INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

 ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur.Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time &Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

 ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

 ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

"THE ROLE OF TECHNOLOGY IN CRIMINAL INVESTIGATIONS UNDER BNSS, 2023: ENHANCING INVESTIGATIONS OR ENDANGERING RIGHTS?

AUTHORED BY - STUTI SARAWAGI

INTRODUCTION: NEED FOR REFORM

A man is arrested in 2021 for voicing dissent on social media, accused under laws originally framed to suppress Indian nationalists in 1870. In court, his lawyer argues for bail—but the judge is bound by a procedural framework older than India's Constitution. The irony? The smartphone he used is smarter than the laws used to prosecute him.

In 2019, the tragic *Dr. Priyanka Reddy* case in Hyderabad shook the nation. The young veterinarian was brutally assaulted and murdered, and her body was set ablaze. Public outrage reached a boiling point—not just because of the heinousness of the crime, but due to the systemic delays and procedural red tape that marked the initial phase of the investigation. Despite the presence of CCTV footage, GPS tracking, and digital communication trails, the investigation was sluggish, hampered by bureaucratic layers, lack of inter-agency coordination, and outdated procedural requirements under the Code of Criminal Procedure, 1973.[1]

What followed was even more controversial—the encounter killing of the accused by the police, raising serious concerns about extra-judicial responses being valorised due to a broken justice system. This event sparked a nationwide debate: *Was the system so archaic that people began endorsing instant justice over due process?*

This case was not an outlier. It underscored a deeper institutional inertia, a criminal procedural framework that had not kept pace with technological evolution or public expectations. At a time when cybercrime, AI-based surveillance, and digital forensics have become critical to investigations, the reliance on 50-year-old procedural codes, many inherited from colonial laws,

[1] Sangeetha Devi Dundoo, Rape, Rage, and an Exchange of Fire, *The Hindu* (Dec. 7, 2019), https://www.thehindu.com/news/national/telangana/rape-rage-and-an-exchange-of-fire/article61606028.ece.

 ISSN: 2582-6433

exposed glaring gaps.

It mirrors the clash between India's fast-evolving digital society and its archaic criminal justice machinery. The Indian Penal Code (1860), Code of Criminal Procedure (1973), and Indian Evidence Act (1872) were not built for encrypted data, AI-based surveillance, or online financial crime. They were tools of imperial control, not instruments of justice in a constitutional democracy.

India in 2025 is grappling with a staggering arrear of more than 52 million pending cases in various courts according to the National Judicial Data Grid.[2] The pending cases doubled in the last 20 years and at the disposal rate at which it is being done today, it would take more than 300 years to dispose of all the pending cases in India. Of these, over 180,000 have been pending for over three decades.[3] District and subordinate courts up to 2025 account for nearly 87% of the case backlog, which are around 4.5 crore against 5.1 crore with a rise of 0.63 per cent in more than a month.[4] The Indian legal system, which continues to cling to traditional British-era ways, is one of the leading causes of judicial delay. Lawyers spend hours debating orally and submitting lengthy written statements, although time and again the government has proposed reforming these practices—abolishing handwritten depositions and shortening witness examination. These findings bring out the need to transcend outdated systems and embrace advanced technology to improve judicial efficiency.

It requires a more holistic solution to involve technological integration towards better efficiency. The E-Courts mission has managed to bring about an integration of as many as 2,600 district courts onto a computerised system, raising the availability of case information as well as the disposal rates by 30%.[5] Similarly, adjudication through the internet in terms of video conferencing accelerated disposal of cases by 50% in 2022 and were a boon in the COVID-19 pandemic.[6] The

[2] National Judicial Data Grid, https://njdg.ecourts.gov.in/njdg_v3/ (last visited April 10, 2025).
[3] The Grueling Course of Litigation in India, CIVILSDAILY (2024), https://www.civilsdaily.com/news/the-grueling-course-of-litigation-in-india/#:~:text=Total%20Pending%20Cases:%20As%20of%202024%2C%20there,court%20levels%2C%20including%20district%20and%20Supreme%20Court.&text=Backlog%20of%20Cases:%20The%20increasing%20backlog%20due,judicial%20system%2C%20perpetuating%20a%20cycle%20of%20inefficiency.
[4] India's Legal Bottleneck: Rising Backlogs and Missing Fast Track Courts, HINDU BUS. LINE (Mar. 17, 2025), https://www.thehindubusinessline.com/data-stories/data-focus/indias-legal-bottleneck-rising-backlogs-and-missing-fast-track-courts/article69324793.ece.
[5] Press Information Bureau, Govt. of India, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2085127 (last visited Mar. 17, 2025).
[6] Press Information Bureau, Govt. of India, https://pib.gov.in/Pressreleaseshare.aspx?PRID=1807613 (last visited Mar. 17, 2025).

