LexScriptaMagazine.com ISSN: 2583-8725 Vol. 03 - Q4 Oct - Dec, 2025

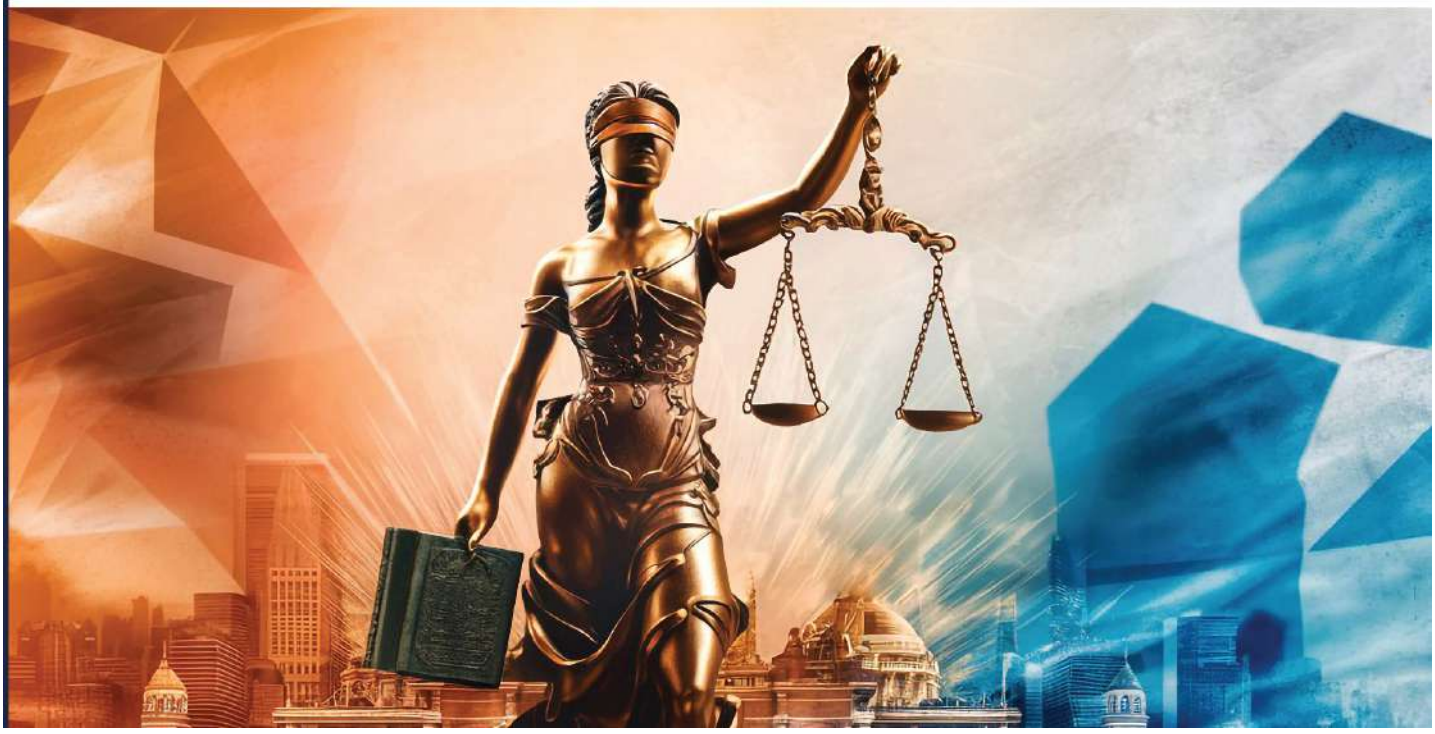
ISSN: 2583-8725

Lex Scripta Journal

Quarterly Online and Print Edition

Law & Policy

"Join the League of National & International Scholars"



EDITORIAL TEAM

LEX SCRIPTA MAGAZINE OF LAW AND POLICY (VOL-2, ISSUE-3)

