ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

Gaps in Global Governance for AI-Assisted Cross-Border Cloud Forensics and the Imperative for the Multi-Jurisdictional Investigative Protocols for AI-Informed Digital Evidence (MIP-AIDE) Framework

***Francis Chidiebele Ekwempu**

Unizik Business School, NAU, Nigeria

DOI: https://doi.org/10.51583/IJLTEMAS.2026.150500068

Received: 30 April 2026; Accepted: 04 May 2026; Published: 01 June 2026

ABSTRACT

The rapid globalization of digital services has made international cloud data transfers essential, yet these processes frequently collide with divergent regional privacy regimes, such as the conflict between the U.S. CLOUD Act (Clarifying Lawful Overseas Use of Data Act) and the European Union's General Data Protection Regulation (GDPR). Current cross-border evidence acquisition relies on slow Mutual Legal Assistance Treaties (MLATs) or fragmented extraterritorial laws that often bypass data sovereignty. Furthermore, the integration of artificial intelligence (AI) in forensics introduces "black box" opacity, which threatens the admissibility of digital evidence and undermines due process. This research addresses these structural failures by proposing the MIP-AIDE framework to unify jurisdictional and AI accountability standards.

Objectives

The primary objectives are to design a tiered procedural protocol that computationally embeds international compliance rules to resolve extraterritorial conflicts; define technical standards that translate forensic AI outputs into judicial admissibility criteria, such as error rates and bias audits; and innovate a governance paradigm that integrates Cloud Service Providers (CSPs) as auditable partners in the legal process.

Methods

This project employs a mixed-method approach consisting of three phases: (I) doctrinal legal analysis and benchmarking of international standards like the Daubert and Mohan criteria; (II) a technical review of Explainable AI (XAI) techniques like SHAP and LIME; and (III) Design Science Research (DSR) to synthesize these findings into the MIP-AIDE framework.

Results

The framework delivers three core components: a Legal Gateway Decision Matrix for automated compliance checking; Minimum Technical Explanatory Requirements (MTERs) to package AI outputs into court-admissible artefacts; and a Collaborative Stewardship Model using Service Level Agreements (SLAs) to formalize the role of CSPs.

Conclusions

MIP-AIDE closes the protocolization, AI-admissibility, and non-state actor governance gaps. By providing a concrete, computable solution, the framework ensures that AI-assisted forensics achieve the speed, transparency, and legitimacy required for 21st-century digital justice.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

Keywords: MIP-AIDE Framework, Cloud Forensics, Cross-Border, Explainable AI (XAI), Collaborative Stewardship

INTRODUCTION

The swift progression of digital globalization has rendered international cloud data transfers indispensable for multinational organizations. However, these transfers increasingly conflict with divergent privacy and data protection regimes, most notably between the United States and regions like the European Union (Patterson, 2025). This tension underscores the need to ensure that digital evidence from the cloud is obtained swiftly, legally, and in a forensically sound manner, particularly when AI is involved.

The borderless nature of cloud data paralyzes cross-border evidence access, often relying on the U.S. CLOUD Act or slower mechanisms like Mutual Legal Assistance Treaties (MLATs) (Perault & Salgado, 2024). Concurrently, the "black box" opacity of AI tools in data analysis undermines due process, rendering critical digital evidence inadmissible in courts (Dou & Dou, 2025). This article proposes the Multi-jurisdictional Investigative Protocols for AI-Informed Digital Evidence (MIP-AIDE) framework as a unified governance solution to these jurisdictional and AI accountability challenges.

The MIP-AIDE Protocol replaces fragmented legal and technical standards with a comprehensive model, delivering key outcomes: a Legal Gateway Decision Matrix to navigate conflicts (e.g., CLOUD Act vs. GDPR), Minimum Technical Explanatory Requirements (MTERs) for standardizing AI evidence admissibility, and a Collaborative Stewardship Model incorporating Cloud Service Providers (CSPs) for accelerated evidence disclosure. This framework advances interdisciplinary knowledge in law, forensics, and XAI.

Objectives

a) To design a tiered, procedural protocol that computationally embeds international compliance rules, resolving conflicting extraterritorial access demands (e.g., CLOUD Act vs. GDPR) and ensuring rapid, legally sound acquisition.
b) To define a technical standard that translates the outputs of forensic AI (error rates, feature importance, bias audit reports) into the specific criteria required for judicial admissibility (e.g., the Daubert standard).
c) To innovate a governance paradigm that formally integrates Cloud Service Providers (CSPs) as auditable, responsible partners in the legal process.

