iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** VII **Month of publication:** July 2026

DOI: https://doi.org/10.22214/ijraset.2026.84102

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue VII July 2026- Available at www.ijraset.com

Digital Criminal Justice: Evaluating the Digital Reforms Introduced under the Bharatiya Nyaya Sanhita and Bharatiya Nagarik Suraksha Sanhita

Mr. Virendra Kumar[1], Ms. Sakshi[2], Deepannita Medhi[3]
[1]*Assistant Professor, Royal College of Law, Ghaziabad*
[2]*B.A.LL.B., School of Law, Jigyasa University, Dehradun*
[3]*LL.M., National Law University and Judicial Academy, Assam*

Abstract: ***India's 2023 criminal law overhaul through the Bharatiya Nyaya Sanhita (BNS) and Bharatiya Nagarik Suraksha Sanhita (BNSS) marks a decisive statutory turn towards a technology-enabled criminal process, expressly integrating electronic communication, audio-video electronic means and digital records across investigation, trial and appeal. This paper examines the digital criminal-justice reforms embedded in these new codes, focusing on provisions relating to e-FIRs, electronic service of summons and warrants, audio-video recording of evidence, online proceedings under Section 530 BNSS, and the reconfiguration of offences to address cyber-enabled harms under BNS. It situates these reforms against earlier, largely ad hoc reliance on video-conferencing and electronic evidence, and against Supreme Court jurisprudence in Lalita Kumari, Anvar P.V., Shafhi Mohammad and Justice K.S. Puttaswamy on FIR registration, electronic evidence standards and privacy. Using a qualitative doctrinal methodology, the paper analyses statutory text, leading case law and emerging commentary to evaluate whether digitisation, as envisaged by BNS and BNSS, advances access to justice, efficiency and cyber-crime governance without compromising fair-trial guarantees and informational privacy. It argues that while the new codes significantly enhance the legal infrastructure for digital complaints, electronic process, virtual hearings and cyber-crime prosecution, they defer critical questions of authentication, data protection, standardisation and capacity-building to subordinate rules and institutional practice, risking uneven or rights-insensitive implementation. The paper concludes with normative recommendations: comprehensive procedural rules on electronic communication and evidence, robust privacy and data-protection safeguards tailored to criminal-justice data, measures to bridge the digital divide, sustained capacity-building for criminal-justice actors, and doctrinal clarification on electronic evidence and remote hearings under the new regime. These measures, it contends, are essential if India's move towards digital criminal justice is to remain consistent with constitutional commitments to equality, dignity and due process.***

Keywords: ***Digital criminal justice, Bharatiya Nyaya Sanhita (BNS), Bharatiya Nagarik Suraksha Sanhita (BNSS), e-FIR and electronic summons, Electronic evidence and video-conferencing, Cyber-crime and privacy rights.***

I. INTRODUCTION

India's criminal justice system has historically been characterised by delay, excessive formalism and limited access, problems which have been exacerbated in an era where crime increasingly involves digital elements and cross-border communication. Recognising both technological change and systemic inefficiencies, Parliament enacted three new criminal law codes in 2023 the Bharatiya Nyaya Sanhita, 2023 (BNS), the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) and the Bharatiya Sakshya Adhiniyam, 2023 to replace the Indian Penal Code, the Code of Criminal Procedure and the Indian Evidence Act respectively.[1][2][3][4][^5]

These enactments, which came into force in 2024–25, constitute the most far-reaching overhaul of Indian criminal law since colonial codification, with a pronounced emphasis on digitisation of processes, electronic communication and the formal recognition of audio-video technologies for trials and evidence. While the broader reforms engage substantive offences and procedural safeguards, this paper focuses specifically on the digital criminal-justice reforms introduced by the BNS and BNSS and evaluates their potential and limitations from the perspective of access to justice, due process and cyber-crime governance.[6][7][^8]

The central research question is: to what extent do the digital reforms in the BNS and BNSS meaningfully transform India's criminal process towards a technology-enabled, rights-respecting and efficient system, and what challenges remain for effective implementation?

©IJRASET: All Rights are Reserved

The paper argues that although the new codes significantly expand the legal infrastructure for electronic communication, e-FIRs, electronic service, audio-video recording and digital evidence, they leave critical questions of privacy, security, standardisation and capacity-building to subordinate legislation and institutional practice, creating a risk of uneven or rights-insensitive digitisation.[9][10][^8]

II. RESEARCH BACKGROUND

The push towards a "digital criminal justice system" in India predates the 2023 codes. Since at least the mid-2000s, courts and police have experimented with video-conferencing for remand and testimony, computerisation of records and online filing of complaints. The COVID-19 pandemic accelerated this trend, prompting the Supreme Court in Suo Motu Writ (Civil) No. 5 of 2020 to issue guidelines under Article 142 directing all courts to use video-conferencing to ensure continued access to justice while maintaining social distancing. Parallel initiatives such as the e-Courts Mission Mode Project and state-level electronic evidence and video-conferencing rules further normalised technology in judicial administration.[11][12][13][14]

However, pre-BNSS reliance on technology often rested on ad hoc judicial directions rather than clear statutory authority, raising concerns over legal validity, uniformity and safeguards. At the same time, the rise of cyber-crime and the ubiquity of digital communication exposed gaps in existing legal frameworks. The Information Technology Act, 2000 created specialised offences and procedural powers, but the Indian Penal Code and the Code of Criminal Procedure did not clearly integrate digital harms or digital modes of procedure. Questions of admissibility and reliability of electronic evidence led to significant Supreme Court jurisprudence in Anvar P.V. v. P.K. Basheer and Shafhi Mohammad v. State of Himachal Pradesh, which emphasised, but also complicated, the standards under Section 65B of the Evidence Act.[15][16][17][18][19][12][^14]

