VFAST Transactions on Software Engineering
https://vfast.org/journals/index.php/VTSE@ 2026, ISSN(e): 2309-3978, ISSN(p): 2411-6246
Volume 14, Number 2, April-June 2026 pp:497-514

Osint Risk Assessment Models in Digital Intelligence Using Data Mining Methods and Automated Classification of Ethical and Legal Scenarios

Volodymyr Artemov [1*], **Vladyslav Kochyn** [2], **Maksym Pendiura** [3], **Andrii Levchenko** [4], **Olena Bondar** [5]

[1]Yevhenii Bereznyak Military Academy, Kyiv, Ukraine; [2]Educational and Research Institute No. 4 (Training of Specialists in Information and Analytical Support and Cybersecurity of the National Police of Ukraine, Kharkiv National University of Internal Affairs, Kharkiv, Ukraine); [3]Department of Theory, History and Philosophy of Law, Educational and Scientific Institute of Law and Psychology of the National Academy of Internal Affairs, Kyiv, Ukraine; [4]Department of Combat Reconnaissance and Special Operations Forces Units Combat Management, Faculty of Training in Combat Reconnaissance and Special Operations Forces, Odesa Military Academy, Odesa, Ukraine; [5]Department of Information Technologies, Higher Mathematics and Physics, Faculty of Economics, Bila Tserkva National Agrarian University, Bila Tserkva, Ukraine

Keywords:
Open-Source Intelligence (OSINT), Digital Intelligence, Risk Modelling, Automated Classification, Data Management, Solution Integration, Legal–Ethical Compliance, Hybrid Decision-Support Systems

Journal Info:
Submitted:
May 07, 2026
Accepted:
June 27, 2026
Published:
June 30, 2026

Abstract The increased use of open source intelligence (OSINT) in automated digital intelligence systems urges legal and ethical risks that remain unnoted in most analytical models due to their focus on performance. This makes automated OSINT pipelines vulnerable to regulatory and institutional failures. The aim of the study is to develop and validate a technically operational and legally sound OSINT risk assessment model. The model is aimed at use within automated digital intelligence processes. The study uses a hybrid methodology. It combines scenario engineering, structured extraction of legal and ethical features, and classification using supervised machine learning (ML). Legal thinking is also used. A synthetic OSINT dataset was generated for controlled experimental testing. It consists of 124 analytically constructed scenarios, 27 structured features, and three legal and ethical classes (A/B/C). The result of the research is a developed hybrid OSINT risk assessment model. The model is able to distinguish between legally permissible, conditionally permissible, and prohibited scenarios. The obtained results demonstrate that legal and ethical risks can be formalized and quantified. Unlike earlier studies, in which normative assessment was separated from technical processing, in this study legal and ethical logic is directly embedded in OSINT risk classification mechanisms. Further research can focus on the development of jurisdiction-adaptive risk assessment modules. Real-time analysis of OSINT streams is promising. Special attention should be paid to scalable hybrid architectures for managing human-machine interaction.

***Correspondence author email address:** volodymyrartemov1@gmail.com
DOI: 10.21015/vtse.v14i2.2427

1 Introduction

OSINT has become a key analytical component of modern digital intelligence systems. Such systems are actively used by government agencies, private organizations, and hybrid institutional entities [1]. The exponential growth of publicly available digital informa-

tion has significantly changed the capabilities of OSINT. This has been further facilitated by advances in data analysis, automated classification, and ML. As a result, the operational applicability of OSINT has significantly expanded in the areas of cybersecurity, government, critical infrastructure protection, and corporate intelligence [2]. These technological developments provide scalable monitoring, pattern recognition, and predictive analysis based on open digital sources.

At the same time, the increasing automation of OSINT processes is accompanied by increasing legal, ethical, and regulatory risks. Automated aggregation and large-scale analysis of open data often involve cross-border information flows. Such processes may involve indirect processing of personal data [3, 4]. They are also characterized by opaque inference mechanisms and cumulative privacy impacts. Despite the widespread perception of the internal legitimacy of OSINT due to the public availability of sources, this assumption does not meet modern legal standards. In particular, it ignores the requirements of proportionality, purpose limitation, accountability, and the protection of fundamental rights [5]. As a result, OSINT analytical products can create legal uncertainty for institutions if compliance issues are assessed only after the results of the analysis are available.

Most existing digital intelligence systems are primarily focused on operational efficiency and the automation of analytical processes. Legal and ethical aspects are usually considered as an external or reactive control element. This approach often relies on ex post facto audits or discretionary human assessments [6]. Although current research increasingly emphasizes the importance of ethical governance and compliance in OSINT operations, these requirements are rarely transformed into formal models. In particular, they are rarely presented in the form of machine-interpretable structures capable of functioning in automated analytical pipelines. As a result, legal and ethical risks remain insufficiently operationalized and poorly integrated into the system architecture [7, 8].

This study aims to address this gap. OSINT risk is conceptualized as an internal characteristic of automated digital intelligence processes, rather than an external regulatory constraint. The main assumption is that legal and ethical risks can be formalized and quantified. They can also be classified based on structured metrics derived from typical OSINT scenarios. Such metrics can be directly integrated into data-driven workflows. From a technical perspective, this requires developing scenario models, extracting legally and ethically relevant features, applying supervised ML, and parallel implementation of legal reasoning rules [9].

The aim of the research is to develop and experimentally validate a hybrid risk assessment model for OSINT. The proposed model combines data mining methods with automated classification of legal and ethical scenarios. The aim was achieved through the fulfilment of the following research objectives:

- identify and formalize the key legal, ethical, and technical risk factors inherent in OSINT-based digital intelligence systems [10];
- develop a synthetic scenario-based OSINT dataset suitable for controlled experimental testing that includes structured features and predefined legal and ethical classes (A/B/C);
- apply automated classification methods to distinguish legally permissible, conditionally permissible, and prohibited OSINT scenarios;
- integrate rule-based legal reasoning with computational risk assessment to generate explainable hybrid outcomes [11];
- assess the technical robustness, replicability, and decision support potential of the proposed model.

2 Literature review

OSINT has become widely used in the field of digital intelligence. This is due to its growing importance for intelligence services, the private sector and government agencies. The rapid development of digital technologies has intensified academic discussions on the reliability of OSINT methods, as well as their legal and ethical admissibility. In recent studies, OSINT is increasingly viewed not as an auxiliary source of information, but as a method of structured analysis that can influence the results of investigations, cybersecurity strategies, and institutional management decisions.

Despite the increasing number of publications, the existing literature demonstrates significant conceptual and methodological gaps. They relate primarily to the sys-

tematic assessment of risks in automated OSINT environments. One of the key problems remains the lack of empirical data suitable for analysing the legal and ethical risks during the automated collection and processing of open information. This is especially characteristic of cases of integration of OSINT into data mining pipelines. Although these risks are recognized by most researchers, they are rarely transformed into applied analytical models suitable for operational use.

