
RECONSTRUCTING PROOF IN THE DIGITAL AGE: THE MADHYA PRADESH AMENDMENT ON ELECTRONIC EVIDENCE UNDER THE BHARATIYA SAKSHYA ADHINIYAM AND BHARATIYA NAGRIK SURAKSHA SAHITA

Aryan Leander Wishard, PhD, Renaissance University, Indore, Madhya Pradesh¹

Namaswi Gupta, LLM, Vikram University, Ujjain, Madhya Pradesh²

ABSTRACT

The Madhya Pradesh Gazette notification dated June 25, 2026, issued by the Home Department, has introduced a state-level amendment concerning electronic evidence under the Bharatiya Sakshya Adhiniyam, 2023 and the Bharatiya Nagarik Suraksha Sanhita, 2023. The amendment is a significant step in the legal paradigm, especially for present day criminal adjudication which largely depends on digital records such as mobile phone extractions, CCTV footage, emails, metadata, call detail records and platform-based communications. This article examines the legal and constitutional significance of such a state intervention, in consultation with the Hon'ble High Court of Madhya Pradesh, in the law governing electronic evidence. It argues that any amendment in this field must be assessed against four benchmarks: authenticity, procedural integrity, investigative efficiency and fair trial protection. While a state-specific framework may improve the collection and proof of digital material, it also raises serious concerns regarding legislative competence, privacy, chain of custody and the possibility of diluted evidentiary safeguards. The general rules cover the reception, storage, retrieval, access management and preservation of electronic records in courts. The article concludes that the value of these 'general rules' lies not merely in modernizing procedure, but in whether it creates a system in which digital evidence becomes easier to prove because it is more reliable, not because scrutiny is reduced.

Keywords: electronic evidence, digital forensics, Bharatiya Sakshya Adhiniyam, Bharatiya Nagarik Suraksha Sanhita, Madhya Pradesh, admissibility, criminal procedure.

¹ PhD, Renaissance University, Indore, Madhya Pradesh

² LLM, Vikram University, Ujjain, Madhya Pradesh

Introduction

The law of evidence is undergoing a practical transformation. The burden of proof in criminal cases is no longer restricted primarily through oral testimony and physical documents; they are increasingly built around mobile phone records, surveillance footage, social media communications, geolocation data, server logs and forensic extractions from digital devices. In this setting, electronic evidence is no longer superficial, but foundational to criminal adjudication. The enactment of the **Bharatiya Sakshya Adhiniyam, 2023** and the **Bharatiya Nagarik Suraksha Sanhita, 2023** reflects the Indian legal system's attempt to reframe evidence and procedure in light of these technological realities³.

The Madhya Pradesh Gazette notification dated June 25, 2026, concerning electronic evidence under these statutes, deserves careful scholarly attention⁴. A state amendment in this field is significant not only because it addresses a pressing evidentiary challenge, but also because it occupies a constitutionally sensitive area where criminal procedure, evidentiary reliability, and individual liberty intersect. The problem of electronic evidence is not merely one of technological adaptation. It is equally a problem of legal trust: how should courts determine that a digital record is authentic, untampered, and fairly obtained?

This article examines the normative and doctrinal implications of the Madhya Pradesh amendment as a legal development in the emerging architecture of digital criminal justice. It argues that reforms concerning electronic evidence are justified only when they reduce uncertainty without weakening safeguards. In other words, appreciation of electronic evidence has become easier only because the legal system has become better at preserving and authenticating it.

Legislative Background

The **Bharatiya Sakshya Adhiniyam, 2023** replaced the Indian Evidence Act, 1872 and now governs the admissibility, relevancy, and proof of evidence in judicial proceedings⁵. The **Bharatiya Nagarik Suraksha Sanhita, 2023** replaced the Code of Criminal Procedure,

³ The Bharatiya Sakshya Adhiniyam, No. 47 of 2023, India Code; The Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, India Code.

⁴ Madhya Pradesh Gazette, Home Department, Notification dated June 25, 2026.

⁵ The Bharatiya Sakshya Adhiniyam, No. 47 of 2023, India Code.

1973 and regulates investigation, search, seizure, documentation, and trial process⁶. Together, these statutes create the procedural and evidentiary framework within which electronic records are discovered, preserved, certified, and presented before courts.

The need for legal adaptation in this sphere is obvious. Unlike traditional documents, electronic records can be duplicated perfectly, altered invisibly, stored remotely or generated automatically without human authorship in the conventional sense. Their reliability depends not on appearance alone, but on system integrity, forensic method, and chain of custody. Indian courts have long grappled with this issue, especially in relation to certification requirements for electronic records and the extent to which procedural noncompliance should affect admissibility⁷.

