explained when courts may rely on OSINT-derived material and what legal record must accompany it. This made it possible to separate work that primarily described investigative or analytical use from work that more directly addressed admissibility, authenticity, integrity, privacy, and judicial review.

First, Soni and Poonia[38] described AI-assisted OSINT detection in cyber-forensic work, but they did not explain under which legal conditions a court may admit the resulting material or what record must accompany it. The present article addressed that omission by restating the issue through legality, authenticity, preservation, and judicial assessment.

[38] SONI, N.; POONIA, R. "AI-Driven open-source intelligence in digital forensics for cybercrime investigation", Journal of Collective Sciences and Sustainability, v. 1, n. 1, 2025, pp. 1–8. https://doi.org/10.64189/css.25405

Similarly, Meng[39] showed how AI-based governance tools could organize online material, but the study did not state how such outputs satisfied ordinary evidentiary requirements. This article moved the issue into a legal register by asking whether the source could be identified, whether the digital copy remained intact, and how a court should assess the resulting material.

Breuer[40] showed the practical value of OSINT registries for reconstructing illicit structures, but the legal problem of admissibility remained secondary. The present study treated that problem directly by identifying the minimum legal conditions under which such material may be relied on in criminal proceedings.

Rathod et al.[41] focused on the detection of darknet material and on analytical performance. That work did not show how the collected material should be recorded, verified, and presented so that a court could assess authenticity and evidentiary value. The present study supplied that legal perspective.

From a different perspective, Bennani and El Maysour[42] examined the ethical and political status of OSINT. Their analysis was valuable, but it did not answer the narrower criminal-procedure question of when open-source material becomes usable evidence. This article addressed that question through ordinary legal categories rather than through broad conceptual framing.

Soler et al.[43] showed the usefulness of AI-assisted aggregation and verification techniques, but they did not explain what legal consequences followed if the source could not be identified or if the method of capture was insufficiently recorded. The present study made those consequences explicit.

Zhou et al.[44] emphasized the changing character of OSINT content over time. That point was important for analysis, but in legal terms it raised a more specific problem: whether the party relying on the material could prove what exactly had been captured and preserved. The present study therefore treated volatility as an issue of integrity and proof.

Cohen et al.[45] examined adaptive terrorist networks and highlighted the filtering capacity of AI-assisted OSINT systems. However, they did not analyze the legal threshold at which processed online material became admissible evidence. This article focused on that threshold.

[39] MENG, W. "AI-enhanced OSINT evidence governance: Academic integrity, platform disposition, and national security risk assessment in the case of Shanghai Maritime University's "First-Class Undergraduate Major" Controversy", 2025. https://doi.org/10.2139/ssrn.5560703

[40] BREUER, N. "Testing the reliability of OSINT network data for investigating organised crime infiltration of legal-market businesses", Global Crime, 2025b, pp. 1–25. https://doi.org/10.1080/17440572.2025.2567277

[41] RATHOD, D. M.; PADHYA, M.; NATU, A. M.; CHAUDHARI, N.; VIBHUTE, A. "DarkCatalog: A vision-first, parser-independent framework for forensic harvesting of TOR hidden services", 2025. https://doi.org/10.2139/ssrn.5641694

[42] BENNANI, H.; El MAYSOUR, M. A. "L' "Open source intelligence"a l'ere numerique: Un spectreethico-politique entre pouvoir, preuves et limites judiciaires", Revue droit societe, v. 6, n. 17, 2025, pp. 5–18. Available at: https://journals.sms-institute.com/wp-content/uploads/2025/07/BENNANI-Hniya.pdf (accessed on 18 October 2025).

