TECHNOLOGICAL TRANSFORMATION IN CRIMINAL INVESTIGATION: NAVIGATING PROGRESS AND PRIVACY UNDER THE BHARATIYA NAGARIK SURAKSHA SANHITA, 2023

Arshad Alam, Assistant Professor, Sardar Patel Subharti Institute of Law, Swami Vivekanand Subharti University, Meerut

ABSTRACT

The Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023[1] marks a transformative shift in India's criminal procedural framework, replacing the colonial-era Code of Criminal Procedure, 1973.[2] The new law institutionalizes digital integration across every phase of the criminal justice process, including e-FIR registration,[3] electronic communication of summons, digital casetracking systems, and audio-visual recording of search, seizure, and statement-recording procedures. These initiatives aim to promote expeditious investigation, strengthen evidentiary integrity, and enhance judicial transparency.

However, rapid technological adoption also introduces complex concerns relating to data protection, cyber-vulnerabilities,[4] surveillance risks, and institutional capacity-building**.** This paper critically examines the operational architecture of BNSS-driven digital reforms, interrogates constitutional implications particularly in light of the fundamental right to privacy and procedural fairness[5] evaluates practical implementation challenges, and proposes a rightsbased framework to ensure that technological modernization complements the constitutional ethos of justice, liberty, and due process.

[1] Government of India. (2023). *Bharatiya Nagarik Suraksha Sanhita, 2023.* Gazette of India, Ministry of Law and Justice.
[2] Government of India. (1973). *Code of Criminal Procedure, 1973* (CrPC). Gazette of India.
[3] BNSS, 2023, Sections 173, 176, 180 & 193 (Digital documentation, e-FIR, electronic service, and electronic trial procedures).
[4] Ministry of Electronics & Information Technology. (2023). *Digital Personal Data Protection Act, 2023.* Government of India.
[5] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

Introduction: Context and Need for Reform

India's criminal justice system has long grappled with systemic delays, case backlogs,[6] inadequate infrastructure, and procedural bottlenecks, resulting in significant barriers to timely access to justice. With the proliferation of cyber offences, increasing digital communication, and evolving patterns of organized crime, traditional investigative mechanisms have proven insufficient.[7]

Against this backdrop, the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023 introduces a digital-first investigatory ecosystem, signalling a shift toward technologically-assisted law enforcement. The statute mandates digital documentation of investigations, e-registration of First Information Reports (e-FIR), electronic service of summons and warrants, integration of forensic technologies, video-recording of evidence-gathering processes, and interlinking of police records with national databases.

This legislative transformation reflects growing public demands for a transparent, accountable, and efficient criminal justice architecture. Yet, technological empowerment must operate within the constitutional guardrails of privacy, proportionality, and procedural fairness. The Supreme

Court's landmark ruling in *Justice K.S. Puttaswamy v. Union of India* (2017)[8] firmly established the right to privacy as a fundamental right, requiring all State-led digital initiatives to conform to principles of legality, necessity, and proportionality.

Thus, while BNSS-driven modernization promises enhanced efficiency and investigative capacity, it simultaneously necessitates robust safeguards, ethical data governance, and institutional preparedness to prevent misuse, digital coercion, and algorithmic bias.

Key Technological Innovations under BNSS, 2023

1. Electronic FIR and Complaint Platforms

[6] National Crime Records Bureau. (2022). *Crime in India 2022* (Vol. 1, p. xxvi). Ministry of Home Affairs. *(Foreword section discussing pendency)*
[7] Government of India. (2023). *Bharatiya Nagarik Suraksha Sanhita, 2023* (pp. 112–114). Gazette of India. *(Chapter on investigation procedures & electronic evidence)*
[8] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, 266–270. *(Privacy as a fundamental right & proportionality test)*

The BNSS institutionalizes the electronic registration of First Information Reports (e-FIRs),[9] removing the requirement for victims or informants to physically visit a police station. This reform enhances accessibility, particularly for individuals in remote or rural regions, women facing domestic or sexual violence, persons with disabilities, and other vulnerable groups who may fear retaliation or intimidation in physical complaint-filing settings.

In addition to improving access, e-FIRs are automatically time-stamped, creating a verifiable digital trail and promoting procedural transparency. The provision complements the concept of Zero FIR, permitting the filing of complaints at any police station irrespective of territorial jurisdiction, thereby expediting the initiation of investigation in urgent matters such as cybercrime, physical assault, and kidnapping cases.