Current Challenges in Cross-Border Forensics

Cloud forensics faces a complex set of challenges, stemming from both technical and institutional sources. These challenges affect data acquisition, preservation, analysis, privacy, and legal compliance (Alenezi, 2023). Multi-layered frameworks, encompassing technical, legal, and institutional dimensions, have been suggested to support forensic readiness and intellectual property protection, concurrently fostering cross-sector collaboration (De & Chakraborty, 2025). Nevertheless, these models are largely theoretical and do not provide operational protocols that can reconcile conflicting legal requirements with the demands of real-time cloud forensics.

Jurisdictional Conflict: Law vs. Location

The tension between territorial sovereignty and extraterritorial data access lies at the heart of contemporary scholarship. The landmark United States v. Microsoft Corp. (2013–2018) case illustrated the limits of traditional jurisdiction when U.S. authorities' requests for data held in Ireland instigated a significant change (Lather et al., 2025). The ensuing CLOUD Act of 2018 redefined jurisdictional boundaries, prioritizing provider control over data location (Patterson, 2025). This approach allowed for the creation of bilateral agreements, which avoided the lengthy processes often associated with Mutual Legal Assistance Treaties (MLATs). These treaties can be time-consuming, sometimes taking more than ten months to complete (Perault & Salgado, 2024). Although these mechanisms facilitate expedited access, they simultaneously generate direct conflicts with data-localization policies implemented in other regions, most notably within the European Union.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

European academic discourse highlights the GDPR's emphasis on accountability, while simultaneously acknowledging its limitations in fully safeguarding users from data misuse by platforms like Android and iOS (Ucar & Yalcintas, 2023). Article 48 explicitly forbids data transfers predicated solely on third-country directives, such as those stemming from the CLOUD Act, unless they are supported by international accords (Voigt & von dem Bussche, 2024). This creates a persistent "compliance dilemma," wherein the extraterritorial scope of U.S. Legal frameworks can conflict with EU data sovereignty (Amoo et al., 2024). Moreover, comparative studies show that these different regulatory systems hinder the efficient gathering of evidence in international investigations.

The AI-Admissibility Challenge: Opacity vs. Integrity

A growing body of work warns that AI-informed evidence must satisfy thresholds of integrity, authenticity, reliability, and methodological transparency to be judicially admissible (Okunrobo Perez, 2025). Concerns include authenticity, tampering prevention, chain of custody, and methodological transparency, potentially extending trials (Gentry, 2024). Traditional chain of custody practices, which are system-focused and infrastructure-driven, need to be improved to better serve digital forensics (Nath et al., 2024). In Nigeria, for instance, the admissibility of AI-generated evidence is complicated by the stipulations of the Evidence Act (Orji, 2024). AI may yield errors from biases or opacity, threatening fair trials (ALF, 2025). Furthermore, global legal cases, including those involving self-driving vehicles, illustrate how the absence of established standards can impede judicial processes (UNESCO, 2023). Consequently, conventional chain-of-custody protocols, which were developed for physical evidence, are insufficient for managing AI-generated digital outputs.

Governance and Non-State Actor Exclusion

Algorithmic accountability research highlights the potential for "black box" systems to undermine defendants' rights and due process (Dou & Dou, 2025). Algorithmic transparency detects discrimination and complies with data security, aligning obligations with standards (Zharova, 2023). A cloud governance framework integrates AI automation, security, and compliance for risk management (Folorunso et al., 2024). Inadequate international collaboration, varying frameworks, and judicial misunderstandings hinder progress (Olber, 2021). Further study, examines the ethical and regulatory aspects of Explainable Artificial Intelligence (XAI), proposing standardised methods to guarantee fairness, accountability, and compliance with rules in AI implementation (Chinnaraju, 2025).

Moreover, Current cross-border legal solutions primarily emphasize state-to-state mechanisms like MLATs and CLOUD Act agreements (Perault & Salgado, 2024). But both agreements overlook the pivotal role of Cloud Service Providers (CSPs) as key gatekeepers of evidence (Chivers, 2019). However, MIP-AIDE will develop service-level agreements (SLAs) and governance integrating CSPs, resolving compliance dilemmas.

