INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 12 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

E-FILING OF CASES AS A TOOL FOR JUDICIAL DIGITALIZATION: OPPORTUNITIES AND CHALLENGES IN INDIA

AUTHOR – TISHA T, STUDENT AT CYBER SPACE LAW AND JUSTICE DEPARTMENT, SCHOOL OF EXCELLENCE IN LAW

BEST CITATION – TISHA T**,** E-FILING OF CASES AS A TOOL FOR JUDICIAL DIGITALIZATION: OPPORTUNITIES AND CHALLENGES IN INDIA, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 6 (12) OF 2026, PG. 01-10, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT

The foundation of Phases II and III of India's e-Courts Integrated Mission Mode Project is the digitalisation of judicial operations via Electronic Filing (e-Filing). This empirical non-doctrinal study explores the operational effectiveness, structural friction, and human-computer interactions inside Indian court e-Filing platforms, going beyond normative legal analysis and statutory demands. This study offers practical empirical insights into digital court administration based on a systematic empirical survey of active advocate practitioners (N=11) and a thorough qualitative thematic analysis of registry procedures. According to the survey, systemic satisfaction is still stuck in a "average usability trap" (72.7% neutral rating), despite baseline adoption being absolute (100% active usage). Rigid document upload restrictions (45.5%) and frequent server disruptions (90.9% agreement on reason) were noted as major operational friction factors. The foundation of Phases II and III of India's e-Courts Integrated Mission Mode Project is the digitalisation of judicial operations via Electronic Filing (e-Filing). This empirical non-doctrinal study explores the operational effectiveness, structural friction, and human-computer interactions inside Indian court e-Filing platforms, going beyond normative legal analysis and statutory demands. This study offers practical empirical insights into digital court administration based on a systematic empirical survey of active advocate practitioners (N=11) and a thorough qualitative thematic analysis of registry procedures. According to the survey, systemic satisfaction is still stuck in a "average usability trap" (72.7% neutral rating), despite baseline adoption being absolute (100% active usage). Rigid document upload restrictions (45.5%) and frequent server disruptions (90.9% agreement on reason) were noted as major operational friction factors.

Keywords: Judicial Digitalization, E-Filing Systems, Empirical Legal Studies, Indian e-Courts Project, Court Administration, Legal Informatics, Institutional Infrastructure.

1. INTRODUCTION

The Indian administration of justice faces an unprecedented backlog, with pendency figures exceeding 50 million cases across District Courts, High Courts, and the Supreme Court of India.[1] To address this crisis of docket explosion and administrative delay, the e-Committee of the Supreme Court

[1] National Judicial Data Grid / Ministry of Law & Justice

launched the ambitious e-Courts Integrated Mission Mode Project under the National e-Governance Plan. Designed across three distinct phases, the initiative aims to digitize court management, automate registry operations, and introduce electronic filing (e-filing) as the primary intake mechanism for legal actions.

E-filing was envisioned as a transformational tool capable of democratizing access to justice. By enabling advocates and litigants to submit pleadings, pay court fees, upload evidentiary annexures, and obtain digital case numbers round-the-clock without physical registry attendance, the system promised to compress filing timelines, eliminate physical paper handling, and enhance institutional transparency.

However, while judicial policy discourse frequently treats digital implementation as synonymous with institutional efficiency, empirical legal scholarship cautions against equating technological deployment with user adoption. This study bridges the gap between normative policy intent and operational reality by investigating the frontline experiences of legal advocates navigating Indian court e-filing portals[2].

2. LITERATURE REVIEW & THEORETICAL FRAMEWORK

The theoretical framework of this study rests at the intersection of Socio-Legal Studies, Technology Acceptance Modeling (TAM),[3] and Institutional Infrastructure Analysis. In classic legal theory, procedural access is evaluated primarily through doctrine—analyzing statutory rules of procedure, limitation periods, and court standing. Nondoctrinal empirical scholarship, however, shifts the analytical lens to the material conditions under which procedural rights are exercised.

2.1 The Technology Acceptance Model in Judicial Systems

Davis's Technology Acceptance Model (TAM) posits that user adoption of technology is dictated by two primary variables: Perceived Usefulness (PU)[4] and Perceived Ease of Use (PEOU). In the context of judicial administration, legal practitioners represent a specialized end-user cohort. Unlike consumers using commercial applications, advocates operate under strict statutory deadlines, procedural rules, and professional liability. Consequently, technical failure during judicial e-filing does not merely cause inconvenience; it risks the forfeiture of legal remedies through limitation bar or default dismissal.

2.2 International Comparative Perspectives on E-Filing

Global experiences with judicial e-filing reveal distinct evolutionary tracks:

United States (CM/ECF & PACER): The Federal Courts' Case Management/Electronic Case Files system established early mandatory e-filing. While highly reliable, it faced critique for paywalling public records—a flaw India avoided by offering free access via the e-Courts portal.

[2] Supreme Court e-Committee Phase III Vision Document
[3] Davis, 1989
[4] World Bank Group, 2021

United Kingdom (HMCTS Reform)[5]: The HM Courts & Tribunals Service implemented single-cloud digital filing with automated verification, drastically reducing registry turnarounds but requiring significant court staff retraining.

European Union (e-CODEX): Designed for cross-border judicial interoperability, emphasizing strict cryptographic standards and automated XML data exchange between national registries.

2.3 The Indian Trajectory: From Paper to Hybrid Friction

Scholarship on Indian legal technology[6] (Datt & Sharma, 2021; Susskind,[7] 2019) highlights a persistent phenomenon: the "hybrid burden". Rather than replacing manual paper workflows with digital pipelines, court registries frequently layer digital mandates on top of existing physical filing requirements, creating duplicate operational costs for litigators.

3. EMPIRICAL RESEARCH METHODOLOGY

To evaluate the real-world performance of judicial e-filing, an empirical survey was conducted among active advocate practitioners in India . The study deployed a mixed-methods design, combining structured quantitative metrics with qualitative text fields[8].

The quantitative component comprised 10 closed-ended ordinal and categorical questions capturing respondent demographics, usage frequency, usability ratings (5-point Likert scale), primary system obstacles, perceived delay causes, and priority areas for reform. The qualitative component collected open-text commentary detailing procedural friction, technical failures, and registry interaction experiences.

4. EMPIRICAL FINDINGS: PROFILE & USABILITY METRICS

Analysis of respondent demographics demonstrates that the empirical dataset represents frontline active advocates engaged in regular court practice across District and High Courts[9].

100% ACTIVE E-FILING USERS	63.6% STANDING < 1 YEAR	72.7% RATE USABILITY AS "AVERAGE	90.9% CONFIRM TECH DELAYS

[5] Legal Services Board UK, 2021
[6] Datt & Sharma, 2021
[7] Susskind, 2019
[8] Lipsky, 2010 — Street-Level Bureaucrac
[9] NCAER Report, 2022

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 12 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

Table 1: Detailed Demographic Profile and System Engagement Breakdown ($N=11$)

Variable description	Category sub-group	Absolute count (n)	Sample share (%)
Standing / practice experience	Junior advocates (less than 1 year)	7	63.6%
	Mid-level advocate (1 to 5 years)	4	36.4%
E-filing usage pattern	Regular users (primary filing mechanism)	6	54.5%
	Occasional user (secondary mechanism)	5	45.5%
General system perception	Average/functional interface	8	72.7%
	Good/ user - friendly interface	3	27.3%
	Poor / unusable interface	0	0.0%

4.1 Analysis of Usability and Interface Comfort

The quantitative data reveals a crucial insight regarding system perception: the portal is not viewed as hostile or unworkable, but rather as a basic, unrefined utility. When asked to evaluate overall system ease on a 5-point Likert scale (1 = Very Difficult, 5 = Very Easy), 63.6% ($n=7$) chose rating 3 (Moderate/Neutral), while 18.2% ($n=2$) chose rating 4 (Easy) and 18.2% ($n=2$) chose rating 2 (Difficult). Crucially, zero respondents selected rating 1 (Very Difficult) or rating 5 (Very Easy)[10].

This clustering in the middle scale demonstrates an "Average Usability Trap"—the system performs fundamental data submission tasks, but lacks the speed, polish, and error-handling expected of modern digital infrastructure[11].

[10] *See* NAT'L JUDICIAL DATA GRID (NJDG), *Institutional Case Pendency Statistics and Digital Intake Performance Data*, MINISTRY OF L. & JUST. (2024)
[11] *See* Fred D. Davis, *Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology*, 13 MIS Q. 319, 319–40 (1989).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 12 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

Table 2: 5-Point Likert Distribution — Ease of E-Filing System Operation

Likert score	Qualitative descriptor	Response count (n)	Percentage share (%)
Score 1	Very difficult	0	0.0%
Score 2	Difficult	2	18.2%
Score 3	Moderate/average	7	63.6%
Score 4	Easy	2	18.2%
Score 5	Very Easy	0	0.0%

5. THE "AVERAGE USABILITY TRAP" HYPOTHESIS

A major finding of this empirical research is the concentration of responses in Likert Score 3 (63.6% "Moderate/Average"), combined with 0.0% responses at both extreme ends (Score 1 and Score 5). When combined with general perception data (72.7% rating the system as "Average"), this pattern supports the "Average Usability Trap" Hypothesis[12].

This hypothesis posits that state-operated public software infrastructure achieves baseline functional utility— allowing users to complete mandatory data submissions—but fails to provide the speed, reliability, and modern user experience (UX) standards found in commercial digital platforms. Users do not find the platform unusable, but experience persistent micro-frictions that slow down work and increase administrative effort.

5.1 Cross-Tabulation: Experience Standing vs. System Perceptions

To examine whether professional experience influences technology adaptation, data on practice standing was cross-tabulated against perceived system ease of use.

Analysis indicates that junior advocates (<1 year standing) report higher adaptability to interface quirks, yet express greater frustration with technical delays due to tight filing deadlines. Mid-level practitioners (1–5 years standing) show higher tolerance for procedural delays but express strong critique regarding redundant paper filing mandates enforced by court registries.

6. DEEP DIVE: SYSTEMIC BOTTLENECKS & TECHNICAL FRICTION

While broad usability ratings indicate baseline functional acceptability, probing specific technical touchpoints uncovers severe systemic bottlenecks that hamper legal practice. Table 3 presents the breakdown of primary operational difficulties encountered by practitioners[13].

Table 3: Primary Technical & Operational Difficulties Encountered in E-Filin

Operational obstacle category	Primary choice (n)	Percentage share (%)	Impact severity level
Document upload	5	45.5%	Critical operational

[12] SUPREME COURT OF INDIA E-COMMITTEE, *Phase III Vision Document for the e-Courts Integrated Mission Mode Project* 12–15 (2023).
[13] HM COURTS & TRIBUNALS SERV., *HMCTS Reform Programme Projects Explanatory Document* 8–12 (2021).

limitation (size caps & compression)			barrier
Technical & server infrastructure outages	2	18.2%	High systemic impact
Complex workflow & lack of technical guidance	2	18.2%	Moderate administrative
Court fee payment gateway drops & failure	1	9.1%	High financial risk
Security , privacy & OTP authentication errors	1	9.1%	Moderate technical friction

7. The Document Upload Crisis and File Size Thresholds

As demonstrated in Table 3, 45.5% of respondents identified document uploading as their single greatest operational hurdle[14]. Current judicial e-filing guidelines enforce strict file size caps—frequently restricting individual PDF uploads to 5 Megabytes (5MB) per file or capping entire petitions at 20MB.

In trial and appellate litigation, pleadings routinely include extensive annexures, lower court judgment records, certified deeds, witness depositions, and documentary evidence running into hundreds of pages. To comply with 5MB upload restrictions, advocate offices must perform extreme PDF compression or split single legal filings into dozens of fragmented sub-files[15].

7.1 Infrastructure Reliability and Limitation Period Risks

Server instability during peak filing hours represents a major operational vulnerability. The survey measured practitioner agreement on whether technical glitches directly contribute to filing delays[16].

Table 4: Practitioner Agreement on Technical Glitches as Drivers of Filing Delay

Response scale option	Respondent count (n)	Percentage share (%)	Consensus metric
Strongly agree	4	36.4%	
Agree	6	54.5%	90.9% combined consensus

[14] Gautam Datt & Rahul Sharma, *Digital Transformation of the Indian Judiciary: Evaluating the Impact of the e-Courts Project*, 18 J. L. TECH. & PUB. POL'Y 145, 152–58 (2021).
[15] RICHARD SUSSKIND, ONLINE COURTS AND THE FUTURE OF JUSTICE 45–52 (2019).
[16] DORY REILING, TECHNOLOGY FOR JUSTICE: HOW INFORMATION TECHNOLOGY CAN SUPPORT JUDICIAL REFORM 89–104 (2010)

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 12 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

8. **IMPACT ON PROFESSIONAL EFFICIENCY & ACCESS TO JUSTICE**

A primary goal of judicial digitalization is compressing case processing timelines and reducing physical court travel expenses[17]. The empirical data presents a nuanced picture of whether e-filing has realized these objectives in practice[18].

Table 5: Practitioner Sentiment on Time Savings vs. Court Visit Reductions

Sentiment indicator	Saves professional time (%)	Reduces physical visits (%)
Strongly agree	0.0%	18.2%
Agree	18.2%	27.3%
Neutral / undecided	45.5%	36.4%
disagree	27.3%	9.1%
Strongly disagree	9.1%	9.1%

8.1 Time Savings Evaluation

As detailed in Table 6, practitioner opinion on time savings is divided: 36.4% disagree or strongly disagree that e-filing saves time, 45.5% remain neutral, and only 18.2% agree. This negative sentiment reflects the additional non-legal labor required to reformat PDF documents, resolve portal errors, and perform duplicate physical filings.

8.2 Physical Court Attendance Reductions

Regarding whether e-filing reduces physical court visits, empirical sentiment is more positive: 45.5% of respondents agree or strongly agree that physical visits have declined, while 36.4% remain neutral, and 18.2% disagree[19].

Where registries strictly enforce digital-only workflows without demanding physical paper backups, advocates experience tangible reductions in physical travel[20]. However, in courts where registry staff insist on receiving physical files, the need for physical visits remains unchanged.

9. MACRO ASSESSMENT OF JUDICIAL DIGITALIZATION

Despite day-to-day operational frustrations, overarching practitioner sentiment regarding the broader initiative of judicial digitalization remains receptive and forward-looking[21]. Figure 2 and Table 7 detail respondent assessments of whether e-filing has improved judicial efficiency overall.

Table 6: Overall Practitioner Assessment — Has E-Filing Improved Judicial Efficiency?

