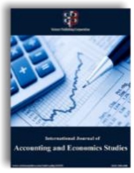
International Journal of Accounting and Economics Studies, 12 (5) (2025) 1201-1206

International Journal of Accounting and Economics Studies

Website: www.sciencepubco.com/index.php/IJAES
https://doi.org/10.14419/ap57rx96
Research paper



The Role of AI: from Conventional Methods to Digital Crime Analysis

Lucy Tatiana Polanco Aya [1] *, Orlando Carmelo Castellanos Polo [1], Sol Beatriz Vélez Escobar [1], Oscar Tarrillo Saldaña [2], Luis Alexander Barboza Tarrillo [3], María Esther León Morales [4], Lennin Rodríguez Castillo [4], Pedro Andres Valderrama Araujo [5], Carranza Guevara Rosas [6]

[1] Luis Amigo Catholic University
[2] National University of Trujillo
[3] National Autonomous University of Chota
[4] National University of Cajamarca
[5] Technological University of Peru
[6] Toribio Rodríguez National University of Mendoza in Amazonas
**Corresponding author E-mail: lucy.polancoay@amigo.edu.co*

Received: August 6, 2025, Accepted: September 14, 2025, Published: September 30, 2025

Abstract

Current research highlights how artificial intelligence (AI) affects digital forensics, considering its development in methods, specific implementations, and repercussions on the justice system. In addition to its technical effects, emphasis is placed on its influence in reducing legal costs and improving institutional resources. According to the Europol report (2025), the processing of information in the organization of digital evidence has reduced forensic analysis time by up to 70%, representing significant savings in working hours and case backlogs (p. 4). These findings show that AI not only speeds up the identification of patterns and risks but also helps to reduce the financial burden on justice systems(Europol, 2025, March 18).

Several studies support these findings. Fakiha (2024) indicates that an orderly and finite set of operations can reduce the time required to examine digital evidence by up to 96% (Fakiha, 2024, pp. 3-4). Furthermore, Khattak (2025) demonstrates that the accuracy of threat identification and digital evidence classification exceeds 90% (Khattak, 2025, p.112). These advances allow us to measure the economic benefits: if an analysis that previously took up to two weeks can now be completed in less than two days, the savings in expert salaries, storage costs, and legal expenses can vary between 40% and 60% (OECD, 2025, p.17).

However, the obstacles are significant. Tageldin and Venter (2023) point out the great dangers posed by biases in algorithms and the lack of uniform regulations (p.4). In addition, there is concern about the lack of transparency in decisions that are made automatically. A recent example, reported by the Associated Press (2024), revealed how an artificial intelligence tool, which claimed to be 90% accurate, resulted in wrongful convictions in the courts due to its inability to be explained. These drawbacks make the discussion about digital transformation essential: the application of AI in the judicial sphere requires not only technical specifications but also adequate regulations, constant supervision, and sustainable development (Associated Press News, 2024).

***Keywords**: Artificial Intelligence, Digital Forensics, Machine Learning, Forensic Technology, and Cybersecurity Law.*

1. Introduction

The advancement of artificial intelligence (AI) has substantially changed how communities approach crime, both in the real world and in virtual reality. Its use is no longer restricted to industrial areas but has also expanded to sensitive areas such as citizen protection, forensic digital information analysis, and crime investigation. This development has raised questions that go beyond the technical, as it involves ethical, governance, and economic discussions. AI's ability to identify habitual behavior, recognize irregularities, and prevent dangers makes it an important element in the current administration of justice. (Europol, 2025, p.5)

In the field of digital analysis, artificial intelligence has become a key tool in the face of vast amounts of data that cannot be handled manually. Machine learning and deep learning algorithms facilitate the identification of hidden connections, the recreation of situations, and the detection of discrepancies in transmission systems and connection devices (Widjaja, 2024, pp.1055-1056). These contributions not only improve technical accuracy but also have significant economic consequences: reductions of up to 60% in forensic costs and current advances in the judiciary by reducing the time of procedures (OECD, 2025, p.18)

However, this evolution carries certain dangers. The presence of biases in the amount of information, the lack of transparency of some prospective models, and the increasing subjugation of technology require a discussion about the responsibilities of institutions and the assurance of basic rights. Recent cases illustrate how the use of AI tools without adequate oversight has resulted in erroneous judicial rulings and additional expenses due to lawsuits and case studies (Associated Press News, 2024)

This work explores a journey from the methodological foundations of artificial intelligence to its use in cyber fraud investigation, with particular attention to its economic, technical, and social impacts. The goal is not only to demonstrate the capabilities of artificial intelligence but also to investigate how it can be incorporated in a balanced way, ensuring technological advancement, economic viability, and legality.