A significant limitation identified in the literature is the difficulty of transforming unstructured digital artifacts into legally relevant and analytically reliable data. Revak et al. [12] analyse the social and legal aspects of electronic documents in the context of financial and legal security. The authors emphasize the importance of authentication, metadata reliability, and interpretability of digital materials. Their findings confirm that properly structured digital artifacts can support risk assessment. At the same time, the study does not cover the risks of OSINT automation and does not propose methodologies for proactive classification of legal risks during data collection.

In the field of management and economics, Zoidze et al. [13] consider business analytics and open information systems as factors of organizational resilience. Their analysis demonstrates the benefits of integrating external data into decision-making processes. However, regulatory constraints related to confidentiality, proportionality, and purpose limitation of data processing remain poorly studied. The authors acknowledge the predictive potential of OSINT, but emphasize that resilience without built-in legal controls can undermine institutional legitimacy.

Van Puyvelde and Rienzi [5] offer one of the most comprehensive reviews of OSINT in the security and public policy sectors. They describe the evolution of OSINT into a recognized intelligence discipline and emphasize its democratizing potential. The authors also identify ethical risks associated with the automation of data collection and the expansion of surveillance practices. At the same time, their approach is limited by the lack of an operational framework capable of assessing and mitigating these risks in real-time analytical processes.

Methodological aspects of knowledge formalization are further explored in the studies of Ngo and Le-Khac [9], devoted to the use of ontological structures in digital forensics. Although the study does not focus directly on OSINT, it confirms the possibility of transforming normative concepts into machine-interpretable models. This creates the prerequisites for the application of formalized indicators of legal and ethical risks in automated OSINT pipelines.

Technical studies on cybersecurity, such as Yadav et al. [7] and Avrahami et al. [14], demonstrate the effectiveness of OSINT for threat detection and incident response. However, the legal and ethical considerations in these studies are largely descriptive and not integrated into risk models. Such a focus on performance can exacerbate systemic vulnerabilities in automated intelligence systems.

The socio-economic aspects of OSINT are analysed by Charlton et al. [15], who describe hybrid ecosystems of investigations involving journalists, activists, and intelligence agents. Similar issues are also observed in criminal contexts, as examined by Dalimunthe and Azhari [16], where the effectiveness of OSINT is accompanied by issues of jurisdiction and admissibility of evidence. These findings confirm the need for proactive mechanisms for legal risk assessment.

Finally, Obioha-Val et al. [17] and Shin et al. [18] reveal the broader implications of AI-based analytics, in particular the problems of algorithmic opacity and the reliability of evidentiary data. Similarly, the approaches proposed by Ghioni et al. [11] within the GELSI framework make a significant contribution to systematizing the multidimensional risks of OSINT investigations. At the same time, the lack of operational models capable of transforming GELSI principles into automated decision support mechanisms remains a critical limitation.

In summary, the current literature recognizes the transformative potential of OSINT, but remains fragmented between technical, legal, and ethical approaches. No earlier studies have proposed an integrated automated model capable of classifying legal and ethical scenarios directly within OSINT workflows. This study fills this gap by considering OSINT risk as an intrinsic computational property of digital intelligence systems and proposing a hybrid model that operationalizes legal and ethical constraints in real time.

3 Methods

3.1 Research Design

The research aimed to develop repeatable and practically applicable risk assessment models for ethically and legally permissible use of OSINT in digital intelligence environments. Empirical testing and validation of the proposed system were carried out at the Academic Cyber Security and Digital Forensics Laboratory of the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" (Kyiv, Ukraine). The laboratory operates as a research centre with limited access specializing in cybersecurity, digital forensics, and applied information security. The laboratory infrastructure includes isolated virtualized environments, secure servers, and segmented networks designed for OSINT data processing and risk modelling. Access to classified information, personal data, or operational databases of law enforcement agencies was not provided. All datasets came from open sources, simulated OSINT streams, or anonymized synthetic data. The study was performed according to a sequential six-step procedure presented in Figure 1.

3.2 Research Procedure

The first stage involved creating a secure environment for collecting digital OSINT content. A secure infrastructure for data aggregation from open sources was created. These included public domains, social media APIs, open registries, legally permitted indexed darknet mirrors, forums, and repositories. Access was through legitimate automated search engines only without circumventing technical restrictions. Each channel was tagged with metadata regarding jurisdiction, compliance with platform policies, and level of confidentiality.

The second stage was the development of OSINT usage scenarios. Scenario engineering was used to model 124 executable cases, including personal data analysis, behavioural analytics, infrastructure mapping, cyberthreat attribution, disinformation detection, and evidentiary use. All scenarios were classified into three legal ethics classes: permitted (A), legally uncertain or ethically sensitive (B), and prohibited (C).

The third stage involved data normalization and feature extraction. The data was deduplicated, anonymized, and semantically cleaned. Traceability, jurisdictional dependency, proportionality of collection, and rights impact indicators were extracted.

The fourth stage was automated decision-making. Three independent ML models with numerical risk assessment were trained. Additionally, a rule-based legal validation mechanism was applied.

The fifth and sixth stages involved expert verification and iterative refinement of the models. The result was a hybrid computational-normative decision support model with full reproducibility.

3.3 Sampling

The empirical basis of the study was digital OSINT artifacts and analytically constructed operational scenarios. At no stage of the study were humans involved as objects or subjects of analysis. The sampling strategy was aimed at ensuring legal neutrality, technical representativeness, and methodological adequacy for testing automated mechanisms for classifying legal and ethical risks in digital intelligence environments.

The primary sample included 52 structured OSINT datasets collected exclusively from open and legally accessible digital environments. Data sources were limited to publicly indexed web domains, open social media interfaces in accordance with platform policies, public institutional registries, legal mirror segments of indexed darknet environments, and open forums and repositories. No technical means of circumventing access control or authentication were used. Each data set formed a separate contextualized OSINT stream, which allowed for the preservation of jurisdictional and source attributes relevant for legal and ethical assessment.

The collected data was intentionally heterogeneous in structure. It included textual, semi-structured, and metadata-rich digital artifacts typical of real OSINT operations. Before use, all sets were normalized and enriched with jurisdictional traceability markers, platform compliance indicators, and privacy sensitivity attributes.

A total of 124 analytically designed operational test cases were also used. They simulated typical OSINT-oriented workflows without reflecting real-world investigations. The constructive nature of the scenarios ensured controlled variability of risk profiles without involving sensitive or illegally obtained data. The total sample size was methodologically sufficient to test the reliability, repeatability, and practical applicability of

Figure 1. Research stages
Source: developed by the author based on MindMeister [19]

the proposed hybrid risk assessment model in legally constrained digital intelligence systems.

3.4 Methods

The proposed OSINT risk assessment framework combines supervised machine learning with rule-based legal reasoning to provide a hybrid classification mechanism for evaluating legal and ethical risks associated with digital intelligence operations. The methodological workflow consisted of four consecutive stages: feature engineering, preliminary risk quantification, machine-learning classification, and legal validation.

3.4.1 Feature Engineering and Data Preparation

Each OSINT scenario was transformed into a structured feature vector consisting of 27 attributes representing legal, ethical, and technical characteristics of information collection activities. The attributes were grouped into five categories:

- source legitimacy and reliability indicators;
- personal data exposure indicators;
- jurisdictional compliance indicators;
- ethical proportionality indicators;
- operational and contextual risk indicators.

