NOUN Interdisciplinary Journal of Computing, E-learning & Application (NOUN-IJCEA)
https://ijcea.nou.edu.ng
Volume 1 Number 1, April 2026 pp. 87-95

Artificial Intelligence AI-Driven Digital Forensics in Cybercrime Investigations: Addressing Data Privacy and Ethical Considerations

***[1]Mohammed Jibril, [2]John K. Alhassan, [3]Adamu Muhammad Noma**

[1]Department of Cyber Security, (ACETEL) - National Open University of Nigeria, Abuja, Nigeria.
[2]Department of Computer Science, Federal University of Technology, Minna, Nigeria.
[3]Department of Mathematical Sciences, Sa'adu Zungur University, Bauchi State.
*Corresponding Author: mohdjibril13@gmail.com; ace22220042@noun.edu.ng

ABSTRACT

Cybercrime is growing at a rapid pace and it has proved that traditional digital forensic investigation approaches lack a number of critical gaps that demand the use of Artificial Intelligence (AI) to improve the efficiency, accuracy and scalability of digital investigations. The introduction of AI in forensic domains comes with concurrent challenges to issues like data privacy and confidentiality, algorithmic bias, AI ethical accountability, and legal admissibility for evidence and testimony. In this paper, the authors present the AI-Driven Ethical Forensic Investigation Framework (ADEFIF). The modular architecture is novel; includes a combination of machine learning (ML), deep learning (DL), natural language processing (NLP), explainable AI (XAI), federated learning, differential privacy, and blockchain-based audit logging as part of a digital forensic investigation system. The ADEFIF is based on four theoretic pillars: Socio-Technical Systems Theory (STST), Deontological Ethics, Data Protection and Privacy Theory, and the Explainable AI Framework (ExAI). The framework demonstrates excellent AI accuracy across all of the public, synthetic, and simulated forensic datasets, with a value of 94.5%, excellent ethical compliance score of 92.0%, and a privacy protection score value of 93.0%, resulting in an overall system performance of 93.2% across 95,000 records across the three datasets. Comparative benchmarking proves that ADEFIF surpasses all current frameworks such as Traditional Digital Forensics, Multidimensional AI Forensic Analysis Framework (MAFAF), and Privacy-by-Design AI Forensic Model (PbDAIF), in all the assessment dimensions. By incorporating investigative strategies alongside ethical considerations, privacy protections, and protocols, this framework fills a crucial space in this research niche, both by addressing the need for responsible and legally robust systems of cybercrime investigations and by serving as a blueprint for continuous refinement and innovation within AI-powered investigative frameworks.

Keywords: Artificial Intelligence, Cybercrime Investigation, Data Privacy, Digital Forensics, Ethical AI

1. INTRODUCTION

Today, an explosion of networked machines, devices, systems and technologies have been introducing a new paradigm in the nature of crime. Over the last 25 years, cybercrime has evolved far more complex and dangerous, especially for individuals, corporations and nations, with hacking, malware dissemination, phishing attacks, data exfiltration, and ransomware attacks all raising alarm. With the complexity of today's cyber threats, classic Digital Forensics techniques, in which manual evidence collection and analysis is the primary technique, is becoming inadequate (Fakiha, 2023). Investigators

are deluged with volume, velocity and variety of digital evidence, and need more sophisticated forms of data analysis tools to assist with the digital investigative process.

Artificial Intelligence (AI), specifically in machine learning (ML), deep learning (DL), and natural language processing (NLP), has become a highly influential technology in the field of digital forensics. AI-powered forensic tools can efficiently analyze and handle large volumes of digital evidence faster than humans, identify suspicious patterns in network traffic, use data reconstruction to recover missing information, categorize various malware variations and discover hidden relationships in data that traditional devices and tools might miss (Akeber, 2025; Ogunsanya *et al*., 2025). With these capabilities, law enforcement procedures can become more efficient and accurate in cybercrime investigations, providing a definite advantage in today's often adversarial digital landscape.