Commentary on the 2023 codes highlights that one of the primary legislative objectives was to incorporate technological advances into the criminal process by explicitly recognising electronic communication, audio-video electronic means and digital records across investigation, trial and appeal. The BNSS in particular is framed as modernising procedure through e-FIRs, electronic summons and warrants, digital evidence-gathering and online trials, while the BNS updates certain offence-definitions to respond to cyber-enabled harms such as cyber-stalking and dissemination of obscene material through electronic means.[20][16][10][6][^9]

This research situates the digital reforms within broader debates on criminal-justice reform in India, including concerns about over-criminalisation, police discretion and infrastructural deficits, and within global trends that emphasise technology as both an enabler and potential threat to fair trial rights and privacy. It engages doctrinal analysis of statutory text, case law and secondary literature to evaluate whether digitisation, as envisaged in the BNS and BNSS, advances or undermines constitutional guarantees under Articles 14, 19 and 21.[8][21][^22]

III. SCOPE AND LIMITATIONS OF THE STUDY

A. *Scope*

The paper is confined to evaluating the digital-procedure and digital-offence dimensions of the Bharatiya Nyaya Sanhita and Bharatiya Nagarik Suraksha Sanhita. It focuses on:

1) Provisions in BNSS that authorise or mandate electronic communication, e-FIRs, electronic service of process, audio-video recording of evidence and online trials, with particular attention to sections 173, 94, 231, 254, 265, 266 and 530.[10][6][^8]
2) Provisions in BNS that engage cyber-crime or digital modalities of offending, such as those relating to electronic publication of obscene material, voyeurism, cyber-stalking, identity-related offences and other offences committed through electronic means.[16][23][^20]
3) The interaction of these provisions with the Bharatiya Sakshya Adhiniyam (particularly electronic records), the Information Technology Act, 2000 and relevant Supreme Court case law on electronic evidence and video-conferencing.[17][19][^9]
4) Policy instruments and rules such as the Nyaya-Shruti application and model video-conferencing rules, insofar as they operationalise Section 530 BNSS and related provisions.[24][8]

B. *Limitations*

Several limitations shape the analysis:

1) Temporal limitation: Many provisions of the BNS and BNSS have been recently enforced, and empirical data on implementation, case-law under the new codes and field-level impact remains limited. The evaluation is therefore primarily doctrinal and normative, supplemented by early commentary rather than comprehensive empirical assessment.[25][6]

2) Institutional variation: Digitisation efforts vary widely across states, districts and courts in terms of infrastructure, training and local rules. The paper cannot capture all such variations and instead discusses structural challenges and opportunities.[12][11]
3) Evidence constraints: Detailed, official English versions of some subordinate rules (for example, state-level e-FIR SOPs and Nyaya-Shruti implementation circulars) are not uniformly available in public domain, limiting granular analysis of procedural safeguards.[26][24]
4) Substantive criminal-law focus: While BNS introduces numerous changes to substantive offences, this paper restricts itself to those with clear digital or cyber-crime dimensions and does not attempt a wholesale assessment of all offence-reforms.
5) Comparative perspective: The paper refers briefly to international trends but does not undertake a full comparative study with other jurisdictions' digital criminal-justice reforms due to space constraints.

IV. RESEARCH METHODOLOGY

The study adopts a qualitative doctrinal methodology, characteristic of public-law scholarship, supplemented by limited policy analysis.

1) Statutory analysis: The primary method is close reading of the BNS and BNSS texts as notified, with emphasis on provisions explicitly referencing electronic communication, audio-video electronic means and digital evidence. Authoritative versions from India Code and the Ministry of Home Affairs are treated as primary sources.[3][4][7][5][^1]
2) Case-law analysis: The paper analyses key Supreme Court precedents relevant to digital criminal justice, notably Lalita Kumari v. Government of Uttar Pradesh on FIR registration, Anvar P.V. v. P.K. Basheer on admissibility of electronic evidence, Shafhi Mohammad on flexibility in Section 65B compliance, Justice K.S. Puttaswamy v. Union of India on privacy, and the suo motu video-conferencing guidelines.[27][18][19][22][14][17]
3) Secondary literature: Academic articles, commentaries and practitioner notes on the new codes and on electronic communication under the BNSS and BNS are used to interpret legislative intent, highlight implementation challenges and identify doctrinal debates. These include work on electronic communication, cyber-crimes under BNS and legal challenges of digital evidence under the new laws.[28][23][6][9]
4) Policy and institutional documents: Government press releases and circulars relating to Nyaya-Shruti, model video-conferencing rules and e-FIR SOPs are examined to understand administrative frameworks supporting statutory digitisation.[26][8][^24]
5) Normative evaluation: The collected material is assessed against constitutional benchmarks of equality, fair trial, procedural reasonableness and privacy, drawing on fundamental rights jurisprudence. The paper is therefore not empirical but normative and analytical, aimed at highlighting doctrinal strengths and implementation risks.[29][22]

