INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA).*

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

A LEGAL FRAMEWORK FOR WATERMARKING AND FINGERPRINTING AI OUTPUTS WITH REFERENCE TO LOGISTICS TECHNOLOGY

AUTHORED BY - M. GOMATHI SUBRAMANIAN & DR. JENIFFER STELLA
LL.B. Student (Reg. No. 23122118), School of Law, VISTAS, Chennai
Assistant Professor, Department of Legal Studies, School of Law, VISTAS, Chennai

ABSTRACT

The rapid adoption of artificial intelligence in India's logistics sector has created a commercially significant but legally unaddressed problem: the absence of any statutory mechanism to authenticate, trace, or verify AI-generated commercial documents. Logistics platforms routinely use AI to produce profit and loss (P&L) statements, route optimisation and tracking (ROT) reports, and automated invoices — documents that carry direct legal and financial consequences. Under India's current legal framework — comprising the Copyright Act, 1957, the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, and the Indian Evidence Act, 1872 — these documents enjoy legal status but face no requirement for watermarking, model fingerprinting, or provenance logging at the point of production. This article examines that gap through a doctrinal and comparative methodology, drawing on the European Union's Artificial Intelligence Act, 2024 and the NIST AI Risk Management Framework as comparative benchmarks. It argues that the logistics sector's established chain-of-custody framework — barcodes, RFID tags, electronic waybills — provides a practical and legally instructive model for an AI output authentication standard. Five targeted legislative recommendations are proposed: mandatory watermarking under an amended IT Act; a national AI Model Registry; blockchain provenance standards for high-value documents; an AI Document Fiduciary category under the DPDP Act; and a phased implementation timeline. The article concludes that holding AI-generated logistics documents to the same authentication standard already applied to physical goods is not a radical reform — it is a logical and overdue extension of principles that Indian commercial law has long recognised.

ISSN: 2582-6433

Keywords: *Artificial Intelligence, Watermarking, Digital Provenance, Logistics Technology, IT Act 2000, DPDP Act 2023, EU AI Act, Fingerprinting, Chain of Custody, Indian Law*

I. Introduction

India's logistics industry is one of the fastest-growing sectors in the national economy. Freight companies, warehouse operators, and supply chain managers increasingly deploy AI-powered platforms that automatically generate legally significant commercial documents — monthly profit and loss statements, route optimisation and tracking reports, and customer invoices — without human authorship. The efficiency gains are substantial. The legal risks are largely unrecognised.

When a document is produced by an AI system rather than a human being, three questions of legal significance arise: how do you prove the document is genuine? How do you prove it has not been altered after generation? And how do you identify which AI model produced it, and whether that model was lawfully trained? Under India's current statutory framework, there is no answer to any of these questions. No law requires AI systems to embed a watermark in the documents they produce. No fingerprinting standard records the identity of the model. No provenance obligation tracks the document from production to use.

This article argues that this is a serious and commercially costly legal gap — one that creates specific fraud risks in the logistics sector and leaves AI-generated documents legally indeterminate in precisely the contexts where they matter most: tax audits, contract disputes, insurance claims, and regulatory proceedings. The argument draws on a productive analogy: India's logistics sector has already solved the equivalent problem for physical goods. Every shipment carries a verifiable identity through barcodes, RFID tags, and waybills. The law should now extend that principle to the AI-generated documents that accompany those shipments.

II. The Existing Indian Legal Framework and Its Limitations

India has several statutes that apply, in varying degrees, to AI-generated commercial documents. None of them was designed with AI-generated documentation in mind, and none provides an authentication standard.

A. Copyright Act, 1957

Section 2(d)(vi), inserted by the 1994 amendment, provides that for computer-

ISSN: 2582-6433

generated works, the 'author' is the person who causes the work to be created. This gives AI-generated logistics documents copyright protection and identifies a legal owner.[1] However, copyright protection addresses ownership, not authenticity. It confirms who owns the document — not whether the document is genuine, unaltered, or traceable to a specific AI model version.

B. Information Technology Act, 2000

Section 4 gives electronic records legal validity equivalent to paper documents. Sections 65 and 66 criminalise tampering with computer source documents and computer-related offences respectively.[2] Section 43A imposes data protection obligations on entities handling sensitive personal data. These provisions are valuable but reactive: the IT Act punishes tampering after it is detected but does not require AI platforms to embed authentication mechanisms at the point of document generation. Written in 2000, before generative AI existed commercially, it contains no provisions on watermarking, model fingerprinting, or provenance logging.