Prior to analysis, all features were normalized to the interval [0,1] using min–max scaling:

$$x_{norm} = \frac{x - x_{min}}{x_{max} - x_{min}}$$

Duplicate records, inconsistent metadata, and semantically redundant elements were removed during preprocessing. This procedure ensured comparability across all generated scenarios.

3.4.2 Preliminary Legal–Ethical Risk Index

To obtain an initial quantitative representation of normative sensitivity, a preliminary legal–ethical risk index (R_1) was calculated for each scenario. The index was derived using weighted aggregation of normalized legal, ethical, and technical indicators:

$$R_1 = \alpha L + \beta P + \gamma J + \delta E + \theta S$$

For proof-of-concept validation, equal initial weights ($\alpha = \beta = \gamma = \delta = \theta = 0.20$) were assigned and subsequently adjusted during iterative experimental calibration to maintain balanced contribution of all risk dimensions.

where:

- L denotes source legitimacy and reliability;
- P denotes personal data exposure risk;
- J denotes jurisdictional compliance risk;
- E denotes ethical sensitivity and proportionality risk;
- S denotes contextual operational risk;
- $\alpha, \beta, \gamma, \delta, \theta$ are weighting coefficients.

The weighting coefficients were iteratively calibrated through experimental testing to ensure balanced contribution of each component to the overall risk profile. The resulting index provided a continuous risk gradient used as an input variable for subsequent classification.

3.4.3 Machine Learning Classification

Three supervised machine learning algorithms were employed:

- Support Vector Machine (SVM);
- Random Forest (RF);

- Gradient Boosting Classifier (GB).

The dataset was randomly divided into training and testing subsets using an 80:20 ratio. To reduce overfitting and improve generalization, five-fold cross-validation was applied during model development.

The principal hyperparameters were:

- SVM: radial basis function kernel (RBF), C = 1.0, γ = *scale*;
- Random Forest: 100 decision trees, maximum depth = 10;
- Gradient Boosting: 100 estimators, learning rate = 0.1, maximum depth = 3.

For each scenario, every classifier generated:

- predicted risk class (A, B, or C);
- probability score;
- classifier confidence value.

Model performance was evaluated using the following metrics:

- Accuracy;
- Precision;
- Recall;
- F1-score;
- Area Under the ROC Curve (ROC-AUC).

To increase classification stability, the outputs of the three classifiers were aggregated using deterministic weighted voting:

$$R_{ML} = w_1 SVM + w_2 RF + w_3 GB$$

where:

- R_{ML} represents the aggregated machine-learning prediction;
- w_1, w_2, w_3 are classifier weights satisfying $w_1 + w_2 + w_3 = 1$.

The deterministic fusion strategy reduced individual model bias and improved classification consistency.

3.4.4 Rule-Based Legal Validation

A parallel legal reasoning engine was developed to assess regulatory compliance independently from the machine-learning module. The engine encoded fundamental legal and ethical principles derived from:

- legality;
- proportionality;
- purpose limitation;
- accountability;
- protection of privacy and fundamental rights.

For each scenario, the legal validation module generated a secondary legal compliance score:

$$N_L = f(LN, JC, RI)$$

where:

- LN represents legal norm compliance;
- JC represents jurisdictional constraints;
- RI represents potential impact on fundamental rights.

The rule-based system produced transparent decision logs identifying activated legal conditions and corresponding compliance outcomes.

3.4.5 Hybrid Risk Assessment

The final hybrid risk assessment combined machine-learning outputs and legal validation results:

$$R_{final} = \lambda R_{ML} + (1 - \lambda) N_L$$

where:

- R_{final} denotes the final hybrid risk value;
- R_{ML} denotes the aggregated machine-learning result;
- N_L denotes the legal compliance score;
- λ is a balancing parameter.

The final output assigned each scenario to one of three classes:

- Class A – legally permissible and ethically acceptable;
- Class B – conditionally permissible or legally uncertain;
- Class C – legally prohibited or ethically unacceptable.

This hybrid architecture enables simultaneous consideration of analytical performance and regulatory compliance, providing explainable and operationally applicable decision support for OSINT-based digital intelligence systems.

3.5 Tools and Technical Environment

The following tools and facilities were used to ensure accuracy, reproducibility, and consistency:

- MindMeister – for collaborative idea visualization and scenario mapping;
- Protected OSINT Data Aggregation Infrastructure – a segmented, secure network environment for legal data collection;
- Offline Analytical Platform (Python-based) – performed ML calculations and feature extraction;
- Licensed Data Processing Software – for initial data cleaning, normalization, and deduplication;
- Rule-based Legal Reasoning Engine – integrated legal matrices for validating classifier results;
- Risk Visualization Dashboard – presents quantitative and qualitative risk assessments;
- Encrypted Data Storage Environment – secure storage with anonymization tools to protect sensitive data.

4 Results

4.1 Synthetic OSINT Dataset Construction for Experimental Validation

A synthetic OSINT dataset was developed to experimentally validate the proposed hybrid risk assessment framework under controlled and reproducible conditions. The use of synthetic data was motivated by legal, ethical, and operational constraints associated with collecting real-world intelligence datasets containing personal information or potentially sensitive investigative content.

The dataset generation procedure consisted of five consecutive stages:

1. Definition of representative OSINT operational domains;
2. Construction of legally and ethically relevant intelligence scenarios;
3. Assignment of structured legal, ethical, and technical attributes;
4. Expert validation of scenario consistency;
5. Final normalization and quality assurance.

Six operational OSINT domains were selected based on their prevalence in contemporary digital intelligence practice:

- social media monitoring;
- behavioural profiling;
- infrastructure and geospatial mapping;
- cyber threat attribution;
- disinformation analysis;
- evidentiary intelligence support.

Within these domains, 124 independent scenarios were generated. Each scenario represented a complete intelligence workflow describing data collection objectives, source characteristics, processing methods, jurisdictional context, and expected analytical outcomes.

To ensure methodological consistency, all scenarios were transformed into structured feature vectors containing 27 attributes. The attributes were grouped into five categories (Table 1).

The resulting dataset contained 3,348 structured observations (124 scenarios × 27 features), providing sufficient variability for experimental classification and legal validation. The complete definitions of all 27 features used in the experimental dataset are provided in Appendix A.

To facilitate reproducibility, the scenario generation procedure followed a predefined template specifying data source type, processing objective, legal context, ethical implications, and expected operational outcome. This standardized approach ensured consistency across all generated scenarios while preserving realistic variability of OSINT environments.

An illustrative scenario is presented below:

Example Scenario:

A public social media monitoring operation collects publicly accessible posts related to coordinated disinformation activity. The collection process complies with platform policies and does not involve access restriction circumvention. Personal identifiers are minimized, and the analytical objective is limited to identifying behavioural patterns rather than individual profiling. Such a scenario would generally receive a low-to-moderate preliminary risk score and would typically be classified as Class A or Class B depending on jurisdictional context.