V. DIGITAL REFORMS UNDER THE BHARATIYA NAGARIK SURAKSHA SANHITA

A. *E-FIR and Electronic Complaints*

One of the most significant digital innovations introduced by BNSS is the possibility of filing complaints and first information reports electronically. Section 173 BNSS allows victims of cognisable offences to submit information electronically, obviating the need to physically attend a police station. Commentators note that this provision is intended to reduce logistical barriers and ensure prompt registration of complaints, particularly for vulnerable victims or those in remote locations.[30][31][^6]

The Supreme Court in Lalita Kumari made registration of FIR mandatory where information discloses a cognisable offence, and cautioned against using preliminary inquiry to defeat this mandate. BNSS modifies this landscape by providing structured scope for preliminary inquiry in certain categories of cases, while simultaneously offering e-FIR mechanisms that, in principle, facilitate timely complaint-lodging. From a digital-justice perspective, e-FIRs can advance accessibility and reduce opportunities for police refusal, but they also raise questions about authentication, digital literacy and the potential for misuse or frivolous complaints.[31][27]

Moreover, implementation depends on robust back-end systems and clear standard operating procedures. The Bureau of Police Research and Development has issued SOPs on Zero FIR and e-FIR in the context of the new laws, stressing standardised formats, verification mechanisms and integration with crime-record systems. These SOPs are crucial to ensuring that e-FIRs are more than formal authorisation that they translate into practical, secure and user-friendly complaint channels.[^26]

B. *Electronic Summons, Warrants and Digital Process Service*

BNSS introduces provisions enabling courts and police to issue and serve summons and warrants electronically. Section 94 BNSS explicitly empowers courts and the officer-in-charge of a police station to summon "any document or thing", including digital

evidence such as electronic communications (messages, call recordings, emails) and electronic devices like mobile phones, laptops and cameras. The section also allows search and seizure of such devices and data in specified circumstances, including where the person in possession is unlikely to produce them voluntarily.[2][6][^25]

Beyond Section 94, Section 530 BNSS provides a transformative umbrella provision whereby "all trials, inquiries and proceedings" under BNSS including issuance, service and execution of summons and warrants may be held in electronic mode by use of electronic communication or audio-video electronic means. This statutorily recognises electronic service and virtual process execution, which were previously conducted under judicial discretion or local rules.[32][10]

Commentary emphasises that electronic service can minimise delays in serving process, reduce excuses of non-receipt and improve tracking of compliance. At the same time, it implicates due-process concerns: courts must ensure accurate identification of recipients, reliable electronic addresses, notice of proceedings and mechanisms for confirmation of receipt. Constructive service doctrines, if applied uncritically in a digital context, could risk ex parte orders against persons who lack effective access to electronic communications.[6][10]

C. *Audio-Video Recording of Evidence and Virtual Proceedings*

BNSS builds on prior ad hoc use of video-conferencing by explicitly authorising audio-video electronic means for recording evidence and conducting hearings. Government press releases highlight that Sections 254 and 265 (evidence for prosecution) and 266 (evidence for defence) permit recording of evidence and examination of witnesses by audio-video electronic means, while Section 530 allows all trials, inquiries and appellate proceedings to be held in electronic mode.[10][8]

Section 530 is widely described as a paradigmatic shift in criminal procedure, providing statutory foundation for virtual court proceedings, digital record-keeping and remote participation by parties and witnesses. It is framed broadly to cover not only trials and appeals but also miscellaneous applications, interim orders, bail hearings and case-management conferences. The Nyaya-Shruti application has been developed as a technological platform to facilitate virtual appearance of accused persons, witnesses, police officials, prosecutors and experts via video-conferencing.[32][8][24][10]

Supreme Court guidelines on video-conferencing issued during COVID-19 confirm that such measures may be used at all stages of judicial proceedings and that courts must provide facilities for litigants lacking technology. BNSS codifies this approach, but practical implementation requires standards for audio-video quality, identity verification, record-keeping, and protocols for handling technical failures.[14][11][12][24]

D. *Electronic Access to Case Materials and Digital Records*

BNSS also incorporates electronic communication into the delivery of case materials. Section 231 allows statements, confessions and other documents to be furnished electronically to the accused in cases triable by the Court of Sessions, ensuring timely access to prosecution materials. Electronic provision of documents is intended to reduce physical delays, support digital case-files and enhance transparency.[8][6]

At the same time, electronic disclosure requires safeguards relating to confidentiality, data protection and the digital divide. Accused persons who lack devices or stable connectivity may be disadvantaged if electronic delivery is treated as equivalent to physical service. Proper implementation demands hybrid systems that preserve rights while leveraging digital efficiency.[22][10]

VI. DIGITAL REFORMS UNDER THE BHARATIYA NYAYA SANHITA

A. *Offences Involving Electronic Communication and Cyber-Crime*

The Bharatiya Nyaya Sanhita updates and reorganises offences to reflect digital realities, often complementing the Information Technology Act rather than replacing it. Secondary literature identifies several BNS provisions relevant to cyber-crime: offences relating to obscenity and pornography committed electronically, voyeurism through electronic capture or dissemination, cyber-stalking, data and device theft, and defamation or promotion of enmity via electronic communication.[23][20][15][16]

For instance, provisions addressing publication or transmission of obscene material explicitly cover electronic modes, imposing imprisonment and fines with enhanced penalties for recidivism. Voyeurism offences criminalise capturing or publishing images of a woman's private acts without consent, including where such capture or publication occurs through mobile phones or online platforms. Stalking provisions extend to monitoring or contacting a woman through electronic means, thereby recognising cyber-stalking and online harassment as offences.[20][15][16][23]

