



INDIAN JOURNAL OF  
LEGAL REVIEW

VOLUME 6 AND ISSUE 5 OF 2026

INSTITUTE OF LEGAL EDUCATION



## INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN – 2583-2344

(Open Access Journal)

Journal's Home Page – <https://ijlr.iledu.in/>

Journal's Editorial Page – <https://ijlr.iledu.in/editorial-board/>

Volume 6 and Issue 5 of 2026 (Access Full Issue on – <https://ijlr.iledu.in/volume-6-and-issue-5-of-2026/>)

### Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 73059 14348 – [info@iledu.in](mailto:info@iledu.in) / [Chairman@iledu.in](mailto:Chairman@iledu.in)



© Institute of Legal Education

**Copyright Disclaimer:** All rights are reserve with Institute of Legal Education. No part of the material published on this website (Articles or Research Papers including those published in this journal) may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher. For more details refer <https://ijlr.iledu.in/terms-and-condition/>

# “ARTIFICIAL INTELLIGENCE AS A TOOL FOR EVIDENCE AND INVESTIGATION IN INTERNATIONAL CRIMINAL LAW”

**AUTHOR** – SHILPI KUMARI, ADVOCATE & LL.M STUDENT AT AMITY UNIVERSITY PATNA

**BEST CITATION** – SHILPI KUMARI, “ARTIFICIAL INTELLIGENCE AS A TOOL FOR EVIDENCE AND INVESTIGATION IN INTERNATIONAL CRIMINAL LAW”, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 6 (5) OF 2026, PG. 01-05, APIS – 3920 – 0001 & ISSN – 2583-2344.

### ABSTRACT

Artificial intelligence (AI) is changing how international criminal investigators collect, sort, authenticate, and present evidence. The shift is driven by the digital turn in atrocity documentation: conflicts now generate enormous volumes of user-generated videos, social-media posts, satellite images, geolocation data, intercepted communications, and sensor-derived material. International criminal law (ICL), however, remains anchored in fair-trial guarantees, adversarial testing, and cautious evidentiary assessment. This article examines AI as a practical investigative tool rather than as a substitute decision-maker. It argues that AI is most valuable in five functions: triage of large datasets, pattern detection, linkage analysis, authenticity checks, and courtroom visualization. Drawing on recent ICC practice, open-source investigation standards, and contemporary scholarship, the article shows that AI can strengthen accountability when deployed inside a rigorous legal framework. Yet it also identifies serious risks: bias in training data, black-box outputs, synthetic media, privacy intrusions, chain-of-custody gaps, and unequal technological capacities between prosecution and defense. The central claim is that AI should

be used as an assistive layer under strong human oversight. In ICL, the measure

of success is not whether AI is impressive, but whether it produces evidence that is reliable, explainable, contestable, and consistent with the rights of the accused and the interests of victims.

ICC OTP Link, 2024	74,803 submissions and 401,488 electronic files received through the secure evidence-submission platform.
eyeWitness to Atrocities, end-2022	48,000+ media files captured with the controlled-capture app; 41 dossiers submitted to accountability mechanisms.
eyeWitness, 2023	27 dossiers to accountability mechanisms; more than 80 documenters trained across 6 countries.
SITU / Al Hassan case, 2024	First ICC trial reported to feature an interactive digital evidentiary platform integrating videos, photos, satellite imagery, and 3D data.

*Source note: ICC Office of the Prosecutor Annual Report 2024 / OTP news release; eyeWitness outcome reports and related publications; SITU Research project materials.*

### 1. INTRODUCTION

International criminal investigations have always faced unusual evidentiary burdens. Prosecutors

must reconstruct mass violence that often occurred years earlier, across remote territories, amid trauma, insecurity, and deliberate destruction of proof. Today those challenges coexist with an information surplus. Instead of too little data, investigators often confront too much. Open-source imagery, witness media, drone footage, satellite archives, messaging-

app records, and platform metadata can be abundant, but they are dispersed, fragile, and uneven in quality. Recent scholarship describes digital

open-source information as a significant and growing source of evidence in ICL, especially where investigators cannot safely access crime scenes or where witness testimony alone is insufficient (McDermott, Koenig, & Murray, 2021; Gillett, 2023).