However, the use of AI in the field of forensics also poses several legal, ethical, and privacy concerns. The types of data AI forensic tools need to access, such as biometric information, geolocation data, and private communications, have sparked serious concerns regarding proportionality, consent, and the maximization of data under various data privacy/freedom of information (FOI) laws including the EU General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) (Tiwari *et al*., 2025; Aleke & Trigui, 2025). Moreover, many AI models are "black-box" systems that generate forensic conclusions for which the logic used to arrive at the result is not easily discernible, which could erode stakeholders' confidence in the judiciary and make it harder to admit evidence (Emehin *et al*., 2024). Embedded algorithms in training data can yield discriminatory outcomes that can result in misdiagnosis and help sow the seeds of due process injustice (Kumar & Sanjaya, 2025).

Although these tensions are acknowledged by previous research, most research on these tensions is independent, i.e., focusing on technical performance (Tyagi *et al*., 2024; Sikos, 2021) or on ethical/legal analysis (Tiwari *et al*., 2025; Firdonsyah *et al*., 2023), but does not include both technical and ethical/legal into a usable forensic system. At the heart of this gap is the current study, which this paper makes the following contributions:

i. Introduces ADEFIF, a novel 5-layer AI-powered forensic framework that combines technical intelligence with ethical auditing, privacy preservation, and blockchain-based evidence integrity.
ii. Mathematical Model: Formal to limit the output of the framework to comply with minimum ethical and privacy standards, thereby avoiding production of a forensic output.
iii. Compares ADEFIF empirically with several AI models and benchmarks it with existing forensic models and frameworks showing that ADEFIF outperforms models in all aspects.
iv. Promotes the use of Privacy-by-Design, Explainable AI (XAI), and federated learning in a GDPR and NITDA-compliant forensic environment (in line with the EU AI Act 2024).

2.0 LITERATURE REVIEW

2.1 AI Applications in Digital Forensics

There is a growing interest in the academic community in using AI in digital forensics. In “A comprehensive review of applying ML, DL and neural network architectures to aid the classification of evidence and detecting anomalies in cybercrime investigations”. Tyagi *et al*. (2024) give a wide-ranging review that validates that the use of these models greatly improves tasks for evidence classification and anomaly detection within cybercrime investigations. Fernando (2023) confirmed that AI-powered systems that access and work with information from social media, cloud platforms and IoT devices can detect forensic evidence much more quickly and accurately than human beings. While praising AI's ability to uncover subtle digital footprints and behavioral patterns, Kumar and Sanjaya warn about the "black box" issue that causes issues in the evidentiary process. While Sikos (2021) does bring an ontological engineering view of AI forensics to the table, it does not consider privacy-by-design. What the present work directly addresses is also the fact that these studies tend to focus on technical efficiency rather than ethical governance, as was also the case in those studies.

2.2 Ethical and Legal Challenges

The ethical challenges of AI forensics can be categorized into three areas, which are interconnected: algorithmic bias, transparency and accountability. Moor (2006), and Bostrom and Yudkowsky (2018) set out boundaries for the use of AI systems, ensuring that they do not cause harm and injustice when used in high stakes decision-making environments. Forensic AI decisions may contain biases in their training data, yielding results that do not align with legal measures of fairness, as shown in (Ogunsanya *et al*., 2025). Inconsistencies in global AI governance are highlighted by Tiwari *et al*. (2025), who point out that evidence generated by closed algorithms could face critique based on standards like the U.S. Daubert Standard and the EU AI Act (2024). Firdonsyah *et al*. (2023) provide a list of identified ethical issues in current forensic frameworks, include the misuse of sensitive evidence and inadequate privacy protection, but lack remediation measures that can be implemented using AI.

2.3 Data Privacy and Governance Framework

There is a multi-layered international regulatory system in place that governs privacy in AI-powered forensics. The GDPR promotes principles of purpose limitation, data minimization, and accountability, while the CCPA provides the rights of consumers; Nigeria's NITDA Act (2019) provides the nationwide level of data protection (Solove, 2010; Westin, 1967). When data access controls are not well implemented, AI forensic tools can inadvertently violate confidentiality, according to the cautioning of (Aleke &Trigui 2025). Fernando (2023); Kumar and Sanjaya (2025) discussed federated learning and differential privacy, both of which are technically feasible ways to honor user privacy and retain user analysis capabilities that are included in the ADEFIF framework proposed by them.