However, the existing body of research reveals three significant shortcomings:

- A lack of operational guidelines for balancing extraterritorial obligations with the safeguarding of national sovereignty, referred to as the protocolization gap;
- The absence of uniform technical standards for the judicial validation of AI-generated evidence, referred to as the AI-admissibility gap;
- The exclusion of CSPs from governance frameworks, despite their crucial function as data custodians, which constitutes the non-state actor governance gap.

The identified weaknesses directly relate to the challenges mentioned in this paper, thus confirming the limitations of fragmented national or bilateral approaches.

RESEARCH METHODOLOGY

The research project will use a mixed-method approach incorporating doctrinal legal analysis, analytical benchmarking, and design science research (DSR).

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

Phase I: Legal and Regulatory Mapping

The analysis will compare the U.S. Daubert Standard with common law approaches like Canada's Mohan criteria (Macturk et al., 2025).

Phase II: Technical requirements for AI systems

The project will review state-of-the-art Explainable AI (XAI) techniques like SHAP and LIME to determine their effectiveness in producing human-readable explanations (Chinnaraju, 2025).

Phase III: Synthesis and Protocol Development

The final phase will employ Design Science Research (DSR) to create and validate a core research artefact. It will involve integrating legal and regulatory mappings, as well as technical requirements for AI systems, into the MIP-AIDE framework. A model will be established for collaborative stewardship to define roles and standard Service Level Agreements (SLAs) for law enforcement and Cloud Service Providers. The framework will be validated through simulated case studies focused on multi-jurisdictional cloud crime scenarios, assessing legal compliance and operational feasibility.

Proposed Position: The MIP-AIDE Framework

The MIP-AIDE framework offers a solution to these limitations by synthesizing current research within a unified, interdisciplinary governance model. This framework moves beyond theoretical models to provide operational protocols that reconcile conflicting legal requirements with real-time forensic demands. Jurisdictional harmonization will be supported as follows;

Legal Gateway Decision Matrix

It will provide procedural protocol that computationally embeds international compliance rules, resolving conflicting extraterritorial access demands (e.g., CLOUD Act vs. GDPR) and ensuring rapid, legally sound acquisition.

A rule engine or basic decision-support system that uses computers to add specific limits based on the laws of different areas, such as CLOUD Act qualifiers, GDPR Article 48 exceptions, and data localization laws. Input parameters include requesting jurisdiction, data location, CSP jurisdiction, offense classification, and urgency tier. Output is a binary-compliant path plus required safeguards (e.g., “CLOUD Act route permitted only with bilateral agreement and GDPR equivalent safeguards”). The matrix can be expressed as a deterministic finite automaton or encoded in a policy language (e.g., XACML or Rego), enabling automated pre-request compliance checking by CSPs.

Hence, this example demonstrates that the matrix not only identifies legal barriers but also actively directs requests along compliant procedural pathways, ensuring both access to evidence and regulatory compliance.

Hypothetical Scenario

To demonstrate the practical feasibility of the Legal Gateway Decision Matrix, a core component of the MIP-AIDE framework, below is a **hypothetical investigation** involving a U.S. federal request for data hosted in France. The matrix functions as a rule engine or decision-support system that computationally embeds international compliance rules to resolve conflicting extraterritorial access demands. This approach not only identifies legal barriers but also actively directs requests along compliant procedural pathways, ensuring both access to evidence and regulatory compliance.

Phase 1: Input Parameters

In this scenario, a U.S. law enforcement agency requires evidence stored on a cloud server located in France. The following parameters are fed into the matrix:

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

1. **Requesting Jurisdiction:** United States.
2. **Data Location:** France (European Union).
3. **CSP Jurisdiction:** United States (e.g., a major U.S. Cloud Service Provider).
4. **Offense Classification:** Serious Crime (e.g., Organized Cybercrime).
5. **Urgency Tier:** High (Emergency access required).

Phase 2: Matrix Evaluation Logic

The matrix evaluates the inputs against specific legal constraints identified in the **"Gaps in Global Governance for AI-Assisted Cross-Border Cloud Forensics."**.