 ISSN: 2582-6433

use of e-filing has streamlined case-filing, reducing 30% of paperwork and 50% of processing time.[7] Electronic payment systems have reduced 70% of transaction time, while Fast Track Courts have disposed of 1.5 lakh cases at a faster rate, reducing pendency of priority cases by 20%.[8]

Advanced technology has transformed the criminal justice field, bringing both new possibilities and challenges to the table. While modern offenders can use technology to commit sophisticated crimes and evade detection, law enforcement officials can also benefit from advanced tech as they uncover criminal activity and deliver justice.

The Bharatiya Nagarik Suraksha Sanhita, 2023, (BNSS) introduced as part of a trilogy of new laws, promises to fulfill that. It aims to decolonize, modernize, and digitize India's criminal law.[9] This paper explores whether the BNSS achieves that goal, particularly in the realm of criminal investigations, and whether the embrace of technology enhances due process or opens the door to new forms of state overreach.

TECHNOLOGICAL INTEGRATION IN BNSS: EMBRACING A NEW ERA IN CRIMINAL INVESTIGATION

The Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) was introduced in Lok Sabha on August 11, 2023, to replace the Code of Criminal Procedure, 1973 (CrPC). The Bill was examined by the Standing Committee on Home Affairs and after incorporating some recommendations of the Committee, the Bharatiya Nagarik Suraksha (Second) Sanhita, 2023 (BNSS2) was introduced on December 12, 2023.[10] The Act was published in the Official Gazette after receiving presidential approval and was enacted on July 1, 2024.[11]

[7] Rahul Tyagi, Backlog of Cases Making Imbalance to Scale of Justice, 2(7) Int'l J. Legal Res. & Analysis 13 (Oct. 2024), https://www.ijlra.com/paper-details.php?isuur=3462 (last visited Mar. 17, 2025).
[8] Ibid.
[9] Apurva Kadao, Digital Transformation in the Light of New Criminal Laws, *A.K. Legal & Associates* (July 27, 2024), https://aklegal.in/digital-transformation-in-the-light-of-new-criminal-laws/.
[10] PRS Legislative Research, The Bharatiya Nagarik Suraksha (Second) Sanhita, 2023, https://prsindia.org/billtrack/the-bharatiya-nagarik-suraksha-second-sanhita-2023 (last visited Apr. 18, 2025).
[11] Radha Ranjan & Manvendra Kumar Tripathi, The Role of Technology in Enhancing the Efficiency of the Bhartiya Nagarik Suraksha Sanhita 2023, in *Crime and Consequences: A Comprehensive Guide to Criminal Laws in India* 179, 179–189 (Nidhi Dahiya & Mahima Sharma eds., Singhal Law Publications 2024), https://www.researchgate.net/publication/387503611_THE_ROLE_OF_TECHNOLOGY_IN_ENHANCING_THE_EFFICIENCY_OF_THE_BHARTIYA_NAGARIK_SURAKSHA_SANHITA_2023.

 ISSN: 2582-6433

The Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, marks a significant shift from the colonial legacy of the Code of Criminal Procedure (CrPC), embracing a modern, citizen-centric, and technologically integrated approach to criminal justice. One of its most transformative features is the systematic integration of technology at every stage of the criminal process—from investigation and summons to evidence collection and trial. These changes are not merely cosmetic but signify a shift in how justice is envisioned, accessed, and delivered in a digital age.

I. FILING OF INFORMATION AND REGISTRATION OF FIR

The BNSS starts by acknowledging the role of technology in redefining procedural concepts. New definitions such as "audio-video electronic means" and "electronic communication" have been added to the preliminary definitions, under Section 2 of BNSS,[12] laying the groundwork for how justice will be administered in a technology-inclusive environment. These definitions are not limited to abstract terminology—they underpin how summonses, notices, evidence, and even FIRs can be electronically managed.