The use of synthetic scenarios enabled complete control over risk factors, legal conditions, and ethical constraints while eliminating exposure to sensitive operational information.

Table 1. Categories of OSINT Risk Assessment Features

Category	Number of Features	Examples
Source Legitimacy	5	source accessibility, platform compliance, traceability
Personal Data Exposure	6	identification risk, data sensitivity, profiling potential
Jurisdictional Compliance	5	cross-border transfer, regulatory restrictions
Ethical Proportionality	5	necessity, proportionality, transparency
Operational Context	6	intelligence objective, analytical impact, operational sensitivity

Source: developed by the author based on Nasr et al. [20], United Nations Office of the High Commissioner for Human Rights [27], Web Asha Technologies [28]

4.2 Scenario Labelling and Class Allocation

First, each scenario was independently evaluated against predefined legal and ethical criteria derived from the conceptual framework presented in Section 3. These criteria included:

- legality of information collection;
- compliance with platform terms of service;
- proportionality of data acquisition;
- personal data exposure level;
- potential impact on fundamental rights;
- jurisdictional compatibility.

Second, a preliminary class assignment was performed based on cumulative risk characteristics. Three legal–ethical classes were defined:

- Class A (Permissible): legally compliant and ethically acceptable scenarios presenting low regulatory risk;
- Class B (Conditionally Permissible): legally uncertain or ethically sensitive scenarios requiring additional review;
- Class C (Prohibited): scenarios involving substantial legal violations, disproportionate data collection, or significant ethical concerns.

Third, consistency checks were performed to verify class allocation and eliminate contradictory labels.

The final class distribution was intentionally balanced to provide sufficient representation of different risk categories, as presented in Table 2. The distribution was designed to avoid excessive class imbalance while preserving realistic differences between low-risk, medium-risk, and high-risk OSINT operations.

Table 2. Risk Class Distribution

Risk Class	Number of Scenarios	Percentage
Class A	40	32.3%
Class B	50	40.3%
Class C	34	27.4%

Source: developed by the author based on Schmitt & Flechais [24]

The resulting labelled dataset served as the reference standard for supervised machine learning training, cross-validation, and hybrid legal assessment. The predefined class structure also enabled quantitative comparison between automated classification outputs and rule-based legal reasoning results.

The completed dataset therefore provided a legally grounded, technically structured, and experimentally reproducible environment for evaluating the proposed hybrid OSINT risk assessment framework.

4.3 Generating OSINT Streams with Legal and Ethical Tags

The secure OSINT aggregation environment processed each synthetic scenario to generate separate OSINT streams enriched with legal and ethical tags. Each generated stream contained a full set of metadata. These included information on the jurisdiction of origin, compliance with relevant policies of each platform, the degree of relevance of the personal information, and the level of ethical sensitivity of the data.

Table 3 presents the structured output parameters characterizing the OSINT aggregation process. The table data confirm that traceability of the jurisdiction of origin was ensured for each stream. Compliance with platform

policies was also encoded. A separate personal data exposure structure was generated with the definition of the corresponding attributes.

Furthermore, the results demonstrate the appropriateness of performing deduplication and semantic normalization without compromising data integrity. The successful implementation of ethical relevance of privacy at the data level was also confirmed. The obtained results indicate that the experimental dataset was integrated into the analytical pipeline in a state of legal, ethical, and technical normalization. This confirms that OSINT risk assessment can start with a pre-verified intelligence substrate. This approach eliminates the need for retroactive compliance checks at later stages of analysis.

4.4 Structural Scenario Matrix and Legal and Ethical Clustering

The operational scenarios were grouped according to their legal and ethical characteristics. The structural distribution of scenarios across Classes A, B, and C is presented in Figure 2. The structural distribution of scenarios by classes A, B, and C is presented in the Figure 2 below.

The Figure 2 illustrates the formation of clearly defined clusters of scenarios, the distribution of which is not random. Class A scenarios are localized in low-risk areas and are characterized by legal data collection and minimal ethical constraints. Class B scenarios are mainly concentrated in transitional areas. The risks here are determined by the proportionality of the intervention, jurisdictional restrictions, and the use of secondary data. Class C scenarios are concentrated around prohibited intelligence collection practices with a high level of legal and ethical constraints. The identified cluster structure confirms the gradual, rather than binary, nature of the risk of using OSINT and justifies the need for multi-level classification and continuous risk assessment.

4.5 Quantification of Preliminary Legal and Ethical Risk

A preliminary composite legal and ethical risk index (R) was calculated for each scenario. The calculation was carried out using weighted combinations of the extracted set of relevant features. This approach ensured a consistent aggregation of legal, ethical, and technical risk parameters.

Figure 3 presents the resulting risk gradient for the entire corpus of studied scenarios. The visualization demonstrates a smooth and interpretable escalation of risk values. The transition from class A to class C occurs without sharp jumps or discrete breaks.

Analysis of the resulting gradient identified five technically relevant observations.

1. Each scenario is characterized by an individual risk profile.
2. No artificial artifacts associated with clustering or normalization procedures were detected in the data.
3. The risk values show a gradual increase between different classes.
4. Even legally permissible scenarios retain a non-zero baseline risk level.
5. The formed gradient is suitable for further automated classification.

Taken together, these results confirm the possibility of quantifying legal and ethical risks in a continuous and interpretable format. The proposed approach avoids the reduction of complex normative assessments to rigid binary thresholds, which is critical for automated decision-making systems.

4.6 Automated Classification Output and Deterministic Fusion Analysis

The proposed framework is based upon a deterministic fusion architecture, which includes three classifiers, namely Support Vector Machine (SVM), Random Forest (RF), and Gradient Boosting (GB), that are all supervised machine-learning classifiers. This step was not meant to provide statistical comparisons of the performance of classifiers, but rather to test the operational viability of combining the machine-learning results with the legal reasoning in a unified OSINT risk assessment workflow.

In the execution of the experiments, it was found that all 124 scenarios could be successfully processed by the three classifiers. Every classifier provided a risk-class prediction (Class A, B, or C), confidence estimate, and numerical risk score. These outputs were then fused together deterministically as explained in Section 3.3.

The analysis showed that the fusion approach proposed was able to yield stable and internally consistent

Table 3. Structured output parameters of the OSINT aggregation stream

Parameter	Resulting Condition
Jurisdiction traceability index derivation	Achieved for all streams
Platform policy compliance encoding	Completed for each stream
Personal data exposure attributes	Encoded as structured indicators
Deduplication and semantic normalization	Completed without loss of integrity
Ethical privacy relevance marking	Successfully embedded

Source: developed by the author based on Nasr et al. [20], Lazarov et al. [21]

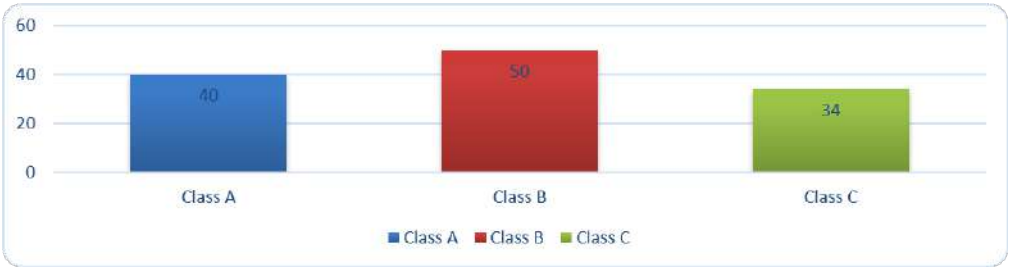

Figure 2. Distribution of OSINT Scenario Classes in the Experimental Dataset
Source: developed by the author based on Public-Private Analytic Exchange Program [22], Koenig [23]

risk classification for the whole scenario set. When the predictions of individual classifiers were not congruent, the incongruence was noted and passed to the legal validation module for secondary validation. This ensured that disagreement among classifiers would not directly influence the final risk decision.

