# DIGITAL EVIDENCE AND ELECTRONIC SURVEILLANCE IN INDIA: A CRITICAL ANALYSIS OF THE BSA 2023 AND BNS 2023

Anmol Yadav, LL.M. (Criminal Law and Criminal Justice Administration), Uttar Pradesh State Institute of Forensic Science (UPSIFS), Lucknow

## 1. Introduction

In the modern world, a person's digital footprint often speaks louder than a witness. A WhatsApp conversation may reveal the circumstances of a crime, CCTV footage may identify an offender, and mobile location records may place an individual at a particular location. At the same time, the same technology can be used to invade privacy, manipulate information, and create evidence that appears genuine but is fundamentally misleading. The challenge before Indian criminal jurisprudence is therefore not merely to embrace technology, but to ensure that its use remains consistent with justice, dignity, and constitutional liberty.

The enactment of the Bharatiya Sakshya Adhiniyam, 2023 (BSA) and the Bharatiya Nyaya Sanhita, 2023 (BNS), which came into force on 1 July 2024, marks an important phase in the transformation of India's criminal justice system. While the BSA governs the recognition and admissibility of evidence, the BNS defines criminal offences and their punishments. Together, they operate within a wider legal framework that includes the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), the Information Technology Act, 2000, and constitutional protections. Their effectiveness must ultimately be judged not by their modern terminology, but by their ability to reconcile effective law enforcement with individual rights.

## 2. Digital Evidence under the Bharatiya Sakshya Adhiniyam, 2023

One of the significant features of the BSA is its express recognition of electronic and digital records within the law of evidence. Section 2 includes electronic records within the definition of documents, while Sections 61 to 63 address their legal recognition and admissibility. Emails, server logs, messages, digital files, location data, and other electronically stored information can consequently play a central role in judicial proceedings.

Section 63, which carries forward the framework previously contained in Section 65B of the Indian Evidence Act, 1872, prescribes conditions for the admissibility of specified electronic records produced as computer output. The statutory certificate requirements are intended to establish the source and manner of production of such records and to support their reliability.

This development is necessary because criminal investigations increasingly depend upon evidence that exists beyond the physical crime scene. Digital records can help reconstruct events, establish communication between individuals, and corroborate or contradict oral testimony. Yet legal recognition must not be confused with unquestionable reliability. A screenshot can be fabricated, an audio recording manipulated, and a digital file altered without obvious signs of interference.

The distinction between admissibility and evidentiary weight is therefore fundamental. A record may satisfy the formal requirements for admission but still raise serious questions about authenticity, completeness, context, or attribution. The fact that a message originated from a particular account does not automatically establish who sent it or whether the recipient's interpretation is correct.

In Anvar P.V. v. P.K. Basheer (2014), the Supreme Court emphasised the statutory safeguards governing electronic evidence under the former evidence law. In Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020), the Court reaffirmed the importance of the certificate requirement under Section 65B, subject to the legal principles explained in that judgment. These decisions remain important interpretive background, although the BSA's own provisions must now be applied to proceedings governed by the new enactment.

The central concern is that procedural compliance should not become a substitute for scientific scrutiny. Courts and investigators must examine the integrity of digital records, their chain of custody, the reliability of extraction methods, and the possibility of alteration. Without trained forensic personnel, secure evidence storage, and independent verification, the promise of digital evidence may become a source of wrongful accusation rather than a pathway to truth.

### 3. Electronic Surveillance: Security versus Privacy

Electronic surveillance presents a more difficult constitutional question. CCTV cameras, telephone interception, internet monitoring, GPS tracking, and digital data collection can assist

in preventing crime and investigating serious offences. However, surveillance also creates the possibility of continuous monitoring of individuals who have neither committed an offence nor attracted any legitimate suspicion.

The Constitution of India does not treat privacy as an insignificant interest that must yield automatically to investigative convenience. In Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), a nine-judge Bench of the Supreme Court recognised privacy as a fundamental right protected under Article 21 and other freedoms guaranteed by Part III of the Constitution. Restrictions on privacy must satisfy the applicable constitutional requirements, including legality, a legitimate state aim, proportionality, and appropriate safeguards against abuse.

This principle has particular relevance to electronic surveillance. The power to investigate a crime does not create an unrestricted licence to monitor private communications, track movements, or collect personal information. Surveillance must have a lawful basis and must be proportionate to the objective pursued.

The BNS should be understood in this context. It consolidates and revises substantive criminal law, including offences involving organised criminal activity, terrorism, and other forms of unlawful conduct. It is not, however, a comprehensive statutory code governing every aspect of electronic interception or surveillance. The legal authority and procedure for interception, investigation, and related measures must also be examined under applicable legislation, including the Information Technology Act and the Telecommunications Act, 2023, together with relevant rules and constitutional principles.