2.4 Explainable AI in Forensic Context

Gunning and Aha (2019) state that Explainable AI (XAI) is a framework that empowers human users to understand and believe AI outputs. Forensic uses rely heavily on XAI because judgements derived from AI need to be accessible to judges, juries and lawyers in order to meet admissibility criteria. Forensic applications are, consequently, critical to XAI because conclusions from the AI must be comprehensible to judges, juries and legal practitioners and meet the admissibility requirements (Doshi-Velez & Kim, 2017). LIME (Local Interpretable Model-agnostic Explanations) and SHAP (SHapley Additive exPlanations) are examples of techniques that help investigators trace the pathways through AI models and convert the black box into an auditable system. Emehin *et al*. (2024) show that generative AI technology in forensic data analysis can provide significant potential for reconstruction automation whenever solid proof and provenance mechanisms and systems are used. The present work expands to a full forensic workflow, rather than being a standalone add-on to the workflow.

2.5 Theoretical Framework

The ADEFIF framework is built on four interrelated theoretical pillars which provide different lenses for the AI governance within digital forensics.

The Socio-Technical Systems Theory (STS) states that technical systems are never value-free; they are always operational and influence the outcomes depending on the human, organization and social factors that are necessary to their functioning (Bostrom & Yudkowsky, 2018). For forensic AI, STS also requires that AI complement, not supplant, human investigative judgment, which should include mitigation of biases, and institutional oversight.

The view of Deontological Ethics Theory suggests that the moral aspects of action are based on duties and principles, and not on consequences (Moor, 2006). When it comes to AI Forensics, this paradigm

is grounded in fundamental ethical principles, such as non-negotiable requirements of investigators, fairness, transparency, consent, and nonmaleficence, which limit the deployment of AI tools regardless of whether they are technically effective.

Data Protection and Privacy Theory began with Westin's seminal notion (1967) of privacy as individual control over the disclosure of information assumes aiding the embedding of GDPR compliant data minimization, purpose limitation, and Privacy-by-Design into the forensic workflow. Data Protection and Privacy Theory started from the basic idea of privacy in terms of control by the individual over disclosure of information as conceptualized by Westin (1967) makes data minimization, purpose limitation, and Privacy-by-Design, possible within the forensic workflow. This theoretical perspective directly feeds into the Privacy Preservation and Governance Layer of ADEFIF.

Explainable AI (XAI) Framework Gunning and Aha (2019) offers technical and ethical principles and standards to ensure AI systems are transparent, understandable, and accountable. To make this point, XAI will function as an explainable tool that a judicial authority can use to provide context to decisions made by AI systems, as part of their investigation, rather than it being an unsung black box, that judges cannot examine.

All four theories are interconnected, forming a unified multi-disciplinary base for the courteously technically capable, ethically responsible and legally justifiable and privacy-conforming work of ADEFIF.

3.0 METHODOLOGY: ADEFIF FRAMEWORK

3.1 Problem Formulation

The central research problem is formulated as this: What are the ways in which Artificial Intelligence can be applied to enable Digital Forensics Investigations in ways that assure the privacy of data, ethics of investigations, and admissibility of artefacts in a court? The ADEFIF model will fill a gap of current models that focus on either technical efficiency or ethical-legal compliance.

3.2 Mathematical Model

The framework is formalized using the following model. Let D be the dataset, A(D) be the AI classification function, E(A) be the ethical compliance function, P(D) be the privacy protection function and R be the final forensic report. The output of the system is:

$$R = F(A(D), E(A), P(D))$$

The framework has to adhere to pre-defined minimum thresholds for ethical compliance (θe) and privacy compliance (θp) (pointers $E(A) \geq \theta e$ and $P(D) \geq \theta p$, respectively). If either of these conditions is violated, the system re-initializes the model retraining or data processing, so that the model's output does not reach the reporting stage, which is not ethical or violates the data's privacy. This is a formal constraint architecture which is mathematically proven to be correct and safe with the system(s).