A state amendment concerning electronic evidence is therefore likely motivated by practical concerns arising in criminal justice administration: delayed certification, inconsistent forensic protocols, uncertainty in proving digital extractions, and disputes regarding the authority of investigating officers or technical experts. Such concerns are legitimate. But the legal response to them must preserve the distinction between flexibility and dilution.

The Distinct Nature of Electronic Evidence

Electronic evidence presents difficulties unknown to conventional documentary proof. First, it is highly **volatile**. A digital record may be deleted, overwritten, encrypted, remotely altered, or automatically modified through ordinary system use. Delay in seizure may therefore result in evidentiary destruction.

Second, it is **replicable without visible change**. A copy of a file may be indistinguishable from its source, thereby complicating conventional notions of “original” and “copy.” The law must therefore rely on technical markers such as metadata and hash values to establish integrity.

Third, electronic evidence is often **context-dependent**. A message, video, or extracted file may derive meaning only when placed within a larger evidentiary architecture involving device ownership, account access, time stamps, transmission pathways, and forensic analysis.

⁶ The Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, India Code.

⁷ Anvar P.V. v. P.K. Basheer, (2014) 10 S.C.C. 473 (India); Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 S.C.C. 1 (India).

Fourth, it is **privacy intensive**. A smartphone or laptop may contain a complete map of an individual's associations, movements, preferences, and communications. Investigative access to such devices raises questions that extend well beyond evidentiary doctrine into constitutional liberty and informational privacy⁸.

These characteristics explain why electronic evidence cannot be treated merely as a digital substitute for paper records. It requires distinct legal handling at every stage of criminal process.

The Likely Purpose of the Madhya Pradesh Amendment

Although the precise text of the amendment is not reproduced here, a state intervention directed at electronic evidence under the Bharatiya Sakshya Adhiniyam and Bharatiya Nagarik Suraksha Sanhita may reasonably be understood as addressing one or more of the following concerns: the mode of proving electronic records, the authority of certifying officials, the role of forensic laboratories, the protocol for device seizure and preservation, and the reduction of procedural objections in digital-heavy prosecutions.

Such a reform would reflect a broader institutional recognition that criminal courts increasingly depend upon digital records. In cases involving cybercrime, financial fraud, sexual violence, organized criminal activity, conspiracy and even ordinary offences supported by CCTV or mobile evidence, the absence of clear rules can derail adjudication. Yet the legitimacy of procedural streamlining depends on whether it preserves meaningful safeguards. Where digital material can be manipulated with ease, evidentiary shortcuts are particularly dangerous.

Thus, the likely purpose of the amendment should be understood as administrative rationalization, but its legal validity must be measured in terms of reliability and fairness.

Admissibility, Certification and Authenticity

The most important doctrinal issue in electronic evidence law remains **authentication**. Courts must be assured that the digital material presented is what it purports to be, that it was generated or stored within a reliable system, and that it has not been materially altered. Indian jurisprudence has repeatedly emphasized the importance of statutory compliance in proving

⁸ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).

electronic records, particularly where the original device is not itself produced before the court⁹.

A state amendment may seek to relax procedural rigidity by broadening the class of persons competent to certify or authenticate an electronic record. This may include designated officers, custodians of electronic systems, or forensic examiners. Such reform may be defensible where modern digital ecosystems make conventional authorship models impractical. For example, CCTV data, cloud storage logs, or telecom-generated records often require institutional rather than personal certification.

However, the law must avoid collapsing **authentication** into mere official assertion. If the amendment permits admission of digital material without sufficient guarantees of integrity, then the reform would not modernize evidence law; it would weaken it. Flexibility is acceptable only where substitute safeguards remain robust.

The doctrinal principle should therefore be clear: procedural simplification must not erode evidentiary trustworthiness.

Search, Seizure, and Chain of Custody

The second crucial issue lies in the procedural handling of digital material under the Bharatiya Nagarik Suraksha Sanhita. Electronic evidence is uniquely vulnerable to contamination. A device may be powered on, accessed, copied, or searched in a manner that modifies logs, changes metadata, or compromises the evidentiary value of the underlying data. Once contamination occurs, the authenticity of the entire digital chain may become contestable.