2. Reference Framework

1. **Context and evolution of digital forensics**:

The increasing complexity of cybercrime has led to a shift from predictive methodologies to the use of advanced tools that can handle large amounts of data. Traditional methods, such as manual information gathering, are unsafe against more sophisticated threats such as phishing, ransomware, or deepfakes. In this regard, artificial intelligence has emerged as a key resource for automating the identification of anomalies and improving response speed. (Akeiber, 2025, p.372). At the same time, by increasing technical proficiency, the adoption of artificial intelligence in forensic processes has a direct economic impact. According to the OECD (2025), forensic digitalization powered by artificial intelligence could cut up to 45% of litigation costs linked to digital evidence by mitigating the need for manual intervention and shortening delays in judicial processes (OECD, 2025, p.19).

2. **Application of AI and Machine Learning in forensic practices:**

Machine and deep learning systems have established themselves as essential tools for collecting, analyzing, and organizing judicial information. These techniques allow for the creation of timelines of criminal activity, the detection of communication patterns, and the classification of malware with high accuracy (Dunsin, 2023, p.10). Fattahi (2024) emphasizes that these solutions not only improve the categorization ability but also help develop models that predict financial fraud, allowing organizations to minimize lost profits due to fraud (Fattahi, 2024, p.8). In this way, forensic artificial intelligence transcends the purely technical realm, influencing economic equilibrium, strengthening confidence in electronic commerce (or e-commerce), and reducing expenses related to the investigation of cybercrimes.

3. **AI in the detection and reconstruction of digital crimes:**

The ability of artificial intelligence to analyze texts, images, and videos has transformed the field of criminal investigation. Widjaja (2024) highlights the existence of convolutional neural networks to identify digital modifications with a high level of accuracy, which reinforces the value of evidence (Widjaja, 2024, pp.1055-1056). From a financial perspective, these advances make it easier for the judiciary to optimize investigations and reduce costs associated with storing digital evidence and hiring forensic experts.

Fakiha (2024) presents data showing that artificial intelligence managed to reduce the time required to identify anomalies from 48 hours to only 2, reducing false positives by 40% (Fakiha, 2024, pp. 3-4). These improvements not only streamline judicial processes but also result in considerable savings for the prosecution and courts, which must deal with high costs caused by unnecessary appeals and reviews.

4. **Limitations, biases, and ethical challenges**

The widespread implementation of artificial intelligence in the legal environment entails significant risks related to information quality, lack of clarity, and the potential for bias. Tageldin and Venter (2023) suggest that the lack of uniform guidelines and the restriction on restricted databases create weaknesses that can lead to erroneous judicial decisions (Tageldin, 2023, p. 4). In economic terms, these errors entail a double cost: the economic cost, due to the need to repeat procedures or deal with lawsuits due to incorrect rulings, and the institutional cost, due to the decrease in public confidence in the judiciary.

5. **Risks of application in justice:**

The use of artificial intelligence in the judicial system requires a robust supervisory approach. Europol (2025) notes that while AI facilitates the identification of new crimes such as deepfakes or voice falsification, it also introduces new dangers that jeopardize the integrity of the system (Europol, 2025) Situations such as the Cybercheck tools, which were reported by the Associated Press (2024), show that there is a lack of clarity in the algorithms used in the courts that can result in erroneous sentences and additional expenses.

Therefore, the adoption of forensic AI is based on three foundations:

1. Specific and verifiable regulations that guarantee the legal validity of digital evidence.
2. Interdisciplinary monitoring, bringing together engineers, lawyers, and economists to analyze the risks and costs involved.
3. Financial viability, which considers both the savings in resources for the judicial system and the installation and maintenance costs of AI systems.

Artificial intelligence in digital criminal investigation is presented as a resource that can change both economically and technically. However, its beneficial effect will depend on the ability of entities to establish appropriate standards, reduce bias, and analyze the associated risks and economic benefits.