[43] SOLER, R.; DAWSON, M.; COLINA, M. "Automated target profiling: Leveraging artificial intelligence for open-source intelligence collection", International Conference KNOWLEDGE-BASED ORGANIZATION, v. 31, n. 1, 2025, pp. 184–190. https://doi.org/10.2478/kbo-2025-0023

[44] ZHOU, B.; FANG, B.; WANG, Y. "The application of the MDATA cognitive model in open source intelligence analysis", In Lecture notes in computer science. Singapore: Springer Nature Singapore, 2025, pp. 148–180. https://doi.org/10.1007/978-981-96-3528-3_6

[45] COHEN, D.; ELALOUF, A.; CITRINOWICZ, D. "Uncovering Salafi jihadist terror activity through advanced technological tools", Journal of Policing, Intelligence and Counter Terrorism, 2025, pp. 1–17. https://doi.org/10.1080/18335330.2025.2478553

Palmieri et al.[46] proposed an agent-based AI architecture for OSINT processing, but their account remained centered on analytical orchestration rather than on evidentiary law. The present study instead asked how such outputs should be documented and verified before a court could rely on them.

Finally, Tınas and Tuncal[47] discussed OSINT mainly in strategic and political terms. By contrast, this article treated OSINT as a problem of criminal evidence and concentrated on legality, authenticity, preservation, and judicial assessment.

The discussion showed that the existing literature still dealt more readily with the usefulness of OSINT than with the legal conditions of its use in criminal proceedings. The main unresolved questions concerned lawful collection, identification of source, preservation of integrity, privacy limits, and the distinction between admissibility and evidentiary weight. The present study addressed these questions by restating dispersed materials in a form more closely aligned with criminal procedure doctrine.

6. Limitation

The proposed legal test was developed at the doctrinal level and was not verified through direct analysis of a larger body of case files or through observation of courtroom practice. The study therefore could not determine how consistently the identified requirements were applied in day-to-day proceedings. Its limits stemmed from the available body of reported legal materials and from differences in how jurisdictions recorded and published decisions dealing with OSINT-derived material.

7. Recommendations

Given the doctrinal character of the study, the next step should consist in testing the identified legal requirements against actual criminal case materials. Such work would show how courts and prosecutors distinguished between defects affecting admissibility and defects affecting evidentiary weight. It would also help clarify whether Ukrainian practice required legislative amendment, judicial guidance, or only more consistent procedural recording of online material.

8. Conclusions

The comparative legal assessment identified not different legal principles, but different levels of clarity in how Ukraine and the examined European materials regulated OSINT-derived evidence. Tables 2–4 showed that the recurring legal questions concerned lawful collection, authenticity, preservation of integrity, procedural recording, and judicial assessment.

The analysis of procedural stages in Table 5 identified the points at which OSINT-derived material most readily lost evidentiary force: unclear source, insufficient record of capture, weak preservation of integrity, and inadequate verification. Table 6 therefore restated the same findings as minimum legal safeguards for the use of such material in criminal proceedings.

The study confirmed that OSINT-derived material may be assessed within the ordinary law of evidence if courts and parties can establish lawful collection, identifiable source, preservation of integrity, and sufficient procedural recording. In

[46] PALMIERI, E. A.; GHANEM, M. C.; SOWINSKI-MYDLARZ, V.; DUNSIN, D. "A framework for embedding generative and agentic AI in Open Source Intelligence", Authorea Preprints, 2025. https://doi.org/10.36227/techrxiv.175623135.54287545/v2

[47] TINAS, M.; TUNCAL, D. "OSINT in the techno-political era: From intelligence collection to exerting influence", Security, Law, and Influence in the Age of Techno-Politics, 2025, pp. 69–86. https://doi.org/10.4018/979-8-3373-7406-2.ch003

this respect, the article provided a doctrinal basis for closer alignment between Ukrainian practice and European approaches without removing the differences that still remained. Practically, the findings may assist legal qualification of OSINT-derived material at the pre-trial stage and may support clearer judicial reasoning on admissibility and evidentiary weight in digitally mediated investigations.