Similarly, theft provisions explicitly mention mobile phones, data and computer hardware or software, allowing prosecution of cyber-theft activities under general criminal law alongside specialised IT Act offences. In each area, BNS is framed as a general-law

framework that applies unless special laws like the IT Act, 2000 are triggered, reflecting the principle that special statutes prevail where applicable.[15][16][^17]

These reforms address concerns that traditional criminal law categories were ill-equipped to respond to digital harms like non-consensual intimate-image sharing, trolling and identity theft. By integrating electronic modes of offending into general offences, BNS facilitates mainstreaming of cyber-crime prosecution and reduces procedural complexity arising from overlapping statutes.[20][15]

B. Relationship with the IT Act and Bharatiya Sakshya Adhiniyam

Despite these expansions, BNS does not displace the Information Technology Act, which remains the primary legislation for certain cyber-offences and intermediaries' liability. Commentary stresses that BNS provisions should be read as complementary rather than duplicative; for example, obscenity and data-theft may be prosecuted under both BNS and IT Act depending on facts and statutory elements.[16][15]

The Bharatiya Sakshya Adhiniyam, replacing the Indian Evidence Act, carries forward and updates rules on electronic records and digital evidence. Much of the Supreme Court jurisprudence on Section 65B of the Evidence Act particularly Anvar P.V. and Shafhi Mohammad will inform the interpretation of new evidence provisions, which continue to require certificates or other authentication for electronic records.[18][19][9][28][^17]

The interaction between BNS substantive offences, BNSS procedural innovations and the new evidence code therefore frames a holistic digital criminal-justice ecosystem. The coherence of this ecosystem will depend on how courts reconcile earlier case law on electronic evidence with new statutory language and technological capacities.

VII. CASE LAW AND DOCTRINAL DEVELOPMENTS RELEVANT TO DIGITAL CRIMINAL JUSTICE

A. Lalita Kumari and FIR Registration in a Digital Age

In Lalita Kumari v. Government of Uttar Pradesh, a Constitution Bench held that registration of FIR under Section 154 CrPC is mandatory where information discloses a cognisable offence, and that police cannot avoid this duty by resorting to indefinite preliminary enquiry. The Court emphasised that FIR registration is part of the "procedure established by law" under Article 21, protecting both complainant and accused rights by ensuring formal initiation of investigation.[27][31]

Commentary on BNSS notes that the new code introduces express scope for preliminary enquiries in certain categories (such as medical negligence, matrimonial disputes, corruption and commercial offences), altering the strictness of Lalita Kumari while retaining the principle that serious complaints must be formally registered. In the context of e-FIRs and electronic complaints, this raises complex questions: digital channels may facilitate complaints but may also be used to screen or filter allegations before formal registration.[^31]

Ensuring that digitisation does not become a new avenue for denial of FIR registration will require clear statutory and judicial guidance on when preliminary enquiries are permissible, how electronic complaints are logged and how complainants can challenge non-registration.

B. Anvar P.V., Shafhi Mohammad and Electronic Evidence Standards

The Supreme Court's decisions in Anvar P.V. v. P.K. Basheer and Shafhi Mohammad v. State of Himachal Pradesh are central to understanding digital evidence in India. In Anvar, the Court overruled earlier flexibility in Navjot Sandhu and held that electronic records are admissible only if accompanied by a certificate under Section 65B(4), clarifying that general rules on secondary evidence do not apply to electronic records. The judgment stressed strict compliance with statutory conditions to prevent manipulation or unreliability of digital evidence.[33][17][^18]

Shafhi Mohammad, however, recognised practical difficulties where electronic evidence is produced by parties who cannot secure certificates from device owners and suggested that Section 65B should not be read as an absolute bar where electronic evidence is otherwise reliable and necessary. Subsequent decisions have attempted to reconcile these approaches, but doctrinal uncertainty persists.[34][19][^35]

Under the new evidence code, similar issues will arise as courts confront digital evidence generated by platforms, intermediaries or third-party devices. BNSS's embrace of audio-video recording and electronic case-files will require consistent standards for authentication, chain of custody and admissibility, ideally clarified through rules or practice directions rather than ad hoc judicial improvisation.

C. Justice K.S. Puttaswamy and Privacy in Digital Criminal Process

In Justice K.S. Puttaswamy v. Union of India, a nine-judge bench of the Supreme Court affirmed that the right to privacy is a fundamental right derived primarily from Article 21, encompassing informational privacy, decisional autonomy and bodily integrity. The Court held that any invasion of privacy must satisfy three requirements: legality (existence of law), legitimate state aim and proportionality, including procedural safeguards.[29][22]

These principles are highly relevant to digital criminal-justice reforms. Search and seizure of electronic devices and communications under Section 94 BNSS, and the use of digital surveillance or data-collection mechanisms, implicate informational privacy and require justification under Puttaswamy's proportionality framework. Similarly, extensive audio-video recording of proceedings, digital storage of testimonies and electronic disclosure of case materials create large data-trails that must be protected against misuse, unauthorised access or profiling.[2][22][^8]

The absence of a dedicated data-protection statute tailored to criminal-justice data aggravates these concerns. While general data-protection legislation is evolving, criminal-justice digitisation demands specific safeguards concerning retention, access, encryption, anonymisation and sharing.[21][36]

D. Supreme Court Guidelines on Video-Conferencing

During the COVID-19 pandemic, the Supreme Court, acting under Article 142, issued comprehensive guidelines for court functioning through video-conferencing, authorising all courts to adopt video technologies, directing High Courts to frame rules and mandating that facilities be provided for litigants without adequate technology. The Court underscored the need to balance public-health concerns with the fundamental right of access to justice.[37][12][^14]

These guidelines, along with High Court-level rules on electronic evidence and video-conferencing (for example, the Delhi High Court's Electronic Evidence and Video Conferencing Rules, 2025), form an important backdrop to BNSS Section 530. Statutory authorisation enhances legal certainty, but prior judicial experience offers practical lessons on managing technical issues, ensuring confidentiality, preventing witness coaching and maintaining decorum.[13][11]

BNSS must be implemented in harmony with these guidelines, leveraging technology as a facilitator rather than a barrier to fair and open justice.