[17] WORLD BANK GROUP, DOING BUSINESS 2020: ENFORCING CONTRACTS AND JUDICIAL AUTOMATION IN DEVELOPING ECONOMIES 62–67 (2021).
[18] LEGAL SERVS. BD. UK, EVALUATION OF DIGITAL COURT REFORMS AND ACCESS TO JUSTICE FOR SELF-REPRESENTED LITIGANTS 14–22 (2021).
[19] Code Civ. Proc. § 148A (1908) (India); *see also* The Limitation Act, 1963, § 5 (India) (governing condonation of delay caused by administrative or technical impediments).
[20] *See* Information Technology Act, 2000, § 5 (India) (granting legal recognition to electronic signatures for authentication of court filings).
[21] *See* SUPREME COURT OF INDIA, *e-Filing 3.0 User Manual: Standard Operating Procedure for Advocates and Litigants-in-Person* 14–18 (2022).

Assesment category	Response count (n)	Percentage share (%)	Strategic socio- legal insight
Strongly agree Agree	1 3	9.1% 27.3%	36.4% positive sentient : early adopters experiencing workflow gains

This finding offers a clear signal for judicial policy makers: advocate practitioners are willing partners in digital transformation. Resolving underlying technical glitches and administrative duplication will unlock widespread practitioner endorsement and operational efficiency gains.

10. PRACTITIONER REFORM PRIORITIES & STRATEGIC ROADMAP

To identify targeted institutional remedies, respondents ranked primary reform priorities required to optimize e-filing performance[22]. Table 7 outlines these priorities alongside recommended policy implementation pathways.

Table 7: Practitioner Reform Priorities for System Enhancement (N=11)[23]

System reform priority	Preference (%)	Institutional implementation pathway
Faster document verfication	36.4%	Establish SLA- backed 24-hour verification timelines for registry srutinizers
Simplified filing procedure	36.4%	Streamline web form,introduce smart field pre-filing and guided UI wizards
Better server & portal performance	27.3%	Migrate to scalable cloud architecture and increase file size caps to 50MB
Advocate training & help desks	0.0%	Core functionality upgrades prioritized over external user training
Cybersecurity & encryption	0.0%	Baseline security assumed,usability fixes demanded immediately

[22] *See* M.P. Jain, *Indian Constitutional Law* 1420–25 (8th ed. 2018) (discussing Article 21 rights to speedy trial and procedural access).
[23] *See* Anita Kushwaha v. Pushap Sudan, (2016) 8 SCC 509, 532 (India) (holding that access to justice is a fundamental right guaranteed under Article 21 of the Constitution of India).

10.1 Analysis of Reform Preferences

The data reveals a clear demand for core backend and workflow improvements over secondary support measures: 100% of practitioner reform votes focused on core system functional upgrades[24] (36.4% Faster Verification, 36.4% Simplified Procedure, 27.3% Better Server Performance), with zero votes assigned to external training or cybersecurity

11. POLICY RECOMMENDATIONS & IMPLEMENTATION ROADMAP

Based on empirical findings and qualitative analysis, this study proposes a three-pillar policy roadmap to transition Indian judicial e-filing into an efficient digital ecosystem.

11.1 Pillar I: Infrastructure Expansion & Technical Standardization

Technical bottlenecks are the primary driver of practitioner frustration. Addressing these friction points requires targeted infrastructure upgrades:

- Dynamic Cloud File Allocation & 50MB Size Caps: Upgrade portal storage backends to support

single-file uploads up to 50MB, utilizing server-side compression and automatic background OCR processing to reduce client-side file preparation burdens.

- High-Availability Server Architecture: Implement load-balanced cloud server infrastructure designed to handle peak filing hours (3:00 PM – 5:00 PM and 11:00 PM – 12:00 AM) without performance degradation or system timeouts[25].
- Automated Payment Gateway Reconciliation: Integrate real-time payment webhooks with state treasuries, featuring automatic retry loops and instant transaction verification to eliminate unrefunded dropped fee payments.

11.2 Pillar II: Procedural Rationalization & Administrative Oversight

Technology alone cannot resolve judicial inefficiency if legacy bureaucratic practices remain unchanged. Procedural reforms must accompany technological upgrades:

- Strict Ban on Duplicate Physical Filings: Issue binding practice directions across all High Courts and District Courts prohibiting registries from demanding physical paper backup files for matters successfully efiled with digital signatures.
- Service Level Agreements (SLAs) for Scrutiny: Mandate a strict 24-hour deadline for registry verification of e-filed cases, supported by automated dashboard alerts for supervisory judges to track pending verification backlogs[26].
- Standardized Defect Taxonomy & Inline Annotations: Replace generic registry objection tags with a standardized drop-down defect taxonomy and direct PDF annotation tools, allowing advocates to easily identify and correct filing errors.

[24] E-COMMITTEE, *supra* note 2, at 45 (outlining proposed Cloud Computing and SaaS migration pathways).
[25] *See* BAR COUNCIL OF INDIA, *Rules of Professional Standards and Advocate Disciplinary Rules*, r. 12 (1975) (addressing advocate liability for filing defaults).
[26] M.P. Jain & Anita Kushwaha v. Pushap Sudan

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 12 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

11.3 Pillar III: User-Centric Design & Integrated Platform Architecture

To lower operational complexity, judicial portals should adopt modern interface design standards:

- Guided Multi-Step Filing Wizards: Redesign portal filing forms into step-by-step guided wizards featuring real-time data validation to prevent data entry errors prior to submission.
- Unified Advocate Access Portal (Single Sign-On): Consolidate disparate regional e-filing portals into a unified national access portal linked to Bar Council of India (BCI) practitioner databases[27].

12. COMPARATIVE EMPIRICAL FRAMEWORK: PRE- AND POST-REFORM PATHWAYS

To demonstrate the practical impact of the proposed policy recommendations, Table 8 compares current operational friction points against projected outcomes following targeted reforms.

Table 8: Comparative Analysis of Current E-Filing Workflows vs. Reformed Digital Pathways

Workflow dimension	Current operational reality (status quo)	Reform target state (post - policy action)
Document uploads	5MB hard cap, cilent-side PDF compression,risk of illegible text	50MB file limits,dynamic server -side compression &auto-OCR.
Physical duplication	Duplicate physical paper filing mandatory in many registers.	100% paperless workflow, binding ban on redundant paper submission.
Payment processing	Dropped payment transactions require manual treasury refund claims.	Integrated multi-bank webhooks with instant reconciliation & auto-retry.
Registry verification	Unpredictable turnaround (1-5days), generic defact notice	24-hours SLA guarantee,standardized defect taxonomy & inline PDF feedback
System availability	Frequent server timeouts during peak filing hours (3-5pm)	Auto- scaling cloud infrastructure with 99.9% uptime SLA

12.1 Evaluating System Progression Through Technological Acceptance Metrics

Applying the Technology Acceptance Model (TAM) framework to the post-reform target state indicates that resolving baseline operational friction directly enhances Perceived Ease of Use (PEOU)[28].

[27] Limitation Act, 1963 & BCI Professional Rules
[28] Datt & Sharma, 2021 & Susskind, 2019

As PEOU improves, practitioner compliance shifts from forced administrative adherence to active professional preference, driving broader digital transformation across the legal sector.

13. CONCLUSION & INSTITUTIONAL SYNTHESIS

Electronic filing systems represent a critical pillar of India's vision for a modernized, accessible, and transparent judicial system. This non-doctrinal empirical research study demonstrates that legal practitioners have fully embraced digital court platforms as an integral component of routine litigation practice (100% active usage across the respondent cohort). However, user experience remains constrained within an "average usability trap"

(72.7% neutral rating), burdened by persistent technical bottlenecks and redundant paper filing mandates[29].

The empirical investigation identifies three primary operational vulnerabilities requiring immediate policy attention:

1. Inflexible Document Storage Infrastructure: Capping file uploads at 5MB creates substantial nonbillable overhead for advocate offices, forcing unnecessary document splitting and file quality degradation[30].

2. The Hybrid Paper-Digital Paradox: Mandatory demands for physical paper backups alongside

electronic submissions eliminate time savings and double operational costs for litigating parties.

3.Financial and Scrutiny Delays: Payment gateway timeouts without real-time reconciliation, combined with slow, opaque registry defect notifications, undermine confidence in digital court workflows[31].

Importantly, empirical findings reveal zero ideological resistance from the legal bar toward judicial digitalization. Advocate practitioners view digital transformation as a necessary step forward for court administration. By implementing targeted cloud infrastructure upgrades, enforcing strict scrutiny SLAs, eliminating duplicate paper requirements, and adopting user-centric portal designs, the Indian judiciary can realize the full potential of Phase III of the e-Courts project—building a modern, paperless, and efficient system of justice.

REFERENCES

1. e-Committee, Supreme Court of India. (2023). Phase III Vision Document for the e-Courts Integrated Mission Mode

Project. New Delhi: Supreme Court of India Press

2. Datt, G., & Sharma, R. (2021). "Digital Transformation of the Indian Judiciary: Evaluating the Impact of the e-Courts Project." Journal of Law, Technology & Public Policy, 18(2), 145–172.

3. Davis, F. D. (1989). "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology." MIS Quarterly, 13(3), 319–340.

[29] NCAER Report, Reiling, World Bank, LSB UK
[30] Lipsky, Street-Level Bureaucracy
[31] e-Committee Phase III Cloud Vision

4. Lipsky, M. (2010). Street-Level Bureaucracy: Dilemmas of the Individual in Public Service. 30th Anniversary Edition. New York: Russell Sage Foundation.

5. National Council of Applied Economic Research (NCAER). (2022). Evaluating Court Infrastructure, E-Filing

Adoption, and Judicial Productivity Across Indian District Courts. New Delhi: NCAER Reports.

6. Reiling, D. (2010). Technology for Justice: How Information Technology Can Support Judicial Reform. Leiden: Leiden University Press

7. Susskind, R. (2019). Online Courts and the Future of Justice. Oxford: Oxford University Press

8.World Bank Group. (2021). Doing Business 2020: Enforcing Contracts and Judicial Automation in Developing

Economies. Washington, D.C.: World Bank Publications.

9. Legal Services Board UK. (2021). Evaluation of Digital Court Reforms and Access to Justice for Self-Represented Litigants. London: LSB Research Series

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 12 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

ARTIFICIAL INTELLIGENCE AND THE LAW OF EVIDENCE: RECONCEPTUALISING AUTHENTICITY, PROOF AND JUDICIAL RELIABILITY IN INDIA

AUTHOR – PRABHNOOR KAUR MAKKAR**,** LL.M STUDENT AT UNIVERSITY INSTITUTE OF LEGAL STUDIES, CHANDIGARH UNIVERSITY, MOHALI, PUNJAB, INDIA

BEST CITATION – PRABHNOOR KAUR MAKKAR, ARTIFICIAL INTELLIGENCE AND THE LAW OF EVIDENCE: RECONCEPTUALISING AUTHENTICITY, PROOF AND JUDICIAL RELIABILITY IN INDIA, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 6 (12) OF 2026, PG. 13-29, APIS – 3920 – 0001 & ISSN - 2583-2344.

Abstract

Generative artificial intelligence has influenced drastically the evidentiary value of electronic data. AI systems can generate images, videos, conversations and texts that can seem real events. This phenomenon creates new challenges in defining the connection between electronic communication and reality. This paper analyzes if Indian rules of evidence can cope with the challenges of AI-generated and AI-modified materials based on Bharatiya Sakshya Adhiniyam, 2023 and IT Act, 2000. The research clarifies the difference between electronic record integrity, authenticity and admissibility, as well as the role of verification, provenance, forensic examination and AI identification. The paper provides examples of the most significant cases, such as *Anvar P.V. v. P.K. Basheer*, *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* and *Pune Bar Association v. Union of India*, and shows what the approach of US law and European legislation regarding to AI.[32]This paper points out that merely adhering to the formal requirements associated with electronic records is not sufficient proof of the veracity of any synthetic representation.

***Keywords*:** Artificial Intelligence; AI-Generated Evidence; Deepfakes; Bharatiya Sakshya Adhiniyam, 2023; Electronic Evidence; Digital Authentication; Evidentiary Reliability; Fair Trial.

1. INTRODUCTION

The functioning of judicial authorities is based on their ability to process information provided in order to prove disputable facts. Documents, photos, video/audio recordings, electronic messages as well as expert opinions are the means of judicial practice reconstruction of events. Though these kinds of proof were never safe from dealings, the usual procedures of their obtaining have provided identified points of reference to determine authorship, authenticity of evidence. The development of generative artificial intelligence has complicated this process considerably.[33]

[32] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473; *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1; *Pune Bar Association v. Union of India*, W.P. (C) No. 599 of 2026, order dated 22 May 2026; Federal Rules of Evidence, Rules 702 and 901; Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024.

[33] Robert M. Chesney and Danielle Keats Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 *California Law Review* 1753.

Generative artificial intelligence can create digital content that imitates human behavior expression, physical appearance, voice, surroundings, events that took place. A photo can show a person at a place they never visited and an audiovisual recording can reproduce a person's appearance and voice without their participation. An AI-generated dialogue can witness the conversation that has never taken place.[34] The problem does not lie in defining if a digital document has been modified after its creation anymore. It involves proving whether the document was created without any analog of events in reality.

This occurrence brings to the fore a key assumption related to evidentiary use of photos and audio recordings that assumes realistic digital content is usually based on direct observation of the represented events. The tendency of digital content to be convincing may as a result create an impression of evidentiary value that is largely disproportionate to its real reliability.[35]

The difference between electronic and AI-generated evidence should be underlined. Electronic evidences typically deal with the information that has been stored, transmitted, or produced through electronic mediums. AI-generated evidence may include electronic information whose meaning or context has been created or significantly modified in the process of AI operation. The two categories are not exclusive and often overlap as AI-generated material can be an electronic record and vice versa, like an authentic electronic recording which would undergo AI-assisted transformation.[36]

Currently, the law in India deals with electronic evidence according to rules regarding admissibility, certification, expert opinion, and proof of documentary content. The Bharatiya Sakshya Adhiniyam, 2023 ("BSA") which became effective on July 1, 2024 has acknowledged the presence of electronic and digital records in terms of documentary evidence.[37] Sections 61-63 are particularly related to the admissibility of electronic records and Section 39 provides for expert opinion on issues that require expert knowledge, e.g., electronic and digital information.[1]

The main point of this paper is that the problem of evidence raised by generative artificial intelligence arises from the difference between the authenticity of the digital creation and the factual validity of the event presented in it. Indian evidence law serves as a solid basis for the admissibility of electronic records, but the implementation of this law in AI-generated evidence should entail the distinction between the authentication of the record, verification of the event, reliability of method, and significance of evidence.