9. References

Agalliu, P.; Agalliu, T. "Proposing a human-rights-based approach in open-source intelligence", In Lecture notes in networks and systems. Cham: Springer Nature Switzerland, 2025, pp. 48–54. https://doi.org/10.1007/978-3-031-95200-5_6

Aji, M. P.; Assidiq, M. H.; Sugiyanto, S.; Wijaya, E. S.; Wicaksono, A. P. "Design a profiling tool using OSINT (open source intelligence)", In The 1st brawijaya international conference on chemical engineering (bromine) 2024. AIP Publishing, 2025, art. no. 050013. https://doi.org/10.1063/5.0258515

Artemov, V.; Ishchenko, Y.; Rusnak, A.; Trepak, V.; Denysenko, M. "The role of American intelligence in shaping foreign policy strategies", Edelweiss Applied Science and Technology, v. 8, n. 5, 2024, pp. 1385–1399. https://doi.org/10.55214/25768484.v8i5.1842

Ayobami, U. "Automated metadata extraction and correlation techniques for digital evidence analysis in cybercrime investigations", International Journal of Research Publication and Reviews, v. 6, n. 6, 2025, pp. 101–124. https://doi.org/10.55248/gengpi.6.0625.2177

Bennani, H.; El Maysour, M. A. "L' "Open source intelligence"a l'ere numerique: Un spectreethico-politique entre pouvoir, preuves et limites judiciaires", Revue droit societe, v. 6, n. 17, 2025, pp. 5–18. Available at: https://journals.sms-institute.com/wp-content/uploads/2025/07/BENNANI-Hniya.pdf (accessed on 18 October 2025).

Bollikonda, V. B.; Kiran, K. V. D. "Unveiling the hidden: Exploring challenges in dark web investigation using measurement sensors", Journal of Cybersecurity and Information Management, v. 15, n. 1, 2025. https://doi.org/10.54216/jcim.150113

Breuer, N. "Investigating the internal structure of mafias using open-source intelligence" (Doctoral dissertation, University of Oxford, 2025a). Available at: https://ora.ox.ac.uk/objects/uuid:77533443-112f-42d6-baba-599b77c17142 (accessed on 18 October 2025).

Breuer, N. "Testing the reliability of OSINT network data for investigating organised crime infiltration of legal-market businesses", Global Crime, 2025b, pp. 1–25. https://doi.org/10.1080/17440572.2025.2567277

CANTELLI-Forti, A.; Longo, G.; Lupia, F.; Russo, E. "WEFT: A consistent and tamper-proof methodology for acquisition of automatically verifiable forensic web evidence", International Journal of Information Security, v. 24, n. 2, 2025. https://doi.org/10.1007/s10207-025-00991-8

Chermak, S. M.; Freilich, J. D.; GREENE-Colozzi, E.; Klein, B. R. "Open-Source research in criminology and criminal justice", Annual Review of Criminology, 2025, pp. 141-170. https://doi.org/10.1146/annurev-criminol-022422-013842

Cohen, D.; Elalouf, A.; Citrinowicz, D. "Uncovering Salafi jihadist terror activity through advanced technological tools", Journal of Policing, Intelligence and Counter Terrorism, 2025, pp. 1–17. https://doi.org/10.1080/18335330.2025.2478553

Colley, T.; Dylan, H. "The war on open-source intelligence", The Washington Quarterly, v. 48, n. 3, 2025, pp. 147–162. https://doi.org/10.1080/0163660x.2025.2554477

CRAWFORD-Holland, S.; Smith, P. B.; Williams, A. "Law's capture of human rights focused open-source investigation", London Review of International Law, v. 33, n. 1, 2025, pp. 93–113. https://doi.org/10.1093/lril/lraf007

Djamadi, N.; W. Badu, L.; Towadi, M. "The use of digital evidence in law enforcement efforts in human trafficking cases", Estudiante Law Journal, v. 7, n. 3, 2025. https://doi.org/10.33756/eslaj.v7i3.33365

Dragomir, A. N.; Morari, B. A. "The global fight against crime on the dark web. Legal responses and technological innovations", Legea şi Viaţa, v. S, 2025, pp. 83-93. Available at: https://ibn.idsi.md/vizualizare_articol/230518 (accessed on 18 October 2025).