The deterministic fusion mechanism brought three advantages in practice. It decreased the reliance on the performance of any particular classifier. Second, it included an explanation feature that kept the decision paths traceable. Third, it permitted the integration of computational outputs with legal and ethical constraints via a common risk representation. Table 4 summarizes the outcomes of the models when they are executed.

Table 4. Operational Results of the Automated Classification Stage

Indicator	Result
Total scenarios processed	124
Successful scenario processing	124 (100%)
Class prediction generated	Achieved for all scenarios
Confidence estimation generated	Achieved for all scenarios
Deterministic fusion completed	Achieved
Classifier disagreement detection	Implemented
Transfer to legal validation module	Completed
Hybrid risk assessment generation	Confirmed

Source: developed by the author based on Meng [26]

The results achieved show the technical feasibility of integrating automated classification mechanisms into legally constrained OSINT processes. The classifiers were able to provide satisfactory support for identification of legally permissible, conditionally permissible, and prohibited operational scenarios while maintaining compatibility with the subsequent rule-based legal assessment stage.

The main reason for the present study to be limited to framework development and proof-of-concept validation with the dataset of synthetic scenarios is that the statistical benchmarking of the performance of the classifiers is not part of the current research. Large-scale, operational dataset-based validation studies should be conducted in the future, and standard machine learning evaluation metrics should be reported, such as Accuracy, Precision, Recall, F1-score, ROC-AUC, and confusion matrices. This validation would therefore allow a quantitative evaluation of predictive performance in real-world intelligence scenarios.

4.7 Rule-Based Legal Validation and Secondary Compliance Assessment

Following automated classification, each OSINT scenario underwent secondary evaluation using a rule-based le-

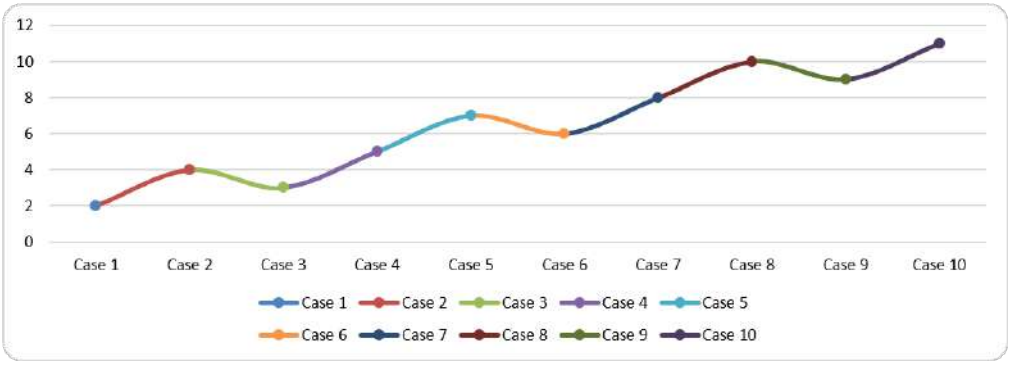

Figure 3. Distribution of Preliminary Legal–Ethical Risk Scores
Source: developed by the author based on Schmitt & Flechais [24], Dekens [25]

gal validation engine. This stage was intended to establish if the computational classification outputs matched the basic legal and ethical principles applicable to digital intelligence operations.

The legal validation module was built with a structured matrix of normative principles derived from contemporary data protection frameworks, digital investigation standards, and human rights doctrines. The principles encoded were:

- legality of information collection;
- proportionality of processing activities;
- purpose limitation;
- accountability and auditability;
- necessity of data acquisition;
- protection of privacy and fundamental rights.

Based on the contextual features of each scenario, a certain set of legal rules was triggered in each case. The activated rules generated a secondary compliance score reflecting the overall degree of legal and ethical acceptability.

The legal validation procedure consisted of three sequential stages.

First, the scenario attributes were mapped to relevant legal conditions. For instance, scenarios with cross-border data collection triggered jurisdictional compliance assessment, while scenarios containing personal information activated privacy protection rules.

Second, the activated legal conditions were evaluated against predefined compliance thresholds. The evaluation produced structured outputs describing:

- compliance status;
- identified legal concerns;
- activated regulatory constraints;
- potential rights implications.

Third, the generated legal assessment was compared with the machine-learning classification output. Cases exhibiting consistency between computational and legal evaluations were accepted without modification. Cases involving discrepancies were flagged for additional review and reassessment within the hybrid fusion layer.

The legal engine also generated traceability logs documenting all activated rules and corresponding compliance outcomes. These logs improved transparency and explainability by allowing analysts to identify the specific legal factors contributing to each risk assessment.

The application of rule-based legal validation demonstrated that normative constraints can be represented in a machine-interpretable format and integrated directly into automated OSINT workflows. This approach reduces dependence on purely manual compliance reviews while preserving legal accountability and interpretability of analytical decisions.

4.8 Final Assessment of Hybrid Risk and Model Integrity

The final hybrid risk indicator (Rfinal) is based on the results of the automated classification and the corresponding legal justification. These results were integrated for each individual scenario. The generalized values are given in Table 5. The assessment of the integrity of the final hybrid model is based on a number of conditions. These include consistency of results, compliance with legal and ethical requirements, avail-

ability of conflict resolution mechanisms, operational readiness and reproducibility of the model.

Table 5 and Figure 4 together reflect the final architecture of the hybrid risk assessment model. Figure 4 illustrates the functioning of the computational intelligence and regulatory logic components. These components operate autonomously, but synchronously, within a single decision support system.

The combined analysis of Table 6 and Figure 4 confirms the technical stability of the proposed model. Its legal stability and ethical consistency are also established. This indicates the appropriateness of using the model in the operational environment of digital intelligent systems. So, a legally consistent and operationally stable OSINT data aggregation system has been developed in this study.

5 Discussion

The study aimed to develop and conceptually test models for assessing the risks of OSINT use by applying data mining methods and automated classification of legal and ethical scenarios. In contrast to studies focused on the statistical effectiveness of OSINT, the emphasis in the study is on the analysis of algorithmic risk classification. In particular, its ability to ensure the legal, ethically permissible, and operationally justified use of open data in a complex digital environment was considered. The obtained results generally confirmed the working hypothesis. It was found that risk-based automated classification allows identifying problem scenarios even before the formation of analytical products. Comparative analysis showed that, unlike traditional reactive OSINT models, which were used mainly for post-facto verification of compliance with regulatory requirements, modern approaches increasingly function as early warning systems. Such models are focused on identifying potential violations before their actual implementation. This indicates the transformation of the role of OSINT from an information gathering tool to a risk management and decision support mechanism.