## 2. THE DIGITAL TURN IN INTERNATIONAL CRIMINAL LAW

AI matters because it can process this environment at scale. Machine-learning systems can cluster thousands of files, detect repeated objects or locations, transcribe and translate multilingual speech, compare versions of videos, flag likely manipulation, and map relationships across time, place, and actors. The point is practical: AI can reduce the time between raw collection and legally usable evidentiary analysis. At the same time, criminal adjudication cannot accept “machine says so” reasoning. Article 69 of the Rome Statute still requires the Court to assess relevance, probative value, and prejudice to a fair trial. Digital sophistication does not displace legal scrutiny.

The Berkeley Protocol recognizes that open-source information can provide leads, intelligence, and direct evidence in legal processes, especially when investigators lack timely physical access to crime scenes. It was designed precisely because digital investigations require replicable methods if judges are to assess quality and reliability. Likewise, the ICC Office of the Prosecutor has invested in secure digital intake and evidence-management tools. In 2024 the Office reported receiving 74,803 submissions, including more than 400,000 electronic files, through OTP Link, its secure evidence-submission platform. The scale alone illustrates why manual review is increasingly inadequate.

## 3. CORE INVESTIGATIVE USES OF AI

AI contributes most effectively before the final legal judgment stage. First, it helps with triage. Investigators dealing with tens of thousands of files need systems that can deduplicate content, classify media by type, sort by location or time markers, and prioritize likely crime-relevant items. Second, AI enables pattern detection. Computer vision can identify recurring

military vehicles, craters, uniforms, damaged structures, or detention settings across large collections of imagery. Natural-language processing can detect recurring names, places, commands, or threats across testimony and communications. Third, AI supports linkage analysis. In mass-atrocity cases, responsibility often depends on connecting acts to broader campaigns, policies, or command chains. AI-assisted graph analysis can reveal relationships among units, incidents, intermediaries, and digital accounts that might otherwise remain hidden.

Fourth, AI can assist authentication. This is especially important in a world of edited clips, recycled

footage, and increasingly persuasive synthetic media. AI-based forensic tools can check compression patterns, lighting inconsistencies, frame anomalies, and source conflicts. They are not infallible, but they can generate hypotheses for human experts to test. Fifth, AI can improve presentation. In the Al Hassan case, SITU Research’s digital platform assembled videos, photographs, 3D data, and satellite imagery into an interactive reconstruction of Timbuktu; SITU described it as the first time an ICC trial featured such a digital evidentiary platform. This did not replace witness or documentary proof. Rather, it organized heterogeneous evidence so that judges could better understand space, movement, and context.

## 4. WHY AI IS ATTRACTIVE TO PROSECUTORS

For prosecutors, AI promises three major advantages. The first is speed. A human team

can spend months reviewing material that an AI-assisted workflow can sort in days. The second is breadth. International crimes are seldom proven through a single dramatic item; they are established through accumulation, corroboration, and pattern. AI helps identify that pattern across immense datasets. The third is consistency. When properly validated, AI tools can apply the same screening criteria across large collections, reducing some forms of ad hoc human inconsistency.

Recent writing on AI and ICL emphasizes precisely this point: the value of AI lies in handling the quantity and heterogeneity of conflict-generated material rather than in automating guilt determinations. Used well, it can free investigators to focus on legal theory, contextual analysis, witness strategy, and corroboration. It can also help victim-centered work by surfacing underreported incidents that might be buried in massive archives. In that sense, AI may widen the evidentiary field rather than narrow it.