One of the most citizen-friendly provisions of the BNSS is the acceptance of information about an offence through electronic communication—commonly referred to as e-FIR. This inclusion allows individuals to report crimes electronically, with the requirement that their signature be obtained within three days before the report is formally taken on record.[13] This innovation is coupled with a formal statutory recognition of the concept of Zero FIR, mandating police officers to register a case even when the offence occurred outside their jurisdiction, thereby preventing delays in lodging complaints.[14]

II. INVESTIGATION AND EVIDENCE COLLECTION

Accountability in search and seizure operations has historically been a grey area in criminal investigations. To remedy this, the BNSS mandates the video recording of the entire process of search and seizure, including the preparation of the list of seized items and obtaining witnesses'

[12] Bhartiya Nagarik Sanhita, No. 46 of 2023, § 2(1)(a), 2(1)(i) (India).
[13] Bhartiya Nagarik Sanhita, No. 46 of 2023, § 173 (India).
[14] Ibid.

 ISSN: 2582-6433

signatures.[15] This provision allows for the use of mobile phones for such recordings, bringing much-needed transparency and curbing potential abuse during raids and searches.

The legislation brings significant improvements to the transmission of case materials between the police and judiciary. Police reports can now be forwarded to magistrates electronically,[16] ensuring timely communication and reduced physical dependency. This provision is particularly important when the report involves digital or electronic evidence, requiring the inclusion of a detailed chain of custody to maintain evidentiary integrity.

The BNSS also introduces a victim-centric approach by mandating that police inform victims or informants of the investigation's progress within 90 days, which may also be done through electronic communication.[17] This ensures that victims are not left in the dark and reinforces the participatory nature of the justice process.

III. SUMMONS, WARRANTS, AND PRE-TRIAL PROCEDURES

In a major departure from traditional practices, the issuance and service of summonses can now be done electronically. The BNSS enables courts to authenticate summons via digital signatures or photographs,[18] and the service of such summonses can also be done through electronic means like email or messaging platforms.[19] This is supported by the requirement to maintain a register of contact information such as phone numbers and email addresses of parties being summoned, ensuring not just efficiency but accountability in service.[20]

In line with ensuring fairness and avoiding procedural delays, the BNSS includes specific provisions to facilitate timely delivery of case documents to the accused. The investigating officer must now submit indexed copies of the police report and related documents to the magistrate, who is then responsible for sharing the same with the accused within 14 days of appearance or

[15] Bhartiya Nagarik Sanhita, No. 46 of 2023, § 105 (India).
[16] Bhartiya Nagarik Sanhita, No. 46 of 2023, § 193(3)(i) (India).
[17] Bhartiya Nagarik Sanhita, No. 46 of 2023, § 193(3)(ii) (India).
[18] Bhartiya Nagarik Sanhita, No. 46 of 2023, § 63 (India).
[19] Bhartiya Nagarik Sanhita, No. 46 of 2023, § 70 (India).
[20] Bhartiya Nagarik Sanhita, No. 46 of 2023, § 64 (India).

 ISSN: 2582-6433

production.[21] Importantly, these documents can be provided electronically under Section 230[22] of BNSS thereby reducing the logistical burden on both courts and the accused.

Similarly, in sessions triable proceedings initiated via complaints, the statements and documents can be shared in electronic form, further emphasizing technological efficiency.[23]

IV. JURISDICTION, COGNIZANCE AND ELECTRONIC EVIDENCE

Recognizing the borderless nature of modern digital crimes, the BNSS expands the jurisdiction of courts in cases involving offences committed via electronic communication. For example, offences involving false communication or cyber fraud can now be tried in the court where such communication was either sent or received.[24] Likewise, for crimes committed outside India, the local jurisdiction where the complaint is lodged can assume authority, and evidence received from abroad can be submitted electronically.[25]

Furthermore, magistrates are now empowered to take cognizance of offences based on electronically transmitted police reports.[26] This provision also facilitates electronic handling of complaints and recognition of digital documentation. Provisions surrounding the transmission of such reports also accommodate the inclusion of electronic chains of custody for digital evidence, acknowledging the challenges of handling such evidence in cyber and digital crimes.

V. TRIAL AND EXAMINATION

Perhaps the most visible technological intervention is in the conduct of trials. The BNSS extensively permits the use of audio-video conferencing for recording evidence, examining witnesses, or even interacting with the accused. From framing of charges under Section 251,[27] to depositions during sessions trials under Section 254,[28] and from examination of witnesses in

[21] Bhartiya Nagarik Sanhita, No. 46 of 2023, § 193(8) (India).
[22] Bhartiya Nagarik Sanhita, No. 46 of 2023, § 230 (India).
[23] Bhartiya Nagarik Sanhita, No. 46 of 2023, § 231 (India).
[24] Bhartiya Nagarik Sanhita, No. 46 of 2023, § 202 (India).
[25] Bhartiya Nagarik Sanhita, No. 46 of 2023, § 208 (India).
[26] Bhartiya Nagarik Sanhita, No. 46 of 2023, § 210 (India).
[27] Bhartiya Nagarik Sanhita, No. 46 of 2023, § 251 (India).
[28] Bhartiya Nagarik Sanhita, No. 46 of 2023, § 254 (India).