2. STUDY ISSUE AND IMPORTANCE

The expansion of the use of AI-generated or AI-processed digital content raises the problem of which criteria should be used by the judiciary when assessing the authenticity and validity of electronic records. Although the BSA defines the terms "electronic and digital records and indicates the criteria for admissibility", the application of the specified standards to data created by artificial intelligence is the issue that is still developing in law.[38]

[34] Ibid.
[35] Paul W. Grimm, Maura R. Grossman and Gordon V. Cormack, 'Artificial Intelligence as Evidence' (2021) 19 *Northwestern Journal of Technology and Intellectual Property* 9.
[36] Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, ss. 2(1)(d), 2(1)(e), 61–63.
[37] Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, ss. 2(1)(d), 2(1)(e), 61–63; Ministry of Home Affairs, Notification S.O. 849(E), dated 23 February 2024.
[38] Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, ss. 2(1)(d), 2(1)(e), 61–63.

The problem is particularly important in cases where a party relies on photographs, videos, voice recordings, and electronic communications as concrete evidence of an event in question. As a result, a court inquiry should not only examine the way these pieces of evidence were obtained, but also whether the evidence is connected to the actual event, whether the AI used in producing evidence manipulated the content and whether the information available supports the fact in question.[39]

Therefore, the research issue goes beyond the admissibility of AI-generated evidence, to the applicability of the current system of evidence to separate a valid piece of electronic evidence from a trusted documentation. This distinction affects the evidence collection process, authentication, expert evaluation, and challenges caused by the counterparty and proof weight determination.

The article by *Chesney and Citron* highlights the effects of synthetic media on privacy, democracy and national security issues, while demonstrating that such credible fake materials can challenge the entire audiovisual trustworthiness. The importance of their work to the law of evidence stems from the fact that synthetic media can lead to not just the manipulation of information but also the manipulation of the trust that is given to the evidentiary form, by which information has been conveyed.[40]

The academic work of Grimm, Grossmann and Cormack on AI as evidence gives an additional viewpoint through an exploration of the relationship between the AI technologies and the legal processes of evaluation of information. Their research plays a key role in making the dichotomy between the operation of the AI system as such and the conclusions made based on the results of its functioning and this becomes especially important when the courts rely on algorithmic results or AI-produced materials.[41]

Scholars in India have begun looking into the application of BSA to the AI-generated and deepfake evidence.Budget plain: New research on Section 63 touch upon the matters of legislative endorsement, validation, and features of AI-generated content.

3. THE LITERATURE EMPHASIZES THE IMPORTANCE OF DIGITAL PROVENANCE.

The Coalition for Content Provenance and Authenticity (C2PA) provided technical specifications for recording and confirming data related to the origin and history of digital materials.[42] While using such tools can provide information about content production and changes, such information wouldn't prove the validity of the content itself.

The literature is already vast, but some of the issues require additional analysis. The two questions of admissibility of electronic evidence and authenticity of synthetic content are frequently discussed without distinguishing the legal aspects involved. Detection techniques are often viewed as the main answer, despite the fact that limitations are known. The relationship of such concepts as provenance, certification and the truth of facts also requires doctrinal clarifications. This paper addresses this issues

[39] Paul W. Grimm, Maura R. Grossman and Gordon V. Cormack, 'Artificial Intelligence as Evidence' (2021) 19 *Northwestern Journal of Technology and Intellectual Property* 9.
[40] Robert M. Chesney and Danielle Keats Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 *California Law Review* 1753.
[41] Paul W. Grimm, Maura R. Grossman and Gordon V. Cormack, 'Artificial Intelligence as Evidence' (2021) 19 *Northwestern Journal of Technology and Intellectual Property* 9.
[42] Coalition for Content Provenance and Authenticity, *Content Credentials: C2PA Technical Specification*, available at: https://spec.c2pa.org/ (last visited 14 November 2026).

from the point of view of treating the artificial intelligence-generated evidence as a classification and judicial reasoning problem instead of a separate technology that should either be allowed or banned.

4. RESEARCH QUESTIONS, OBJECTIVES AND METHODOLOGY

4.1 Research Questions

The study aims at answering the following questions:

1. Does Indian law on electronic evidence properly distinguish the authenticity of documents from the truth of the event in question?
2. Do the provisions of the BSA (Sections 39 and 61–63) provide the legal and procedural guarantees for the analysis of AI-produced and modified evidence?
3. Can the concepts of certification, hashing and digital provenance guarantee the reliability of synthetic evidence, or shall their importance for law be limited to narrow sphere of integrity and creations of e-records only?
4. Can AI-detection methods and digital forensic process provide information on the authenticity of a digital document, in spite of their methodological limitations?
5. Does comparative law provide any useful rules to improve the Indian court practice in evaluating AI-generated evidence without establishing a presumption of exclusion?

4.2 Aim of the Research

The aims of the study include evaluation of the existing legislative framework regulating electronic evidence, study of relevant case law, differentiation between technical integrity and factual authenticity, assessment of shortcomings of detection and provenance mechanisms, and recommendations for assuring the judicial evaluation of AI-generated materials.

4.3 Research Methodology

The research applies doctrinal methodology, analytical methodology as well as comparative law methodology. It is based on the study of legal provisions, relevant court decisions, literature on legislation and technical norms related to AI-generated evidence. The comparative analysis process is done by the means of studying the relevant rules of the US law of evidence and the European Union legislation regulating AI.[43]

5. THE INTERPRETATION OF AI-BASED EVIDENCE: TYPES AND RELEVANCE

The phrase "evidence derived from AI" does not necessarily refer to a single type of proof. What constitutes reliable evidence based on AI technology depends upon whether such technology produces the information in question directly or modifies the already existing data, supports its processing, or reproduces lost evidence. In order to make a thorough legal analysis, it is important to distinguish various types of AI involvement.

[43] Federal Rules of Evidence, Rules 702 and 901, United States of America; Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024.

The term "fully AI-generated content" refers to the content produced by generative systems of AI without the original information being recorded. For example, a synthetic video depicting a person performing an act that never took place belongs to this category. This content can be highly realistic but it does not prove that the event has occurred.[44]

AI-modified evidence denotes existing digital records that have undergone alterations thanks to artificial intelligence technology. The change can happen in different forms, like facial alterations, speech changes, introduction of other objects, etc. The degree of modification matters because in some cases, a modified element can influence the factual meaning of evidence significantly.[45]

AI-assisted evidence implies the introduction of AI technology to process or analyze existing evidence. For instance, AI can serve for transcription or noise reduction, image improvement, translation, or extracting specific information from records. The reliability of the evidence generated by AI will equally depend on the nature of processing and the degree of changes made to the original data.[46]

AI-reconstructed evidence refers to evidence created by reconstructing the missing or damaged parts of the record. Such reconstruction can be valuable in investigations, but the reconstructed parts should not be understood as direct evidence of an event. The distinction between real and reconstructed evidence is critical whenever the evidence is presented to address the issue of some specific factual claims.[47]The significance of the role of AI in evidence depends on its role in that evidence.

5.1 Digital Integrity Versus Factual Authenticity

Tension of ideas must exist if we want to talk about digital integrity and factual authenticity.

Digital integrity refers to whether or not the evidence was changed at any stage of its lifetime or how one can establish its identity and keep track of it. Digital integrity can be proved by utilizing hash values, protective measures, and chain-of-evidence documentation, etc.[48]

Factual authenticity describes whether the content is the honest representation of the matter being depicted. For example, even though the photograph remains unchanged, it can depict some image that was artificially created.[49]

The differentiation works in the reverse direction as well. An authentic recording can be legitimately improved or manipulated which can create a new file but keep the key data about the event. Hence, the judicial practice does not imply excluding such a piece of evidence just because it was generated on the processed file.

Therefore, when the moment of making a judicial evaluation of AI evidence comes, three separate issues have to be solved at least: whether the electronic record was preserved properly; whether the

[44] Robert M. Chesney and Danielle Keats Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 *California Law Review* 1753.
[45] Paul W. Grimm, Maura R. Grossman and Gordon V. Cormack, 'Artificial Intelligence as Evidence' (2021) 19 *Northwestern Journal of Technology and Intellectual Property* 9.
[46] Ibid.
[47] Ibid.
[48] Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, s. 63(4) and the Schedule; Coalition for Content Provenance and Authenticity, *Content Credentials: C2PA Technical Specification*.
[49] Robert M. Chesney and Danielle Keats Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 *California Law Review* 1753.

content of the record was authentic concerning the event; whether the information is authentic enough to draw the conclusions set for from it.[50]

6. THE INDIAN STATUTORY FRAMEWORK

6.1.Electronic Evidence in the Bharatiya Sakshya Adhiniyam 2023

The BSA is the latest legal instrument to regulate evidence in the country, which incorporates some recommendations about electronic and digital records in terms of evidentiary value.[51]

Particularly important in this context are Sections 61-63.[52] Section 61 deals with admissibility of electronic records while Section 62 deals with proof of such records according to Section 63 which contains provisions relating to legal requirements for electronic evidence produced by computer systems.

The significance of this legislation lies in its recognition of the necessity of special procedures for electronic information. It is necessary to note that the electronic records might be reproduced, transferred and presented with the help of different systems and devices. Thus, there is a need for certification and various prescribed technical details determining all the necessary conditions for the production of such records.

Section 63 contains a Schedule providing for particulars necessary for certification. The Schedule presents information about electronic record as well as about the computer or communication device including prescriptive requirements for certification. The structure consists of Parts A and B, and the latter one contains the expertise.[53]The statute and technical parameters define the essence of certification. Certification indicates that the record was produced in accordance with particular systems and that specific technical requirements of establishing the certificate were satisfied. However, certification alone does not determine whether the information was obtained as a result of a true observation of an event rather than through artificial generation.

This is particularly relevant in the case of artificial audio-visual content. The certification may accurately describe the electronic record itself and the process of its production, while the content itself presents a non-existent event. Therefore, the requirements for admissibility of electronic records should not be used as a means of obtaining valid proof of factual authenticity of the information contained in an electronic file.[54]

6.2 Section 39 and Expert Opinion

Section 39 of the BSA provides for the importance of expert opinion on the issues needing specialization. The provision includes the opinion on the data transmitted or stored electronically.[55] Expert examination is crucial when authenticity cannot be established based on observational facts alone. Digital forensics experts examine metadata, encoding peculiarities, discrepancies, or source information.The analysis they conduct will help the court determine whether a document has been changed, whether there is a

[50] Paul W. Grimm, Maura R. Grossman and Gordon V. Cormack, 'Artificial Intelligence as Evidence' (2021) 19 *Northwestern Journal of Technology and Intellectual Property* 9.
[51] Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, ss. 2(1)(d), 2(1)(e), 61–63.
[52] Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, ss. 61–63.
[53] Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, s. 63(4) and the Schedule.
[54] *Pune Bar Association v. Union of India*, W.P. (C) No. 599 of 2026, order dated 22 May 2026 (Supreme Court of India); Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, s. 63.
[55] Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, s. 39(1)–(2).

number of features pointing to synthetic production, or whether the materials in evidence are consistent with the production process.

It must be stated that the court has to make a distinction between an expert conclusion regarding the technical specifics of the document and the final legal decision on its authenticity and evidential significance. Section 39 provides specific context for expert aid but it does not transfer the function of the judge to the expert.[56]

6.3 Section 79A of Information Technology Act, 2000

According to Section 79A of Information Technology Act, 2000, the Central Government has the right to appoint an electronic evidence expert who will provide the necessary expert analysis of the electronic evidence.[57]

The courtroom and law enforcement would encounter less difficulty when interested in investigating the electronic records and resolving technical concerns thanks to the presence of a certified examiner. However, this legal recognition of the expert does not mean that it is possible to validate any AI-created data solely by means of one technical approach.

The analysis of the artificial material implies that it is necessary to deal with various aspects of generative processes, source data, modifications that took place, and restrictions imposed by detection technologies.

6.4 Use of Hash Technique for Certification

Recently, hash values have become quite common in digital forensic practices used to determine and compare files.[58] A hash function generates a value that corresponds to the given data. At the same time, since the same data with the same approach is processed each time, one usually expects that the value produced will remain the same.

This means that it is possible to determine whether the file remained the same during the processing of an electronic record since the two processes will produce different values.Nonetheless, a hash value does not provide any indication as to if the content was authentic at the time of its creation. It does not show who authored the said file and under what circumstances, and whether the information presented is valid in terms of facts. It could be said that the synthetic recording possessed the same unchanging hash value as the authentic one.[59] Hashing serves to identify digital content and observe changes, rather than serving as an autonomous means for determining the truth of an audiovisual representation.[60]

[56] Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, s. 39(1)–(2).
[57] Information Technology Act, 2000, No. 21 of 2000, s. 79A.
[58] *Pune Bar Association v. Union of India*, W.P. (C) No. 599 of 2026, order dated 22 May 2026 (Supreme Court of India); Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, s. 63(4) and the Schedule.
[59] Paul W. Grimm, Maura R. Grossman and Gordon V. Cormack, 'Artificial Intelligence as Evidence' (2021) 19 *Northwestern Journal of Technology and Intellectual Property* 9.
[60] Coalition for Content Provenance and Authenticity, *Content Credentials: C2PA Technical Specification*, available at: https://spec.c2pa.org/ (last visited 14 November 2026).

6.5 The Relationship between Certification and Reliability

One of the recurring problems associated with the issue of AI-generated evidence is linking compliance with electronic-record certification with the general conclusion about evidentiary reliability that may be drawn from it.

As far as certification and reliability are concerned, they are interrelated but different things. Certification may prove that certain technical parameters have been adhered to while creating the electronic record while reliability concerns the ability of the record to be reasonably supportive of the claims it is meant to prove. So satisfying the requirement of Section 63 cannot be regarded as an automatic solution of the problem of synthetic true information.[61]

7. JUDICIAL PROCESSES AND THEIR MEANING FOR AI EVIDENCE

7.1 *Anvar P.V. v. P.K. Basheer*

In *Anvar P.V. v. P.K. Basheer* the Supreme Court looked into the admissibility of electronically produced evidence under Section 65B of the Indian Evidence Act of 1872. The Court clarified the requirements for producing electronic evidence and pointed out the importance of evidence certification.[62]

The judgment laid the first stone for the admissibility of electronic evidence by saying that electronic evidence has to comply with statutory rules on computer data and it is important for the applicability of electronic data. Nevertheless, Anvar has not dealt with synthetic content or the factual accuracy of images produced via artificial intelligence.