This distinction matters. A criminal statute may define conduct as an offence without independently authorising every investigative technique that the police might consider useful. The existence of a legitimate investigative objective cannot, by itself, cure an absence of legal authority or procedural safeguards.

## 4. A Critical Appraisal of the BSA and BNS

The principal strength of the new framework lies in its recognition that criminal justice must respond to technological change. Traditional evidence such as eyewitness accounts and physical documents remains important, but it can no longer adequately address crimes involving encrypted communications, digital transactions, online fraud, and remotely

coordinated activity.

Nevertheless, the reforms leave important practical questions:

- **First,** the BSA's provisions on admissibility do not, by themselves, establish a comprehensive system of safeguards for the collection, preservation, and forensic examination of every digital record. A certificate may address statutory requirements, but it cannot independently guarantee that the original data was lawfully obtained, accurately extracted, or free from manipulation.

- **Second,** there is a growing imbalance between the technical sophistication of investigative tools and the resources available to many investigating agencies and courts. Digital evidence requires specialised knowledge. Without proper training, even genuine evidence may be mishandled, while fabricated or misleading material may escape adequate scrutiny. Access to reliable forensic facilities should not depend upon the financial resources of a particular State or the social position of an accused person.

- **Third,** the possibility of surveillance being used selectively or excessively remains a serious concern. Digital monitoring can expose intimate relationships, political associations, professional communications, and personal beliefs. The harm may extend beyond the individual under investigation, affecting journalists, lawyers, whistle-blowers, and ordinary citizens whose communications become part of a wider data collection exercise.

- **Finally,** the BNS and BSA must be assessed alongside the BNSS and the laws governing interception and data protection. Their provisions cannot be read in isolation. A coherent criminal justice framework requires clarity about who may authorise surveillance, the circumstances in which it is permissible, how collected data must be secured, and what remedies are available when unlawful monitoring occurs.

## 5. The Way Forward

India needs a framework that treats technological capability and constitutional accountability as complementary rather than competing objectives. Investigating agencies should follow standardised protocols for digital searches, forensic imaging, metadata preservation, cryptographic verification, and documented chain of custody. Independent technical

examination should be available where authenticity is seriously disputed.

Surveillance powers must be accompanied by meaningful authorisation procedures, necessity and proportionality assessments, time limits, secure retention practices, and effective oversight. Unnecessary data should not be retained indefinitely, and individuals should have access to appropriate remedies where their rights have been unlawfully infringed, subject to legitimate investigative requirements.

Judicial institutions must also develop greater technical capacity. Judges and lawyers should be equipped to understand the limitations of metadata, location records, artificial intelligence-generated content, and deepfakes. At the same time, the State must invest in forensic infrastructure and ensure that procedural protections remain meaningful for persons who cannot afford independent experts.

Most importantly, the legal system must remember that digital evidence represents human lives and relationships. Behind every message, location record, or intercepted conversation is a person whose liberty, reputation, or dignity may be affected by its interpretation.

## 6. Conclusion

The BSA 2023 and BNS 2023 represent an important stage in the modernisation of Indian criminal law. The BSA provides a framework for recognising and proving electronic records, while the BNS updates substantive criminal law for a changing society. Yet technological modernisation alone cannot guarantee justice.

The real test lies in ensuring that digital evidence is reliable, surveillance is lawful, and investigative power remains subject to constitutional restraint. A criminal justice system must be capable of identifying the guilty without treating every citizen as a potential suspect. It must protect victims without sacrificing the rights of the accused, and embrace innovation without abandoning human dignity.

Ultimately, the legitimacy of India's digital criminal justice system will depend not on how much information the State can collect, but on how responsibly it uses that information. Technology may assist the search for truth, but fairness, accountability, and respect for liberty must remain its guiding principles.

## References & Suggested Sources for Publication


- The Bharatiya Sakshya Adhiniyam, 2023 (BSA) — particularly Sections 2, 61, 62, and 63.
- The Bharatiya Nyaya Sanhita, 2023 (BNS) — Substantive Criminal Law Framework, Ministry of Home Affairs.
- Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1 — Landmark Supreme Court judgment on Privacy.
- Anvar P.V. v. P.K. Basheer (2014) 10 SCC 473 — Primary decision on admissibility of electronic evidence.
- Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) 7 SCC 1 — Reaffirming certificate requirements for electronic evidence.
- PRS Legislative Research — Legislative Brief on the Bharatiya Sakshya Bill, 2023.