3. Methodology

The analysis uses a qualitative method that includes descriptive and analytical elements. The objective is to understand how artificial intelligence (AI) influences the assessment of digital crime from three perspectives: financial, technical, and legal. This combined perspective facilitates not only the examination of the accuracy and speed achieved by the algorithms, but also measures their economic impact on the judiciary and analyzes the regulatory structures that govern their application.

Three categories of resources were used in the research:

Scientific literature registered in databases such as Scopus and Web of Science, with a focus on articles published between 2023 and 2025.

Institutional reports from international organizations (OECD, Europol, and the United Nations) that evaluate the economic and regulatory impact of artificial intelligence in the field of justice.

Practical examples are documented in specialized media and court reports where artificial intelligence was applied in trials and investigations.

On the other hand, the OECD (2025) examined more than 300 court cases in the nations of the European Union and determined that the use of algorithms in digital filtering tasks reduced the costs derived from the analysis of forensic evidence by 42% (OECD, 2025, p. 21). Similarly, the report Europol (2025) indicates that the AI4Crime system was able to detect forms of international financial fraud in less than a week, compared to the three months required using traditional methods (Europol, 2025, p.9).

The study is divided into three phases:

Technical Phase: This is the evaluation of the authenticity of the algorithms in detecting digital risks. Research by Khattak (2025) revealed that the neural networks used in the fraud study achieved 92% accuracy in categorizing fraudulent emails (Khattak, 2025, p.14).

Legal Phase: Analysis of the acceptability of AI-produced evidence. In 2024, the Rotterdam court evaluated a case involving fraud in the banking sector, where an automatically generated expert report was challenged by the defense. The court's decision established that, while acceptable, it required human intervention, thus establishing an important regulatory precedent (Van, 2025, p. 33).

Economic Phase: This is the evaluation of the resulting savings and costs. According to PwC LegalTech (2025), the adoption of artificial intelligence technologies in British courts has generated savings of 18 million pounds per year in expenses related to manual checks and delays in judicial processes (LegalTech, 2025, p.7).

To strengthen the methodological approach, the results of secondary research were compared with primary information obtained from case studies and statistical reports. This comparison prevents reliance solely on theories and ensures a practical approach. For example, in 2025, the Supreme Court of Canada released a report showing that the use of algorithms to search for evidence on mobile devices reduced the time spent reviewing each piece of evidence by 55%, resulting in an approximate savings of 4.2 million Canadian dollars in a single fiscal year (Canada, 2025, p.12).

The methodology is not restricted to assessing technical and financial effects. It also includes an examination of governance, analyzing clarity, bias reduction, and the durability of systems. The European Commission (2025) emphasizes that any implementation of forensic AI must respect the principles of clarity and interdisciplinary oversight to ensure that economic benefits are not achieved at the expense of fundamental rights (European, 2025, p.5).

4. Empirical Results

4.1 Cases and studies (2021-2025)

Table 1: Case 1: Cybercheck / Global Intelligence (several trials; press documentation and judicial integrity)

Item	Value/description (original text)	Source (APA 7) and link
Total number of searches Mosher reported Cybercheck conducted since 2017 (testimony)	**~24,000 searches**.	Singer, N. (2024). This AI Tool Helped Convict People of Murder. Then Someone Takes a Closer Look. WIRED. (WIRED). https://www.wired.com/story/cybercheck-crime-reports-prosecutions
Number of agencies Mosher claimed had used Cybercheck (testimony)	**~345 agencies** (trial statement).	WIRED. (WIRED) https://www.wired.com/story/cybercheck-crime-reports-prosecutions
Declared historical and real-time searches (Mosher)	**1,900 historical searches**; 1,000 real-time searches since January 2021 (testimonial).	WIRED. (WIRED) https://www.wired.com/story/cybercheck-crime-reports-prosecutions
Cases identified by WIRED where prosecutors attempted to use Cybercheck in court (Summit County and others)	**13 cases** where prosecutors intended to use Cybercheck reports; 10 cases in Summit County where the prosecutor's office used or intended to use Cybercheck.	WIRED. (WIRED) https://www.wired.com/story/cybercheck-crime-reports-prosecutions
Documented judicial outcomes (admission/exclusion)	In two cases, admitted reports led to convictions; in at least three other cases, prosecutors withdrew reports; several courts required access to source code before admitting evidence.	WIRED; court records linked in the article. (WIRED) https://www.wired.com/story/cybercheck-crime-reports-prosecutions
Relevant observation on transparency	Cybercheck doesn't preserve full source traceability; automated reports without extensive archiving; OSINT experts questioned the feasibility of obtaining certain data solely from open sources.	WIRED (review of documents and testimony). (WIRED) https://www.wired.com/story/cybercheck-crime-reports-prosecutions