ISSN-2583-8725
Vol - II, Issue - III
Published by INTEGRITY EDUCATION INDIA

New Delhi
First Floor, 4598/12-B, 1st Floor,
Padam Chand Marg, Daryaganj,
New Delhi, Delhi 110002
Phone: +91 98 11 66 62 16 (M)
Phone: +91 70 11 60 56 18 (M)

Bengaluru
Jallahalli East
Bengaluru, Karnataka. India.
Phone: +91 98 11 66 62 16 (M)
Email: publisher.integrity@gmail.com

USA
New Jersey
14 Grandview Ave, Upper Saddle River,
NJ-07458, USA
Phone: +14805226504 (M)

London
37 Degree Media
64, Hodder Drive, Perivale, London UB68LL.
United Kingdom.
Phone: +44 7950 78 18 17 (M)
Website: integrityeducation.co.in

For any Query / Feedback
Phone: +91 98 11 66 62 16 (Vineet Sharma)

Printed in India @ New Delhi

ISSN: 2583-8725

Lex Scripta Journal

Quarterly Online and Print Edition

Law & Policy

"Join the League of National and International Scholars"

LEX SCRIPTA MAGAZINE
JOURNAL MAGAZINE BY INTEGRITY EDUCATION INDIA

LexScriptaMagazine.com ISSN: 2583-8725 Vol. 03 - Q4 Oct - Dec, 2025

Lex Scripta Journal

DIGITAL TRANSFORMATION OF CRIMINAL INVESTIGATION IN INDIA: A STUDY OF E-FIR, ZERO FIR, AND ONLINE COMPLAINT SYSTEMS

Author
Nitesh Kumar Singh

LEX SCRIPTA JOURNAL
JOURNAL MAGAZINE BY INTEGRITY EDUCATION INDIA

DIGITAL TRANSFORMATION OF CRIMINAL INVESTIGATION IN INDIA: A STUDY OF E-FIR, ZERO FIR, AND ONLINE COMPLAINT SYSTEMS

Nitesh Kumar Singh[1]
Department of Law
Dr. Harisingh Gour Vishwavidyalaya, Sagar, Madhya Pradesh
niteshsinghbhu9@gmail.com

Abstract

The landscape of criminal investigation in India is undergoing a foundational transformation, driven by digitalization and legislative reform. The enactment of the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, marks a paradigm shift from a colonial-era, procedure-centric model to a victim-centric, accessible, and efficient justice delivery framework. This article provides a comprehensive analysis of this digital evolution, focusing on three pivotal innovations: E-FIR, Zero FIR, and integrated online complaint systems. It argues that while these mechanisms, as codified under BNSS Section 173, significantly bridge long-standing accessibility and accountability gaps, particularly for women, marginalized communities, and victims of cybercrime, their implementation is fraught with systemic, infrastructural, and socio-legal challenges. Through doctrinal and empirical analysis, the article examines the historical context from the Code of Criminal Procedure, 1973, to the post-Nirbhaya reforms, culminating in the BNSS. It delves into the procedural nuances, judicial backing, and technological infrastructure underpinning these tools, supported by National Crime Records Bureau (NCRB) data and case studies from states like Uttar Pradesh and Delhi. The analysis also critically addresses the persistent digital divide, risks of procedural misuse, privacy concerns in light of the Digital Personal Data Protection Act, 2023, and institutional resistance. By incorporating comparative perspectives from global models like the UK's online crime reporting, the article proposes a nuanced reform roadmap. It concludes that the success of India's digital investigative shift hinges not on technology alone, but on concurrent investments in police sensitization, rural digital literacy, robust cyber-security, and an ethical framework for

[1] Research Scholar & Author

Artificial Intelligence, ultimately forging an integrated e-justice ecosystem that truly serves the *Nagarik* (citizen).