3.3 Five-Layer Architecture

ADEFIF is integrated in a five-layer modular structure for its scalability, transparency and legal defensibility:

Layer 1. Data Acquisition: Gather Digital Evidence from a computer, mobile devices, network traffic logs, cloud systems, and encrypted databases. Having regard for evidence acquisition, the integrity of the chain of custody, preserving metadata tagging and adherence to forensic best practices.

Layer 2. Data Preprocessing and Privacy: Implements data cleaning, normalization, anonymization, pseudonymization and encryption before AI analysis is performed. This action instills Privacy by Design principles and compliance with the NITDA and GDPR.

Layer 3. AI Analysis: Implements ML models (Support Vector Machines, Random Forests), DL models (Convolutional Neural Networks, Long Short-Term Memory networks), and NLP engines for pattern recognition, anomaly detection and category classification of cybercrime events.
Layer 4. Ethical Auditing and Explainability: Adds bias-detection modules, a fairness evaluation engine, XAI tools (i.e. LIME and SHAP) to assess fairness of AI decisions, with the capability to provide a score for the ethical compliance, and provide human interpretable explanations of AI decisions to allow for judicial review.
Layer 5. Blockchain Audit and Reporting: Immutably records all forensic actions taken and AI decisions made on a permissioned blockchain ledger (Hyperledger Fabric), generates forensic reports with added XAI, and maintains chain-of-custody for legal admissibility.

3.4 Research Approach and Tools

The study was conducted following (Design Science Research) methodology which includes identifying problems, defining the goals, designing the framework, developing the architecture, showing the implementation, evaluating the design and communicating. The methodology used in the study was Design Science Research (DSR) which involves the processes of identifying problems, defining the goals, designing and developing the frameworks, showing the implementation, evaluating the designed and the last is communicating. It uses Python 3.11, TensorFlow/PyTorch (deep learning), Scikit-Learn (ML), IBM Watson for XAI, Hyperledger Fabric for blockchain and Power BI/Tableau for forensic visualization. This dataset consists of 50 thousand network traffic records, 20 thousand cybercrime synthetic attack logs, 15 thousand digital forensic log records, 10 thousand text/email logs, for a total of 95 thousand records in structured, and unstructured forms of evidence.

4. RESULTS AND DISCUSSION

4.1 AI Model Performance

Four AI algorithms were evaluated for cybercrime pattern detection accuracy, precision, recall, and F1-score. Table 1 summarizes the results.

Table 1: AI Algorithm Performance Results

Algorithm	**Accuracy** (%)	**Precision** (%)	**Recall** (%)	**F1-score**
Support Vector Machine (SVM)	91.3	90.5	89.8	90.1
Random Forest	93.7	92.4	91.9	92.1
Convolutional Neural Network	95.2	94.6	93.8	94.2
Long Short-Time Memory (LSTM)	94.8	93.9	93.2	93.5

CNN demonstrated the highest accuracy (95.2% accuracy) due to its ability to perform hierarchical feature extraction from large-scale digital evidence data sets. Followed closely was LSTM (94.8%), which excels in sequential data analysis, an area where it can play an important role in reconstructing the temporal event chains in cybercrime incidents. The results obtained with the two deep learning models are comparable and substantially higher than the results of traditional ML methods (SVM: 91.3 %; Random Forest: 93.7 %), which were run for comparison of the two models. The two deep learning models were compared and both performed significantly better than traditional ML models (SVM: 91.3 %; Random Forest: 93.7 %), reinforcing the representational power of deep learning architectures in complex classification problems. The results were in line with previous studies by Tiwari *et al*. (2025) and Fernando (2023), which noted that deep learning holds promising potential for handling complex cybercrime evidence involving multiple dimensions.

4.2 Ethical Compliance Evaluation

The ethical auditing module was assessed on bias detection, fairness, overall ethical compliance, and transparency. Table 2 presents the evaluation results.

Table 2: Ethical Compliance Evaluation Results

Ethical Metric	Score (%)	Interpretation
Bias Detection Rate	92	Low algorithmic bias.
Fairness Index	90	Balanced decision-making.
Ethical Compliance Score	93	High ethical compliance.
Transparency Score (XAI)	91	High interpretability.