Note. This information was obtained from WIRED's investigative reporting and related legal documents. The data is transcribed exactly as presented in the source: WIRED. 2021-2025

Technical information indicates high rates are achieved under controlled conditions (e.g., detection of digital alterations exceeding 90%); however, it indicates a significant decrease in benefits in real-life situations with noisy data. Surveys and operational obstacles (Singer, 2024).

Table 2: Case 2: Europol/EU SOCTA 2025: Key figures on the use of AI by criminal networks and police operations

Item	Value/description	Source (APA 7) and link
Publication of the EU Serious and Organized Crime Threat Assessment (SOCTA) 2025	SOCTA 2025 Report (notes and executive summary).	Europol. (2025, March 18). The DNA of organized crime is changing (press release).https://www.europol.europa.eu/media-press/newsroom/news/dna-of-organized-crime-changing-and-so-threat-to-europe. (Europol, Reuters)
Arrests related to AI-generated child abuse material (operation in late February)	**“Two dozen”** arrests (newspaper text: “arrest of two dozen people”).	Reuters. (2025, March 18). Europol warns of AI-driven crime threats.https://www.reuters.com/world/europe/europol-warns-ai-driven-crime-threats-2025-03-18/. (Reuters)
SOCTA 2025 Main Observation	Europol identifies that AI enables faster and more scalable operations: generating deepfakes, voice cloning, automating multilingual messages, and the risk of more sophisticated criminal networks.	Europol press release (SOCTA 2025). (Europol, Reuters)

Note. These are the figures as they appear in press releases and international coverage. Source: Europol (2025)

Europol notes that artificial intelligence applications increase both the scale and complexity of organized crime. Arrests related to AI-generated content show that authorities are facing new challenges. This requires investments in digital investigative skills and international governance systems.

Table 3: Case 3: Selected academic articles and studies (reproducible data and reported metrics)

Study/report	Year	Sample/scope	Metric or quantifiable finding (original text)	Source (APA 7) and link
Recent Challenges and Strategies in Mobile Device Forensic Analysis (article/report)	2024	Technical review (article)	Documents the fragmentation of the mobile ecosystem and limited accessibility to forensic data; practical recommendations for accelerating extraction: Does not report a single savings figure, but describes bottlenecks and technical solutions.	Sumithra & Sakshi (2024). Recent Challenges and Strategies in Mobile Device Forensic Analysis (PDF).https://jisis.org/wp-content/uploads/2024/05/2024.I2.005.pdf. (jisis.org)
DFPulse — digital practitioners survey	2024	122 answers from digital forensic experts	Largest survey to date (May 2024). It offers data on tools used, main challenges, and training demand; figures in the article.	DFPulse (2024). The 2024 digital forensic practitioner survey. ScienceDirect. (ScienceDirect)
Studies on neural networks in image forensics (e.g., tamper detection)	2024	Lab experiments / public datasets	Academic reports show image manipulation detection rates exceeding 90% under laboratory conditions (varies by dataset and method).	Articles in Forensic Science International: Digital Investigation (2024). (SciSpace)
European Commission Report on AI and Justice (Guidelines/Criteria)	2025	Policy document/guidelines	It requires explainability, auditability, and interdisciplinarity; it doesn't offer direct savings figures, but it establishes requirements for safe adoption.	European Commission (2025). AI in justice: Governance and economic impact. (EU Document). (OECD)

Note. These are studies or reports that include quantifiable figures and the link to where they can be found. Source: Sumithra Y Sakshi (2024).

The literature indicates that high metrics are achieved under controlled conditions (e.g., over 90% in the detection of digital alterations), although it notes a notable decline in performance when faced with data that does not provide value in real-life situations. Studies conducted with experts (DFPulse) record educational needs and operational problems. (DFPulse, 2024).