7.2 *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal*

The Supreme Court reconsidered the e-evidence framework afterwards in Arjun *Panditrao Khotkar v. Kailash Kushanrao Gorantyal.*[63] The Court affirmed the significance of Section 65B certification concerning secondary electronic evidence and explained the issues concerning the authenticity of electronic records and when a certificate could be obtained.[64]

This ruling is important since it explains the links between electronic record, computer output and the legislative conditions for admissibility. In addition, it demonstrates that the law of electronic evidence cannot be viewed through the lens of merely examining the appearance or credibility of the digital content. For AI evidence the ruling offers a basis but does not provide a full answer. In particular, the question whether a record adheres to the legislative requirements is not the same as whether its content corresponds to the event occurred.[65]

7.3. *Pune Bar Association V. Union of India*

The judgment of the Supreme Court in the case of *Pune Bar Association v. Union of India* dated 22 May 2026 is important in understanding the present-day legal situation under BSA. The case questioned in lawfulness and constitutional validity of requirements regarding certification of evidence introduced by

[61] Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, ss. 39 and 63(4).
[62] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.
[63] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.
[64] Ibid.
[65] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473; *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.

the new regulatory law on electronic evidence. The Court sustained these requirements of the law but left the question of people's qualifications for signing Part B of the Schedule unanswered.[66]

The importance of the judgment lies in the fact that it proves the significance of regulation of the rules on technical certification as well as an expert element related to the electronic evidence.

7.4 Pooja Ramesh Singh vs. Jammu and Kashmir Bank

In the case of *Pooja Ramesh Singh vs. Jammu and Kashmir Bank,* the Supreme Court settled the question of whether the information produced by AI was legally valid and contained fake references.[15] The case shows the risks of relying on AI-generated data without verifying whether it is true or not.[67]

The case does not give an answer to the question of admissibility of deepfake pictures, videos, and synthetic audio-visual evidence but demonstrates the problem of AI-generated data being reliable and trustworthy, while containing false information. It is essential to note that the analogy should be scrutinized.[68]

Collectively, these courts' findings illustrate that Indian law acknowledges the importance of electronic record certification, expert knowledge and authenticator verification in a progressive manner. The legal basis for the issues related to AI-based evidence has been established; however, the issue of distinguishing between the integrity of the records and the accuracy of facts has not been fully clarified.

Digital provenance concerns information about the origin, creation, and further fate of digital contents.[69] It can contain information about the gadgets and software used to make a record, processing steps, source materials, and its changes.

8. THE COALITION FOR CONSENT

The Coalition for Content Provenance and Authenticity has established technical standards for recording and verifying content provenance.[70] Essentially, content credentials provide information about how the digital content was created and modified, which is helpful for the users and investigators to know the method of the creation of any document.

Such mechanisms may be useful where digital evidence has been processed multiple ways. A provenance report shows whether digital material is created, altered or subjected to a particular procedure. It may also help find discrepancies between what has been said about the production of such material and the information incorporated in the provenance record.

8.1 Chain of Custody and Preservation

Chain of custody is the process of documenting the handling of evidence from its acquisition through its examination to its presentation.[71]

[66] *Pune Bar Association v. Union of India*, W.P. (C) No. 599 of 2026, order dated 22 May 2026 (Supreme Court of India).
[67] *Pooja Ramesh Singh v. Jammu and Kashmir Bank Ltd.*, Civil Appeal No. 11950 of 2025, 2026 INSC 668, judgment dated 2 July 2026 (Supreme Court of India).
[68] Ibid.
[69] Coalition for Content Provenance and Authenticity, *Content Credentials: C2PA Technical Specification*, available at: https://spec.c2pa.org/ (last visited 14 November 2026).
[70] Ibid.
[71] Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, s. 63(4) and the Schedule.

In cases where information has been impacted by AI processing, preservation needs to include the original document, the processed document, as well as the processing information.[72] While chain of custody helps prove that an item under examination is the same as what was collected, it does not prove the authenticity of the original document. It is possible to maintain a synthetic document in an unbroken chain of custody.[73] While the chain of custody can show that the document being analyzed is identical to the document collected, it cannot prove that the document represents reality.

The difference between preservation and verification emphasizes the fact that preservation and verification should be regarded as two different components of the evidence examination. Such technologies are able to identify visible discrepancies, statistical tendencies, acoustic features, artifacts of compression, and other elements that relate to technologies of generation.

However, despite being able to facilitate forensic investigations, these technologies' results cannot be viewed as firm proof. For example, a system trained on a specific data or generation technique may act differently under non-familiar conditions. Compression, scaling, editing, and other operations may affect the detection of the method applied.

According to studies on deepfake detection, there are problems of generalization, stability, and the ability to detect material created by unfamiliar methods.[74] While a detector works well in lab conditions, there is no guarantee that it will behave correctly in real life. The matter of false positives is an important one since all real photographs or videos can appear to be wrongly classified as synthetic ones creating a problem for the investigation.

8.2. The Function of Human Experts

Expert evaluation is vital as automatic detection methods cannot independently answer all evidence-related queries. A qualified expert can see the environment of the specimen reviewed, define the limitations of a certain technique and make a decision about whether a deeper evaluation is needed.[75]

In particular, a technically valid report must separate features observed, analytical conclusions and findings. It has to define the material examined, the methods used, related limitations and confidence level founded on the available data.

If the examiner is not able to determine whether the recording is artificial, it is imperative to state the lack of a decisive result. An uncertain outcome should not lead to the conclusion about either the authenticity or forgery of the material.

The court is responsible for determining the effect of expert findings by references to the available evidence and the legal criteria.[76]

[72] Coalition for Content Provenance and Authenticity, *Content Credentials: C2PA Technical Specification.*
[73] Paul W. Grimm, Maura R. Grossman and Gordon V. Cormack, 'Artificial Intelligence as Evidence' (2021) 19 *Northwestern Journal of Technology and Intellectual Property* 9.
[74] David Güera and Edward J. Delp, 'Deepfake Video Detection Using Recurrent Neural Networks' (2018) 2018 IEEE International Conference on Advanced Video and Signal Based Surveillance 1.
[75] Paul W. Grimm, Maura R. Grossman and Gordon V. Cormack, 'Artificial Intelligence as Evidence' (2021) 19 *Northwestern Journal of Technology and Intellectual Property* 9.
[76] Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, ss. 39 and 63.

9.EVIDENCE LAW IN THE USA

The Federal Rules of Evidence provide important rules when assessing authentication and expert evidence. According to rule 901, sufficient information to support a conclusion that the evidence submitted is what the party claims it to be should be available.[77] The provision allows for authentication by presenting evidence, among which testimony, unique features, and other evidence contributing to the process of identification.

The expert evidence is governed by rule 702, which obliges the expert to meet the requirements regarding specific skills, assistance of the fact-finder, availability of data, reliability of methods and principles used.[78]

The United States has also considered proposals regarding deepfake evidence and the challenges of authentication of audiovisual evidence because such talks indicate that classical principles of authenticity may require modifications in case of digital evidence, like the one produced using modern technology. However, it is essential to point out that the establishment of additional rules associated with deepfakes is different from the current general principles of authenticity and expert evidence.

The value of American law is that it focuses on contextual authenticity; it proves that the existence of technological manipulation does not require the establishment of a separate admissibility rule for each group of digital evidence.

European Union Artificial Intelligence Act introduces the obligation of transparency in relation to the specified kinds of AI-generated or manipulated content.[79] Article 50 lays down some transparency requirements, such as the ones concerning synthetic content and deepfake materials. Thus, the EU regulations should be treated primarily in a practical sense of the regulatory mechanism of transparency rather than as a whole evidence model.[80]

9.1 Lessons for India

Therefore, certain lessons can be derived from the case of the European Union. Third, disclosure of material AI involvement may improve the ability of parties and courts to The disclosure of AI involvement in a significant way could be instrumental in enabling the parties as well as courts to better assess information in electronic form.

These principles could help strengthen the application of the BSAwhile avoiding mechanical importation of foreign rules and principles of regulation. The Indian law of evidence needs to function consistently with the statutory framework and the Constitution.

[77] Federal Rules of Evidence, Rule 901(a), United States of America.
[78] Federal Rules of Evidence, Rule 702, United States of America.
[79] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024, art. 50.
[80] Regulation (EU) 2024/1689, art. 50.

10. CRITICAL REMARKS: REDEFINING AUTHENTICITY AND EVIDENCE

10.1 The Insufficiency of Binary Thinking

The problem of AI-generated material is presented through the binary lens of being either admissible or inadmissible due to its alleged manipulability. Both solutions do not shed light on the essence of the issue.

The absolute bar may drive courts away from the use of true electronic evidence that underwent legitimate AI-related processing. Electronic techniques such as image enhancement, transcription, restoration, and so on may help in the analysis of evidence without causing any doubts regarding its authenticity.[81] Denying the admissibility of all such materials will result in the reduction of the evidentiary potential of electronic information.

The appropriate perspective must be able to realize that the intervention of AI is relevant for authentication and reliability but it is not the determinant factor for defining either of them. The evidential importance of a digital record is determined by the method of obtaining it, the factual claim on the base of which it is created, the verifier available and the surrounding situation.

10.2 The Difference between Authenticity and Evidential Weight

Authentication and evidential weight are not synonyms. Authentication is concerned with whether the material is actually the record or representation claimed by its proponent. Evidential weight is the measure of how much this material supports the factual claim to be proved.[82]

The record may be authenticated and still have its content disputed. The record may be authentic and be missing important information, present material in a misleading manner or fail to prove the claim sought. Synthetic representations may be accurately identified as such and still be of little value, but this should not be presented as a proof of an event that never happened.The acknowledgment of the difference is of great importance due to the reason that legal assessment should not be stopped once the piece of evidence is submitted in front of the court.

10.3 Involvement of AI and Claims Related to the Evidence

The severity of AI involvement has to be analyzed in reference to the claim made with respect to the evidence. An original recording of an event will convey quite different meaning when compared with a recording which is produced as illustrative reconstruction. The transcript created via the help of AI would definitely help understand the audio record but it should not replace the examination of the original record where the authenticity is in question.[83]

10.4 The Hazard of Dependence on Technical Systems

Technical systems play an important part in identifying discrepancies in digital materials. However, their importance may be exaggerated when construed as a conclusive factor.[84]

[81] Paul W. Grimm, Maura R. Grossman and Gordon V. Cormack, 'Artificial Intelligence as Evidence' (2021) 19 *Northwestern Journal of Technology and Intellectual Property* 9.
[82] Ibdi.
[83] Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, ss. 39 and 63.
[84] *Pune Bar Association v. Union of India*, W.P. (C) No. 599 of 2026, order dated 22 May 2026 (Supreme Court of India).

A stable hash value shows the consistency of certain forms of an electronic document but not the real authenticity of its contents. The provenance of digital assets may show the creation history without proving its authenticity. The detection tool may show the signs of artificiality of the material without actually confirming that the event really happened.

The threat appears when the technical result is transformed into a general conclusion of a legal nature without sufficient justification. Courts must define the specific question which was answered by means of this particular technique and should avoid treating it as the quintessence of the evidence inquiry.

10.5 Fair Trial and Ambiguous Evidence

The use of AI-based evidence must be in compliance with the principles of fair trial.[85] In case of the criminal cases, fabricated evidence may have a catastrophic impact on the suspect. In case the disputed recording is used as a significant piece of evidence, the chance for testing the recording becomes even more important. It may be said that accusations of artificial intelligence could be used to discredit authentic evidence.[86] A claim that an audio-visual material may have been made artificially should not automatically make it untrustworthy.

The court should differentiate between a particular claim and one that has some grounds falling short of believable evidence. If the challenge indicates specific evidence, a more thorough examination shall be conducted when the challenge does not provide sufficient grounds, the existence of AI-generated materials will, nevertheless, not negate evidence otherwise believed to be reliable.

11. PROPOSALS FOR ADDRESSING THE ISSUE IN COURT

The previous discussion shows that the existing rules of evidence in Indian law do not indicate the necessity to exclude AI-produced evidence automatically or to abandon the system of certification of electronic records.[87] There is a need for the application of a more straightforward approach to interpretation of the relationship of digital evidence, its creation process, and the factual statement on which it is based.

11.1 Disclosure of Material AI Involvement

If AI has significantly contributed to or changed content used as evidence of a real-life situation, then the evidence of that involvement should be included in the evidence process. The disclosure should state, as far as it is possible to do, the kind of AI use, the aim of processing, and whether the material was generated from the existing or created independently.[88]

The requirement has to be adequate. Routine processing does not necessarily require the same level of disclosure as the creation or replacement of a person's appearance, voice, and activities. The important thing is whether the realization of AI influences the significance of the evidence.[89]

[85] Constitution of India, art. 21; *Maneka Gandhi v. Union of India*, AIR 1978 SC 597; *Zahira Habibulla H. Sheikh v. State of Gujarat*, (2004) 4 SCC 158.
[86] Robert M. Chesney and Danielle Keats Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 *California Law Review* 1753.
[87] Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, ss. 39, 61–63.
[88] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024, art. 50.
[89] Paul W. Grimm, Maura R. Grossman and Gordon V. Cormack, 'Artificial Intelligence as Evidence' (2021) 19 *Northwestern Journal of Technology and Intellectual Property* 9.

Disclosing information would help the opponent determine the reasons for getting rid of the evidence and the court to decide if the additional expertise will be needed. It may also decrease the probability of synthetically generated information claimed to be an uninterrupted record of the event. A synthetic representation does not have to be true, while a genuine recording can be trusted even if no source verification has taken place.

11.2 Preservation of original material and processing history.

To the extent possible and reasonable, preservation of original material shall be encouraged in case of the effect of AI processing over digital evidence. Original files, produced versions and relevant information about processing can help in understanding whether the final representation is in line with the original or if it brought essential changes.[90] The process of preservation should include sufficient materials that can document the process such as acquisition, transfer, research and storage traces. Hash values can assist in distinguishing different versions, whereas chain of custody records can provide the information about the treatment of evidence.[91]

The non-existence of an original source must not automatically imply that one should be excluded. There may be appropriate cases where the original cannot be located, damaged or inaccessible. In such cases, the court needs to investigate the reasons of the absence, the credibility of information at hand and whether the restrictions can be worked around with the aid of other evidence.

11.3 A Clear and Methodically Correct Expert Evaluation

Expert evaluation must be focused towards resolution of the authenticity or reliability issue brought before the court. The expert evaluation must indicate what kind of materials have been studied, what methodology was used, what conclusions were drawn from the examination and what limitations of the research are relevant.[92]

When using AI detection devices, it should clarify how such devices operate, under what conditions their operation is validated and the characteristics of their errors, to the extent this information is known.[93] The expert's function must always be one of clarification rather than dictation of the actual judicial decision. A technical examiner may provide data about the peculiarities of laboratory material, the chance of manipulations, or the usefulness of the detection technique. The position of the court, however, should be to determine the relevance of the disclosed information proved in the light of the other proofs.