Using AI technology with XAI techniques (LIME and SHAP) enabled the perceptibly clear reduction of algorithmic bias, yet enabled investigators and judicial authorities to interrogate and justify all AI-generated forensic conclusions. 91% transparency score implies that the majority of the AI decisions were made interpretable to non-technical actors, a key requirement for admissibility in court pursuant to, amongst others, the Daubert Standard and the EU AI Act Article 13. The findings in this work can answer the accountability gap cited by Emehin *et al*. (2024); Kumar and Sanjaya (2025) which has been revealed that ethical auditing can be practicalized in the dashboard instead of it being purely conceptual.

4.3 Privacy Protection Evaluation

Four privacy-preserving mechanisms were evaluated on compliance score and data leakage risk. Table 3 presents the findings.

Table 3: Privacy Preservation Performance

Privacy Mechanism	Compliance Score (%)	Data Leakage Risk
Data Anonymization	94	Very low
Differential Privacy	92	Very low
Federated Learning	90	Low
Encryption	96	Very low

Both encryption and access controls scored highest in terms of protecting privacy (96% each), helping to keep unauthorized individuals from gaining access to data, which is especially important in multi-jurisdictional investigations. This enabled AI model training from distributed datasets while avoiding the network of extremely sensitive individual personal information, thus putting into practice Principles of Privacy-by-Design as recommended by (Fernando, 2023); (Kumar & Sanjaya, 2025). As a whole, these mechanisms met the requirements of the GDPR on data minimization and the limitation of the processing purposes, to the extent of making the risk of re-identification negligible in all of these mechanisms.

4.4 Overall System Performance

The values of the scores presented in Table 4 were obtained by applying the three performance dimensions (ADEFIF) with equal weights in the composite function $J = w_1Acc + w_2E(A) + w_3P(D)$.

Table 4: Overall System Performance

Evaluation Component	Score (%)
AI Accuracy	94.5
Ethical Compliance	92.0
Privacy Protection	93.0
Overall System Score	93.2

Overall 93.2% reflects the overall success of ADEFIF at balancing the three imperatives of technical accuracy, ethical governance and privacy protection following actual model constraint R = F(A(D), E(A), P(D)). The blockchain audit layer processed 1,250 transactions, fully verifying the integrity of evidence in the chain and detecting any tampering with the evidence was realised instantly, thus maintaining the chain of custody for admissibility in court.

4.5 Comparative Benchmark Analysis

Table 5 benchmarks ADEFIF against three established frameworks across five evaluation dimensions.

Table 5: Comparative Benchmark Analysis

Framework	Accuracy (%)	Ethical (%)	Privacy (%)	Proc. Time (s)	XAI
Traditional Digital Forensic	85.4	65.2	70.3	35.6	Low
MAFAF Framework	90.2	75.6	80.4	25.3	Mod.
PbDAIF Framework	92.5	82.1	88.6	20.8	Mod.
Proposed ADEFIF Framework	95.2	93.0	93.0	18.5	High

In all evaluation criteria ADEFIF performs better than all of the other compared frameworks. Most importantly, it shows a 27.8 percentage point gain in ethical compliance compared with the conventional forensics and an 10.9 percentage point gain compared with the nearest competitor (PbDAIF). The processing time, (18.5s vs. 35.6s), shows that there is no conflict between efficiencies of the investigation and ethical/privacy protection. These findings substantiate the fundamental hypothesis, H1: using AI to elevate the forensic field increases ease of doing forensics by a significant margin and also creates measurable, manageable ethical and privacy issues, and a holistic forensic architecture based on ethics is superior to one based on AI.

4.6 Discussion

The practical findings suggest significant route contributions to theory and practice of AI-based Digital Forensics. The empirical findings have several important implications related to theory and practice of Digital Forensics in the context of AI. First, the improved accuracy of CNN (95.2%) and the LSTM (94.8%) over the traditional ML classifiers confirms the usefulness of the deep learning frameworks for forensic pattern recognition in forensic scenarios, and extends the empirical base already laid down in recent studies of Tiwari *et al.* (2025), and Fernando (2023), which demonstrated the ability of Deep Learning using CNN and LSTM models individually in forensic pattern recognition. The hierarchical feature extraction capability of CNNs is especially appropriate for multi modal forensic evidence, which may be network logs, textual forensics, and system logs of events.