C. Digital Personal Data Protection Act, 2023

The DPDP Act establishes accountability obligations for Data Fiduciaries — entities that determine the purpose and means of processing personal data. A logistics AI platform handling driver or customer personal data would fall within this framework.[3] However, the DPDP Act addresses personal data protection, not document authentication. An AI-generated P&L statement is a financial document, not a personal data record, and the DPDP Act imposes no authentication requirements on commercial AI outputs.

D. Indian Evidence Act, 1872

Section 65B governs the admissibility of electronic records in court proceedings. It requires a certificate from a responsible official confirming the record's genuineness and ordinary-course production.[4] This is a useful evidentiary safeguard, but it depends entirely on human certification after the fact. It does not require AI systems to embed built-in authentication at the moment of generation, and provides no tool to resolve disputes about whether a document was produced by an AI system at all, or whether it was altered post-generation.

The combined effect of these provisions is that AI-generated logistics documents have legal status but no authentication standard. Table 1 summarises the gap:

ISSN: 2582-6433

Document	What Law Covers	What Law Does Not Cover
P&L Statement	Copyright ownership; electronic record validity (IT Act s.4)	No watermark; no fingerprint log; no provenance obligation
ROT Report	Electronic admissibility (Evidence Act s.65B); tampering offence (IT Act s.65)	No authentication at generation; no AI model identification
Automated Invoice	Digital signature validity; GST compliance rules	No AI watermark; no model version record; no tamper standard

Table 1: Legal Coverage and Gaps for AI-Generated Logistics Documents

III. The Critical Gaps: Watermarking, Fingerprinting and Provenance

A. No Watermarking Mandate

A digital watermark is embedded information that identifies a document as AI-generated, records the AI system that produced it, the date and time of production, and a unique document identifier. It is invisible to a casual reader but detectable by a verification tool. Like the security thread in a currency note, a watermark proves the document's genuine origin. India has no law requiring AI systems to embed watermarks in their outputs. For a logistics company, this means an AI-generated invoice is indistinguishable — legally and technically — from an altered or fabricated version.

B. No Model Fingerprinting Registry

Model fingerprinting records which specific version of an AI system produced a given output, along with the training data used and the parameters applied. Watermarking proves a document is genuine; fingerprinting proves the model that produced it was lawful. India has no AI model registry — public or private — where systems used for commercial document generation must be registered. If a logistics company's AI invoicing platform has a software update that introduces a calculation error, there is no fingerprint record to identify which invoices were produced by the faulty version.

C. No Provenance Obligation

Provenance is the complete history of a document — its creation, transmission, and any modifications. In physical logistics, provenance is established by waybills, delivery

ISSN: 2582-6433

confirmations, and customs stamps. For AI-generated documents, no Indian law requires a provenance record. Documents arrive in the hands of customers, auditors, and courts with no verifiable history of their journey from the AI system.

D. Specific Fraud Risks in Logistics

These gaps create three concrete fraud risks. Invoice fraud involves altering AI-generated invoices after production — changing amounts, delivery details, or payment account information. Because no watermark records the original output, alterations may be undetectable. P&L manipulation involves altering AI-generated financial reports to misrepresent profitability for investor, lender, or tax purposes. ROT record fabrication involves creating or altering delivery records to conceal non-performance or diversion of shipments. All three are practically undetectable without authentication records.

The inconsistency with physical logistics standards is striking, as Table 2 illustrates:

Standard	Physical Logistics	AI-Generated Documents
Identity Marker	Barcode / RFID — legally significant	No watermark required by law
Chain of Custody	Waybill / bill of lading with signatures	No provenance log required
Authenticity Check	Customs stamp, GST serial number	No fingerprint / model registry
Tamper Evidence	Physical seals, locked containers	No tamper-evident standard
Court Admissibility	Well-established; routinely admitted	Possible under s.65B but no built-in authentication

Table 2: Physical vs AI-Generated Logistics Documentation Standards

IV. Comparative Analysis: EU AI Act and NIST Framework

A. EU Artificial Intelligence Act, 2024

The EU AI Act is the world's first comprehensive AI governance law. It applies a risk-based framework: high-risk AI systems — including those generating financial documents and compliance records — must satisfy strict traceability and transparency obligations. Providers

ISSN: 2582-6433

must maintain detailed technical documentation throughout the system's operational life.[5] The Act also mandates that AI-generated content — including synthetic documents — carry markings that identify them as AI-generated. This is a direct watermarking requirement.

Critically, the EU AI Act imposes obligations on both providers (system builders) and deployers (companies that use AI in their operations). A logistics company deploying an AI invoicing platform is a deployer with specific obligations: maintaining records of the AI system's use and ensuring that outputs are appropriately authenticated. This dual-accountability model addresses the risk that regulatory obligations are simply passed back and forth between software developers and end-users without either party bearing clear responsibility.