11.4 Proportionate Authentication and Adversarial Testing

The level of authentication necessary is determined by the nature of the evidence at issue and the circumstances of the challenge. In adversarial testing, there can be an investigation of the creator of the evidence, questioning of the expert witness, comparing the evidence with its source, and looking

[90] Coalition for Content Provenance and Authenticity, *Content Credentials: C2PA Technical Specification*, available at: https://spec.c2pa.org/ (last visited 14 November 2026).
[91] Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, s. 63(4) and the Schedule.
[92] Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, s. 39(1)–(2); Federal Rules of Evidence, Rule 702, United States of America.
[93] David Güera and Edward J. Delp, 'Deepfake Video Detection Using Recurrent Neural Networks' (2018) 2018 IEEE International Conference on Advanced Video Based Surveillance 1.

into the circumstances surrounding it.[94] The intensity of this investigation should be consistent with its importance.

This approach is not intended to place a new burden of proof for every document generated by electronics. It should only confirm that the questioned digital evidence undergoes an appropriate validation checking. Judiciary findings about authenticity and evidential weight

The court reasoning must keep the two concepts apart - the admissibility of the electronic record and its final evidential weight. In cases where there is a valid dispute concerning the electronic evidence, the court must state the main grounds based on which it received its conclusion about authenticity.[95]

12. FINDINGS AND DISCUSSION

The research carried out in this paper yielded several important findings.

The first finding is that AI-generated proof is not limited to one kind of evidence only. Fully generated product, AI altered documents, restored material and AI supported processing present different matters regarding origin, authenticity and reliability.[96]

The second finding is that the BSA serves as an important legal basis for admissibility of electronic evidence. Clauses 61-63 and the Schedule define the criteria for admissibility of electronic evidence, whereas Clause 39 presents the conditions for expert opinion forming.[97]

The third finding is that digital integrity and factual authenticity are two different concepts concerning evidence. Hash values and running processes help find out the changes made to the digital evidence but do not allow to state the fact of the evidence showing the reality.[98]

The fourth finding is that the judicial practice of the Supreme Court provides guidance for assessing AI-generated evidence. The cases of Anwar P.V. and Arjun Panditrao Khotkar illustrate the importance of legal certification under the previous electronic evidence law.[99] While hash values and preservation techniques may help detect modifications made to digital records, they alone cannot determine whether the record captures reality correctly.[100]

Fifthly, specialized investigation and AI detection equipment can be of help in assessing synthetic materials but their results should be taken into account in connection with their methodological limitations. Results of detection cannot be seen as indisputable evidence of synthesis or genuineness.[101]

GRASP - EDUCATE - EVOLVE

[94] *Zahira Habibulla H. Sheikh v. State of Gujarat*, (2004) 4 SCC 158.
[95] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473; *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.
[96] Paul W. Grimm, Maura R. Grossman and Gordon V. Cormack, 'Artificial Intelligence as Evidence' (2021) 19 *Northwestern Journal of Technology and Intellectual Property* 9.
[97] The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), ss. 39, 61–63 and the Schedule.
[98] Coalition for Content Provenance and Authenticity (C2PA), *C2PA Technical Specification, Version 2.2*, available at: https://spec.c2pa.org/specifications/specifications/2.2/specs/ContentCredentials.html (last visited 14 November 2026).
[99] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473; *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.
[100] *Pune Bar Association v. Union of India*, W.P. (C) No. 599 of 2026, order dated 22 May 2026 (Supreme Court of India); Coalition for Content Provenance and Authenticity (C2PA), *C2PA Technical Specification, Version 2.2*, available at: https://spec.c2pa.org/specifications/specifications/2.2/specs/ContentCredentials.html (last visited 14 November 2026).
[101] National Institute of Standards and Technology, *Reducing Risks Posed by Synthetic Content: An Overview of Technical Approaches to Digital Content Transparency*, NIST AI 100-4 (2024); Marc Gorriz-Blanch et al., *An Evaluation of Generated/Manipulated Image Detection*, BBC Research & Development White Paper WHP 414 (2024)

The implications of the above-mentioned points confirm the key thesis of this piece of writing, namely, the law has to differentiate between the authenticity of an electronic document and the authenticity of a situation it describes besides relying on the inference drawn from that document.[102]

CONCLUSION

Generative artificial intelligence raises an important obstacle to the evidentiary value of digital information. It is now possible to create real photographs, videos, audio records and other representations without the occurrence of real-life events. Thus, the basis for the assumption that the existence of digital content indicates that the event has taken place has been weakened. The situation further requires more thorough consideration of the problem of the admissibility, authenticity and evidential reliability of electronic records.

The legal framework of India is a good starting point for dealing with the problem of electronic records use in court. The BSA acknowledges the existence of electronic and digital records and lays down a legal basis for their admissibility through Sections 61-63 and the relevant Schedule. Section 39 provides the basis for the expert opinion in the area requiring special knowledge, which includes the use of electronic and digital information.

The comparative analysis of the U.S. law of evidence and the EU's AI transparency framework shows that authentication, reliability and disclosure have to be distinguished. These ideas can be taken into account in the Indian framework in relation to contextual authentication, expert analysis and AI disclosures. Nevertheless, this method should be implemented with regard to the existing provisions of the Indian law and proceedings.

BIBLIOGRAPHY

A. Constitutional and Statutory Material

1. The Constitution of India, 1950.
2. The Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023.
3. The Information Technology Act, 2000, No. 21 of 2000.
4. The Indian Evidence Act, 1872, No. 1 of 1872.
5. Regulation (EU) 2024/1689, Artificial Intelligence Act, 2024.

B. Judicial Decisions

Indian Cases

1. *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.
2. *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.
3. *Pooja Ramesh Singh v. Jammu & Kashmir Bank Ltd.*, 2026 INSC 668.
4. *Pune Bar Association v. Union of India*, W.P. (C) No. 599 of 2026, order dated 22 May 2026.

[102] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473; *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1; *Pune Bar Association v. Union of India*, W.P. (C) No. 599 of 2026, order dated 22 May 2026 (Supreme Court of India).

Foreign Cases

1. *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993).

C. Books and Research Articles

1. Chesney, Bobby & Danielle Keats Citron. "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security." 107 *California Law Review* 1753 (2019).

2. Grimm, Paul W., Maura R. Grossman & Gordon V. Cormack. "Artificial Intelligence as Evidence." 19 *Northwestern Journal of Technology and Intellectual Property* 9 (2021).

D. Institutional and Technical Publications

1. Coalition for Content Provenance and Authenticity, *C2PA Technical Specification*, Version 2.4 (2026).
2. National Institute of Standards and Technology, *Digital Evidence Preservation: Considerations for Evidence Handlers*, NISTIR 8387 (2022).
3. Federal Rules of Evidence, Rules 702 and 901 (United States).
4. Advisory Committee on Evidence Rules, *Proposed Amendment to Federal Rule of Evidence 901: Deepfakes*, committee materials (2025–2026).

E. Online Sources

1. India Code, Government of India, https://www.indiacode.nic.in.
2. Supreme Court of India, https://www.sci.gov.in.
3. C2PA Technical Specifications, https://spec.c2pa.org.
4. NIST, https://www.nist.gov.
5. European Union AI Act Service Desk, https://ai-act-service-desk.ec.europa.eu.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 12 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

MISUSE OF GENERATIVE AI IN CYBER CRIMES: DEEPFAKES, IDENTITY THEFT, AND ONLINE FRAUD

AUTHOR – TISHA . T, STUDENT AT CYBER SPACE LAW AND JUSTICE (SCHOOL OF EXCELLENCE IN LAW)

BEST CITATION – PRABHNOOR KAUR MAKKAR, MISUSE OF GENERATIVE AI IN CYBER CRIMES: DEEPFAKES, IDENTITY THEFT, AND ONLINE FRAUD, PROOF AND JUDICIAL RELIABILITY IN INDIA, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 6 (12) OF 2026, PG. 30-39, APIS – 3920 – 0001 & ISSN - 2583-2344.

Abstract

The rapid democratization of generative artificial intelligence (GenAI) has precipitated a structural transformation in the cyber threat landscape. Unlike traditional discriminative machine learning systems designed to classify or predict patterns, generative architectures—including Generative Adversarial Networks (GANs), diffusion models, neural audio codecs, and Large Language Models (LLMs)—synthesize high-fidelity text, audio, imagery, and video that are increasingly indistinguishable from authentic human output. This paper examines the weaponization of generative AI across three interconnected domains of cybercrime: synthetic media and deepfake exploitation, biometric and synthetic identity theft, and hyper-personalized online fraud. It analyzes how generative tooling collapses the marginal cost of sophisticated social engineering, bypasses legacy authentication safeguards, and facilitates "Crime-as-a-Service" ecosystems. From a legal and doctrinal perspective, the study evaluates the friction between emerging synthetic threats and existing statutory frameworks across the United States, the European Union, and India, while addressing constitutional constraints under free speech jurisprudence and evidentiary vulnerabilities in judicial proceedings, notably the "liar's dividend." Finally, the paper proposes an integrated governance framework combining cryptographic content provenance, heightened Know-Your-Customer (KYC) verification standards, and targeted statutory reforms to restore epistemic trust and accountability in digital ecosystems.

Keywords: Generative Artificial Intelligence, Deepfakes, Synthetic Identity Theft, Cyber Fraud, Social Engineering, Digital Forensics, Cyber Law

1. Introduction

The proliferation of generative artificial intelligence represents one of the most consequential technological inflection points of the twenty-first century. While foundation models and multimodal generative systems offer transformative gains in scientific discovery, software engineering, healthcare diagnostics, and creative industries, their dual-use archi-tecture inherently lowers barriers to malicious exploitation[103]. Historically, high-impactcyber operations required substantial technical expertise, bespoke infrastructure, and manual reconnaissance to craft convincing lures or forge authentic

[103] See generally Miles Brundage et al., The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation 16–20 (2018) (analyzing the dual-use nature of artificial intelligence systems and how capability gains expand the threat surface across digital, physical, and political security domains).

credentials. Generative AI disrupts this economic equilibrium by automating the production of deceptive artifacts at scale, enabling threat actors with modest technical proficiency to execute operations that previously demanded state-sponsored or organized syndicate resources[104].

At the core of this paradigm shift is the transition from analytical software to generative synthesis. Large Language Models (LLMs) generate contextually coherent, culturally nuanced, and grammatically flawless prose across dozens of languages; diffusion architectures and Generative Adversarial Networks (GANs) render photorealistic faces and realtime video overlays; and neural text-to-speech engines clone human vocal timbres from mere seconds of reference audio[105]. When operationalized by cybercriminals, these capabilities converge to undermine the foundational trust assumptions of digital communication: that a voice on a telephonecall belongs to the purported speaker, that a live video feed reflects physical presence, and that a well-crafted electronic message originates from a legitimate counterparty.

2.Technical Architecture of Malicious Generative AI

Understanding the legal and forensic challenges of AI-enabled cybercrime requires examining the mechanisms through which synthetic artifacts are produced. Modern generative pipelines rely on distinct neural architectures tailored to specific data modalities, each presenting unique exploitation pathways.

2.1 Core Generative Modalities

First, visual synthesis relies predominantly on Generative Adversarial Networks (GANs), Variational Autoencoders (VAEs), and latent diffusion models. In a GAN framework, a generator network creates candidate images while a discriminator network evaluates their authenticity against real training distributions, iteratively refining output realism through zero-sum adversarial training[106]. Latent diffusion models, which have largely superseded GANs in high-resolution image and video generation, operate by iteratively denoising random Gaussian noise conditioned on text or image embeddings[107]. In cybercrime, autoencoders and real-time face-swapping pipelines extract latent facial expressions from a source actor and map them onto a target identity, enabling live impersonation during video conferencing sessions

Second, neural voice synthesis and zero-shot voice cloning utilize acoustic foundation models trained on vast corpora of human speech. By disentangling linguistic content from speaker identity embeddings, modern voice-cloning architectures replicate prosody, cadence, emotional inflection, and background acoustic characteristics from short audio samples harvested from social media posts, voicemail greetings, or public earnings calls[108].

[104] See Robert Chesney & Danielle Keats Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 Calif. L. Rev. 1753, 1758–62 (2019) (observing that machine-learning driven synthesis democratizes the capacity to fabricate hyper-realistic audiovisual media).
[105] See Ian J. Goodfellow et al., *Generative Adversarial Nets*, in 27 Advances in Neural Information Processing Systems 2672, 2672–75 (2014); Jonathan Ho et al., *Denoising Diffusion Probabilistic Models*, in 33 Advances in Neural Information Processing Systems 6840, 6840–42 (2020).
[106] Goodfellow et al., *supra* note 3, at 2673.
[107] See Robin Rombach et al., *High-Resolution Image Synthesis with Latent Diffusion Models*, in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition 10684, 10685–87 (2022).
[108] See Ye Jia et al., *Transfer Learning from Speaker Verification to Multispeaker Text-To-Speech Synthesis*, in 31 Advances in Neural Information Processing Systems 4480, 4481–83 (2018).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 12 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

Third, transformer-based Large Language Models predict token sequences across vast context windows, enabling autonomous text generation, code synthesis, and interactive dialogue[109].Unlike static phishing templates, LLMs maintain stateful multi-turn conversations, dynamically adapting tone, psychological pressure, and technical vocabulary to mirror a victim's organizational context.

The Democratization of Offenses and "Crime-as-a-Service

Although frontier commercial models incorporate reinforcement learning from human feedback (RLHF) and safety guardrails designed to refuse harmful prompts, threat actors routinely circumvent these controls through adversarial "jailbreaking," prompt injection, or fine-tuning open-weight models with safety alignment layers removed[110].Furthermore, underground cybercrime marketplaces have commercialized malicious generative capbilities under a "Crime as-a-Service" (CaaS) model, offering subscription access to uncensored LLMs, turnkey deepfake webcam emulators, and automated voice-cloning APIs[111].

Model Architecture	**Primary Modality**	**Malicious Cybercrime Applications**
Autoencoders & GANs	Facial video & real time face swapping	Live KYC biometric bypass; executive video impersonation; non-consensual intimate imagery.
Latent Diffusion Models	High-resolution static & dynamic imagery	Forged identity documents; fabricated evidentiary photographs; fraudulent e-commerce listings.
Neural Audio / TTS Models	Zero-shot voice cloning & real-time voice conversion	Vishing (voice phishing); virtual kidnapping extortion; authorization of fraudulent wire transfers.
Large Language Models (LLMs)	Contextual text, multi-turn dialogue	Hyper-personalized spear-phishing; Busi

[109] See Ashish Vaswani et al., *Attention Is All You Need*, in 30 Advances in Neural Information Processing Systems 5998, 5999–6002 (2017).
[110] See Andy Zou et al., *Universal and Transferable Adversarial Attacks on Aligned Language Models*, arXiv:2307.15043, at 1–3 (2023) (demonstrating automated adversarial suffixes capable of bypassing alignment filters across aligned language models).
[111] See Europol, *ChatGPT: The Impact of Large Language Models on Law Enforcement* 4–7 (2023) (detailing how threat actors exploit LLMs for phishing, disinformation, and malware development).