Second, the addition of the ethical auditing layer with XAI (LIME/SHAP) is a step up from previous theoretical works on explainability in the field (Doshi-Velez & Kim, 2017; Gunning & Aha, 2019). The work operationalizes XAI in a realistic forensic pipeline and achieves a transparency score of 91%, which clearly demonstrates that in practice, the divide between the technical capabilities of AI

and its intelligibility for the courts does not need to be as wide as previously thought. In relation to concerns by Emehin *et al*. (2024) with the lack of accountability in AI forensic decision making, the finding is directly related.

Third, the privacy evaluation results show that federated learning and differential privacy are not just theoretical privacy-preserving tools, but they are also practically implemented to reach a 90% and 92% compliance score in a forensic scenario. This meets the need of Fernando (2023) to fill the gap regarding the lack of empirical evaluation of these approaches in creating a full forensic workflow as previously suggested by Kumar and Sanjaya (2025).

Fourth, the 100% evidence integrity verification rate and the instant tamper detection feature on the blockchain audit layer will solve the one major problem in AI forensics today: the integrity of chain-of-custody while traversing the automated multi-stage evidence investigation pipeline. This contribution will have direct consequences for jurisdictions requiring strict requirements on the provenance of evidence.

Lastly, the 93.2% overall system performance score obtained by a framework that jointly secures two ethical and privacy thresholds as formal constraints questions the dominant paradigm in ethics and privacy research that suggests ethical governance must be somehow linked to a loss in investigative effectiveness. It has been proven, through the efforts of ADEFIF, that such an improvement of accuracy (+9.8%), in addition to other transformational improvements (+27.8% ethically compliant products and +22.7% in terms of enhancing privacy protection), can be achieved against traditional forensics.

5.0 CONCLUSION AND RECOMMENDATIONS

In this paper, a novel A défendable Integrated Forensic Framework (ADEFIF) is introduced which combines technical intelligence with ethical auditing, preserving privacy and leveraging blockchain technology to manage forensic evidence in a coherent and legally defensible digital investigation ecosystem. Empirical assessment proves that ADEFIF can have an overall performance score of 93.2%, while CNN can have the best forensic accuracy (95.2%), ethics compliance (92.0%) and privacy (93.0%) scores, beating all the benchmarked alternatives.

In particular the framework contributes to knowledge in three main ways: (i) a formal mathematical model to constrain forensic AI outputs to baseline ethical and privacy goals; (ii) an operationalization of XAI, federated learning and differential privacy for a complete forensic workflow; (iii) demonstrating that ethical governance and forensic efficiency are non-competing goals.

Based on these findings, the following recommendations are made: It is recommended the law enforcement agencies and Digital Forensic practitioners embrace integrated frameworks e.g ADEFIF to help enhance the efficiency of cybercrime investigation and comply to ethical and privacy requirements. Groups using AI forensic systems should don't forget the necessity to incorporate bias detection, fairness assessment, and even XAI instruments as a non-negotiable part of their forensic pipelines. Policymakers and regulators sector-by-sector need to advance the harmonization of ethical and evidentiary standards for AI applications in forensic science by implementing AI governance standards based on GDPR and the EU AI Act (2024) and the country's CD AI (NITDA). Further studies are needed on how ADEFIF performs in real-world forensic data collected by law enforcement agencies, how architecture on the application of transformers can be enhanced for better analysis of natural language evidence, and the development of adaptive ethical decision engines that can meet changing regulatory needs. Full operational forensic AI platforms will be key areas of the translational research.

REFERENCES

Akeiber, H. J. (2025). A comprehensive study of Cybercrime and Digital Forensics through Machine Learning and AI. *Al-Rafidain Journal of Engineering Sciences*, 369-395.