This is why chain of custody is central to electronic evidence. Proper practice ordinarily requires documentation of seizure, imaging or cloning of storage media where feasible, preservation of original devices, recording of hash values, sealing and labelling, restricted access logs, and transparent movement of material to forensic units¹⁰. These are not purely technical requirements. They are legal safeguards that permit the court to infer continuity and reliability.

⁹ Supra note 7.

¹⁰ B. Guttman. *Digital Evidence Preservation Considerations for Evidence Handlers*, NIST Interagency Report NIST IR 8387.

A well-drafted amendment could strengthen criminal justice by standardizing these requirements across the State. Such standardization would benefit both prosecution and defence. Prosecutors gain stronger evidentiary credibility; accused persons gain a clearer basis to challenge irregular collection or possible tampering. In digital cases, procedural discipline is the legal foundation of substantive justice.

Forensic Expertise and the Evidentiary Role of Laboratories

Electronic evidence frequently reaches the courtroom only after forensic extraction and interpretation. Deleted files, encrypted chats, IP logs, geolocation records, call metadata, and surveillance enhancements all depend upon specialized technical processes. A state amendment may therefore seek to assign greater evidentiary weight or clearer statutory recognition to forensic laboratories and their reports.

Such a development can improve efficiency. Trial courts need dependable institutional mechanisms for understanding digital material. But forensic reliance also creates risks. If courts accept technical reports uncritically, expertise may displace adjudication. Proprietary software, undocumented extraction protocols, or opaque analytical methods may become the hidden basis of conviction.

Therefore, even where a forensic report is granted significant evidentiary value, the accused must retain the right to inspect methodology, challenge conclusions, and seek meaningful cross-examination where necessary. The legitimacy of digital forensics in criminal process depends on transparency and contestability, not merely on technical sophistication.

Constitutional and Federal Concerns

A state amendment affecting central criminal legislation necessarily engages questions of constitutional structure. Criminal law and criminal procedure belong to a domain where Parliament and State legislatures operate within a defined federal arrangement. Accordingly, a state-specific rule on electronic evidence must be assessed for consistency with the constitutional scheme governing legislative competence and repugnancy¹¹.

Beyond competence, the amendment must also satisfy substantive constitutional standards.

¹¹ India Const. art. 246; India Const. art. 254.

Electronic evidence law implicates the right to equality under **Article 14** and the guarantee of fair, just, and reasonable procedure under **Article 21** of the Constitution of India¹². It also intersects with the constitutional recognition of privacy as an aspect of personal liberty. Broad seizure powers, weak filtering standards, or presumptive acceptance of official digital certifications may therefore invite constitutional challenge.

For this reason, the amendment cannot be defended solely on grounds of administrative convenience. In criminal process, convenience is not a substitute for legality. Any reform governing electronic proof must remain anchored in fairness, proportionality, and reviewability.

Normative Appraisal

The Madhya Pradesh amendment, if carefully designed, may represent a constructive attempt to align evidentiary law with technological reality. The advantages are obvious: reduced procedural confusion, more coherent forensic practice, greater clarity for courts, and potentially faster adjudication in cases where digital records are decisive.

Yet the risks are equally significant. Digital evidence is easy to mishandle and, in some contexts, easy to manipulate. Weak certification models, overbroad device searches, insufficient chain-of-custody norms, and excessive judicial deference to forensic reports can each produce serious miscarriages of justice. Moreover, institutional disparities across police units and lower courts may result in inconsistent implementation.

The amendment should therefore be judged not by whether it accelerates proof in the abstract, but by whether it creates a more disciplined ecology of proof. The ideal legal regime is one in which electronic evidence becomes procedurally smoother because investigative practices have become more rigorous, not because evidentiary standards have become easier to bypass.

Conclusion

The Madhya Pradesh Gazette notification of June 25, 2026, concerning electronic evidence under the Bharatiya Sakshya Adhiniyam, 2023 and the Bharatiya Nagarik Suraksha Sanhita, 2023, reflects a deeper transition in Indian criminal justice. The system is moving from material

¹² India Const. arts. 14, 21.

records to digital traces, from physical exhibits to forensic images and from conventional documentary proof to technologically mediated adjudication. In this environment, reform is necessary. But reform must be principled.

Electronic evidence law occupies a difficult intersection of technology, procedure and liberty. The challenge is not merely to make digital evidence admissible, but to make it trustworthy. A constitutionally sound and institutionally effective amendment would standardize collection, preserve integrity, support authentic certification and maintain the accused's right to challenge forensic proof. Its success would lie in ensuring that modern criminal justice becomes both more technologically capable and more legally accountable.