 ISSN: 2582-6433

warrant cases under Section 265,[29] to examination of the accused under Section 308,[30] the BNSS seeks to embed virtual interaction as a legitimate mode of procedural conduct.

This transformation is also spatially supported, as State Governments are empowered to designate specific locations where such audio-video electronic means can be conducted.[31] Additionally, Section 316 establishes that the signature of the accused must be taken within 72 hours of their virtual examination to preserve procedural safeguards.[32] Furthermore, when documents or reports prepared by public servants, experts, or officers are introduced in court, their successors may depose on their behalf if needed, and this process too can be carried out through audio-visual means.[33] Such provisions are indicative of a robust system that values both procedural economy and technological compatibility.

VI. JUDGMENT AND FINAL PROCEEDINGS

Even at the final stages of the trial, technology finds its place. If the accused is in custody, they may be presented to hear the verdict through audio-video means,[34] minimizing logistical challenges while respecting procedural norms.

Perhaps the most revolutionary provision in terms of technological integration is Section 530, which allows for all aspects of trials, investigations, and procedures to be conducted electronically.[35] This provision is the legal embodiment of a digital justice ecosystem, enabling full-fledged paperless operations and virtual proceedings that are not only cost-effective but also inclusive, particularly in remote or underserved areas.

This technological overhaul under the BNSS underscores India's readiness to transition towards a more responsive and efficient criminal justice system. Far from being a cosmetic digitization effort, these provisions reflect a substantive commitment to procedural fairness, accountability, and accessibility, hallmarks of a truly modern legal system. Yet, as with any technological

[29] Bhartiya Nagarik Sanhita, No. 46 of 2023, § 265 (India).
[30] Bhartiya Nagarik Sanhita, No. 46 of 2023, § 308 (India).
[31] Bhartiya Nagarik Sanhita, No. 46 of 2023, § 265, § 266 (India).
[32] Bhartiya Nagarik Sanhita, No. 46 of 2023, § 316 (India).
[33] Bhartiya Nagarik Sanhita, No. 46 of 2023, § 336 (India).
[34] Bhartiya Nagarik Sanhita, No. 46 of 2023, § 392 (India).
[35] Bhartiya Nagarik Sanhita, No. 46 of 2023, § 530 (India).

 ISSN: 2582-6433

intervention, the real test lies in implementation, data protection, and ensuring that digital justice does not compromise due process.

ENHANCING INVESTIGATIONS OR ENDANGERING RIGHTS?

While the integration of advanced technology tools enable monitoring agencies to solve cases better along with improved operational efficiency, the implementation of new technology systems creates multiple problems about personal privacy and civil rights protection in addition to data abuse risks.

Security technologies including surveillance along with DNA forensics, fingerprint analysis, digital evidence, and artificial intelligence bolster Indian criminal investigations but they compromise core constitutional rights of citizens in the country.

In today's India, surveillance no longer needs trench coats or tailing cars. All it needs is code. Spyware like Pegasus infiltrates a phone silently, enabling state agencies to read messages, listen to calls, and even activate cameras, without a trace or a warrant.[36] Investigative powers, once constrained by procedure and privacy safeguards, now operate in a grey zone. The promise of "digital policing" is seductive, but when used without oversight, it risks transforming a democracy into a database—and citizens into case files. Although it is irrefutable that surveillance technologies, including CCTV, facial recognition systems, drone surveillance, and body-worn cameras, integrated into Indian policing have strengthened criminal investigations, the dangers of technological integration on rights of individuals is undeniable.[37]

As already discussed the BNSS authorizes police to deploy electronic and digital technology during investigations thus improving evidence collection and case management. CCTV networks with high-definition quality enable law enforcement to track criminal activities and restore crime

[36] Office of the High Commissioner for Human Rights, Spyware and Surveillance: Threats to Privacy and Human Rights Growing, UN Report Warns, U.N. Press Release (Sept. 16, 2022), https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report.
[37] Caroline Wilson Palow & Jonah Mendelsohn, The Rise of Surveillance During Protests: A Threat to Fair Trial Rights, *Bar Council of the UK* (Apr. 3, 2025), https://www.barcouncil.org.uk/resource/the-rise-of-surveillance-during-protests-a-threat-to-fair-trial-rights.html.