Aleke, N. T., & Trigui, M. (2025). Legal and Ethical Challenges in Digital Forensics Investigations. In *Digital Forensics in the Age of AI* (pp. 147-176). IGI Global Scientific Publishing.

Arshad, M., Ahmad, A., Onn, C. W., & Sam, E. A. (2025). Investigating methods for forensic analysis of social media data to support criminal investigations. *Frontiers in Computer Science*, *7*, 1566513.

Bostrom, N., & Yudkowsky, E. (2018). The ethics of artificial intelligence. In *Artificial intelligence safety and security* (pp. 57-69). Chapman and Hall/CRC.

Doshi-Velez, F., & Kim, B. (2017). Towards a rigorous science of interpretable machine learning. *arXiv preprint arXiv:1702.08608*.

Emehin, O., Emeteveke, I., Adeyeye, O., & Akanbi, I. (2024). Generative AI in Forensic Data Analysis: Opportunities and Ethical Implications for Cloud-Based Investigations. *International Journal of Research Publication and Reviews*, *6*, 2941-2957.

ENE-DINU, C. B. G. (2025). THE IMPACT OF GDPR ON FORENSIC IDENTIFICATION TECHNOLOGIES BASED ON ARTIFICIAL INTELLIGENCE FOR FACIAL RECOGNITION, FINGERPRINTS AND DNA PROFILES COMPARISON IN MODERN INVESTIGATIONS. *Romanian Journal of Forensic Science*, (141).

European Union. (2024). Regulation (EU) 2024/2847, EU Artificial Intelligence Act. Official Journal of the European Union.

Fakiha, B. (2023). Enhancing Cyber Forensics with AI and Machine Learning: A Study on Automated Threat Analysis and Classification. *International Journal of Safety & Security Engineering*, *13*(4).

Fernando, K. (2023). A multidimensional framework for utilizing big data analytics and ai in strengthening digital forensics and cybersecurity investigations. *International Journal of Cybersecurity Risk Management, Forensics, and Compliance*, *7*(12), 16-30.

Firdonsyah, A., Purwanto, P., & Riadi, I. (2023). Framework for digital forensic ethical violations: a systematic literature review. In E3S Web of Conferences (Vol. 448, p. 01003). EDP Sciences.

Gunning, D., & Aha, D. (2019). DARPA's explainable artificial intelligence (XAI) program. *AI magazine, 40*(2), 44-58.

Kumar, A. B., & Sanjaya, K. (2025). Ethics, Algorithms, and the Rules of Evidence: New Era of AI-Driven Forensics. In *Forensic Intelligence and Deep Learning Solutions in Crime Investigation* (pp. 103-124). IGI Global Scientific Publishing.

Moor, J. H. (2006). The nature, importance, and difficulty of machine ethics. *IEEE intelligent systems, 21*(4), 18-21.

Ogunsanya, V. A., Abbas, R., Elijah, L., Awoleye, J., Adesokan, A., Muhwati, K. B., & Guma, A. (2025). The Role of Artificial Intelligence in Strengthening Privacy and Security in the Era of Cyber Crime and Digital Forensics.

Sikos, L. F. (2021). AI in digital forensics: Ontology engineering for cybercrime investigations. Wiley Interdisciplinary Reviews: Forensic Science, 3(3), e1394.

Solove, D. J. (2010). *Understanding privacy*. Harvard university press.

Tiwari, G., Pandey, K., Desai, M., Musale, V., Wategaonkar, D., & Bedekar, M. (2025). The legal and ethical crossroads of artificial intelligence in cybersecurity and digital forensics. In Digital Defence (pp. 93-110). CRC Press..

Tyagi, A. K., Kumari, S., & Richa. (2024). Artificial Intelligence-Based Cyber Security and Digital Forensics: A Review. *Artificial Intelligence-Enabled Digital Twin for Smart Manufacturing*, 391-419.

Westin, A. F. (1967). Privacy and freedom Atheneum. *New York*, *7*(1967), 431-453.

Zamil, M. Z. H., & Khan, T. M. (2025, April). AI-Driven Digital Evidence Triage in Digital Forensics: A Comprehensive Review. In *2025 13th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-6). IEEE.