Garg, P.; Shrivas, N.; Kalia, A.; Roy, R.; Sharma, S.; Agarwal, G. "OSINT: A Double-Edged Sword", In 2025 First Global Conference on AI Research and Emerging Developments (G-CARED 2025), 2025, pp. 150–157. https://doi.org/10.63169/GCARED2025.p22

Hadiq, D.; Mahdi, I. "The role of occrp's soft power in framing president joko widodo leadership on corruption", INJECT (Interdisciplinary Journal of Communication), v. 10, n. 1, 2025, pp. 385–406. https://doi.org/10.18326/inject.v10i1.4395

Hawa, M. R.; Owda, M.; Owda, A. Y. "Enhancing digital investigation: The role of generative AI (ChatGPT) in evidence identification and analysis in digital forensics", In 2025 12th International Conference on Information Technology (ICIT). 2025, pp. 19-26. https://doi.org/10.1109/ICIT64950.2025.11049120

Hubanova, T.; Shchokin, R.; Hubanov, O.; Antonov, V.; Slobodianiuk, P.; Podolyaka, S. "Information technologies in improving crime prevention mechanisms in the border regions of southern Ukraine", Journal of Information Technology Management, v. 13, 2021, pp. 75-90. Available at: https://scispace.com/pdf/information-technologies-in-improving-crime-prevention-5eh5g6z2hh.pdf (accessed on 18 October 2025).

Kopotun, I.; Nikitin, A.; Dombrovan, N.; Tulinov, V.; Kyslenko, D. "Expanding the potential of the preventive and law enforcement function of the security police in combating cybercrime in ukraine and the EU", TEM Journal, v. 9, n. 2, 2020, pp. 460–468. https://doi.org/10.18421/tem92-06

Kortukova, T.; Kolosovskyi, Y.; Korolchuk, O. L.; Shchokin, R.; Volkov, A. S. "Peculiarities of the legal regulation of temporary protection in the european union in the context of the aggressive war of the russian federation against ukraine", International Journal for the Semiotics of Law, v. 36, n. 2, 2023, pp. 667-678. https://doi.org/10.1007/s11196-022-09945-y

Lazarov, W.; Moravec, V.; Loutocký, P.; Vostoupal, J.; Martinasek, Z. "Comparative analysis of OSINT tools, techniques, and legal aspects", 2025. https://doi.org/10.2139/ssrn.5579220

Melnyk, D. S.; Parfylo, O. A.; Butenko, O. V.; Tykhonova, O. V.; Zarosylo, V. O. "Practice of the member states of the european union in the field of anti-corruption regulation", Journal of Financial Crime, v. 29, n. 3, 2022, pp. 853-863. https://doi.org/10.1108/JFC-03-2021-0050

Meng, W. "AI-enhanced OSINT evidence governance: Academic integrity, platform disposition, and national security risk assessment in the case of Shanghai Maritime University's "First-Class Undergraduate Major" Controversy", 2025. https://doi.org/10.2139/ssrn.5560703

Mulya, A.; Purwanto, S. A.; Damayanti, A.; Polimpung, H. Y.; Pramadi, Y. R.; Putro, P. A. W. "The security intelligence gathering debate between human intelligence (humint) versus technological intelligence (techint)", Greenation International Journal of Law and Social Sciences, v. 3, n. 2, 2025, pp. 572–588. https://doi.org/10.38035/gijlss.v3i2.497

Novikarany, R. "Geoint as a driver of national security", International Journal of Scientific Multidisciplinary Research, v. 3, n. 2, 2025, pp. 237–250. https://doi.org/10.55927/ijsmr.v3i2.66

Palmieri, E. A.; Ghanem, M. C.; SOWINSKI-Mydlarz, V.; Dunsin, D. "A framework for embedding generative and agentic AI in Open Source Intelligence", Authorea Preprints, 2025. https://doi.org/10.36227/techrxiv.175623135.54287545/v2

Pitman, L.; Walsh, L. "Policy considerations of open-source intelligence: A study of bellingcat's online investigation patterns (2014-2024)", International Journal of Cybersecurity Intelligence Cybercrime, v. 8, n. 2, 2025. https://doi.org/10.52306/2578-3289.1202