 ISSN: 2582-6433

locations.[38] The law enforcement utilizes drone capabilities to monitor protests as well as riots and search remote territory thus providing real-time information.[39] The facial recognition system named National Automated Facial Recognition System (AFRS) helps law enforcement agencies track missing persons while assisting with unidentified dead body identifications.[40]

However, AFRS operations in public locations without legal authorisation or court mandate doubts the constitutional protection found in Article 21 of the Constitution.

A young woman, marching peacefully for climate justice, is arrested based on a so-called "toolkit" found in her online drive. What no one says aloud is how the document was accessed, or how her phone data—chats, photos, notes—ended up in police hands without her consent. In a country that guarantees the right to dissent, spyware like Pegasus and sweeping digital surveillance are redefining what it means to protest. The street may be free, but the cloud isn't. The investigation becomes a cloak under which liberty is quietly suffocated.[41] When phones are turned into 24/7 surveillance devices, questions of freedom, privacy, and democratic dissent arise.

Secondly, the criminal justice system heavily depends on DNA technology for investigations that involve sexual assaults and homicides. The law permits authorized forensic examination of bodily substances according to section 349 within the framework of BNSS.[42] The establishment of National DNA Data Bank along with regional databanks enables authorities to compare crime evidence against records of known criminals.[43]

[38] Jason Penny, CCTV Meaning: A Complete Guide, *Stealth Monitoring* (Feb. 3, 2025), https://stealthmonitoring.com/crime-prevention/cctv-meaning-a-complete-guide.
[39] Garrett Connolly, How Drones for Police are Enhancing Law Enforcement Operations, *Elistair* (Mar. 13, 2024), https://elistair.com/resources/police-drones/drones-for-police/.
[40] Automated Facial Recognition System to Help Identify Criminals, Missing Children, *The Times of India* (July 11, 2019), https://timesofindia.indiatimes.com/business/india-business/automated-facial-recognition-system-to-help-identify-criminals-missing-children/articleshow/70177696.cms.
[41] Disha Ravi: Toolkit Case: With Probe Making No Headway, Closure Report May Be an Option, *The Indian Express* (Oct. 27, 2021), https://indianexpress.com/article/cities/delhi/disha-ravi-toolkit-case-with-probe-making-no-headway-closure-report-may-be-an-option-7590653/.
[42] Bhartiya Nagarik Sanhita, No. 46 of 2023, § 348 (India).
[43] Panneerchelvam S & Norazmi MN, Forensic DNA Profiling and Database, *Malays. J. Med. Sci.* 10, no. 2 (2003): 20-26, PMID: 23386793, PMCID: PMC3561883.

 ISSN: 2582-6433

The 2012 Nirbhaya gang rape investigation became stronger thanks to DNA evidence which established a connection between the defendants and the crime where they attacked the victim.[44]

The implementation of DNA databanks leads to multiple ethical conflicts that affect their legal framework. Numerous experts have challenged the DNA Technology (Use and Application) Regulation Bill because its consent regulations appear unclear and the bill does not provide sufficient protections.[45] The right to bodily autonomy might be violated because critics dispute the collection of genetic material from individuals who are only accused rather than convicted.[46]

A corroborating instance of such a tool is the 2020 Gujarat case, which demonstrated false accusation of a young person because of an untrustworthy DNA kit that altered evidence.[47] This incident highlighted problems with laboratory errors and unauthorized sample storage.

Thirdly, the BNSS provides official recognition to digital and electronic evidence collection practices and enables courts to use electronic records as primary evidence as earlier discussed. Law enforcement agencies can now utilize WhatsApp messages, GPS tracking, email data and CCTV video recordings to investigate cybercrime, drug trafficking and terrorism cases.