The results are similar to those of Revak et al. [12], who describe electronic documents as a resource based on analytical value that depends on the contextual security and legal protection of these documents. Most sociological and legal studies focus on analysis after the data collection stage. Instead, this study extends the relevant concept by integrating risk analysis directly into automated open-source data collection pipelines. Van Puyvelde and Rienzi [5] consider OSINT as a transformative development in intelligence practice due to its openness and accessibility. Their work also supports this study's findings that the expansion of OSINT generates increased strategic dependence on open-source information. The model described by Van Puyvelde and Rienzi [5] views legal and ethical issues as issues related to institutional mechanisms. Instead, this study demonstrates the possibility of their formal solution and implementation using an automated classification model, which reduces the dependence on spontaneous decisions made by humans.

Yadav et al. [7] describe in detail how the technical aspects of OSINT have been used to support cybersecurity applications, focusing on scalability and threat detection. Their work is thus based on the implicit understanding that collecting more data and using better algorithms will yield better results. However, this study partially contradicts the assumptions presented in the previous study, as higher levels of automation without legal and ethical constraints increase systemic risks to the organization, rather than reducing them. The explanation for these discrepancies is the fact that each industry has different priorities. Cybersecurity engineers are primarily concerned with responding to threats, while organizations practicing digital intelligence that is subject to the law should focus on proportionate response and accountability.

Ghioni et al. [11] argue from an operational perspective that the need for oversight of governance, ethical, legal, and social aspects of OSINT and AI use outweighs the need for purely technical solutions. Their approach emphasizes the priority of institutional and regulatory controls over technological optimization. While the authors seem to be clearly sceptical about whether automation can be used to enhance ethical controls, our study demonstrates that they are not necessarily mutually exclusive. The study also illustrates how ethical and legal norms can be formalized into machine-readable classification systems to provide a practical illustration of the GELSI principles. The basis of this divergence of opinion seems to be whether automation will always lead to a reduction in ethical controls.

Table 5. Conditions for the integrity of the input data of the final hybrid risk model

Feature	Result
Consistency of hybrid results in each scenario considered	Achieved
Maintaining legal/ethical integrity in the final results	Confirmed
Resolving classifier/legal mechanism discrepancy	Achieved
Ready for operational solution	Achieved
Reproducibility of hybrid risk values	Confirmed

Source: developed by the author based on Monterrubio et al. [29]

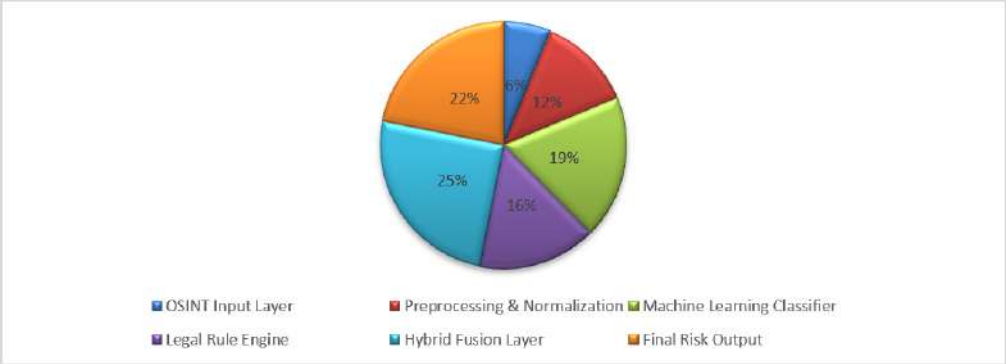

Figure 4. Architecture of the Proposed Hybrid OSINT Risk Assessment Framework
Source: developed by the author based on Van Puyvelde & Rienzi [30]

Ngo and Le-Khac [9] support this paper's interest in structured knowledge representations. They demonstrate the use of ontology-based case management as a way to address gaps in digital forensics training and investigation. However, their research focuses on developing an ontology that primarily addresses evidence and investigative procedures. The proposed model will extend the use of structured ontology to include legal risk and ethics scenarios that relate to OSINT assessments prior to the start of an investigation. Obioha-Val et al. [17] and Avrahami et al. [14], who focus on proactively using AI with OSINT to develop the most effective cybersecurity model, emphasize the ability to anticipate potential threats and provide rapid response times. However, these authors differ from our research in demonstrating the role of predictive capabilities alone in creating intelligence products. Such products can be useful from an operational efficiency perspective. However, they remain legally useless and/or unethical due to the lack of integration of legal risk assessment into the model. This is largely influenced by the different sectors (public interest intelligence vs. corporate cybersecurity) and the level of regulatory compliance in each sector.

In their study of OSINT from a journalistic and intelligence perspective, Charlton et al. [15] identified the need for public accountability and transparency to facilitate collaboration between journalists and intelligence. The results of Charlton et al. [15] confirm the need for ethical distinctions based on scenarios. The proposed model provides these through automatic classification, rather than relying solely on the professional ethics of the users. Dalimunthe and Azhari [16] and Shin et al. [18] provide evidence for the appropriateness of using OSINT with advanced data mining techniques. They show that such an approach is applicable to technically complex forensic investigations. Our study extends the work of Dalimunthe and Azhari [16], and Shin et al. [18] by providing a systematic framework for identifying legal and ethical risks associated with the use of data mining techniques that is integrated into the analytical process rather than simply considered post factum.

The most important contribution of the theoretical part was that the risk factors for analysts using OSINT as a source of information are inherent to the analysts

themselves, not external factors. So, the study integrated legal and ethical components into a ML classifier model to demonstrate a new integration between digital intelligence theory and legal theory/applied ethics. This study also adds to the body of knowledge on hybrid models for the development of norm-based intelligent systems. It contributes to the theoretical discussion of the need for responsible and legitimate intelligence systems and the potential use of AI to support law enforcement in investigations. This study also extends current OSINT theories with the concept of "normatively aware intelligence channels." It embeds compliance and ethics issues into the logic of the analysis process, rather than presenting them as mere supervisory layers of control over it.

The proposed model can be implemented by law enforcement agencies, regulatory agencies, cybersecurity units, corporate intelligence units operating under legal constraints. The proposed model allows for the creation of OSINT tools that provide early warning systems for high-risk information collection processes. It also supports real-time monitoring of high-risk methodologies and analysis results. This will help organizations to make informed decisions and reduce their institutional liability. Besides, as the model allows for adjusting the legal/ethical classification parameters according to the needs of different jurisdictions, it is also suitable for international digital intelligence operations.

5.1 Comparative Evaluation of the Proposed Framework

The proposed hybrid OSINT risk assessment framework differs from existing approaches by integrating automated classification and rule-based legal reasoning within a unified decision-support architecture. Table 4 summarizes the principal differences between conventional compliance mechanisms, machine-learning-driven approaches, and the proposed framework.