	& source code	ness Email Compromise (BEC); polymorphic malware generation.

3 Typologies of Generative AI-Enabled Cyber Offenses

The operational deployment of generative AI spans a wide spectrum of criminal activity, reshaping established offense categories while creating novel attack surfaces.

3.1 Synthetic Media and Deepfake Exploitation

The term "deepfake"—a portmanteau of "deep learning" and "fake"—encompasses synthetic audio, image, or video content manipulated to depict individuals saying or doing things they never did[112]. While public discourse frequently focuses on electoral disinformation and geopolitical influence operations, the most pervasive harms involve targeted interpersonal and financial exploitation.

Non-consensual synthetic intimate imagery (NCII) represents the overwhelming majority of deepfake content circulating online.[113] Accessible nudification applications and fine-tuned diffusion checkpoints allow perpetrators to generate explicit depictions of private individuals using ordinary photographs scraped from social networking platforms. Beyond severe dignitary and psychological trauma, perpetrators weaponize synthetic intimate media for sexual extortion ("sextortion"), threatening to disseminate fabricated imagery to a victim's family, employer, or professional network unless ransom demands are mettives announcing product recalls, regulatory investigations, or bankruptcy filings can trigger algorithmic trading sell-offs within seconds, enabling perpetrators to profit through short-selling strategies before the fabrication is debunked.

3.2 Next-Generation Identity Theft and Biometric Spoofing

Identity theft has evolved from the unauthorized possession of static identifiers—such as Social Security numbers, Aadhaar numbers, or credit card details—to the dynamic synthesis and impersonation of a victim's biometric and behavioral persona. Generative AI accelerates two distinct forms of identity crime: synthetic identity fraud and biometric authentication bypass

In synthetic identity fraud, criminals combine real personally identifiable information (PII) obtained from data breaches with fabricated attributes to construct wholly fictitious personas.[114] Generative models automate the creation of consistent digital footprints for these synthetic identities, generating matching headshot portraits, forged governmentissued identification cards, utility bills, and employment histories to pass automated credit underwriting and open fraudulent financial accounts.

Even more disruptive is the use of real-time generative video and audio injection to defeat remote Know-Your-Customer (KYC) and biometric liveness checks. Financial institutions and cryptocurrency exchanges increasingly rely on facial recognition and active liveness challenges—requiring users to

[112] Chesney & Citron, *supra* note 2, at 1757
[113] See Danielle Keats Citron, *Sexual Privacy*, 128 Yale L.J. 1870, 1919–24 (2019) (examining how non consensual deepfake pornography inflicts severe psychological, reputational, and economic harm on victims)
[114] See Fed. Rsrv. Sys., *Synthetic Identity Fraud in the U.S. Payment System: A Review of Causes and Contributing Factors* 3–6 (2019).

blink, turn their heads, or read randomized digits aloud—to verify identity during remote onboarding.[115] Attackers circumvent these cotrols using virtual camera drivers that inject AI-driven face swapped video streams directly into the application layer, bypassing the physical optical sensor altogether. Coupled with real-time voice conversion, a single operator can simultaneously impersonate hundreds of distinct identity theft victims to drain bank accounts, hijack telecommunications SIM cards, and launder illicit proceeds.

3.3 Hyper-Personalized Online Fraud and Social Engineering

Online fraud schemes, particularly phishing and Business Email Compromise (BEC), have historically suffered from a trade-off between scale and personalization: mass-mailed lures were easily detected due to generic phrasing and linguistic errors, whereas be spoke spear-phishing required labor-intensive research. Large Language Models eliminate this constraint.[116] By ingesting open-source intelligence (OSINT) from corporate websites, LinkedIn profiles, and leaked email threads, LLMs craft context-aware lures referencing ongoing projects, internal jargon, and interpersonal relationships.

In Business Email Compromise and executive impersonation fraud, threat actors com bine LLM-generated correspondence with real-time audio and video deepfakes to authorize fraudulent wire transfers. In high-profile corporate incidents, finance personnel have been deceived into transferring tens of millions of dollars after participating in multi person video conference calls in which every other participant—including the purported Chief Financial Officer—was an AI-generated deepfake reconstructed from publicl available media.[117]

Additionally, generative AI assists fraudsters in building persuasive fraudulent storefronts, pig butchering romance-investment scams, and polymorphic malware. In longconinvestment frauds, conversational agents maintain continuous, emotionally engaing dialogues with targets across messaging platforms, overcoming language barriers and sustaining psychological manipulation over months before steering victims toward fraudulent trading portals.18 Simultaneously, code generating LLMs enable threat actors to obfuscate malware payloads and rewrite scripts dynamically to evade signature-based antivirus detection

4 Legal, Doctrinal, and Evidentiary Challenges

The rapid maturation of generative cybercrime exposes acute doctrinal tensions across substantive criminal law, intermediary liability, constitutional speech protections, and rules of evidence.

4.1 Attribution, Mens Rea, and Intermediary Liability

Establishing criminal liability requires proving both the prohibited conduct (*actus reus*) and the requisite culpable mental state (*mens rea*), anchored to an identifiable perpetrator. Generative AI

[115] See Nat'l Inst. of Standards & Tech. (NIST), *Digital Identity Guidelines: Enrollment and Identity Proofing*, NIST Special Pub. 800-63A, § 4.4 (2017) (establishing standards for remote identity proofing and biometric comparison)

[116] See Julian Hazell, *Spear Phishing with Large Language Models*, arXiv:2305.06972, at 2–5 (2023) (demonstrating that LLMs can generate convincing, personalized spear-phishing emails at minimal cost per target).

[117] See, e.g., Fin. Crimes Enf't Network (FinCEN), *FinCEN Alert on Fraud Schemes Involving Deepfake Media Targetng Financial Institutions*, FIN-2024-Alert004, at 2–4 (Nov. 13, 2024) (documenting typologies in which criminals utilize deepfake audio and video to bypass financial institution verification controls).

complicates attribution at multiple levels. First, synthetic artifacts lack the traditional physical provenance of forged documents or analog recordings, and threat actors frequently route generative API requests through layered anonymization networks and compromised cloud infrastructure. Second, as autonomous AI agents increasingly execute multi-step phishing, reconnaissance, and credential-stuffing workflows with minimal human supervision, prosecutors face doctrinal questions regarding foreseeability and proximate causation when an autonomous system deviates from or expands upon a user's initial prompt.

Equally contentious is the civil and regulatory liability of foundation model developers, hosting repositories, and social media platforms. In the United States, Section 230 of the Communications Decency Act shields providers of interactive computer services from liability as the publisher or speaker of information provided by another information content provider.[118]However, courts have long held that a platform loses Section 230 immunity to the extent it materially contributes to the development of unlawful content.[119] Whether the operator of a generative AI system acts as a neutral tool provider or a co-developer of unlawful synthetic media remains an unsettled frontier of statutory interpretation, particularly where models are specifically fine tuned or marketed for non-consensual faceswapping or voice cloning

4.2 Constitutional Boundaries and Free Speech Protections

Legislative efforts to criminalize or restrict the creation and distribution of deepfakes must navigate rigorous constitutional scrutiny, particularly under the First Amendment to the U.S. Constitution. In *United States v. Alvarez*, the Supreme Court held that false statements of fact are not categorically excluded from First Amendment protection merely because they are untrue; rather, content-based restrictions on false speech generally trigger strict scrutiny unless the speech falls within a historically recognized exception such as defamation, fraud, perjury, or true threats.

Consequently, broadly drafted statutes that prohibit all synthetic media without requiring proof of fraudulent intent, defamatory harm, or non-consensual intimate depiction risk invalidation on overbreadth grounds,[120] as they threaten to chill protected political satire, parody, artistic expression, and commentary. Conversely, statutes narrowly tailored to combat online fraud, identity theft, commercial impersonation, and non-consensual intimate imagery rest on firm constitutional footing, as fraudulent misrepresentation and severe invasions of sexual privacy do not enjoy First Amendment immunity[121]

4.3 Evidentiary Integrity and the "Liar's Dividend"

Beyond substantive offenses, generative AI threatens the integrity of judicial fact-finding. Under Rule 901(a) of the Federal Rules of Evidence, the proponent of an item of evidence must produce evidence sufficient to support a finding that the item is what the proponent claims it is Historically, audiovisual recordings carried substantial persuasive weight as objective witnesses. Today, however, opposing

[118] 47 U.S.C. § 230(c)(1).
[119] See *Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157, 1167–68 (9th Cir. 2008) (en banc).
[120] See *Hustler Magazine, Inc. v. Falwell*, 485 U.S. 46, 50–57 (1988) (affirming robust First Amendment protection for parody and satire involving public figures); see also Chesney & Citron, *supra* note 2, at 1791–95.
[121] See *Illinois ex rel. Madigan v. Telemarketing Assocs., Inc.*, 538 U.S. 600, 612 (2003) ("[T]he First Amendment does not shield fraud.").

parties can challenge authentic digital recordings as AI-generated fabrications, forcing courts to conduct costly forensic inquiries and rely on competing expert testimony under Rule 702 and the *Daubert* standard.

Scholars Chesney and Citron identify a perilous corollary to this phenomenon termed the "liar's dividend": as the public and fact-finders become increasingly aware that hyperrealistic audio and video can be fabricated, bad actors gain a powerful new defense mechanism to dismiss genuine recordings of their misconduct as deepfakes.[122]This epistemicerosion undermines both criminal prosecutions and civil accountability even in cases where no synthetic media was ever used.

5 Comparative Regulatory and Statutory Frameworks

Jurisdictions worldwide are adapting legacy cybercrime statutes while enacting specialized AI governance regimes to address synthetic fraud, identity theft, and deepfake abuse.

5.1 United States Federal and State Approaches

In the United States, federal prosecutors currently rely on technology-neutral criminal statutes to prosecute AI-enabled cybercrimes. Wire fraud under 18 U.S.C. § 1343 criminalizes any scheme or artifice to defraud executed via interstate electronic communications, fully encompassing LLM-driven phishing and deepfake BEC schemes.

Identity theft and aggravated identity theft under 18 U.S.C. §§ 1028 and 1028A prohibit the knowing transfer, possession, or use without lawful authority of a "means of identification" of another person—a definition broad enough to cover biometric identifiers and cloned vocal prints used in connection with predicate felonies.[123]Unauthorized access to computer systems facilitated by AI-assisted credential stuffing or malware falls under the Computer Fraud and Abuse Act (CFAA).[124]

Recognizing enforcement gaps in civil consumer protection, the Federal Trade Com

mission (FTC) promulgated the Rule on Impersonation of Government and Businesses, effective April 2024, which explicitly prohibits materially and falsely posing as a government entity or business and authorizes direct monetary penalties against scammers utilizing AI voice cloning and synthetic communications.[125] At the state level, jurisdictions including California, Texas, New York, and Virginia have enacted targeted statutes criminalizing nonconsensual deepfake intimate imagery, establishing rights of publicity against unauthorized digital replicas, and regulating deceptive synthetic media in electoral campaigns.[126]

5.2 The European Union AI Act and Digital Services Framework

The European Union has adopted a comprehensive, risk-based regulatory architecture anchored by the EU Artificial Intelligence Act (Regulation (EU) 2024/1689). Under Article 50 of the AI Act, providers of

[122] Chesney & Citron, *supra* note 2, at 1785–86.
[123] 18 U.S.C. §§ 1028(a)(7), 1028(d)(7), 1028A
[124]Rule on Impersonation of Government and Businesses, 16 C.F.R. pt. 461 (2024); see also Fed. Trade Comm'n, *FTC Proposes New Protections to Combat AI Impersonation of Individuals*, Press Release (Feb. 15, 2024) (proposing supplemental rules extending impersonation prohibitions to individual likenesses and voices).
[125]18 U.S.C. §§ 1028(a)(7), 1028(d)(7), 1028A.
[126] See, e.g., Cal. Penal Code § 647(j)(4) (criminalizing distribution of non-consensual intimate images); Va. Code Ann. § 18.2-386.2 (extending criminal penalties to falsified intimate video and images); Tenn. Code Ann. § 47-25-1101 *et seq.* (Ensuring Likeness, Voice, and Image Security (ELVIS) Act protecting voice rights against unauthorized AI cloning).

generative AI systems must ensure that synthetic audio, image, video, and text outputs are marked in a machine-readable format and detectable as artificially generated or manipulated. Furthermore, deployers of AI systems that generate or manipulate image, audio, or video content constituting a "deep fake" are legally obligated to disclose clearly that the content has been artificially generated or manipulated, subject to narrow exceptions for authorized law enforcement use or obvious artistic satire[127]

Complementing the AI Act, the Digital Services Act (DSA) requires Very Large Online Platforms (VLOPs) to assess and mitigate systemic risks stemming from the dissemination of illegal content and manipulative deepfakes, including rapid notice and-action mechanisms.38 Meanwhile, the General Data Protection Regulation (GDPR) classifies biometric data used for unique identification as a special category of personal data subject to strict processing prohibitions, providing individuals with erasure and objection rights against unauthorized scraping of their facial images and voice recordings.[128]

5.3 Comparative Perspectives: India and International Harmonization

In India, the rapid expansion of digital public infrastructure and mobile payments has made synthetic voice scams and deepfake impersonation an urgent enforcement priority. Prosecutors invoke several provisions of the Information Technology Act, 2000: Section 66C penalizes identity theft involving the fraudulent or dishonest use of electronic signatures, passwords, or unique identification features; Section 66D criminalizes cheating by personation using a computer resource; and Section 66E penalizes the violation of bodily privacy through the capture or transmission of private images. Additionally, the Bharatiya Nyaya Sanhita, 2023 (BNS), which replaced the Indian Penal Code, provides substantive offenses for cheating by personation, forgery of electronic records, defamation, and outraging the modesty of women, which courts apply to malicious deepfake deployments. The Ministry of Electronics and Information Technology (MeitY) has also issued advisories directing intermediaries under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 to exercise due diligence in identifying and removing deepfakes and misinformation

At the international level, cross-border enforcement remains hampered by jurisdictional fragmentation. The Council of Europe's Budapest Convention on Cybercrime and its Second Additional Protocol facilitate expedited cross-border electronic evidence sharing,[129]while the United Nations Convention against Cybercrime seeks to establish harmonized global criminalization standards for computer-dependent and computer-enabled fraud.

[127] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 2024 O.J. (L 2024/1689) [hereinafter EU AI Act].
[128] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), arts. 9, 17, 2016 O.J. (L 119) 1, 38, 43–44.
[129] Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185; Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence, May 12, 2022, C.E.T.S. No. 224.