VIII. EVALUATION OF DIGITAL REFORMS: BENEFITS AND RISKS

A. Potential Benefits

1) Enhanced access to justice: E-FIRs, electronic complaints and online hearings can reduce geographical and logistical barriers for victims, witnesses and accused persons, particularly in remote or conflict-affected areas. Victims may be more willing to report offences electronically, including sensitive crimes like sexual offences or cyber-harassment.[6][8][^31]
2) Procedural efficiency and transparency: Electronic service of summons and warrants, digital case-files and audio-video recording of evidence can speed up processes, reduce adjournments and enable better monitoring of case progress. Digital records create audit trails and facilitate appellate review, reducing errors associated with manual transcription.[10][8][^6]
3) Improved evidence-gathering and cyber-crime prosecution: Explicit recognition of digital evidence and electronic offences in BNS and BNSS, alongside IT Act provisions, strengthens legal tools to investigate and prosecute cyber-crime. Section 94 BNSS, by allowing search and seizure of digital devices and communications, is particularly relevant for contemporary investigative needs.[25][2][15][20]
4) Integration with broader e-governance: Nyaya-Shruti and e-Courts platforms can integrate criminal-justice digital reforms with wider e-governance initiatives, enabling inter-operability between police, prosecution, judiciary and prisons. This may reduce duplication and improve data-sharing where legally appropriate.[24][8]

B. Risks and Challenges

1) Digital divide and unequal access: Digitisation presupposes access to devices, connectivity and digital literacy, which are unevenly distributed across socio-economic groups and regions. If courts treat electronic modes as default without adequate alternatives, marginalised litigants may struggle to participate effectively.[12][10]
2) Privacy and data-protection concerns: Extensive collection and storage of digital data FIRs, witness testimonies, evidence, surveillance records create significant privacy risks, especially in the absence of stringent data-protection norms for criminal-justice institutions. Data breaches or misuse of sensitive information could undermine trust in the system.[22][2][^8]

3) Due-process and fair-trial safeguards: Remote hearings may affect the ability of judges to assess demeanour, the dynamics of cross-examination and the confidentiality of lawyer–client interactions. Electronic service and constructive digital notice may lead to ex parte decisions where parties lack actual awareness of proceedings.[35][12]
4) Authentication and reliability of digital evidence: As Anvar and subsequent cases underscore, electronic evidence raises complex issues of authenticity, integrity and chain of custody. BNSS's expansion of digital evidence must be matched by clear rules and capacities for forensic analysis and secure handling.[17][33][^18]
5) Institutional capacity and infrastructure: Successful implementation requires investment in hardware, software, training and technical support across police stations, courts and prisons. Resource-constrained jurisdictions may struggle to operationalise Section 530 BNSS beyond token measures.[11][8][^24]
6) Rule-making and standardisation: Many provisions envisage detailed rules or SOPs regarding electronic communication, signatures, service, encryption and retention, which remain to be fully developed and harmonised across states.[[25][26][^10]

IX. SUGGESTIONS FOR STRENGTHENING DIGITAL CRIMINAL JUSTICE UNDER BNS AND BNSS

In light of the above evaluation, several suggestions can be advanced to ensure that digital reforms under BNS and BNSS foster a rights-respecting and effective criminal-justice system.

A. *Comprehensive Procedural Rules on Electronic Communication and Evidence*

First, central and state governments, in consultation with the judiciary, should frame detailed, rights-sensitive rules on electronic communication and evidence. These should cover:

1) Authentication standards for electronic complaints, summons, warrants and orders, including digital signatures, secure email and verified platforms.[26][10]
2) Protocols for electronic service, including mandatory confirmation of receipt, alternative modes where electronic service fails and safeguards against constructive service in the absence of actual knowledge.[^10]
3) Chain-of-custody guidelines for digital devices and data seized under Section 94 BNSS, including hashing, logging and forensic examination.[2][25]
4) Standards for audio-video recording of evidence, identity verification of participants and handling of technical disruptions.[[11][12]

Clarity in rules will reduce ad hoc practices and provide guidance to police, prosecutors and courts.

B. *Data Protection and Privacy Safeguards*

Second, digital criminal-justice reforms must be harmonised with robust data-protection and privacy norms. Drawing on Puttaswamy's proportionality framework, legislation or rules should specify:

1) Purpose limitation and minimisation: data collected through e-FIRs, video-conferencing and digital evidence should be used only for criminal-justice purposes and retained for limited periods.[21][22]
2) Access controls and encryption: role-based access to digital case-files, strong encryption of sensitive data and audit logs for all access to records.[8][24]
3) Rights of data subjects: procedures for accused persons, victims and witnesses to access, correct or seek deletion of certain data where consistent with legal obligations.

Engagement with evolving national data-protection law is essential to avoid siloed or inconsistent standards.