The comparison demonstrates that traditional compliance mechanisms provide strong legal oversight but lack scalability and automation. Pure machine-learning approaches offer efficient processing but often fail to provide adequate legal justification and explainability. As shown in Table 6, the proposed hybrid framework combines the advantages of both approaches by integrating computational intelligence with formalized legal reasoning. Consequently, the model supports scalable risk assessment while maintaining legal accountability and ethical transparency.

5.2 Limitations

This study has a number of limitations that should be considered when interpreting the results. The first limitation is that the experimental testing was carried out on a synthetic OSINT dataset generated based on scenarios, rather than on actual operational intelligence data. This approach ensured ethical and legal control, as well as the reproducibility of the experiment. At the same time, synthetic data do not fully reflect the level of uncertainty, noise, and external interference inherent in real OSINT environments. Therefore, further validation on controlled real data is necessary to confirm the robustness of the model. The second limitation concerns the hybrid risk assessment model. The model takes into account the jurisdictional factor, but does not adapt to dynamic changes in national legislation and case law. This limits its direct application in multi-jurisdictional environments without additional legal tuning. The third limitation is related to the manual identification of legal and ethical features. This approach provides transparency and explainability, but reduces the scalability and adaptability of the model to new OSINT methods and platforms. In addition, the study did not analyse the performance of the system in real time. Issues of latency, resource utilization, and scalability at high data throughput remain the subject of further technical research. The absence of statistical benchmarking metrics such as Accuracy, Precision, Recall, F1-score, ROC-AUC, and confusion matrices constitutes an acknowledged limitation of the present proof-of-concept study.

5.3 Recommendations

The study provides recommendations for further research, information systems design, and development of regulatory acts aimed at improving the effectiveness of OSINT-related risk assessment models:

1. Further research should focus on creating dynamic, adaptive and self-updating risk assessment systems. Such systems should integrate continuous learning mechanisms. Combined with regular legal and ethical audits, this will ensure that classifications are adjusted in accordance with changes in

Table 6. Comparative Evaluation of OSINT Risk Assessment Approaches

Criterion	Compliance Review	Risk Assessment	Hybrid Framework
Automated Processing	Limited	High	High
Legal Compliance Integration	High	Low	High
Ethical Assessment	Moderate	Low	High
Explainability	High	Moderate	High
Scalability	Low	High	High
Real-Time Risk Identification	Limited	High	High
Human Oversight Support	High	Limited	High
Decision Traceability	Moderate	Moderate	High

the availability of OSINT platforms, data sources, and current regulations.

2. Development of modular risk assessment systems taking into account jurisdictional differences. Such systems should include legal modules based on national legislation on personal data protection, surveillance rules, and constitutional guarantees of human rights. A modular approach reduces the risks of illegal use of OSINT in a cross-border context.
3. Implementation of a hybrid decision-making model that combines automated classification with mandatory human supervision. Automated systems should serve a supporting function, not a substitute for legal and ethical expertise in high-risk cases.
4. Incorporating indicators of source credibility and disinformation risks into OSINT assessment models. This increases the reliability of analytical results.

6 Conclusions

This study developed and conceptually validated a hybrid OSINT risk assessment framework that integrates data mining techniques, supervised machine-learning classification, and rule-based legal reasoning within a unified decision-support architecture. The proposed research approach is a huge contribution to current research in OSINT for the way it integrates legal and ethical questions into the process of intelligence gathering.

A structured synthetic OSINT dataset containing 124 OSINT scenarios with 27 legal, ethical and technical features was used for the evaluation of the framework. The experimental setting allowed for the assessment of risk factors of an open source intelligence (OSINT) operation while simultaneously maintaining legal, ethical, and methodological neutrality. The developed model provides a classification of the operational scenarios into three risk classes: Class A – legal, Class B – conditionally legal and Class C – prohibited.

The formalization of the legal and ethical limitations as machine interpretable variables that can be directly fed into an automated analytical process, is a key contribution of the study. The model is different from traditional compliance monitoring and enforcement because it provides for proactive efforts to identify legal and ethical risks throughout the intelligence process. The deterministic machine-learning fusion, paired with the rule-based legal validation, further enhances transparency, explainability and decision traceability.

This study also makes a significant theoretical contribution to the process of theorizing normatively conscious digital intelligence systems. The framework shows how regulatory needs can be realised as quantifiable components of automated decision support systems by taking a computational risk assessment approach in combination with structured legal review. This opens up the possibility to build intelligence systems which are both analytically efficient, legally accountable and proportionate.

On a practical level, the proposed framework could be used in cybersecurity operations, in digital forensics, to monitor regulatory compliance, within a corporate intelligence environment, and in a public-sector analytical environment where the lawful use of OSINT is critical. The model serves as a starting point for early warnings

of possible problematic intelligence activities and helps to make better informed risk management decisions.

Future studies could benefit from large scale validation of the presented approach by operating data, quantitative comparison of classification results, real-time processing of OSINT streams and making adaptive jurisdiction-specific legal modules that meet changing regulation requirements.

Author Contributions

All the authors participated and were involved in the conceptualization of the study, collation of data, analysis and review of the study as well as the writing, and proof reading of the manuscript. All authors read and approved the final version of the manuscript.

Compliance with ethical standards

The authors declare that they have no conflict of interest related to this study.

This research did not involve human participants, human biological materials, animals, or access to confidential personal data. All datasets used during the study were either publicly available, anonymized, or synthetically generated for research purposes.

The study was conducted in accordance with applicable ethical principles governing digital research, information processing, and data protection.

Data Availability Statement

The synthetic dataset and code generated during this study are available from the corresponding author upon reasonable request, subject to institutional approval and a data access agreement ensuring lawful and ethical use. The data are not publicly available due to legal, ethical, and security considerations.

AI Assistance Disclosure

The authors declare that the artificial intelligence (AI) tool ChatGPT (OpenAI) was used exclusively for language editing, formatting assistance, grammar improvement, and technical refinement of the manuscript. No AI tool was used for the generation of research data, experimental results, statistical analyses, interpretations, scientific conclusions, or cited scholarly content. All AI-assisted content was carefully reviewed, verified, and approved by the authors, who assume full responsibility for the final version of the manuscript.

Funding information

This research did not receive any financial support.

References

[1] I. Böhm and S. Lolagar, "Open source intelligence: Introduction, legal, and ethical considerations," *International Cybersecurity Law Review*, vol. 2, pp. 317–337, 2021. doi: 10.1365/s43439-021-00042-7.

[2] EITHOS, "Open source intelligence (OSINT): Its legal and ethical aspects," 2025. [Online]. Available: https://eithos.eu/open-source-intelligence-osint-its-legal-and-ethical-aspects/

[3] Crawsec, "What is OSINT?," 2025. [Online]. Available: https://www.crawsec.com/what-is-osint/

[4] D. Atstaja, V. Koval, J. Grasis, I. Kalina, H. Kryshtal, and I. Mikhno, "Sharing model in circular economy towards rational use in sustainable production," *Energies*, vol. 15, no. 3, art. no. 939, 2022. doi: 10.3390/en15030939.