B. NIST AI Risk Management Framework (USA)

The NIST framework, while voluntary, identifies traceability and transparency as core dimensions of AI trustworthiness. It recommends that organisations maintain documentation sufficient to trace outputs to their source model version and training data.[6] Many global logistics operators use the NIST framework as a practical compliance benchmark for their AI systems.

C. India's Position Against Global Standards

Against these benchmarks, India's position is one of almost complete regulatory absence on AI output authentication. There is no AI-specific legislation, no AI regulator, and no AI-specific enforcement mechanism. As Table 3 shows, the gap is not merely a matter of degree — it is structural.

Standard	EU AI Act (2024) | India (Current Law)
Watermarking	Mandatory for specified AI content | No requirement
Traceability / Fingerprinting	Mandatory for high-risk systems | No requirement — no registry
Provenance Logging	Required documentation for high-risk systems | No equivalent obligation
Deployer Accountability	Specific obligations on deployers | No deployer-specific obligations

ISSN: 2582-6433

Regulatory Body	National authorities + EU AI Office | No dedicated AI regulator
Enforcement	Fines up to €35M or 7% of turnover | No AI-specific enforcement

Table 3: EU AI Act vs India — AI Output Authentication

D. Lessons for India

Three lessons from the comparative analysis are directly applicable. First, a risk-based approach is practically workable: India does not need to regulate all AI outputs equally. AI systems that generate documents used in tax filings, contract disputes, and regulatory proceedings should be classified as high-risk and subject to the most rigorous authentication requirements. Second, deployer accountability is essential: a logistics company that deploys an AI platform must bear clear obligations, not merely the software developer. Third, voluntary standards will not produce universal compliance: document authentication is a public good requiring legal mandate, not industry goodwill.

V. Recommendations: A Proposed Legal Framework

Recommendation 1: Mandatory Watermarking — Amendment to the IT Act, 2000

Any AI system deployed to generate commercial documents — invoices, financial statements, and logistics tracking records — should be legally required to embed a watermark in every document at the moment of production. The watermark should record: (i) the fact that the document was AI-generated; (ii) the identity of the AI platform; (iii) the date and time of generation; and (iv) a unique document identifier. The IT Act, 2000 should be amended to insert a new provision after Section 43A establishing this requirement. Failure to embed a watermark should constitute a failure to maintain proper electronic records, attracting civil and criminal consequences under the existing IT Act framework.

For the logistics sector, this means every AI-generated invoice, P&L report, and ROT record carries a verifiable identity from the moment of production — directly analogous to the RFID tag on every physical shipment.

Recommendation 2: National AI Model Registry

A national AI Model Registry should be established under the IT Act, administered by

ISSN: 2582-6433

CERT-In or a new AI Regulatory Office. All AI systems deployed for commercial document generation should register with this registry, providing model version details, training data summary, and performance benchmarks. Documents produced by registered systems would carry a fingerprint linking them to the registered model version. This registry would enable rapid identification of documents produced by defective or non-compliant model versions — a capability the logistics sector already understands through its use of lot tracking and batch identification in physical supply chains.

Recommendation 3: Blockchain Provenance Standards for High-Value Documents

For high-value AI-generated documents — invoices above a specified threshold, P&L statements used in regulatory filings, and ROT records used as evidence in legal proceedings — the law should require a tamper-resistant provenance record maintained on a blockchain ledger. Blockchain provenance is already deployed by global logistics operators to track physical goods. The IT Act amendment proposed in Recommendation 1 should explicitly recognise blockchain provenance records as valid authentication evidence for AI-generated documents, placing them on an equivalent legal footing to a Section 65B certificate under the Indian Evidence Act.

Recommendation 4: AI Document Fiduciary Category under the DPDP Act, 2023

The DPDP Act, 2023 should be amended to create a new category of 'AI Document Fiduciary' — entities that deploy AI systems to generate documents used for commercial, legal, or regulatory purposes. AI Document Fiduciaries should be required to comply with the watermarking, fingerprinting, and provenance obligations described in Recommendations 1 to 3, and to make authentication records available on request to customers, auditors, and regulators. This amendment uses the DPDP Act's existing institutional framework — the Data Protection Board — rather than requiring a wholly new regulatory body, making it administratively efficient.