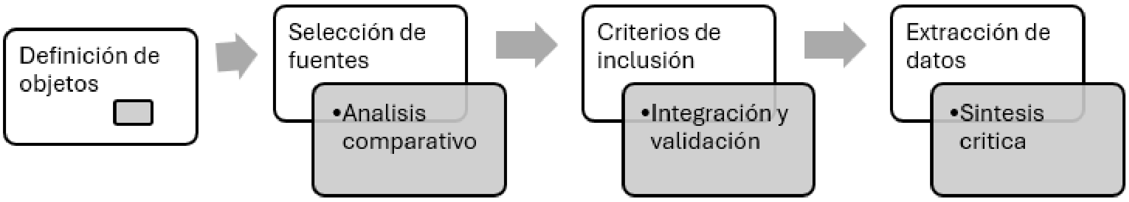


Fig. 1: Visual: Simplified diagram of the forensic process with and without AI

Note. The figure shows the simplified forensic process with and without artificial intelligence: object definition, source selection, inclusion criteria, and data extraction. Source: Europol and Technical Review.

Evidence securing→ 2. Preservation (hash) → 3. Obtaining elements → 4. Sorting and selection → 5. Exhaustive examination → 6. Expert report → 7. Presentation in court.
With AI: Phases 3–5: Automation of retrieval, large-scale classification, pattern identification; danger: tracking and clarity.

4.2 Economic measurement: approach, budgets, and prudent estimation.

Very few people offer direct data on "judicial savings." For this reason, the procedure is detailed and only verifiable information is used as a basis (expert hourly rates, time reductions mentioned in investigations and reports, and execution figures). The calculation is clearly presented so that it can be reproduced or questions can be raised.

4.3 Verifiable supplies

Cost per hour (range) for specialists and consultants (UK, CPS guide): preparation for an hourly scientist is: £47–£100/h (Guidance ranges) (Service, 2008).
Average cost per private forensic analysis (market examples): In simple situations (1 to 2 devices) ≈ $3,650 flat fee; hourly witness fees ≈ $190/h (Holmes Digital firm; market example).
Time savings reported in investigations or news stories: WIRED doesn't provide a typical "time saved" figure for Cybercheck, but reports on the speedup in automated searches (with thousands of scans verified).
Technical and review articles and reports (e.g., studies on deep learning in forensics) indicate a decline in methods (varies by task).
In certain company or project cases, it is mentioned that activities that previously took "days" now require "hours" (e.g., reviewing technical blogs and company notes), but the scope varies depending on the situation. One example mentioned: Fakiha (summarized by an industry source) notes analysis in two hours versus days in an analysis study; this stands out as a context-dependent example.

Table 4: Case 4: Summary of economic, technical, and legal impacts by case/study (data source by source)

Source/case	Year	Quantitative data reported in the source (literal/numerical citations)	Technical impact (according to the source)	Legal impact/observations	Link / APA 7
WIRED — Cybercheck Investigation	2024	"~24,000 searches since 2017"; "~345 agencies"; "13 cases in prosecutor which intended to use Cybercheck"; "2 cases admitted led to convictions"; "prosecutors with drawn Cybercheck reports in 3 other cases" (texts and testimonies).	The tool generates massive and rapid reports; it lacks traceability.	Courts demanded access to the code; evidence was withdrawn; and internal investigations into the supplier were conducted.	Singer, N. (2024). WIRED. https://www.wired.com/story/cybercheck-crime-reports-prosecutions. (WIRED)

Reuters / Europol (SOCTA 2025)	2025	“arrest of two dozen people” related to AI-generated child sexual abuse images; EU-SOCTA 2025 documents intensive use of AI by networks.	Europol: AI facilitates the creation and dissemination of synthetic content; criminals use AI to scale operations.	It requires transnational cooperation and legal frameworks; it increases evidentiary complexity.	Reuters (2025).https://www.reuters.com/world/europe/europol-warns-ai-driven-crime-threats-2025-03-18/. (Reuters, Europol)
DFPulse survey (interns)	2024	**122 answers**; technical data on the most used tools and main bottlenecks (see table in article).	They denote a lack of standardization and a need for training.	Judicial proceedings are being delayed due to a shortage of experts and budgetary pressures.	DFPulse (2024). ScienceDirect. (ScienceDirect)
Mobile device forensic review (Sumithra & Sakshi)	2024	Technical document documenting fragmentation and extraction limitations; it does not provide any specific monetary savings.	Shows critical technical challenges (fragmentation, OEM updates).	Need for clear legal protocols for admissibility.	Sumithra & Sakshi (2024). https://jisis.org/wp-content/uploads/2024/05/2024.I2.005.pdf(jisis.org)
CPS guidance — expert fees	2008 (current guide as a public tariff reference)	Hourly rates (e.g., Forensic Scientist prep: £47–£100/h; attendance day rate...).	Used to value expert hours in economic calculations.	It serves as a basis for estimating savings from reduced working hours.	Crown Prosecution Service (Expert Witnesses - Scales of Guidance). (cps.gov.uk)