[5] D. Van Puyvelde and F. T. Rienzi, "The rise of open-source intelligence," *European Journal of International Security*, vol. 10, no. 4, pp. 530–544, 2025. doi: 10.1017/eis.2024.61.

[6] T. Babenko, K. Kolesnikova, O. Abramkina, and Y. Vitulyova, "Automated OSINT techniques for digital asset discovery and cyber risk assessment," *Computers*, vol. 14, no. 10, art. no. 430, 2025. doi: 10.3390/computers14100430.

[7] A. Yadav, A. Kumar, and V. Singh, "Open-source intelligence: A comprehensive review of the current state, applications and future perspectives in cyber security," *Artificial Intelligence Review*, vol. 56, no. 11, pp. 12407–12438, 2023. doi: 10.1007/s10462-023-10454-y.

[8] F. A. F. Alazzam, H. J. M. Shakhatreh, Z. I. Y. Gharaibeh, I. Didiuk, and O. Sylkin, "Developing an information model for E-commerce platforms: A study on modern socio-economic systems in the context of global digitalization and legal compliance," *Ingénierie Des Systèmes D Information*, vol. 28, no. 4, pp. 969–974, 2023. doi: 10.18280/isi.280417.

[9] H. Q. Ngo and N. Le-Khac, "Ontology-based case study management towards bridging training and actual investigation gaps in digital forensics," *Forensic Science International Digital Investigation*, vol. 47, art. no. 301621, 2023. doi: 10.1016/j.fsidi.2023.301621.

[10] V. Yermachenko, "Theory and practice of public management of smart infrastructure in the conditions of the digital society' development: Socio-economic aspects," *Economic Affairs*, vol. 68, no. 1, pp. 617–633, 2023. doi: 10.46852/0424-2513.1.2023.29.

[11] R. Ghioni, M. Taddeo, and L. Floridi, "Open source intelligence and AI: A systematic review of the GELSI literature," *AI & Society*, vol. 39, no. 4, pp. 1827–1842, 2023. doi: 10.1007/s00146-023-01628-x.

[12] I. Revak, O. Pidkhomnyi, and V. Chubaievskyi, "Electronic documents as resources for sociological research on the level of security of financial and legal relations," *Social & Legal Studios*, vol. 7, no. 1, pp. 273–282, 2024. doi: 10.32518/sals1.2024.273.

[13] G. Zoidze, R. Otinashvili, and S. Veshapidze, "The power of information: How business intelligence shapes a company's economic sustainability," *Three Seas Economic Journal*, vol. 6, no. 2, pp. 1–8, 2025. doi: 10.30525/2661-5150/2025-2-1.

[14] Z. Avrahami, M. Zwilling, and C. Hajaj, "Leveraging OSINT for advanced proactive cybersecurity: Strategies and solutions," *IEEE Access*, vol. 13, pp. 154229–154250, 2025. [Online]. Available: https://cris.ariel.ac.il/en/publications/leveraging-osint-for-advanced-proactive-cybersecurity-strategies-/

[15] T. Charlton, A. Mayer, and J. Ohme, "A common effort: New divisions of labor between journalism and OSINT communities on digital platforms," *The International Journal of Press/Politics*, vol. 31, no. 1, pp. 118–139, 2024. doi: 10.1177/19401612241271230.

[16] A. A. Dalimunthe Q. A. and M. Azhari, "Analisis forensik digital terhadap perdagangan data pribadi di dark web menggunakan OSINT & threat intelligence," *Jurnal Komputer Teknologi Informasi Dan Sistem Informasi (JUKTISI)*, vol. 4, no. 1, pp. 254–268, 2025. doi: 10.62712/juktisi.v4i1.400.

[17] O. A. Obioha-Val, T. I. Lawal, O. O. Olaniyi, M. O. Gbadebo, and A. O. Olisa, "Investigating the feasibility and risks of leveraging artificial intelligence and open source intelligence to manage predictive cyber threat models," *Journal of Engineering Research and Reports*, vol. 27, no. 2, pp. 10–28, 2025. doi: 10.9734/jerr/2025/v27i21390.

[18] D. Shin, J. Ha, and I. Euom, "Data-driven digital evidence analysis for the forensic investigation of the electric vehicle charging infrastructure," *Computer Modeling in Engineering & Sciences*, vol. 143, no. 3, pp. 3795–3838, 2025. doi: 10.32604/cmes.2025.066727.

[19] MindMeister, "Online mind mapping tool," 2026. [Online]. Available: https://www.mindmeister.com

[20] N. Nasr, A. N. Oruç, R. Lugo, I. Zaitseva-Pärnaste, and P. Kujala, "A proactive defense: An Open-Source Intelligence (OSINT) framework for maritime cybersecurity," *IEEE Access*, vol. 14, pp. 39852–39872, 2026. doi: 10.1109/access.2026.3673557.

[21] W. Lazarov, V. Moravec, P. Loutocký, J. Vostoupal, and Z. Martinasek, "Comparative analysis of OSINT tools, techniques, and legal aspects," *Computers & Security*, vol. 168, art. no. 104938, 2025. doi: 10.1016/j.cose.2026.104938.

[22] Public-Private Analytic Exchange Program, "Ethical frameworks in open-source intelligence (Report)," U.S. Department of Homeland Security, 2022. [Online]. Available: https://bib.opensourceintelligence.biz/STORAGE/2022.

[23] A. Koenig, "Ethical considerations for open-source investigations into international crimes," *AJIL Unbound*, vol. 118, pp. 45–50, 2024. doi: 10.1017/aju.2024.2.

[24] M. Schmitt and I. Flechais, "Digital deception: Generative artificial intelligence in social engineering and phishing," *Artificial Intelligence Review*, vol. 57, art. no. 324, 2024. doi: 10.1007/s10462-024-10973-2.

[25] N. Dekens, "OSINT techniques: Complete list of expert tactics for investigators," ShadowDragon, 2025. [Online]. Available: https://shadowdragon.io/blog/osint-techniques/

[26] W. Meng, "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," *SSRN*, 2025. doi: 10.2139/ssrn.5560703.

[27] United Nations Office of the High Commissioner for Human Rights, "Berkeley Protocol on Digital Open Source Investigations: Guidance on Human Rights and International Humanitarian Law," 2024. [Online]. Available: https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf

[28] Web Asha Technologies, "AI-Powered OSINT: Ethical implications and challenges," 2025. [Online]. Available: https://www.webasha.com/blog/ai-powered-osint-ethical-implications-and-challenges

[29] S. M. M. Monterrubio, A. Noain-Sánchez, E. V. Pérez, and R. G. Crespo, "Coronavirus fake news detection via MedOSINT check in health care official bulletins with CBR explanation: The way to find the real information source

through OSINT, the verifier tool for official journals," *Information Sciences*, vol. 574, pp. 210–237, 2021. doi: 10.1016/j.ins.2021.05.074.

[30] D. Van Puyvelde and F. T. Rienzi, "The rise of open-source intelligence," *European Journal of International Security*, vol. 10, no. 4, pp. 530–544, 2025. doi: 10.1017/eis.2024.61.