Evaluation Criteria	Legal / Regulatory Logic Applied	Outcome/Constraint
Offense Classification	Is the crime serious enough to justify extraterritorial access?	**Pass:** The "Serious Crime" classification meets the standard for international evidence acquisition.
GDPR Article 48	Does the request rely solely on a third-country directive (e.g., U.S. CLOUD Act warrant)?	**Conflict:** Article 48 forbids transfers based solely on third-country directives unless supported by an international accord.
CLOUD Act Bilateral Status	Is there an active bilateral agreement between the U.S. and the EU/France?	**Conditional:** Access depends on the existence of a formal executive agreement to bypass slow MLAT processes.

Phase 3: Binary-Compliant Output

The matrix generates a specific procedural path and required safeguards:

Decision

Conditional Permission:

- **Primary Path:** CLOUD Act route is permitted **only if** a bilateral agreement is in place.
- **Required Safeguards:** The data transfer must include **GDPR equivalent safeguards** to ensure regulatory compliance.
- **Technical Mandate:** Any AI-assisted forensics used to analyze the retrieved data must produce **Minimum Technical Explanatory Requirements (MTERs)**, such as error-rate bounds and bias-detection reports, to ensure judicial admissibility.

Final Routing Decision:

Proceed via MLAT request through French authorities

Minimum Technical Explanatory Requirements (MTERs)

It will define and provide verifiable XAI technical standard that translates the outputs of forensic AI (error rates, feature importance, bias audit reports) into the specific criteria required for judicial admissibility, and mandates every forensic AI output to include: Error-rate bounds and confidence intervals; Feature-importance heatmaps

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

with audit trails; Bias-detection reports against protected attributes; Chain-of-custody metadata linking model version, training data provenance, and inference timestamp.

These artifacts will be packaged in a standardized JSON-LD or forensic container format (Patel, 2025). It will give Judges room to assess reliability without requiring AI expertise. MTERs convert the “black box” into a court-admissible artifact.

The MIP-AIDE framework defines Minimum Technical Explanatory Requirements (MTERs) as a verifiable XAI technical standard. These translate the outputs of forensic AI; such as error rates, feature importance, and bias audit reports into the specific criteria required for judicial admissibility for various standards such as the Daubert standard in the U.S., Mohan criteria in Canada, or equivalent reliability thresholds in other jurisdictions (Bhan et al., 2025). MTERs mandate that every forensic AI output package must include the following standardized, machine-readable, and human-interpretable artefacts. These are packaged in a standardized format such as JSON-LD (Giardiello & Turchi, 2023). This packaging enables judges and opposing counsel to assess reliability without requiring deep AI expertise.

Performance Reliability Metrics

To ensure the AI tool's findings are statistically sound, the following thresholds are required:

- **Acceptable Error-Rate Thresholds:** The system must maintain a **False Positive Rate (FPR) ≤ 5%** for classification tasks, as higher error rates may undermine the "beyond reasonable doubt" standard in criminal proceedings.
- **Statistical Confidence Levels:** Forensic AI outputs must be accompanied by a **95% Confidence Interval (CI)**. This provides judges with a measurable range of certainty for the AI’s inference.
- **Sensitivity and Specificity:** Tools must report a minimum **Recall (Sensitivity) of 90%** to ensure that critical evidence is not missed during automated cloud forensic sweeps(Nsor & Bakare, 2025).

Mandatory Bias Audit Dimensions

Algorithmic discrimination poses risks to due process and equal protection, necessitating periodic bias audits for forensic AI. These audits must assess various attributes, such as nationality, ethnicity, gender, and socioeconomic status. The key metrics include disparate impact ratios and false-positive rates, with a 10% variance disparity threshold. If significant bias is found, automated outputs require human review and reduced evidentiary weight. Furthermore, bias records must detail dataset composition and mitigation strategies to uphold fairness and anti-discrimination across jurisdictions.

Bias audits must be conducted and reported against protected attributes to ensure fairness and prevent discriminatory outcomes. Audits should follow frameworks such as NIST AI Risk Management or EU AI Act high-risk system requirements (Md Fokrul Islam Khan, 2025).

To avoid discriminatory outcomes that could violate due process, the AI has to be subjected to automated audits in three specific dimensions:

- Protected Attributes: Audits should test for unequal impacts by national origin, race, and gender to ensure the model’s “feature importance” is not a proxy for protected groups.
- Dataset Representation: The report must contain a class distribution ratio to show that the AI was trained on data reflective of the investigation environment.
- Fairness Metrics: Evidence packets should include equalised odds or demographic parity scores to ensure the AI treats all population subsets equally.
- Disparate Impact: This should fall between 0.8 to 1.25(Anand et al., 2026).