Despite these advancements, the model is not without challenges. Concerns arise regarding the digital divide, identity verification, cyber-security vulnerabilities, misuse through fake complaints, and the risk of excluding technologically disadvantaged populations. A balanced approach that combines public digital literacy initiatives, secure login systems (including Aadhaar-linked OTP access), and police training modules is essential to ensure the equitable functioning of the e-FIR system.

2. Electronic Service of Summons and Legal Documents

The BNSS authorizes the service of legal documents—including summons, warrants, notices,[10] and information orders—through email, SMS, digital portals, and other authenticated electronic means**.** This mechanism is designed to address one of the most persistent logistical delays in criminal procedure: failure or delay in serving summons. Digital audit trails record when notices are issued, transmitted, and received, strengthening accountability and reducing procedural lapses.

However, implementation requires meticulous standards. A uniform authentication protocol, digital signature validation, encrypted delivery platforms, and secure national-level notification dashboards are critical. Without such safeguards, individuals lacking smartphones, stable network access, or digital literacy risk procedural exclusion. To mitigate such risks, hybrid

[9] Government of India. (2023). *Bharatiya Nagarik Suraksha Sanhita, 2023* (pp. 112–114). Gazette of India.
[10] BNSS, 2023, Sections 61–64 (Service of summons and processes digitally).

models (digital + physical service where required) must remain operational.

3. Video Recording and Digital Evidence Protocols

The BNSS mandates audio-video recording of critical procedural stages such as search and seizure, examination of witnesses, and recording of statements. This technological layer aims to deter coercion, torture, forced confessions, and custodial misconduct—historically significant concerns in Indian criminal jurisprudence.

Moreover, the Bharatiya Sakshya Adhiniyam, 2023[11] modernizes evidentiary rules by formally recognizing electronic records, metadata, timestamps, CCTV footage, and body-worn camera recordings as admissible evidence. These reforms are consistent with global developments in digital policing and procedural transparency.

Nonetheless, digital evidence systems demand strict chain-of-custody mechanisms, secure forensic labs, tamper-proof digital lockers, and audit trails to prevent manipulation, deepfakes, data loss, or unauthorized access. State police forces must expand investments in storage servers, encryption, forensic video analytics, and capacity-building programs.

4. Forensic Expansion and Digital Investigation Tools

The BNSS mandates forensic[12] examination in serious offences particularly those punishable with seven years or more imprisonment and requires forensic experts to digitally document their procedures. This represents a paradigm shift from police centric evidence handling toward scientifically validated investigation frameworks**.**

Contemporary policing now integrates tools such as:

- digital forensics labs and cyber-crime units
- mobile data extraction tools
- GPS-based tracking systems

[11] Government of India. (2023). *Bharatiya Sakshya Adhiniyam, 2023* (pp. 88–92). Gazette of India.
[12] BNSS, 2023, Section 176 (pp. 121–123), mandate for forensic investigation in serious offences.

- IP-log tracing and server-based metadata retrieval
- facial recognition systems and biometric matching
- social media analytics and digital footprint mapping

These tools can significantly improve investigative efficiency, especially in cyber-offences, interstate criminal networks, and terror-linked activities. However, heavy reliance on AI-driven profiling and facial recognition requires oversight to avoid wrongful suspicion, algorithmic bias, and privacy violations.

Clear ethical standards, judicial oversight mechanisms, and transparency requirements are essential to avoid unchecked surveillance and ensure compliance with proportionality and legality principles affirmed in *Puttaswamy*.

Privacy and Constitutional Safeguards

India's constitutional architecture places privacy and personal liberty at its core. Article 21 of the Constitution guarantees the right to life and personal liberty, which, as reaffirmed in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, is inseparable from dignity, autonomy, and informational privacy. Any technological surveillance or data-driven investigative process must therefore satisfy the triple-test of legality, necessity, and proportionality,[13] requiring a valid law, a legitimate state purpose, and minimal intrusion into individual rights.

While the BNSS represents a modernized investigatory framework, it presently lacks a comprehensive statutory structure for the retention, access, sharing, and deletion of digital evidence and biometric-linked records. Without clearly-defined retention limits, independent oversight bodies, and auditable digital trails, there exists a heightened risk of mass data capture evolving into unfettered surveillance.[14] The specter of a ―surveillance state‖ is not merely theoretical; expanding police access to facial recognition databases, telecom records, and citizen digital profiles demands strict proportionality-based safeguards and judicial supervision.

[13] J*ustice K.S. Puttaswamy (Retd.) & Anr. v. Union of India*, (2017) 10 SCC 1, para 325.
[14] Agarwal, R. (2022). *Surveillance, privacy and the Indian state: Constitutional tensions in the digital era*. Indian Journal of Constitutional Studies, 5(2), 112–118.