Jurisdiction	Primary Instruments	Key Regulatory & Enforcement Focus
United States	18 U.S.C. §§ 1028, 1030, 1343; FTC Rule 16 C.F.R. pt. 461; State Deepfake Acts	Technology-neutral wire fraud and identity theft prosecution; civil penalties for AI impersonation; state-level NCII and voice rights protections.
European Union	EU AI Act (Reg. 2024/1689); Digital Services Act; GDPR	Mandatory machine-readable watermarking and deepfake disclosure (Art. 50); VLOP systemic risk mitigation; strict biometric data protection.
India	IT Act, 2000 (§§ 66C–66E); Bharatiya Nyaya Sanhita, 2023; IT Rules, 2021	Criminalization of cheating by personation via computer resources; intermediary due diligence and expedited takedown obligations.

6 Technical Countermeasures and Policy Recommendations

Addressing the systemic risks of generative AI in cybercrime requires a coordinated defensein-depth strategy integrating cryptographic[130] provenance, forensic detection, institutional verification reforms, and calibrated statutory updates.

[130] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 3(1)(b) (India).

6.1 Cryptographic Provenance and Forensic Detection

Passive forensic detection—training machine learning classifiers to spot subtle visual or acoustic artifacts such as unnatural blinking,[131] spectral anomalies, or phase discontinuities—is locked in an asymmetric arms race. As generative architectures improve, forensic detectors suffer rapid accuracy degradation against unseen models and post-processing

Consequently, industry consortia and standards bodies are shifting emphasis toward

active cryptographic provenance. The Coalition for Content Provenance and Authentic

ity (C2PA) specification embeds tamper-evident, cryptographically signed metadat manifests directly into media files at the point of capture or generation. Rather than attempting to prove that a file is fake, cryptographic provenance establishes a verifiable chain of custody proving where, when, and by what hardware or generative model an asset was created or edited. Combined with imperceptible statistical watermarking embedded in model weights or token distributions, provenance standards offer a durable mechanism to distinguish authentic recordings from synthetic fabrications.

7 Conclusion

Generative artificial intelligence has fundamentally altered the mechanics of cybercrime, transforming deepfakes, identity theft, and online fraud from bespoke, labor-intensive operations into scalable, automated, and hyper-personalized campaigns. By synthesizing convincing human likenesses, voices, and contextual communications, malicious actors exploit the cognitive heuristics and institutional verification protocols upon which modern digital commerce and social trust depend.

Yet the weaponization of generative AI is neither technologically inevitable nor legally insurmountable. While existing fraud and identity theft statutes provide an essential baseline for prosecution, long-term resilience demands proactive alignment between technical architecture and legal governance. By pairing cryptographic content provenance and robust multi-factor authentication with targeted statutory prohibitions on malicious impersonation and non-consensual synthetic media, legal systems can preserve accountability, protect individual dignity, and safeguard the integrity of digital ecosystems in the generative era.

GRASP - EDUCATE - EVOLVE

[131] Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185; Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence, May 12, 2022, C.E.T.S. No. 224

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 12 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

GENDER- INCLUSIVE CRIMINAL PROCEDURE UNDER BNSS, 2023: AN ANALYSIS OF TRANSGENDER RIGHTS IN INDIA

AUTHOR - NIHARIKA SINGH, STUDENT AT THAKUR RAMNARAYAN COLLEGE OF LAW

BEST CITATION – NIHARIKA SINGH, GENDER- INCLUSIVE CRIMINAL PROCEDURE UNDER BNSS, 2023: AN ANALYSIS OF TRANSGENDER RIGHTS IN INDIA, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 6 (12) OF 2026, PG. 40-51, APIS – 3920 – 0001 & ISSN - 2583-2344.

Abstract :-

The Bhartiya Nagarik Suraksha Sanhita (BNSS), 2023 also known earlier as Criminal Procedure Code (CrPC), 1973 which has shown significant Improvements in the country's criminal legal system. Its main purpose was to update the criminal procedure and overcome the challenges bridging the gap, but it still needs to critically examine Gender inclusive justice for Transgender persons under BNSS, 2023. Although the Transgender Community has already been acknowledged as the "Third Gender" in ***National Legal Service Authority (also known as NALSA) vs. Union of India (2014)***[1] and the Transgender Persons (Protection of Rights) Act, 2019 has also passed, but still in reality Transgender Community often experience Discrimination and Procedural difficulties in the Criminal Justice System.

This research paper critically examines the BNSS focusing mainly on Transgender Rights, specifically referring to procedural issues involving arrest, search, detention, medical examination, recording statement, bail, Custodial measures, and access to justice in reality.

This research paper focuses on the provisions of the Constitution, Acts of the Parliament, Case Laws, and case studies illustrating the experience of Transgender people in the criminal justice system. It establishes that there has been progress towards Gender inclusivity in the BNSS, but still there are some ambiguous procedures and implementation challenges in reality.

This Research paper makes recommendations for changes which includes Legislative Amendments, clear criminal procedure directions under BNSS and institutional reforms to ensure there is Equality, Dignity and Substantive Justice in the Criminal Justice System for Transgender persons.

KEYWORDS- Bhartiya Nagarik Suraksha Sangeeta 2023 BNSS, Transgender rights, Gender inclusive justice, Criminal Procedure, Third Gender, Arrest, Search and Seizure, custody, medical examination, Bail, access to justice, equality, dignity, Procedural Safeguard, Gender identity.

❖ Introduction :-

Criminal Procedure has always been an important component of the Criminal Justice Framework in India as it establishes the working of Criminal Law in reality. It controls the whole process of criminal cases, starting with the reporting of offences, investigation, arrest, search, custody, medical

examination, presenting the accused before the court, sentencing punishment and bail. The failure in even one of these producers would fail the justice system by impacting a person's basic fundamental rights such as liberty, body and dignity of individuals, therefore criminal procedure must ensure to safeguard the constitutional rights of persons who encounter such failure in criminal justice system rather than only the interests of the state and of the victims.

Bhartiya Nagarik Suraksha Sanhita, 2023 (BNSS) is the main legislation that provides guidance on how Criminal procedure will be followed in India. It superseded the Code of Criminal Procedure Code, 1973 and is applicable from 1st July, 2024.

Law has evolved for transgender community by introducing Transgender Persons (Protection of Rights) Act, 2019. The Act included provisions relating to the recognition of Transgender Identity, Welfare, Healthcare, Welfare and Rights. **The Transgender Persons (Protection of Rights) Rules, 2020** states that there are institutional provisions such as **Transgender Protection Cells. Rule 11(5)** mentions that "Every State Government should have a Transgender Protection Cell under the charge of the District Magistrate in each district and to be monitored by the Director General of Police in State by assuring speedy registration, investigation and Prosecution of offences against Transgender persons"[2]

In 2026, the Transgender Persons (Protection of Rights) Amendment Act, 2026 was passed by the Parliament in March 2026, it amended the act by removing the rights of self-identification of gender, replacing it with made medical board certification, narrowing the legal definition of Transgender persons which was widely criticized by civil society groups, activists and human

rights organizations that it is violating their constitutional right and it conflicts with Supreme Court's 2014 Landmark judgement ***NALSA v. Union of India***[3] which upheld self- determination of gender. That's why its Constitutional Validity is under challenge before the Supreme Court currently.

It is important to note that these constitutional and statutory safeguards do not guarantee a comprehensive framework in reality which includes a transgender inclusive procedural framework. The main concern is that the general level of procedural protection in the BNSS is not well understood and effective for transgender persons being ambiguous.

The present research paper therefore explores the issues of gender inclusivity in the criminal procedure mentioned in the BNSS, 2023 with respect to transgender. The intent of the research here is not to determine if the BNSS is 100 % inclusive or not. Rather, it aims to highlight where there is any protection through the existing case by case practice and where it might be better to provide more clarity, guidelines, or reform.

- **Under BNSS that deals with general procedural protections which lacks a specific and comprehensive framework for Transgender persons:-**

The BNSS covers various phases of criminal process such as arrest, search, medical examination, custody, investigation and recording statements but it does not have a specific chapter giving a detailed procedural framework with regard to Transgender persons.

The Constitution of India is the basic document for safeguarding transgender community. "The

equality before law and equal protection of the laws"[4] are guaranteed by **Article 14**. The Supreme Court has interpreted ***(NALSA v. Union of India)***[5] **Article 15**[6] also gives protection to Transgender persons, which bans "discrimination on certain grounds" and **Article 21** is also relevant to the right to life and personal liberty and as interpreted, "the right to live with dignity"[7]. These constitutional provisions are important while dealing in Criminal procedure.

Section 35[8] BNSS describes "when a police officer can arrest a person without a warrant". This provision is same for Transgender persons as for others, and must be interpreted and applied subject to statutory conditions of arrest.

Section 43[9] discusses "the process of arrest and has a specific section on the arrest of women" . It gives protection in respect of the way and timing of the arrest of women subject to the conditions under this section. But the BNSS does not specifically mention how these gender specific provisions will apply in the case of transgender persons, and the issue needs to be carefully interpreted.

Section 49[10] applies to "the search of a person arrested". **Section 49 (2)**[11] explicitly mentions that if the search of a female is required, then the search must be made by another female with "Strict regards to decency". So, there is a general protection given in the above provision about dignity in the search of the person. It doesn't establish or mention a new procedure for the search of transgender individuals. Transgender people therefore be taken into account when considering the use of this provision in the broader statutory framework as well as the constitutional requirement to respect dignity and personal liberty.

"Provision of medical examination is made in certain circumstances" mentioned in **Sections 51, 52 and 53**[12]. These sections are the legal rules on medical examination within the frame of criminal procedure under BNSS. However, they don't establish a specific comprehensive system for Transgender people.

"The security of the identification of a person arrested where an identification of a person is required for investigation" is mentioned in **Section 54**[13]. This section also doesn't provide for a separate procedure relating to Transgender identity.

Section 56[14] talks about "a person who has custody of an accused is under a duty to ensure the health and safety of the accused". **Section 57**[15] requires "the person arrested to be taken before the appropriate magistrate or proper officer without unnecessary delay". If a "person is arrested without a warrant, they can be detained for a period of more than twenty- four hours" in accordance with **section 58**[16], but with a statutory exception that may allow a Magistrate to extend the period of time they may be detained for. However, the BNSS doesn't provide any detail regarding the specific cell where an accused who is transgender can be detained. It thus does not establish a new statutory provision that a transgender person should be detained in the male cell or female cell as many police stations and prisons in India still don't have separate lockups, wards, and toilets for transgender people.

Section 180[17] is an "introduction to the concept of police examination of witnesses", **Section 181**[18] is an "introduction to the concept of statements to Police and their use", **Section 182**[19] is an "introduction to the concept of inducement amid" **section 183**[20] explains "the concept of recording

of confessions and statements by a magistrate". These provisions outline general procedures to be followed for making statements during investigation. They haven't established a separate procedure especially for Transgender individuals or a comprehensive.

Importantly, this does not imply that there is no protection for transgender persons in the BNSS. The general procedural safeguards provided to all persons under the BNSS are provided to Transgender persons. But BNSS itself does not contain a detailed transgender specific procedure but only a general procedure.

- **Gaps and Challenges in application of the BNSS, 2023 for Transgender persons:-**

The BNSS has provisions on arrest, search, medical examination, custody, identification, and investigation as discussed in the previous chapter. These however do not specify any procedures relating to specific situations that could occur where the person concerned is transgendered. The primary issue is not the lack of legal protection which is also important but rather the lack of clear and gender inclusive criminal procedures under BNSS. Which can lead to uncertainty in the implementation of the law. Questions may arise, such as which gender specific safeguard to use and how to take into account the person's gender identity by the police officer.

"The search of an arrested person is allowed" under **Section 49**, and there is a special protection given for the search of a female. But it does not create a separate detailed procedure for the search of transgender individuals. The lack of specific guidance could lead to variations in practice between police authorities. If search is not done with regards to the Transgender person's gender identity or personal situation as Personal search includes physical contact with another person's body and can therefore affect their dignity and privacy as it may be uncomfortable or unsafe for them. Hence, a clear and consistent procedure is needed to ensure that personal searches are conducted in a lawful, respectful, and minimally intrusive manner that does not impact dignity and privacy.

Section 51, 52 and 53 contains provisions for "medical examination under certain circumstances". These provisions provide the general law legal medical examination in criminal proceedings, including examination of an accused and examination of an arrested person. The BNSS does not make any detailed stat about the application of gender- specific safeguards in relation to medical examination of Transgender people. Nor does it provide specific transgender protocol for handling of sensitive personal or medical information collected during the course of the examination. Like during a medical examination, sensitive parts of the body may be examined and private medical information may be required. For Transgender individuals, it may bring up more issues about the Privacy, dignity, and respect to be had into their bodies. So, the issue here is not a lack of medical examination provisions. The difference is that there is no specific guidance for them on how to implement them in a transgender inclusive way.

The lack of specific transgender provisions is one of the most significant issues in practice, in the case of Custodial Placement. Under **Section 56**, it is a duty of the person having custody of an arrested person to exercise reasonable care of the person's health and safety. Further safeguards are set out in **Section 57 and Section 58** under BNSS, regarding presenting accused in front of

Magistrate and detention in excess of 24 hours.

While **Section 56** puts a duty to make reasonable efforts to ensure the health and safety of an accused, the BNSS does not specify the relevant criteria for deciding where a transgender person should be held. It does not specify on the basis of which gender identity one should be placed . It does not state whether or not placement should be determined by sex assigned at birth, legal gender, gender identity, Indy safety, or the preference of the individual. This poses a practical problem in that where the person is detained may have an impact on their physical safety, privacy, and dignity. For instance, an inappropriate placement might be a place where a transgender detainee is harmed, intimidated, or subjected to violence.

The procedures for identifying an arrested person when identification is required are mentioned in **Section 54** of the BNSS. The provision outlines a general identification process and not a specific one on transgender identity. This leaves a space between the need to identify a person for investigation and recording or acknowledging gender identity. There may arise practical problems where the name or gender on an older document does not match the name or gender by which a transgender person identifies. The BNSS does not offer specifics on how this information should be documented regularly by police and in investigation records.

Another issue is related to privacy and confidentiality in criminal procedures. Authorities may need to obtain personal information, identity documents, medical information and other sensitive materials during criminal investigations, information about gender identity, previous name or medical history may be especially personal to a transgender person and in many situations documents are not available with them. The BNSS does not provide for a detailed procedure specifically relating to the collection, recording, storage or disclosure of information and lack of appropriate documents about a person's transgender identity. This can lead to the risk of inappropriate disclosure, inaccurate recording of inappropriate handling of personal information. The question is then whether the general procedure is adequate to ensure the protection of sensitive identity related information.