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

Minimum Metadata for Chain of Custody

To maintain integrity, authenticity, and provenance (extending traditional chain-of-custody practices to AI artefacts), the following minimum metadata fields are required. These should be cryptographically signed (e.g., using SHA-256 hashes or digital signatures) and timestamped with qualified electronic timestamps.

a) **Model Identification:** Name/version, architecture, developer/provider, summary of training data provenance (dataset name, size, source, date of collection).

b) **Inference Details:** Inference timestamp (timezone and precision), input data hash (pre-processing), output data hash, and compute environment (hardware/software stack).

c) **Version Control & Changes:** Commit history or change logs for model weights, hyperparameters, and code, such as in Git.

d) **Custody Trail:** Custodian(s) at each step (CSP, investigator, and analyst), transfer timestamps; access logs; and actions taken.

e) **Integrity verification:** A cryptographic hash of raw input data, processed data, model output, and explanatory artefacts. Any changes are marked with a reason.

f) **Audit & Compliance:** Bias audit report hash, error rate validation report, XAI method utilised (e.g., SHAP values, LIME explanations), human reviewer ID (if appropriate).

g) **Jurisdictional Tags:** Relevant legal frameworks (e.g., GDPR compliance flags) and MIP-AIDE Legal Gateway Matrix output reference.

The Collaborative Stewardship Model

It leverages CSP expertise via formal service-level agreements (SLAs) to provide a governance paradigm that formally integrates Cloud Service Providers (CSPs) as auditable, responsible partners in the legal process. The SLAs between law enforcement agencies and CSPs will designate CSPs as “auditable stewards.” Obligations include real-time MTER generation, preservation of raw logs, and participation in joint transparency audits. CSPs gain legal safe harbor when they comply with MIP-AIDE protocols; investigators gain predictable, forensically sound access.

The MIP-AIDE's approach, therefore, not only resolves the existing conflicts between the CLOUD Act and GDPR, but also redefines how we understand international digital justice. The use of faster methods for gathering evidence across borders makes the process more efficient, compliant, and transparent.

To transition the **MIP-AIDE Collaborative Stewardship Model** from a theoretical concept to a realistic governance framework, the role of Cloud Service Providers (CSPs) must be formalized through rigorous contractual and legal parameters. This model positions CSPs as "auditable stewards" rather than passive data hosts.

SLA Template: Forensic Readiness & Response

The Service Level Agreement (SLA) between Law Enforcement Agencies (LEAs) and CSPs defines the operational benchmarks for evidence disclosure.

- **Evidence Provisioning Latency:** CSPs must fulfill data preservation requests within **4 hours** and full disclosure (following Legal Gateway Matrix approval) within **24–48 hours** for "Urgency Tier 1" cases.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

- **MTER Generation Guarantee:** CSPs are contractually obligated to provide the **Minimum Technical Explanatory Requirements (MTERs)**, including error rates and bias audits, alongside any AI-analyzed data.

- **Uptime for Legal Gateways:** The automated compliance rule engine (Decision Matrix) must maintain **99.9% availability** to prevent investigative delays.

- **Standardized API Access:** CSPs must provide a secure, auditable API endpoint for the transmission of forensic containers (JSON-LD) to ensure data integrity.

Audit Logs and Transparency Reports

To bridge the "non-state actor governance gap," the model mandates high-fidelity record-keeping.

- **Real-Time Preservation Logs:** CSPs must maintain immutable logs of all access to target data, including model versions used for analysis and the identity of the requesting officer.

- **Joint Transparency Audits:** Annual third-party audits must verify that CSPs are applying the **Legal Gateway Decision Matrix** correctly and not bypassing GDPR Article 48 constraints.

- **Public Aggregate Reporting:** Semi-annual reports must disclose the volume of requests received, the percentage of requests denied by the MIP-AIDE matrix, and the average response times, categorized by jurisdiction.

Safe Harbor Conditions

To incentivize cooperation, the framework provides CSPs with legal protection when they adhere strictly to MIP-AIDE protocols.

- **Conflict-of-Law Immunity:** CSPs gain "Legal Safe Harbor" from domestic privacy lawsuits if they can prove the data transfer was authorized by the **Legal Gateway Decision Matrix**.