The Digital Personal Data Protection Act (DPDPA), 2023[15] introduces obligations for lawful processing of personal data and establishes accountability structures. However, broad exemptions for ―sovereign functions‖ and ―public order investigations‖ create interpretive uncertainty when applied to criminal investigations under BNSS. Harmonization between BNSS and DPDPA including data minimization norms, deletion schedules, grievance redress mechanisms, and independent audit frameworks is essential to strike a constitutional balance between efficient law enforcement and fundamental liberties. In a democratic society, technological efficiency must be matched by transparent privacy protocols, judicial authorization, and parliamentary oversight to ensure that security measures do not silently erode civil freedoms.

Balancing Innovation with Due Process

Technological modernization should reinforce principles of fairness and justice. To ensure that digital tools do not undermine constitutional guarantees, several safeguards are critical. Judicial authorization must be obtained for accessing individuals' devices or their communication metadata. Protocols for electronic search and seizure should be detailed and standardized, while robust encryption measures need to be in place for digital evidence. Officer training programs that emphasize ethical investigation and digital competence are particularly necessary as technology becomes increasingly central to routine police work. Convenience for investigators should never take precedence over the procedural rights of the accused and the privacy of individuals.

Balancing Innovation with Due Process

Technological modernization should reinforce, not dilute, foundational principles of fairness, natural justice, and procedural safeguards.[16] As law-enforcement agencies increasingly rely on digital search, biometric tools, and communication interception, it becomes essential to ensure that such tools function within the contours of constitutionally guaranteed rights. Judicial authorization must be mandatory before accessing personal devices, encrypted communication, cloud-stored data, or telecommunication metadata to prevent arbitrary intrusion into private digital spaces. Clear and standardized protocols for electronic search, cloud-forensics, imaging

[15] Digital Personal Data Protection Act, No. 22, Acts of Parliament, 2023 (India). Retrieved from https://www.meity.gov.in/
[16] *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248, ¶ 56.

of devices, and chain-of-custody procedures are critical to maintain evidentiary integrity.[17] Additionally, strong encryption standards and tamper-proof audit trails should be implemented to prevent manipulation of digital evidence and ensure admissibility in court.

Capacity building programs for investigation officers must focus not only on technical competence but also on ethical policing and rights-based investigative conduct, especially as digital surveillance and automated policing tools become normalized. Importantly, administrative convenience or investigative speed must not override the procedural rights of the accused including the right to counsel, protection against self-incrimination, and the presumption of innocence as recognised in domestic constitutional jurisprudence and international fair-trial norms.[18] In an era where the State's technological capacity is rapidly expanding, statutory checks, judicial oversight, and transparent accountability mechanisms are indispensable to prevent misuse and ensure that innovation coexists with liberty, due process, and democratic accountability.

Challenges in Implementation

Despite its progressive aspirations, the BNSS faces formidable challenges in real-world implementation.[19] Uneven technological infrastructure, especially in rural and geographically remote regions, limits the uniform rollout of digital policing systems creating a risk of unequal access to justice. Many police stations still lack stable internet connectivity, digital case management systems, and secure online reporting facilities, resulting in continued reliance on manual record-keeping.

Capacity limitations among law-enforcement personnel further impede effective execution. While the BNSS emphasizes digital evidence and video-based procedures, a considerable number of police officials are yet to receive specialized training in cyber forensics, device imaging, metadata authentication, and courtroom presentation of electronic records. The limited number of accredited cyber-forensic laboratories, combined with significant backlog and inadequate technical manpower, delays timely verification of digital evidence. Weak chain-

[17] National Cyber Forensics Lab. (2022). *Guidelines on Digital Search and Seizure in India* (pp. 18-22). Bureau of Police Research & Development. https://bprd.nic.in/
[18] International Covenant on Civil and Political Rights, art. 14 (Right to fair trial). United Nations. https://www.ohchr.org/
[19] Bhatnagar, R. (2024). *Implementation challenges of BNSS reforms,* National Law University Policy Brief.

of custody practices and lack of standardized protocols increase the probability of evidence tampering or contamination, potentially jeopardizing fair trial rights.[20]

Data security concerns also persist, with several state police databases still operating on insecure or outdated systems, exposing sensitive information to risks of hacking, unauthorized access, and data leakage. Furthermore, low levels of digital literacy among vulnerable communities hinder effective use of online FIR portals, e-summons platforms, and virtual court facilities.[21] Without focused public awareness initiatives and community outreach, technological reforms may inadvertently widen the digital divide, undermining the very goal of accessible and equitable criminal justice delivery.