The Delhi Police has been reported to utilize digital evidence from sources like Google and Facebook in investigations, including those related to communal violence. This includes using geolocation data from Google Maps and analyzing communication records on platforms like WhatsApp and Telegram.[48] The police have also been observed to request information from platforms like Facebook and Meta, and the Delhi High Court has directed these platforms to provide details about their Standard Operating Procedures when law enforcement agencies make

[44] Aditya Nuna & Tejas Gupta, The Role of Forensic Evidence, DNA Tests, and Narco-Analysis in the Indian Legal System, SSRN (Dec. 23, 2024), https://ssrn.com/abstract=5069346.
[45] What is the DNA Bill?, *The Indian Express* (Dec. 21, 2022), https://indianexpress.com/article/explained/what-is-the-dna-bill-8857810/.
[46] Supra note 42.
[47] DNA mismatch, age proof issue: Gujarat HC suspends rape convict's 20-yr sentence, *The Times of India* (Apr. 10, 2025), https://timesofindia.indiatimes.com/city/ahmedabad/dna-mismatch-age-proof-issue-gujarat-hc-suspends-rape-convicts-20-yr-sentence/articleshow/120137559.cms.
[48] Delhi Rioters Had Checked Ownership of Vehicles on e-Vahan Portal Before Setting Them on Fire, *OpIndia* (Sept. 2020), https://www.opindia.com/2020/09/delhi-rioters-had-checked-ownership-vehicles-e-vahan-portal-before-setting-them-on-fire/.

 ISSN: 2582-6433

requests.[49] E-discovery tools streamline investigations by organizing and extracting extensive datasets.

Interestingly, the other side of the coin wherein, police reportedly confiscated protestors' mobile phones during the 2020 Delhi riots to examine private messages without giving any prior notification or obtaining consent bring to light major worries about how digital tools are employed in criminal probes without established legal protections or supervisory judicial mechanisms.[50] Indian authorities are able to acquire sensitive personal data without significant oversight due to the lack of a comprehensive data protection law. These methods endanger privacy rights protected by Article 21 while simultaneously jeopardizing the foundational principles of due process and judicial transparency.

Lastly, it is without doubt that the use of AI in investigations increases efficiency. Indian police departments implement Artificial Intelligence (AI) technology alongside automation systems to process video footage while creating reports and predicting crime patterns. BNSS expands the use of technological tools to complement modern investigative practices. Artificial Intelligence enables financial fraud detection as well as cybercriminal tracking while providing crowd management support during large gatherings such as elections and festivals. The automation of FIR registration and case documentation processes has successfully enhanced both transparency and access.

However, in this age of AI-generated police reports and silent surveillance, the right to privacy has become more than a legal entitlement, it is a battlefield. When law enforcement agencies adopt technologies like artificial intelligence to auto-draft narratives of criminal events, what's at stake is not just efficiency but accountability, transparency, and truth. AI tools are trained on biased data, this risk turning assumptions into evidence, and subjective experiences into machine-written

[49] Delhi High Court Demands SOP Details from Meta (Facebook) and Google on Sharing Information with Police for Investigations, *The420.in* (Oct. 2, 2024), https://www.the420.in/delhi-high-court-demands-sop-details-from-meta-facebook-and-google-on-sharing-information/.
[50] Delhi Rioters Had Checked Ownership of Vehicles on e-Vahan Portal Before Setting Them on Fire, *OpIndia* (Sept. 2020), https://www.opindia.com/2020/09/delhi-rioters-had-checked-ownership-vehicles-e-vahan-portal-before-setting-them-on-fire/.

 ISSN: 2582-6433

scripts that defendants may never get to question. It is warned that such tools can erase the human element from justice and mask errors behind technical jargon.[51]

COMPARATIVE ANALYSIS: TECHNOLOGICAL INTEGRATION IN OTHER JURISDICTIONS

Incorporation of technology into criminal investigations has become a global trend, with several jurisdictions adopting legislative frameworks to facilitate digital evidence gathering while attempting to maintain checks on abuse. The UK's Investigatory Powers Act 2016, also known as the "Snooper's Charter," permits such activities as the interception of bulk communications and data retention.[52] The Act provides that, if there is a necessity for surveillance, a law enforcement officer can get a warrant from a private judge, only then can it be carried out, it is also subject to supervision by independent judges and is based on strict necessity and proportionality.[53] Through the DNA Identification Act 1998, Canada shows an example of the establishment of the National DNA Data Bank for the collection by the state, and the networking of the same prison's genetic register, the aim of the bank then being the matching of profiles between those retained by different agencies. Access to the bank is exclusively granted to the law enforcement agency, namely the Royal Canadian Mounted Police (RCMP), based on the judicial regulations, and it is limited to criminal identification only.[54]

In the US, the Communications Assistance for Law Enforcement Act (CALEA) obliges carriers of communication services to adjust the architecture of their systems in such a way as to accommodate legal surveillance needs.[55] A good example of the efficiencies brought by CALEA is the permission given to service providers to be able to wiretap communications electronically. Nevertheless, the requirement for a court order to be issued before surveillance can be carried out