- **Good Faith Disclosure:** CSPs are protected from liability for "wrongful disclosure" if the automated MTERs provided meet the mandated technical standards at the time of transfer.

- **Standardized Compliance Defense:** Adherence to MIP-AIDE serves as prima facie evidence of "forensic due diligence" in both U.S. and EU courts.

Penalties for non-compliance

To ensure accountability, the model enforces a tiered penalty structure for failures in stewardship.

Failure Category	Description	Penalty/Consequence
Integrity Breach	Failure to provide accurate MTERs or chain-of-custody metadata.	Immediate suspension of Safe Harbor status for the specific investigation.
SLA Latency	Repeated failure to meet the 24 through 48-hour disclosure window.	Liquidated damages as specified in the SLA; potential downgrade in "Trusted Provider" status.
Unauthorized Transfer	Bypassing the Decision Matrix and violating GDPR Article 48.	Heavy financial sanctions (aligned with GDPR's 4% global turnover cap) and potential revocation of operational licenses in that jurisdiction.
Transparency Failure	Concealing logs or failing annual audits.	Mandatory "Corrective Action Plan" overseen by an international judicial ombudsman.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

By integrating these components, the **MIP-AIDE** framework moves beyond state-to-state treaties (MLATs) to include the actual custodians of digital evidence, the CSPs as responsible partners in the pursuit of digital justice.

Addressing the Governance Gaps:

The MIP-AIDE framework is designed to close three critical deficiencies identified in current literature:

a) The Protocolization Gap: It provides the missing operational guidelines for balancing extraterritorial data access with national sovereignty.
b) The AI-Admissibility Gap: It establishes uniform technical standards for validating AI-generated evidence in court.
c) The Non-State Actor Governance Gap: It includes CSPs, who are the real data custodians in the governance framework. This makes sure that their roles and responsibilities are clear when it comes to data protection and following the law.

CONCLUSION

The protocolization gap, AI-admissibility gap, and non-state actor governance gap are no longer tolerable side effects of technological progress; they are structural failures that undermine the rule of law in the cloud era. The MIP-AIDE framework offers a concrete, computable, and interdisciplinary solution that can be prototyped, evaluated, and incrementally standardized. We therefore call upon the computer science community, researchers, standards bodies, and industry to prioritize the development, open-source release, and empirical validation of MIP-AIDE components. Only through such deliberate engineering can AI-assisted cross-border cloud forensics deliver the speed, transparency, and legitimacy that 21st-century digital justice demands.

REFERENCES

1. Alenezi, A. M. (2023). Digital and cloud forensic challenges. arXiv preprint arXiv:2305.03059.
2. ALF. (2025). Underlying Risks of Using AI-Generated Evidence in Nigeria's Justice System. Alliance Law Firm. https://alliancelawfirm.ng/underlying-risks-of-using-ai-generated-evidence-in-nigerias-justice-system/
3. Amoo, O. O., Atadoga, A., Osasona, F., Abrahams, T. O., Ayinla, B. S., & Farayola, O. A. (2024). GDPR's impact on cybersecurity: A review focusing on USA and European practices. International Journal of Science and Research Archive, 11(1), 1338-1347.
4. Anand, S., Gopinath, A., & Periyasami, K. (2026). Evaluating Bias Detection and Mitigation Approaches Across Classical and Large Language Models. IEEE Access, 14, 35074–35095. https://doi.org/10.1109/ACCESS.2026.3669650
5. Bhan, S., Kumar, D. N., Singh, D. V. P., Gope, D. S., Aqib, D. M., Barman, D. P., Joshi, N. V., & Saikia, D. P. R. (2025). Challenges In Admissibility Of Forensic Evidence: A Comparative Analysis Of Legal Standards Across Jurisdictions. International Journal of Environmental Sciences, 11(14).
6. Chinnaraju, A. (2025). Explainable AI (XAI) for trustworthy and transparent decision-making: A theoretical framework for AI interpretability. World Journal of Advanced Engineering Technology and Sciences, 14(3), 170-207.
7. Chivers, W. (2019). Resisting digital surveillance reform: The arguments and tactics of communications service providers. Surveillance and Society, 17(3/4), 517-532.
8. De, M., & Chakraborty, D. K. (2024). Integrating Digital Forensics into Intellectual Property Rights Enforcement: A Framework for Cybercrime Investigation. Journal of Intellectual Property Rights, 29(6), 500-506.
9. Dou, L., & Dou, X. (2025). Towards just AI: Challenges and solution framework for algorithmic discrimination in judicial system. International Journal of Digital Law and Governance, 2(1), 39-81.
10. Folorunso, A., Adewa, A., Babalola, O., & Nwatu, C. E. (2024). A governance framework model for cloud computing: Role of AI, security, compliance, and management. World Journal of Advanced Research and Reviews, 24(2), 1969-1982.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