The general procedure in relation to examination of witnesses by police, statements to police, prohibition of inducement and recording of confessions and statements by a Magistrate is set out in **sections 180 to 183** of the BNSS. The problem is that these provisions do not provide a specific process for recording the gender identity of a Tran person when taking or recording their statement. For instance, if the person's current name or gender identity is not the same as the information in an older document, the BNSS does not give detailed guidance on how the information should be represented in the investigation record. This may result in inconsistency between official records. It can also lead to the individual having to repeatedly identify themselves at various stages of the criminal process. A consistent and standardized process for documenting identity information may then minimize confusion and help to ensure that the person's information is documented accurately and respectfully.

There may be a risk of insensitive or disrespectful treatment during arrest, interrogation, medical examination, or custody, due to the absence of detailed procedural guidance. The BNSS does not

contain a detailed transgender specific procedure on how to address Transgender people, how to communicate with them, or the practical issue of interacting with transgender people. This does not imply that all interactions will be discriminatory, but it does not mean that the treatment of transgender persons will be dependent on the awareness and sensitivity of individual officials if there is no clear guidance. A consistent and respectful treatment would help to ensure that the use of criminal procedure powers does not unduly impact the dignity and privacy of transgender persons.

Another effect of the lack of detailed procedures is that there may be variations in practice from one location to another. The general provisions of the BNSS apply to the criminal justice system. But if the law doesn't explicitly answer a procedural issue related to Transgender, the authorities can take other approaches. For instance, there can be variations in the way authorities deal with the issue of custodial placement or personal search. These differences can leave authorities and transgender people in a state of confusion. A more transparent procedure would then facilitate the consistent treatment and protection of transgender persons by all police stations, custodial institutions and investigating authorities.

The intent of establishing clearer procedures should not be to establish a new criminal procedure system for Transgender people. Rather, the goal should be to ensure that the current protections in the BNSS are clear and effective for Transgender people.

- **Landmark Judicial Decisions and Judicial Approach towards Transgender Rights in India:-**

The Indian judiciary has been a step forward in affirming and expanding the rights of transgender community. Why the Constitution of India guarantees equality, freedom and personal liberty to all persons, transgender people have been socially discriminated against and excluded. So, the Supreme Court and High Court have thus far been important in clarifying the interpretation of the constitutional rights of the transgender people. The judgments are relevant to this study as the criminal procedure is the exercise of the State power upon the body, freedom, privacy, and dignity of an individual. Therefore, the judicial principles emerging from these judgments can guide interpretation and implementation of BNSS, 2023 even in cases whether the judgments are not explicit in their interpretation of the BNSS.

The most significant Landmark Judgment on transgender issues in India was the ***National Legal Services Authority v. Union of India (NALSA judgement) in 2014***[21] by the Supreme Court of India. The Supreme Court recognized transgender persons as a constitutionally, recognized gender category and upheld their right to determine their own gender identity. The NALSA (National Legal Services Authority) itself says the judgement is a landmark step which established the transgender community as the third gender and safeguarded their constitutional rights. The significance of NALSA is that the court did not consider gender merely to be a biological attribute. It acknowledged one's gender identity is a significant aspect of one's personality, dignity, and freedom. The decision in the case also recognized that the rights of transgender persons were guaranteed by the fundamental rights of equal protection of law guaranteed by the Constitution, under which they

cannot be denied equal protection simply because their gender identity does not match the one they were given at birth. The BNSS has some provisions that need gender specific language, such as in relation to arrest, search and medical examination, which is why NALSA is important. The BNSS has been passed since NALSA judgement and does not include a comprehensive procedure for transgender people. Hence, for the benefit of transgender persons, the constitutional principle set out in NALSA constitutes a good interpretive guide for such provisions. However, it is not appropriate to state that NALSA took decisions directly on any issues with the BNSS. The judgement precedes the BNSS and has been used in this research for its constitutional principles concerning gender identity, equality, and dignity

Another Landmark Judgement is of ***Justice K.S. Puttaswamy (Retd.) v. Union of India***[22], ***(2017)***. Here the Supreme Court in a unanimous decision declared that the Right to Privacy is a Fundamental Right according to the Constitution which is connected to dignity, liberty, autonomy, and the freedom of an individual to make their personal decisions. Privacy was thus not just the right to be left alone, but also related to the integrity of the body and personal autonomy. This Judgement tries to give special significance to Transgender persons as criminal procedures may deal with sensitive aspects of a person's life. A person's body and informational privacy is directly impacted through arrest, personal search, medical examination, and collection of personal information. This judgement establishes a constitutional guideline for the exercise of such power. The relevance of this case does not resolve an issue related to transgender people under the BNSS directly. It is important because privacy is a fundamental right in the Constitution. This principle along with NALSA Judgement offers greater safeguard for the privacy and dignity of transgender purchase when engaging with criminal justice proceedings.

Another important Supreme Court judgment is ***Jane Kaushik v. Union of India, 2025***[23]The Supreme Court looked at the outgoing challenges faced by Transgender individuals in accessing the benefits and protection available under the law. The Court observed that though the Transgender Persons (Protection of Rights) and the Transgender Persons (Protection of Rights) Rules, 2020 were enacted there were serious issues with their implementation. The Court stressed that legal rights must not be on paper and that it is the duty of governmental authorities to ensure that these rights are realized. This judgement has particular relevance to the present research paper as it illustrates that mere legislation is not enough. There should also be adequate administrative structures, qualified officials, and procedures to enforce legal rights. The Court itself recognized issues of confidentiality, reasonable accommodation, identity documents and safety and discrimination. It also recommended gender neutral or gender diverse facilities and emphasized the need for confidentiality about transgender identity. These principles can be transferred to police stations, detention facilities, medical examinations, and criminal courts. Its principles may inform the development of Transgender inclusive procedures under the BNSS, although the judgment itself is not a direct interpretation of the BNSS.

The above judicial decisions demonstrate that there are some basic principles that should guide the application of the BNSS in the case of transgender people. First, there must be dignity safeguard throughout the entire criminal process. No person shall be subjected to arrest, search, medical

examination, questioning or custody for the purpose of humiliation, harassment, or unnecessary exposure of a person's gender identity. Secondly, privacy needs to be respected. Information about the transgender persons, identity or medical history should not be shared in an unnecessary manner. Third, equality should be substantive, not merely formal. Treating every person in the same way may not always produce equal protection where a particular group still faces specific procedural difficulties. Fourth, the right to autonomy of individuals and gender identity should be respected. A transgender individual should not be subjected to a criminal procedure that ignores their legally recognized identity without a legitimate reason.

In light of the above judicial development and the gaps identified in the previous chapter, some changes are needed to make the application of BNSS transgender inclusive. The recommendations are for legal and administrative reform and should not be interpreted as mandatory provisions of the BNSS.

The first is to create clear procedure guidelines for police and other authorities that are transgender inclusive when implementing the BNSS. The BNSS is a general procedural law which does not offer detailed guidance in all situations relating to transgender people. An existing set of guidelines issued by the relevant authorities might clarify the application of existing provision and the context of arrest, search, medical examination, custody, identification, documentation, and recording of statements. These guidelines would help to minimize confusion and ensure consistency and practice.

The second suggestion is for personal searches. Section 49 of the BNSS sets out the general principles of search of an arrested person and makes it clear that it is necessary to search a female, she shall be searched by another female with due regards to decency. The provision, however, does not specifically address how this gender based provision should be applied to transgender people. Therefore, a clear procedure should be established to ensure that searches of transgender people are carried out in a way that respects dignity, body, privacy, and personal safety. The process should also avoid unnecessary physical contact and embarrassing treatment.

The third recommendation is regarding medical examination. The BNSS contains provisions regarding medical examination in certain situations in **section 51 to 53**. They do not have a comprehensive transgender inclusive protocol. Therefore, medical examination of a transgender person should only be done for a proper legal or investigative purpose. The individual should be treated with respect and sensitive medical information should be kept confidential unless required by law. There would also be less insensitivity or discriminatory treatment if medical staff involved in criminal proceedings received appropriate professional training.

Fourth recommendation is also one of the most unanswered questions regarding custodial placement and safety. Safeguards for the person's health and safety are contained in **section 56** of the BNSS, which requires a person in custody of an arrested person to take reasonable care of the person's health and safety and safeguards relating to production before a Magistrate and detention beyond the prescribed period are contained in **section 57 and 58** of the BNSS. However, it does not state what kind of cell the transgender person should be put in, male cell, female cell, or a separate

transgender cell. Therefore, it would be inappropriate to claim that the BNSS already provides a particular type of custodial placement. Rather, safety, dignity, individual circumstances, and gender identity should be the basis for appropriate custodial guidelines. The goal should be to avoid sexual violence, harassment, humiliation, and abuse, and to ensure the security of the custodial institution. Any placement decision should also not be made based on an unnecessary isolation of transgender individuals.

Fifth recommendation is to provide special training and sanitation to police officers, prison staff, medical staff, and other criminal justice officials. It is not only the law itself that can be effective but how it is enforced. Training to be provided includes transgender identity communicating with transgender people, arrest, search, medical examination, custody, confidentiality, and interaction with transgender victims, witnesses and accused persons. Real life scenarios would be better for Practical Training, then just giving out theory.

The sixth recommendation is to enhance Magisterial supervision of the treatment of transgender persons in custody. If an arrested person has been brought before a magistrate, any concern about safety, dignity, medical care, or treatment of the arrested person should be addressed. This does not necessitate the establishment of a new judicial process for transgender people. Instead, it would help to ensure that the current judicial protections are effectively implemented in situations where transgender individuals are at a specific risk.

The seventh recommendation is that there should be uniform standards in State and Union Territories. Criminal procedure should not be based on the knowledge of any individual police officer or custodial institution. Uniform guidelines would thus eliminate the lack of constancy and offer more clarity to authority and transgender individuals.

The eighth recommendation is to establish a transparent system for collecting gender specific data in Police and criminal procedure. Information should be recorded accurately on existing forms and systems, and without unnecessary confusion between identity documents, gender identity, and other personal information. Meanwhile, sensitive data should not be made available to individuals who do not have a legitimate need to access it. This recommendation follows the constitutional significance of privacy and dignity recognized in Puttaswamy case the Recognition of gender identity in NALSA.

These recommendations should also be coordinated with existing legal and administrative mechanisms to protect transgender people. The purpose should not be to create a completely separate criminal Justice system for transgender persons, rather the goal should be to clarify, make safer, more respectful, and more capable of handling situations, not explicitly addressed by the current provisions of the BNSS.

The judicial developments mentioned in this chapter, thus offered a solid constitutional foundation to enhance the implementation of the BNSS for transgender people. The Supreme Court has already held that transgender persons have the right to equality, dignity, privacy, autonomy, and equal protection of law. The final hurdle is to make these constitutional principles operational in the procedural practices at the police station, during investigation, medical examination, in custody

and before the court.

Therefore, a criminal procedure that is transgender inclusive does not need to discriminate in favor of transgender persons or establish a completely different procedure under the BNSS. It demands clarity in the absence of law, reasonable safeguards in the presence of specific risks and uniform application of constitutional rights. Clear guidelines, appropriate training, confidentiality protections, safe custodial practices, and effective judicial oversight can help to close the gap between the general safeguards provided by the BNSS and the needs of Transgender persons.

The general principle should thus see that criminal procedure safeguard the dignity of all persons involved in it as well as the administration of Justice. If constitutional values enshrined in NALSA, Puttaswamy and later decisions consistently applied to the criminal Justice system, and if adequate administrative and procedure guidelines are added, India can move to a more inclusive and responsive criminal Justice system for transgender persons.

❖ Conclusion:-

The Bhartiya Nagarik Suraksha Sanita 2023 sets out the general procedure safeguard for arrest, search, medical examination, custody, investigation, and other stages of criminal proceedings that is applicable to transgender persons in general as it is to other persons. The BNSS however, does not offer a specific comprehensive solution to the procedural challenges that transgender persons may encounter in particular areas such as personal search, medical examination, custodial placement, identification, recording of identity related information, confidentiality, and interaction with criminal Justice authorities while the Constitution and judgements like ***NALSA v. Union of India*** and ***Justice K.S. Puttaswamy v. The Union of India*** offers strong protection of equality, dignity, privacy, and personal liberty but still a gap remains between the principles and their application. The study therefore recommends for criminal justice officials to be sensitized and trained, have clear transgender inclusive procedural guidelines, have confidentiality safeguards, have appropriate search and medical procedure, have safe custodial practices, have appropriate recording of identity related information, and have effective judicial oversight. These do not establish a new criminal process for transgender people but will enhance the BNSS and ensure it is implemented effectively. Thus, in answer to the central research question, the BNSS provides General protection but does not offer an adequate and comprehensive gender inclusive procedure framework. Greater procedural clarity, institutional awareness, and consistent application of constitutional values are necessary to ensure that transgender persons receive equal, dignified, safe and substantive Justice throughout the criminal process.

❖ References:-

1) Bhartiya Suraksha Sanhita, 2023 Bare Act
2) Constitution of India Bare Act
3) The Transgender Persons (Protection of Rights) Act, 2019
4) https://transgender.dosje.gov.in The Transgender Persons (Protection of Rights) Rules, 2020

5) https://www.scconline.com
6) https://www.scobserver.in
7) https://thehindu.com
8) www.barandbench.com
9) www.indiankanoon.org
10) https://drishtiias.com
11) https://drishtijudiciary.com
12) www.criminallawjournal.org
13) https://manupatraacademy.com
14) https://researchgate.net
15) https://feminisminindia.com
16) https://www.scribd.com
17) https://www.livelaw.in
18) https://lawvs.com
19) https://theleaflet.in
20) https://ijlmh.com

ENDNOTES

1 https://www.scconline.com

2 https://transgender.dosje.gov.in

3 https://www.scconline.com

4 Constitution of India 1950, art 14

5 https://www.scconline.com

6 Constitution of India 1950, art 15

7 Constitution of India 1950, art 21

8 Bharatiya Nagarik Suraksha Sanhita, 2023,s 35

9 Bharatiya Nagarik Suraksha Sanhita, 2023, s 43

10 Bharatiya Nagarik Suraksha Sanhita, 2023, s 49

11 Bharatiya Nagarik Suraksha Sanhita, 2023, s 49(2)

12 Bharatiya Nagarik Suraksha Sanhita, 2023, ss 51- 53

13 Bharatiya Nagarik Suraksha Sanhita, 2023, s 54

14 Bharatiya Nagarik Suraksha Sanhita, 2023, s 56

15 Bharatiya Nagarik Suraksha Sanhita, 2023, s 57

16 Bharatiya Nagarik Suraksha Sanhita, 2023, s 58

17 Bharatiya Nagarik Suraksha Sanhita, 2023, s 180

18 Bharatiya Nagarik Suraksha Sanhita, 2023, s 181

19 Bharatiya Nagarik Suraksha Sanhita, 2023, s 182

20 Bharatiya Nagarik Suraksha Sanhita, 2023, s 183

21 https://www.scconline.com

22 https://www.scconline.com

23 https://scobserver.in