### 5. LEGAL RISKS AND EVIDENTIARY LIMITS

The same features that make AI attractive also generate legal anxiety. The first concern is reliability. Courts must know not only that a result exists, but how it was produced. Black-box models, proprietary software, and poorly documented training sets create serious disclosure problems. If the defense cannot examine the method, assumptions, and error rate, meaningful adversarial testing becomes difficult.

The second concern is bias. McDermott, Koenig, and Murray warn that both human and machine bias can distort digital investigations by overrepresenting certain places, communities, or crimes while rendering others invisible. AI trained on skewed datasets may reproduce those distortions.

The third concern is authenticity in the age of generative AI. Deepfakes and synthetic voice tools complicate the authentication of digital

evidence and fuel what commentators call the “liar’s dividend,” in which authentic evidence is dismissed as fake because manipulation has become plausible. ICC judges interviewed in recent research did not regard AI as an existential threat to future use of user-generated evidence, but they did stress the need for more judicial and professional training.

The fourth concern is privacy and overcollection. AI can encourage expansive scraping, retention, and cross-platform surveillance.

### 6. ADMISSIBILITY AND FAIR-TRIAL IMPLICATIONS

Under the Rome Statute, the decisive question is not whether evidence is digital or AI-assisted, but whether it is relevant, probative, and fair to admit. That makes AI-generated outputs closer to expert or technical evidence than to self-improving truth. A model’s result should therefore be treated as one element in a chain of proof, not as a final conclusion. Courts should ask: What data entered the system? What preprocessing occurred? What model or rules were used? What is the known error rate? Can the result be independently replicated? Were exculpatory possibilities examined? Was the defense given sufficient disclosure to contest the method?

Gillett’s work on expert evidence and digital open-source information is valuable here. He argues that the court needs disciplined ways to identify who is sufficiently qualified to interpret technically complex digital material. That insight applies with even greater force when AI tools are involved. Investigators, analysts, and expert witnesses must be able to explain not only what a system produced, but why the court should trust it. Without explainability, the probative value of the output shrinks.

### 7. SELECTED EVIDENCE AND PRACTICE

Three developments show how quickly the field is moving. First, the OTP’s use of OTP Link indicates institutional acceptance that digital intake is now a core prosecutorial function, not a peripheral experiment. Second, the

eyeWitness model shows how controlled-capture tools can preserve metadata and chain-of-custody features in ways that ordinary consumer apps often cannot. Third, the AI Hassan platform demonstrates that digital evidence is not only about collection; it is also about intelligible courtroom narration. In complex atrocity trials, visual and spatial organization can materially affect how judges assess contextual evidence.

**8. A FOCUSED FRAMEWORK FOR RESPONSIBLE USE**

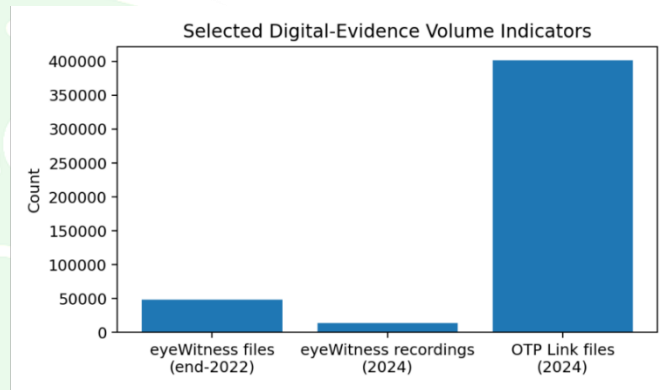
A workable framework for AI use in ICL should contain at least six elements. First, legality: the collection and processing pipeline must comply with applicable legal authority, privacy protections, and disclosure obligations. Second, technical validation: any AI tool used for evidentiary analysis should have documented testing conditions, known limitations, and a process for periodic revalidation. Third, human review: no inculpatory inference should be forwarded without analyst assessment and, where material, independent corroboration. Fourth, documentation: investigators should maintain audit trails showing inputs, versions, prompts or parameters, outputs, and analyst interventions. Fifth, equality of arms: where the prosecution relies materially on AI-assisted analysis, the defense must receive enough information to challenge it. Sixth, judicial literacy: judges require training to ask the right questions about machine-assisted evidence without surrendering legal judgment to technical mystique.