C. *Bridging the Digital Divide*

Third, implementation should incorporate measures to bridge the digital divide. Courts and police should:

1) Maintain physical modes of complaint-lodging and process service alongside electronic channels, with clear guidance that technology is an option, not an exclusive route.[14][12]
2) Provide video-conferencing facilities at court premises or designated centres for litigants without personal devices or connectivity, as mandated by Supreme Court guidelines.[13][12]
3) Offer training, helplines and support for users unfamiliar with digital procedures, in local languages and accessible formats.

These measures will help ensure that digitisation enhances rather than restricts access.

D. Capacity-Building for Police, Prosecutors and Judiciary

Fourth, sustained capacity-building programmes are required. This includes:

1) Training police in handling digital complaints, preserving electronic evidence, and complying with statutory and constitutional safeguards.[25][26]
2) Educating prosecutors and judges on technological aspects of digital evidence, privacy, cybersecurity and video-conferencing modalities.[12][11]
3) Developing specialised forensic units and collaborations with certified labs to support investigations involving complex digital evidence.

Such capacity-building should be continuous and linked to performance metrics.

E. Doctrinal Clarification on Electronic Evidence and Remote Hearings

Finally, the Supreme Court and High Courts should provide doctrinal guidance tailored to the new codes. This may involve:

1) Clarifying the balance between Anvar's insistence on Section 65B certificates and Shafhi Mohammad's practical flexibility in the context of Bharatiya Sakshya Adhiniyam.[19][17]
2) Developing principles on when remote hearings are appropriate in criminal matters, distinguishing between routine procedural hearings and serious trial stages where physical presence may be preferable.[35][12]
3) Articulating standards for evaluating credibility and demeanour via video-conferencing, and for avoiding unfairness due to technical issues.

Such jurisprudence will shape how lower courts implement digital reforms on the ground.

X. CONCLUSION

The Bharatiya Nyaya Sanhita and Bharatiya Nagarik Suraksha Sanhita mark a decisive shift in India's criminal-justice architecture, embedding digital communication, audio-video technology and electronic evidence into the heart of investigation, trial and appeal. E-FIRs, electronic service of process, audio-video recording and online proceedings promise to make criminal justice more accessible, efficient and responsive to cyber-crime realities.[6][8][^10]

Yet digitisation is not inherently rights-enhancing. Without careful attention to privacy, data-protection, fair-trial safeguards, authentication and infrastructural equity, digital reforms can exacerbate existing inequalities and create new vulnerabilities. The trajectory of implementation under BNS and BNSS will therefore depend on how legislatures, courts and criminal-justice agencies interpret and operationalise these provisions, whether they invest in capacity-building and whether they integrate constitutional principles into techno-legal frameworks.

For scholars and practitioners, the digital criminal-justice reforms offer rich terrain for ongoing research: empirical study of e-FIR usage, analysis of case-law under Section 530 BNSS, evaluation of Nyaya-Shruti's impact, and doctrinal exploration of the new evidence code's treatment of electronic records. This paper has offered an initial doctrinal and normative evaluation, emphasising both transformative potential and areas of concern. Future work must continue to interrogate whether India's journey towards digital criminal justice ultimately strengthens or compromises the foundational commitments of the Constitution to fairness, dignity and rule of law.

REFERENCES

[1] Bharatiya Nyaya Sanhita, No. 45 of 2023, Acts of Parliament, 2023 (India).
[2] Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, Acts of Parliament, 2023 (India).
[3] Law.asia, Criminal Justice System Enters the Digital Age (May 21, 2025), https://law.asia/bnss-criminal-justice-reforms/.[^6]
[4] Bureau of Police Research & Dev., SOP on Zero FIR & e-FIR (2024), https://bprd.nic.in/uploads/pdf/SOP_on_Zero_FIR & eFIR - NCL 2023.pdf.[^26]
[5] Medianama, How India's Criminal Law Amendment Bills Will Affect Digital Sphere (June 2, 2024), https://www.medianama.com/2023/08/223-criminal-law-replacement-bills-digital-ecosystem/.[^2]
[6] Anubhav Khandelwal, Electronic Communication under the BNSS and BNS (2025), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5096623.[^9]
[7] Neeraj Tiwari, The Bharatiya Nagarik Suraksha Sanhita, 2023, Indian L. Inst. (2024), http://www.ili.ac.in/pdf/10._Neeraj_Tiwari__F.pdf.[^38]
[8] Drishti Judiciary, Section 530 BNSS, https://www.drishtijudiciary.com/to-the-point/bharatiya-nagarik-suraksha-sanhita-&-code-of-criminal-procedure/section-530-bnss.[^10]
[9] IJFMR, Legal Challenges, Digital Evidence, and New Criminal Laws (2025), https://www.ijfmr.com/papers/2025/2/41627.pdf.[^28]
[10] MCO Legals, Cybercrimes under the Bharatiya Nyaya Sanhita, 2023 (Series 2, Issue 3) (2025).[^15]
[11] Your Law Article, Offences Against Cybercrime under the Bharatiya Nyaya Sanhita, 2023 (Feb. 19, 2026), https://www.yourlawarticle.com/post/offences-against-cybercrime-under-the-bharatiya-nyaya-sanhita-2023-bns.[^20]
[12] Cyber Crime Punishments under BNS (Bharatiya Nyaya Sanhita), Scribd (Sept. 10, 2025).[^16]