Recommendation 5: Phased Implementation Timeline

A phased approach would allow industry adaptation while sending a clear regulatory signal. Phase 1 (0–12 months from enactment): IT Act amendments and AI Model Registry established; CERT-In issues implementation guidance. Phase 2 (12–24 months): Watermarking mandatory for organisations above a specified size threshold; DPDP Act

ISSN: 2582-6433

amendment enacted. Phase 3 (24–36 months): Full provenance and blockchain logging requirements in force for all AI Document Fiduciaries. This timeline mirrors the phased implementation used for the DPDP Act itself, which Indian industry has found manageable.

VI. Conclusion

India's logistics industry has solved the problem of physical document authentication. A shipment moving from Chennai to Mumbai carries a verified identity — barcode, RFID tag, signed waybill — at every stage of its journey. Courts, customs authorities, tax officials, and business partners rely on that chain of authentication every day. The legal infrastructure that makes this possible was built deliberately, through statute, because the commercial stakes of unauthenticated physical goods were too high to leave to industry goodwill.

The commercial stakes of unauthenticated AI-generated documents are equally high — and the legal infrastructure to address them does not yet exist. An AI-generated invoice is as commercially significant as a manually prepared one. An AI-generated P&L report is as legally consequential as an auditor-prepared financial statement. An ROT record produced by an AI tracking system is as evidentiary as a driver's handwritten log. The digital origin of these documents does not make them less important — it makes authentication more urgent, because digital documents are easier to alter than physical ones and harder to verify without built-in authentication mechanisms.

This article has proposed five targeted legislative reforms that would establish an AI output authentication standard for India's logistics sector and, by extension, for India's commercial digital economy more broadly. These reforms are not radical departures from India's existing legal architecture. They are logical extensions of principles — authenticity, chain of custody, accountability — that Indian commercial law has recognised and enforced in the physical domain for decades.

India is actively positioning itself as a global leader in the AI economy. That ambition requires not only the deployment of AI at scale, but the legal infrastructure to make AI-generated outputs trustworthy. An AI document authentication standard is the baseline requirement for that trustworthiness. The reform agenda is clear. The legal tools are available. The logistics sector has shown that authentication works. The law should now make it real for the digital documents that AI systems generate.

ISSN: 2582-6433

FOOTNOTES

[1] The Copyright Act, 1957, s. 2(d)(vi), as amended by the Copyright (Amendment) Act, 1994.

[2] The Information Technology Act, 2000, ss. 4, 65, 66, 43A, as amended by the IT (Amendment) Act, 2008.

[3] The Digital Personal Data Protection Act, 2023, ss. 2(i), 8 (Data Fiduciary obligations).

[4] The Indian Evidence Act, 1872, ss. 65A, 65B, as inserted by the IT Act, 2000; see Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.

[5] European Union Artificial Intelligence Act, Regulation (EU) 2024/1689, Arts. 11–13 (technical documentation and traceability for high-risk AI systems); Art. 50 (transparency obligations for AI-generated content).

[6] National Institute of Standards and Technology, AI Risk Management Framework (NIST AI 100-1), January 2023, Govern 1.1, Map 1.1.

REFERENCES

Statutes and International Instruments

1. The Copyright Act, 1957 (as amended 1994, 2012), Government of India.
2. The Information Technology Act, 2000 (as amended 2008), Government of India.
3. The Digital Personal Data Protection Act, 2023, Government of India.
4. The Indian Evidence Act, 1872 (ss. 65A, 65B inserted by IT Act, 2000).
5. European Union Artificial Intelligence Act, Regulation (EU) 2024/1689, OJ L, 2024.
6. NIST AI Risk Management Framework (AI RMF 1.0), NIST AI 100-1, January 2023.

Cases

7. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
8. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
9. Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.

Books, Articles and Policy Documents

10. Basheer, S. and Khettry, S.P., 'The Jurisdiction of Watermarks: Intellectual Property and Authenticity in the Digital Age', Indian Journal of Law and Technology, Vol. 15, 2019.
11. Krishnamurthy, V., 'India's Digital Personal Data Protection Act: A Comparative Assessment', National Law School of India Review, Vol. 36, 2024.

ISSN: 2582-6433

12. Srinivasan, R., 'AI and the Indian Evidence Act: Are We Ready?', NALSAR Law Review, Vol. 17, 2023.
13. Mittal, A., 'Blockchain as Evidence: Prospects under Indian Law', Journal of Indian Law Institute, Vol. 64, 2022.
14. Ministry of Electronics and Information Technology (MeitY), National Strategy for Artificial Intelligence, June 2018.
15. NITI Aayog, Responsible AI for All: A Use Case Approach, 2021.
16. KPMG India, AI in Logistics: Transforming Supply Chains, 2023.