[51] Jay Stanley, AI-Generated Police Reports Raise Concerns Around Transparency, Bias, *ACLU* (Dec. 10, 2024), https://www.aclu.org/news/privacy-technology/ai-generated-police-reports-raise-concerns-around-transparency-bias.
[52] Alan Travis, *Snooper's Charter* Bill Becomes Law, Extending UK State Surveillance, *The Guardian* (Nov. 29, 2016), https://www.theguardian.com/world/2016/nov/29/snoopers-charter-bill-becomes-law-extending-uk-state-surveillance.
[53] Investigatory Powers Act 2016, c. 25 (U.K.), https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted.
[54] National DNA Data Bank, Royal Canadian Mounted Police, https://www.rcmp-grc.gc.ca/en/forensics/national-dna-data-bank.
[55] Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994).

 ISSN: 2582-6433

is also a clear stipulation from CALEA, thus ensuring full respect for the principles of the judicial processes.

In addition, the US has the Electronic Communications Privacy Act (ECPA) to govern the law enforcement access to stored electronic communications. This act embeds search consent and warrant requirements thereby regulating government access to stored electronic communications. The examples below are indicative of the situation when technological capabilities used by the police should be accompanied by legal protections, in order to preserve the balance between the two opposing sets of rights.[56]

Among others, this clearly shows that it is not just the technology that should be used by law enforcement, but must also be accompanied by legal safeguards, not limited to merely securing warrants, but also the presence of independent oversight bodies, and strict data use limitations serve here as evidence of the fact that the law uses only the necessary rights to gather information, etc. which is legally agreed with the governed people and for the sake of the security of the state.

CHALLENGES TO IMPLEMENTATION AND RECOMMENDATIONS

Notwithstanding such attempts, technological integration remains to confront myriads of weaknesses and constraints in India in light of the nation's context. Although these weaknesses target the prime deficits of technological provisions, they are not insurmountable.

DIGITAL DIVIDE

In India, merely 38% of homes are digitally literate.[57] Can a tech-driven legislation succeed in a Country with One of the Lowest Digital Literacy Rates? This is the biggest challenge to not only the idea of E-Courts, and E-Filing, but the entire premise behind technological provisions as a solution for reform. Although the Indian judiciary has made strides in e-filing and remote hearings, several courts still rely on traditional methods. In a 2023 survey, nearly 60% of judges and lawyers

[56] Stephen D. Gantz & Daniel R. Philpott, Privacy, in *FISMA and the Risk Management Framework* 445, 445–480 (Stephen D. Gantz & Daniel R. Philpott eds., Syngress 2013), https://doi.org/10.1016/B978-1-59-749641-4.00016-3.
[57] Centre for Behavioural and Welfare Economics, Digital Literacy, https://dtnbwed.cbwe.gov.in/images/upload/Digital-Literacy_3ZNK.pdf (last visited April 15, 2025).

 ISSN: 2582-6433

reported feeling insufficiently prepared to utilize digital tools effectively. Digital literacy initiatives and robust digital infrastructure are necessary at the grass-root level. This article underscores the importance of huge investments in technology to render digital platforms available to all strata of society, particularly in rural and disadvantaged areas. This not only implies augmenting internet connectivity but also having education programs that equip individuals with the ability to use digital platforms efficiently.

Where the Supreme Court validated citizens' right to increased accessibility in legal services, the leading case of *Swapnil Tripathi v. Supreme Court of India (2018),*[58] supports this article's suggestion of making citizens digitally empowered in order to provide increased accessibility in legal services.

INFRASTRUCTURE GAPS

While Sections 2(1)(a) and (f), 173, 176(3), and 532 of the BNSS, 2023 lay the groundwork for digitalizing nearly the entire criminal trial process, the implementation poses serious infrastructural challenges. Benefits such as reduced travel time, decreased need for police escort, streamlined access to documents, and decongestion of courtrooms are apparent. However, scaling this system across a nation with such a vast caseload and digital divide is a formidable task. Building and maintaining consistent digital infrastructure in rural and underserved areas, coupled with grassroots-level awareness and accessibility, are crucial. Even in technologically advanced jurisdictions like the United Kingdom, the transition has not been seamless. A March 2024 House of Lords report highlighted issues of technical inconsistency and insufficient transparency, calling the landscape a “new Wild West,” where technological development has outpaced public awareness, governance, and legislation.[59]

OVERSIGHT MECHANISM AND RISKS OF AI MISUSE

A critical concern with digital criminal trials is the misuse of advanced technologies, particularly

[58] Swapnil Tripathi v. Supreme Court of India, 2018 (10) SCC 639.
[59] House of Lords Justice and Home Affairs Committee, *Technology Rules? The Advent of New Technologies in the Justice System*, HL Paper 180 (Mar. 30, 2022), https://publications.parliament.uk/pa/ld5802/ldselect/ldjusthom/180/180.pdf.