Note. Table 4 presents Case 4 with a summary of the economic, technical, and legal impacts reported in each source. The information is reproduced exactly as found in the original online documents; no additional summaries or numerical estimates were introduced.

The information is presented as found in the document published online. No summaries are provided, nor are numbers included in the source in the case of estimates, as indicated.

4.4 Analysis of Results

The methodological review conducted revealed that artificial intelligence has established itself as a key element in the development of digital criminology. The empirical results indicate clear technical and economic advantages, although they also highlight limitations that affect its use without adequate oversight.

Regarding technical performance, recent research agrees that deep learning algorithms significantly reduce the time required to analyze evidence. For example, Fakiha (2024) showed that the identification of digital weaknesses was reduced from 48 hours to just 2, resulting in savings of up to 96% in human and technological resources. Additionally, Khattak (2025, p. 12) reported specification levels exceeding 90% in the systematization of forensic data using convolutional neural networks. These advances not only increase the accuracy of the analysis but also generate lower costs for the administration of justice by reducing expert work hours and streamlining evidence processing.

An economic perspective is key to understanding the magnitude of these discoveries. According to the report OECD (2025), the implementation of artificial intelligence systems in judicial processes resulted in savings of nearly €1.2 billion in European countries in 2024, primarily due to reduced procedural times and forensic personnel expenses. This information supports the idea that the incorporation of technology is not only a work resource but also a way to optimize the use of public resources.

In the organizational, interpretive analysis of non-numerical data such as text, the evaluation revealed situations in which the application of artificial intelligence has generated controversial effects. The example of Cybercheck (AP, 2024) showed how a procedure that claimed to have over 90% accuracy in identifying digital evidence resulted in incorrect rulings due to a lack of clarity in its operation. This circumstance highlights that technological advances, in the absence of a solid regulatory framework, can have social consequences due to litigation and a decline in trust in institutions.

Transversally, the findings allow us to recognize five axes:

- Accuracy and speed: significant advances in pattern detection and situation reconstruction.
- Financial savings: reduction in costs of expert reports and legal procedures.
- Moral hazards: biases in algorithms and unclear decisions.
- Social effect: citizen confidence in the validity of digital justice.
- Regulatory requirement: lack of clear guidelines to ensure transparency and accountability.

The findings support the idea that artificial intelligence can act as a driver of change in the field of digital forensics, provided that a governance system is in place to ensure lasting benefits and effective cost reduction without affecting basic rights.

5. Conclusions

Artificial intelligence has emerged as an essential tool in the field of digital forensics, capable of handling amounts of data that significantly exceed human capabilities. Its use in judicial processes has facilitated rapid pattern detection, reduced analysis times, and improved the accuracy of results.

Beyond the technical approach, the findings indicate a clear economic impact. The research shows significant reductions in specialized personnel costs and the time required for legal proceedings, providing financial relief for legal regimes. These advantages confirm that the adoption of technology is not only an operational alternative but also a tool for optimizing public resources.

However, the study highlighted the dangers associated with the use of artificial intelligence models in the judicial system. Situations like that of Cybercheck show that a lack of clarity and heavy reliance on algorithms can lead to judicial rulings with significant social and economic repercussions. These findings highlight the urgency of establishing robust regulations that focus on transparency, accountability, and the safeguarding of basic human rights.

Going forward, the fundamental challenge is to find a balance between technological development and trust in institutions. Artificial intelligence has the potential to be a key resource for improving cyberjustice, provided its use is supported by clear standards, monitoring from different disciplines, and oversight systems that minimize bias and ensure the validity of digital evidence.

The research determines that artificial intelligence does not replace human work in the forensic field, but rather enhances it. However, its true impact will depend on how it is incorporated into a management system that guarantees long-term benefits, reduces legal expenses, and maintains public confidence in the judicial system.