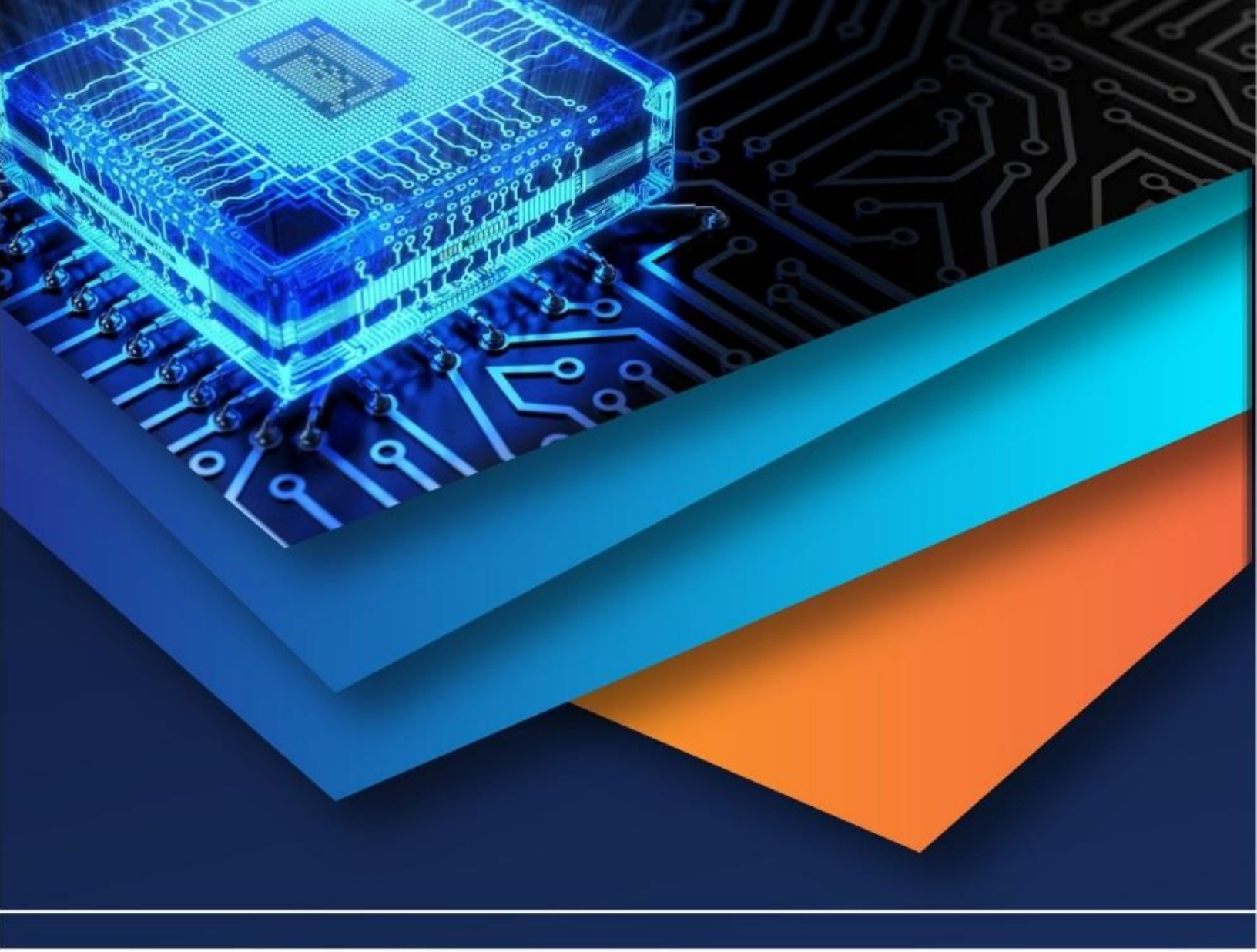
[13] India Code, The Bharatiya Nyaya Sanhita, 2023, https://www.indiacode.nic.in/bitstream/123456789/20062/1/a202345.pdf.[^3]
[14] NCERT, The Bharatiya Nyaya Sanhita, 2023 (Schools Module), https://ncert.nic.in/pdf/module/New_Laws_2023/BNS68-2023E.pdf.[^39]
[15] JETIR, Bridging Physical & Cyber Crimes in Bharatiya Nyaya Sanhita (2024), https://www.jetir.org/papers/JETIR2408430.pdf.[^23]
[16] India Code, Bharatiya Nagarik Suraksha Sanhita, 2023, https://www.indiacode.nic.in/handle/123456789/20099.[^5]
[17] Delhi High Court, Electronic Evidence and Video Conferencing Rules, 2025.[^11]
[18] Press Information Bureau, New Criminal Laws Press Release (Nov. 19, 2025), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2237481&reg=1&lang=1.[^8]
[19] Lalita Kumari v. Government of Uttar Pradesh, (2014) 2 SCC 1.[27][31]
[20] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.[18][17]
[21] Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 SCC 801.[^19]
[22] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.[29][22]
[23] Supreme Court of India, In re: Guidelines for Court Functioning through Video Conferencing during Covid-19 Pandemic, Suo Motu Writ (Civil) No. 5/2020 (Apr. 6, 2020).[14][12]
[24] Supreme Court Observer, Switching to Video (Oct. 8, 2023), https://www.scobserver.in/journal/switching-to-video/.[^14]
[25] IJFMR, The Evolution of Right to Privacy: From K.S. Puttaswamy to Aadhaar (2025).[^21]
[26] Additional policy documents and state-level SOPs on e-FIR, Nyaya-Shruti and video-conferencing, as available.[24][26]