Table 1. Selected institutional and operational data point

Year	Institution / tool	Indicator	Reported figure
2022	eyeWitness to Atrocities	Controlled-capture media files on server	48,000+
2022	eyeWitness to Atrocities	Dossiers submitted to accountability mechanisms	41 total by end-2022; 17 in 2022
2022	eyeWitness to	Human rights defenders	202

9. CRITICAL ASSESSMENT

Even under a careful framework, AI will not solve foundational problems of atrocity litigation. It cannot repair destroyed archives, make absent witnesses appear, or eliminate geopolitical non-cooperation. It may even create new asymmetries by rewarding well-funded investigators and disadvantaging defense



teams with fewer technical resources. Moreover, many supposedly AI-driven conclusions still depend heavily on human labeling choices, contextual interpretation, and threshold settings. In practice, AI often shifts rather than removes discretion.

Figure 1. Selected digital-evidence volume indicators

Note: Metrics are not directly equivalent. The figure compares selected volume indicators reported by eyeWitness to

Atrocities and the ICC Office of the Prosecutor to illustrate the scale problem facing digital investigations.

	Atrocities	trained	
2023	eyeWitness to Atrocities	Dossiers to accountability mechanisms	27
2023	eyeWitness to Atrocities	New partnerships	12
2024	eyeWitness to Atrocities	Photos / videos / audio recordings captured	13,641
2024	ICC OTP / OTP Link	Submissions received	74,803
2024	ICC OTP / OTP Link	Electronic files received	4,01,488

Sources: eyeWitness 2022 Outcome Report; eyeWitness 2023 Outcome Report / 2023 page summary; eyeWitness 2024 Outcome Report page summary; ICC OTP Annual Report 2024 / OTP news release.

Table 2. Principal AI uses in international criminal investigation

AI function	Typical task	Investigative value	Main legal risk
Triage and deduplication	Cluster or remove duplicate media, classify files, prioritize likely crime-relevant items	Cuts review time and reduces backlogs	Overlooking rare but crucial outlier evidenc
Pattern detection	Detect recurring vehicles, craters, buildings, uniforms, or speech patterns	Helps establish campaigns and contextual patterns	False positives, datase skew, and overfitting
Link analysis	Map relationships among actors, incidents, accounts, and locations	Supports command-responsibility and network analysis	Opaque inferential leaps and weak causal assumptions
Authenticity support	Flag editing anomalies, compression artefacts, frame irregularities, or source conflicts	Assists verification and fraud detection	Black-box outputs, uncertain error rates
Translation / transcription	Convert multilingual audio and text into searchable form	Improves accessibility and comparative review	Meaning drift, dialect errors, missed nuance
Courtroom visualization	Integrate imagery, maps, 3D reconstructions, and timelines	Makes complex evidence intelligible to judges	Prejudice through persuasive presentatio

Analytical synthesis based on the Berkeley Protocol, OTP practice, and scholarship by McDermott et al. (2021), Gillett (2023), Elsharkawy (2025), and Bo (2025/2026).