 ISSN: 2582-6433

artificial intelligence and deepfakes. Section 532 of the BNSS allows for virtual witness examinations and trials, which, while efficient, also open the door to potential manipulation. Deepfake technology now makes it nearly impossible to differentiate real individuals from AI-generated replicas. For example, a recent fraud case in the UK involved a finance worker transferring £20 million after being deceived by a deepfake video call, where multiple participants were AI-generated.[60] The same risk, if applied to witness testimonies or accused appearances, could severely undermine the integrity of criminal trials. Despite this, BNSS lacks specific safeguards to authenticate digital appearances or testimony. The legislation must incorporate strict verification protocols and AI-detection mechanisms to prevent misuse.

To mitigate such risks, the establishment of independent supervisory bodies is essential. These oversight institutions should conduct regular audits, investigate technological abuses, and develop best practices to ensure accountability in digital investigations. Without structured checks, the threat of abuse could jeopardize the very essence of due process.

DATA SECURITY AND PRIVACY CONCERNS

The increasing digitization of criminal investigations also raises serious concerns regarding data privacy and security. The volume of sensitive information collected during investigations necessitates robust safeguards against unauthorized access, misuse, or breaches. A balanced framework must be maintained, one that facilitates effective policing without compromising fundamental privacy rights. Clear policies on data collection, retention, and sharing must be drafted and enforced, with particular focus on consent, oversight, and redress mechanisms in case of violations. Without proper legislative safeguards, the risk of systemic overreach remains significant.

POLICE AND JUDICIAL TRAINING

Successful adoption of technological tools in criminal proceedings hinges on the competency of the personnel operating them. Law enforcement officers, judicial staff, and investigators must be

[60] Deepfake CFO Scam Costs Hong Kong Firm $25 Million, *CNN* (Feb. 4, 2024), https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html.

 ISSN: 2582-6433

adequately trained to use digital tools, manage evidence, and uphold digital rights. Specialized training programs in computer forensics, cybersecurity, data governance, and evidence authentication should be institutionalized. Periodic workshops, simulation-based training, and cross-departmental seminars can help bridge the digital literacy gap. Without investing in human capital, even the most sophisticated systems may falter.

CONCLUSION

The Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, is a landmark in the criminal justice system of India, a milestone shift from the colonial procedural codes to a modern technology-driven system. With digital means integrated into it, from e-FIRs and electronic summons to virtual courts and AI-assisted investigations, the BNSS aims to enhance investigation efficacy, reduce delays, and deliver justice at a shorter distance.

But as this essay has illustrated, technological incorporation is a double-bladed sword. It consolidates law enforcement capacities but equally threatens to erase critical concerns of privacy, due process, and overreach on the part of the state. The BNSS's provisions regarding digital evidence, surveillance, and AI policing represent a necessary shift in criminal procedure, especially in an age where cybercrime and digital forensics control investigations. But without robust protections, these technologies risk undermining constitutional rights. The absence of a standalone data protection law, lax oversight mechanisms, and the risk of misuse of AI and facial recognition technologies put at risk the very cornerstones of justice the BNSS was established to safeguard. Comparative analysis with other countries like the UK, Canada, and the US reveals that successful technological integration requires strict judicial control, warrant-based monitoring, and clear-cut limitations on data retention. India must introduce corresponding safeguards, having independent control mechanisms, judicial authorization for monitoring, and transparency in dealing with digital evidence. Further, it is crucial to close the digital divide through infrastructure creation and literacy programs to avoid excluding marginalized communities from the justice system.

 ISSN: 2582-6433

The BNSS is certainly a forward-looking initiative to bring India's criminal justice system into the modern era, but its success depends on balancing efficiency with the protection of rights. While India goes through this revolution, it must ensure that technological advancement does not come at the cost of civil liberties. The future of criminal justice does not merely rest with wiser machines, but with a system that guards fairness, accountability, and the rule of law as well. Only then can the BNSS truly live up to its potential, of a justice system that is not only efficient, but fair as well.