Rahman, M. D. "The art of open source intelligence (OSINT): Addressing cybercrime, opportunities, and challenges", 2025. https://doi.org/10.2139/ssrn.5281845

Rangappa, P.; Muscat, A.; SANCHEZ Lara, A.; Motlicek, P.; Antonopoulou, M.; Fourfouris, I.; ... Kostka, K. "Detecting criminal networks via non-content communication data analysis techniques from the TRACY project", In Lecture notes of the institute for computer sciences, social informatics and telecommunications engineering. Cham: Springer Nature Switzerland, 2025, pp. 340–353. https://doi.org/10.1007/978-3-031-89363-6_20

Rathod, D. M.; Padhya, M.; Natu, A. M.; Chaudhari, N.; Vibhute, A. "DarkCatalog: A vision-first, parser-independent framework for forensic harvesting of TOR hidden services", 2025. https://doi.org/10.2139/ssrn.5641694

Santos, P.; Abreu, R.; Reis, M. J. C. S., Serôdio, C.; Branco, F. "A systematic review of cyber threat intelligence: The effectiveness of technologies, strategies, and collaborations in combating modern threats", Sensors, v. 25, n. 14, 2025, p. 4272. https://doi.org/10.3390/s25144272

Shchokin, R.; Oliinyk, V.; Bondarenko, O.; Kyslenko, D.; Kolos, O.; Tymoshenko, Y. "Sport management in the context of criminal liability for corruption", Retos, v. 48, 2023, pp. 708–719. https://doi.org/10.47197/retos.v48.96768

Soler, R.; Dawson, M.; Colina, M. "Automated target profiling: Leveraging artificial intelligence for open-source intelligence collection", International Conference KNOWLEDGE-BASED ORGANIZATION, v. 31, n. 1, 2025, pp. 184–190. https://doi.org/10.2478/kbo-2025-0023

Soni, N.; Poonia, R. "AI-Driven open-source intelligence in digital forensics for cybercrime investigation", Journal of Collective Sciences and Sustainability, v. 1, n. 1, 2025, pp. 1–8. https://doi.org/10.64189/css.25405

Stegen, J. I. "Leveraging social media intelligence (SOCMINT) in the African intelligence context", Journal of Policing, Intelligence and Counter Terrorism, v. 20, n. 2, 2025, pp. 243–257. https://doi.org/10.1080/18335330.2025.2465529

Suh, B. W.; Kim, W.-W. "Leveraging open source intelligence (OSINT) for cryptocurrency crime investigation using tools and techniques", In 2025 9th international conference on cryptography, security and privacy (CSP). 2025, pp. 12–16. https://doi.org/10.1109/CSP66295.2025.00010

Tınas, M.; Tuncal, D. "OSINT in the techno-political era: From intelligence collection to exerting influence", Security, Law, and Influence in the Age of Techno-Politics, 2025, pp. 69–86. https://doi.org/10.4018/979-8-3373-7406-2.ch003

VAN PUYVELDE, D.; TABÁREZ Rienzi, F. "The rise of open-source intelligence", European Journal of International Security, 2025, pp. 1–15. https://doi.org/10.1017/eis.2024.61

Yazici, T. "Standardizing space technologies as admissible evidence: Legal and ethical frameworks for U.S. courts and the international criminal court", University of Miami International and Comparative Law Review, v. 32, n. 2, 2025, p. 180. Available at: https://repository.law.miami.edu/umiclr/vol32/iss2/4/ (accessed on 18 October 2025).

Zhou, B.; Fang, B.; Wang, Y. "The application of the MDATA cognitive model in open source intelligence analysis", In Lecture notes in computer science. Singapore: Springer Nature Singapore, 2025, pp. 148–180. https://doi.org/10.1007/978-981-96-3528-3_6

Zunino, G. "Digital forensics in corporate simulations: A study of tool efficacy and analysis techniques". (Doctoral dissertation, Politecnico di Torino, 2025). Available at: https://webthesis.biblio.polito.it/35242/ (accessed on 18 October 2025).