REFERENCES

[1] [PDF] THE BHARATIYA NYAYA SANHITA, 2023 NO. 45 OF 2023 An Act to ...
[2] How India's criminal law amendment bills will affect digital sphere - The Home Ministry on August 10 introduced three new amendment bills in the Lok Sabha, in an attempt ...
[3] [PDF] The Bharatiya Nyaya Sanhita, 2023 | India Code
[4] Bharatiya Nagarik Suraksha Sanhita, 2023
[5] Bharatiya Nagarik Suraksha Sanhita, 2023 - India Code - Contains all Enforced Central and State Acts linked with Subordinate Data like Rules,Regulations,Not...
[6] Criminal justice system enters the digital age | India - Law.asia - By digitising key legal processes, the BNSS streamlines procedures, minimises bottlenecks and enhanc...
[7] THE
[8] new criminal laws - Press Release:Press Information Bureau - Section 254 and Section 265 for Evidence for Prosecution and Section 266 for Evidence for Defence of
[9] Electronic Communication under the Bharatiya Nagarik Suraksha Sanhita, 2023 and Bharatiya Nyaya Sanhita, 2023 - This article explores the interplay between "electronic communication" and "audio-video electronic m...
[10] Section 530 BNSS - Drishti Judiciary - Section 530 encompasses the entirety of criminal proceedings within its electronic framework, specif...
[11] [PDF] Electronic Evidence and Video Conferencing Rules, 2025
[12] Guidelines Issued by The Supreme Court of India for ... - Multilaw - In no case shall evidence be recorded without the mutual consent of both the parties by video confer...
[13] [PDF] GOVERNMENT OF INDIA MINISTRY OF LAW AND JUSTICE ... - The main features of the guidelines are: (i). Video conferencing facilities may be used at all stage...
[14] Switching to Video - Supreme Court Observer - The Supreme Court has issued guidelines under Article 142 for implementing video conferencing and ot...
[15] [PDF] Cyber Law: Series 2: Issue 3 - Cybercrimes under the Bhartiya ...
[16] Cyber crime punishments under BNS (Bharatiya Nyaya ... - The document discusses the role of the Bharatiya Nyaya Sanhita (BNS) in addressing cyber crimes, hig...
[17] Anvar P.V v. P.K Basheer: Supreme Court Of India | CaseMine - Stringent Admissibility Standards for Electronic Records under Section 65-B: Anvar P.V v. P.K Bashee...
[18] [PDF] [2014] 11 S.C.R 399 ANVAR P.V. A P.K. BASHEER AND ORS. - Irrespective of the compliance with the requirements of Section 65-B, which is a provision dealing w...
[19] [PDF] Shafhi Mohammad vs The State Of Himachal Pradesh on 30 ... - Electronic evidence was held to be admissible subject to safeguards. Shafhi Mohammad vs The State Of...
[20] Offences Against Cybercrime under the Bharatiya Nyaya Sanhita ... - The exponential growth of information and communication technology has fundamentally altered the soc...
[21] [PDF] The Evolution of Right to Privacy: From K.S. Puttaswamy to Aadhaar
[22] JUSTICE K.S. PUTTASWAMY VS. UNION OF INDIA - The Supreme Court upheld the fundamental right to privacy. However, unlike most fundamental rights, ...
[23] [PDF] BRIDGING PHYSICAL & CYBER CRIMES IN BHARATIYA NYAYA ...
[24] [PDF] “Pursuant to the 'Model Rules on Video Conferencing (Nyaya Shruti ...
[25] [PDF] PARLIAMENT OF INDIA RAJYA SABHA
[26] [PDF] SOP on Zero FIR & e-FIR
[27] [PDF] Mandatory Registration of FIR- Supreme Court Guidelines in Lalita ... - (i) Registration of FIR is mandatory under Section 154 of the Code, if the information discloses com...
[28] [PDF] Legal Challenges, Digital Evidence, and New Criminal Laws - IJFMR
[29] [PDF] IN THE SUPREME COURT OF INDIA CIVIL ORIGINAL JURISDICTION
[30] [PDF] Bharatiya Nagarik Suraksha Sanhita, 2023 - S3waas

[31] Case: Lalita Kumari v Government of Uttar Pradesh - Dhyeya Law - The Supreme Court ruled in favour of Lalita Kumari, stating that: • The police are required to regis...
[32] Section 530 – Bharatiya Nagarik Suraksha Sanhita (BNSS) – Trial And Proceedings To Be Held In Electronic Mode. - Section 530 - Bharatiya Nagarik Suraksha Sanhita (BNSS) - Trial And Proceedings To Be Held In Electr...
[33] Anwar v Basheer - The document summarizes the key issues in the case of Anwar P.V. vs P.K. Basheer regarding the admis...
[34] Electronic Evidence in India: Section 65B of the Evidence Act ... - It has been held in Anvar P V v/s P K Basheer And Others 2014 LawSuit(SC)783 at Para 14 that the Evi...
[35] Trials Via Video Conference: Validity in India - Explore the legal validity of conducting trials through video conference in India. Key Supreme Court...
[36] Constitutionality of Aadhaar Act: Judgment Summary - Plain English summary of the judgment on the constitutional validity of the Aadhaar Act, in Puttaswa...
[37] [PDF] in the supreme court of india
[38] [PDF] THE BHARATIYA NAGARIK SURAKSHA SANHITA, 2023 Neeraj ...
[39] [PDF] THE BHARATIYA NYAYA SANHITA 2023 - NCERT

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)