11. Gentry, E. (2024). 'The Challenges of Integrating AI-Generated Evidence Into the Legal System' (Akerman LLP, 12 June 2024) https://www.akerman.com/en/perspectives/the-challenges-of-integrating-ai-generated-evidence-into-the-legal-system.html.
12. Giardiello, G., & Turchi, F. (2023). Evidence Exchange Standard Package: An Application CASE Ontology Complied for the Preparation of the Evidence Package and Its Exchange. In M. A. Biasiotti & F. Turchi (Eds.), European Investigation Order: Where the Law Meets the Technology (pp. 97–126). Springer International Publishing. https://doi.org/10.1007/978-3-031-31686-9_8
13. LATHER, R., SINGH, D. R., NEHRA, V., & JAIN, S. (2025). Cyber Shield & Scales: Legal Strategy for Digital Defense 2025. Yashita Prakashan Private Limited.
14. Macturk, E. L., Hayes, K., O'Sullivan, G., & Perrault Uptmor, K. A. (2025). Are We Ready for It? A Review of Forensic Applications and Readiness for Comprehensive Two-Dimensional Gas Chromatography in Routine Forensic Analysis. Journal of Separation Science, 48(4), e70138.
15. Md Fokrul Islam Khan. (2025). Risk Management Framework in the AI Act. International Journal of Science and Research Archive, 14(3), 466–471. https://doi.org/10.30574/ijsra.2025.14.3.0688
16. Nath, S., Summers, K., Baek, J., & Ahn, G. J. (2024, October). Digital evidence chain of custody: Navigating new realities of digital forensics. In 2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA) (pp. 11-20). IEEE.
17. Nsor, M., & Bakare, F. A. (2025). Leveraging big data engineering techniques for automated evidence extraction and pattern recognition in cybercrime forensic analysis. World Journal of Advanced Research and Reviews, 27(1), 2532–2553. https://doi.org/10.30574/wjarr.2025.27.1.2818
18. Olber Dr, P. (2021). The survey on cross-border collection of digital evidence by representatives from Polish prosecutors' offices and judicial authorities. Journal of Digital Forensics, Security and Law, 16(2), 3.
19. Orji, N. A. (2024). Admissibility of AI-generated Evidence under the Nigerian Evidence Act, 2023. Available at SSRN 5035075.
20. Patel, D. G. (2025). Securing Cloud Infrastructure Through Ancestry Tracking in Machine Images. IJSAT-International Journal on Science and Technology, 16(3).
21. Perault, M., & Salgado, R. (2024). Untapping the Full Potential of CLOUD Act Agreements. Center for Strategic and International Studies (CSIS).
22. Patterson, T. (2025). Cross-Border Cloud Data Transfers: Case Studies on Balancing US Government Privacy Regulations with Global Business Needs. Available at SSRN 5383863.
23. Okunrobo Perez, S. (2025). Proliferation of e-Evidence: Reliability Standards and the Right to a Fair Trial. European Journal of Crime, Criminal Law and Criminal Justice, 33(1-2), 187-211. https://doi.org/10.1163/15718174-bja10070.
24. Ucar, M., & Yalcintas, A. (2023). GDPR and Digital Protectionism in the EU: The Cases of Android and iOS. Journal of Economic Issues, 57(4), 1079–1094. https://doi.org/10.1080/00213624.2023.2273120.
25. Voigt, P., & Von dem Bussche, A. (2024). The EU General Data Protection Regulation (GDPR): A Practical Guide (Springer Nature Switzerland 2024) https://link.springer.com/10.1007/978-3-031-62328-8
26. Zharova, A. K. (2023). Achieving algorithmic transparency and managing risks of data security when making decisions without human interference: legal approaches. Journal of Digital Technologies and Law, 1(4), 973-993.