Recommendations for Effective Reform

Legal and Policy Recommendations

A clear statutory architecture is required to harmonize BNSS provisions with existing data protection frameworks, particularly the Digital Personal Data Protection Act, 2023. Such alignment must explicitly define data-retention timelines, encryption standards, oversight mechanisms for metadata collection, and mandatory judicial authorization for intrusive digital surveillance.[22] Further, a dedicated Digital Criminal Procedure Code Manual should be enacted, prescribing uniform protocols for search-and-seizure of digital devices, admissibility standards for electronic records, and chain-of-custody safeguards, consistent with constitutional privacy standards and judicial pronouncements. Specialized rules should also be framed for cross-border data requests in cyber-enabled offences, ensuring cooperation without violating due process or privacy guarantees.

Building Institutional Capacity

Institutional readiness is the cornerstone of successful technological transition. The government must significantly expand district-level and regional cyber-forensic laboratories, supported by certified digital-evidence examiners, and invest in secure cloud-based servers with redundancy and fail-safe encryption systems. Block chain based record authentication

[20] *State of Punjab v. Baldev Singh*, (1999) 6 SCC 172, (importance of procedural safeguards in evidence handling).
[21] Internet and Mobile Association of India. (2023). *Digital Literacy in India Report* . https://www.iamai.in/
[22] Digital Personal Data Protection Act, No. 22 of 2023 (India). Ministry of Electronics & IT. https://www.meity.gov.in

may be deployed to create tamper-proof audit trails for digital case files.[23] Regular training programs not only for police, but also prosecutors, judicial officers, and legal aid counsels should emphasize eevidence protocols, cyber-law literacy, ethical artificial-intelligence use, and witness-protection technology. Simultaneously, community-centered digital-rights awareness programs must be organized to empower citizens, particularly in underserved areas, to use e-FIR systems, online court services, and grievance-redress platforms.

Ethics, Oversight, and Citizen Empowerment

As digital policing expands, independent oversight bodies must be institutionalized, combining judicial members, data-protection experts, technologists, and civil-society representatives.[24] Transparent annual audits of surveillance technologies, body cam data, and facial-recognition inputs should be mandated to prevent misuse. AI-based criminological tools should follow ethical frameworks preventing discriminatory profiling, in line with international human-rights standards. Public-facing digital-rights campaigns and legal-aid facilitation must ensure citizens especially economically and socially marginalized groups are aware of their constitutional protections, data rights, and avenues for complaint and redress. A state-supported digital public defender system could be developed to support accused persons in technology-driven investigations, ensuring equality of arms in criminal justice.[25]

Conclusion

The Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023 marks a decisive turning point in India's criminal justice evolution, reflecting a deliberate transition from analogue policing practices to a digitally enabled investigative framework. The reforms introduced — from e-FIR mechanisms and audio-visual recording to forensic-led investigation — hold the promise of enhancing state capacity, promoting procedural transparency, accelerating evidence-collection, and expanding access to justice for vulnerable communities.[26]

Yet, technology is not a substitute for due process. Digital systems, if deployed without stringent oversight, risk normalizing surveillance, facilitating executive excess, and deepening

[23] NITI Aayog. (2021). *Blockchain: The India Strategy* (Part 1, pp. 22-25). Government of India.
[24] *People's Union for Civil Liberties (PUCL) v. Union of India*, (1997) 1 SCC 301,(oversight in surveillance).
[25] Singh, S. & Narayan, V. (2024). Digital transformation and equal access in criminal trials. *Indian Journal of Criminology*, 52(1), 89-95.
[26] Ministry of Home Affairs. (2023). *Press Note on Criminal Law Reforms and Technological Integration* (pp. 4-7). Government of India. https://www.mha.gov.in

structural inequalities in access to justice.[27] Without robust statutory privacy protections, reliable digital infrastructure, trained personnel, and institutional culture grounded in constitutionalism, technological innovation may inadvertently compromise the dignity, liberty, and autonomy of citizens rather than securing them.

The future of BNSS implementation will depend on judicial vigilance, sustained investment in capacity-building, accountable use of data, and ethical standards in cyber-forensics and AIenabled policing. Ultimately, India now stands at a constitutional inflection point: one where the

State's pursuit of modernity must remain firmly tethered to the values of fairness, proportionality, and human dignity. With principled governance and continuous oversight, the BNSS can emerge not merely as a reform statute, but as a model for rights-oriented digital criminal justice in the Global South — a system where innovation strengthens liberty rather than eclipsing it.

[27] Bhatia, G. (2023). *State surveillance and proportionality in digital policing*. *NUJS Law Review*, 16(2), 122-128.