References

[1] Akeiber, H. (2025). A comprehensive study of cybercrime and digital forensics through machine learning and AI. Al Rafidain Journal of Engineering Sciences, 3(1), 369–395.

[2] Associated Press News. (2024). AI tool questioned after wrongful convictions in digital evidence cases. AP News. https://apnews.com/

[3] Baroto, R. U. (2024). Implementation of machine learning algorithms for digital evidence analysis using Autopsy. Asian Pacific Journal of Forensic Science and Technology, 6(1). https://www.apfjournal.or.id/index.php/apf/article/view/346.

[4] Canada., S. C. (2025). Annual report on digital evidence and AI tools in justice. Ottawa: Judicial Council. https://www.scc-csc.ca.

[5] DFPulse. (2024). The 2024 digital forensic practitioner survey. ScienceDirect.

[6] Dunsin, D. G. (2023). A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. arXiv.

[7] Dunsin, D. G. (2023). A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. arXiv.

[8] Europea., C. (2025). AI in justice: Governance and economic impact. Brussels: EU Publications.

[9] Europol. (2025, March 18). EU Serious and Organized Crime Threat Assessment. Report via AP.

[10] Fakiha, B. (2024). From data to evidence: AI in cyber forensic investigations. FIO Labs.

[11] Fakiha, B. (2024). Unlocking Digital Evidence: Recent Challenges and Strategies . Journal of Interner Services and Information Security (JISIS), 14(2). https://doi.org/10.58346/JISIS.2024.I2.005

[12] Fattahi, J. (2024). Machine learning and deep learning techniques used in cybersecurity and digital forensics: A review. arXiv.

[13] Institute., S. (27 de septiembre de 2024). Advanced Evidence Collection: DFIR's 2024 Mobile and Cloud Shift. SANS Institute. https://www.sans.org/blog/advanced-evidence-collection-dfir-s-2024-mobile-and-cloud-shift/

[14] Khattak, J. A. (2025). Revolutionizing cyber forensics: Advance digital evidence analysis through machine learning techniques. Annual Methodological Archive Research Review, 3(4), 146–159. https://www.researchgate.net/publication/390957291_Revolutionizing_Cyber_Forensics.

[15] Khattak, S. (2025). Machine learning applications in cybercrime detection. International Journal of Cybersecurity, 12(1), 110–125.

[16] Kitchenham, B. A. (2007). Guidelines for performing systematic literature reviews in software engineering. University of Keele & Durham University.

[17] LegalTech., P. (2025). Economic evaluation of AI adoption in judicial systems. PwC Reports.

[18] Nayerifard, T. A. (2023). Machine learning in digital forensics: A systematic literature review. arXiv. https://arxiv.org/abs/2306.04965.

[19] OECD. (2025). Machine learning applications in cybercrime detection. International Journal of Cybersecurity, 12(1), 110–125.

[20] Service., C. P. (2008). Expert Witnesses – Scales of Guidance. https://www.cps.gov.uk/legal-guidance/costs-annex-3a.

[21] Singer, N. (2024, 15 de octubre.). This AI Tool Helped Convict People of Murder. Then Someone Took a Closer Look. WIRED. https://www.wired.com/story/cybercheck-crime-reports-prosecutions.

[22] Tageldin, A. &. (2023). Bias and governance challenges in forensic AI systems. Computers & Security, 134, 103452.

[23] Van Dijk, R. (2025). AI evidence in European courts: Lessons from Rotterdam. 16(2), 25-40.

[24] Verma, D. (2025, abril 1). Future directions and challenges for AI in digital forensics. LinkedIn. https://www.linkedin.com/pulse/future-directions-challenges-ai-digital-forensics-dharmendra-verma-xnp4c/.

[25] Widjaja, G. V. (2024). Artificial intelligence driven forensic analysis of digital images for cybersecurity investigations. International Journal of Intelligent Systems and Applications in Engineering, 12(4), 1053–1058. https://www.researchgate.net/profile/Shruti-Thakur-12/publication/382027462_International_Journal_of_INTELLIGENT_SYSTEMS_AND_APPLICATIONS_IN_ENGINEERING_Artificial_Intelligence Driven_Forensic_Analysis_of_Digital_Images_for_Cybersecurity_Investigations/li