**Table 3. Selected literature and policy snapshot**

Source	Contribution	Relevance to AI and evidence
McDermott, Koenig & Murray (2021)	Explains human and machine bias in digital open-source investigations	Warns that AI can reproduce representational and analytical distortions
Koenig (2021 special issue introduction)	Frames new technologies in international-crimes investigations	Places AI inside the broader digital transformation of atrocity evidence
Gillett (2023)	Examines expert evidence and digital open-source information before the ICC	Useful for judging when AI-assisted outputs need expert mediation
Eurojust-ICC-CSO Guidelines (2022)	Sets practical guidance for civil-society evidence handling	Reinforces methodological discipline and preservation requirements
Elsharkawy (2025)	Discusses digital evidence before the ICC and admissibility requirements	Links technical evidence to Article 69 evidentiary assessment
McDermott (2026)	Reports ICC judges' views on user-generated evidence in the AI age	Shows judges see training, not panic, as the immediate institutional need
Council of Europe AI Convention (2024)	Introduces binding human-rights-centered AI obligations	Supports transparency, oversight, accountability, and non-discrimination
UNESCO AI Ethics Recommendation	Sets rights-based governance principles for AI	Useful normative baseline for privacy, proportionality, and accountability

Source note: compiled from the cited academic and institutional materials listed in the references.

**10. CONCLUSION**

AI is already reshaping international criminal practice. The real question is not whether AI will enter ICL, but under what conditions it will do

so legitimately. The current evidence suggests a measured conclusion. AI is highly useful for triage, pattern recognition, linkage analysis, authenticity support, and courtroom

organization of complex digital records. It can reduce investigative delay, widen the evidentiary lens, and help institutions cope with data volumes that are otherwise unmanageable. But its value depends on governance. Reliability, transparency, replicability, and adversarial contestability are not optional additions; they are what transform technical output into legal evidence.

## REFERENCES

1. Bo, M. (2025). Artificial intelligence in the prosecution of international crimes. SSRN working paper / Naval War College Digital Commons version available online.
2. Council of Europe. (2024). Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225).
3. Elsharkawy, M. H. (2025). Digital evidence before the International Criminal Court. *Journal of Law and Emerging Technologies*, 4(1), 323-426. <https://doi.org/10.54873/jolets.v4i1.185>
4. European Commission. (2025). AI Act: regulatory framework and transparency obligations. eyeWitness to Atrocities. (2022). 2022 outcome report: Fighting impunity with verifiable photos and videos.
5. eyeWitness to Atrocities. (2024). 2023 outcome report / public summary page.
6. eyeWitness to Atrocities. (2025). 2024 outcome report: Justice captured.
7. Gillett, M. (2023). Expert evidence and digital open source information. *Journal of International Criminal Justice*, 21(4), 661-690.
8. ICC Office of the Prosecutor. (2023). OTP Link evidence-submission platform announcement.
9. ICC Office of the Prosecutor. (2024). Annual Report 2024 and related news release on law in action for all.
10. Koenig, A. (2021). New technologies and the investigation of international crimes: An introduction. McDermott, Y., Koenig, A., & Murray, D. (2021). Open source information's blind spot: Human and machine bias in international criminal investigations. *Journal of International Criminal Justice*, 19(1), 85-105. <https://doi.org/10.1093/jicj/mqab006>
11. machine bias in international criminal investigations. *Journal of International Criminal Justice*, 19(1), 85-105. <https://doi.org/10.1093/jicj/mqab006>
12. McDermott, Y. (2026). New evidence, new challenges: ICC judges' perspectives on user-generated evidence and judging in an age of artificial intelligence.
13. SITU Research. (2024). ICC digital platform and the Al Hassan case; digital evidence platform used at ICC trial.
14. United Nations Human Rights Office. (2022). Berkeley Protocol on Digital Open Source Investigations.
15. UNESCO. (2021/updated portal). Recommendation on the Ethics of Artificial Intelligence. United Nations. (1998). Rome Statute of the International Criminal Court, Article 69.



GRASP - EDUCATE - EVOLVE



**INSTITUTE OF LEGAL EDUCATION**

*(Managed by I.L.E. EDUCATIONAL TRUST)*

NO. 08, ARUL NAGAR, SEERA THOPPU,  
MARUDHAANDA KURICHI, SRIRANGAM - 620102,  
TAMILNADU, INDIA.

ISSN 2583-2344



9 772583 234004