Key Words: BNSS, e-FIR, Zero FIR, Criminal Investigation, Digital Device

Introduction

"The law must be stable, but it must not stand still." - Roscoe Pound

The concept of justice is intrinsically linked to access. For decades in India, the first step towards seeking criminal justice, the registration of a First Information Report (FIR) was often a labyrinthine ordeal of jurisdictional confusion, procedural opacity, and, at times, outright denial. The physical and bureaucratic barriers to filing an FIR disproportionately affected the vulnerable, turning the police station, meant to be a sanctuary, into a site of further trauma. The digital revolution of the 21st century, however, has precipitated an irreversible change in this dynamic, compelling the criminal justice system to evolve from its paper-bound, station-centric origins.

This article examines the profound digital transformation reshaping India's criminal investigation landscape, a shift now formally codified in the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, which replaces the Code of Criminal Procedure, 1973. At the heart of this transformation are three interlinked digital mechanisms: **E-FIR** (electronic FIR), **Zero FIR**, and **national online complaint portals**. These are not mere technological upgrades but represent a fundamental reorientation towards victim rights, operational efficiency, and transparent accountability.

While the statutory formalization of E-FIR and Zero FIR under the BNSS represents a monumental leap in democratizing access to justice and enhancing investigative agility, the realization of their full potential is contingent upon overcoming deep-seated implementation hurdles, including the digital divide, institutional inertia, and emerging cyber-risks, demanding a holistic, rights-based approach to reform.

The **primary objectives** of this article are:

1. To trace the historical and jurisprudential evolution of FIR registration leading to the digital provisions of the BNSS.

2. To critically analyze the legal architecture, operational procedures, and judicial safeguards governing E-FIR and Zero FIR.
3. To evaluate the benefits, empirical impacts, and systemic challenges of these digital mechanisms through data and case studies.
4. To propose a concrete policy and implementation roadmap for a seamless, secure, and citizen-centric digital investigation ecosystem.

The Scope of the article is firmly positioned in the post-BNSS 2023 context, with retrospective analysis of the CrPC era and the **Justice Verma Committee** reforms to establish a coherent narrative of change. The methodology employs a mixed-method approach: doctrinal analysis of statutes (BNSS, BNS, IT Act), judicial pronouncements (Supreme Court and High Courts), and official guidelines (BPR&D SOPs); and empirical analysis of implementation data from the NCRB, Crime and Criminal Tracking Network & Systems (CCTNS). and specific state police initiatives.

Historical Evolution of FIR Registration in India

The FIR, as the foundational document setting the criminal law machinery in motion, has a history mirroring India's legal-administrative evolution. In the pre-colonial and early colonial period, policing was largely informal and community-based. The formalization began with the Indian Penal Code (1860) and the Criminal Procedure Code (1861, later 1898), which institutionalized the British model of policing. Section 154 of the CrPC, 1898, and its successor in the CrPC, 1973, defined the FIR as information relating to a cognizable offence, recorded by the officer-in-charge of a police station.

The **CrPC, 1973 regime**, while progressive for its time, suffered from critical limitations rooted in its physical and jurisdictional rigidity:

- **Station-Centricity:** An FIR could only be registered at the police station within whose territorial jurisdiction the crime occurred. This ignored the mobility of victims and the complex, multi-jurisdictional nature of modern crime, especially railway crimes or crimes against travellers.
- **Procedural Discretion & Denial:** The infamous phrase "preliminary inquiry" was often misused as a tool for delay, discouragement, and outright refusal, particularly in sensitive

cases involving powerful accused or crimes against women and marginalized sections. The discretion to investigate before registering often became a barrier to registration itself.

- **Form Over Substance:** The emphasis on written, signed complaints created hurdles for the illiterate, the traumatized, or those unable to physically visit a specific police station.

The judiciary, recognizing these failings, began to intervene forcefully. The landmark case of ***Lalita Kumari v. Govt. of Uttar Pradesh*** It was a watershed moment. The Supreme Court's 5-Judge Constitution Bench mandated the compulsory registration of FIR in cognizable offences, allowing a preliminary inquiry only in a narrow window specifically for offences relating to matrimonial disputes, commercial offences, medical negligence, and corruption, and even then, to be concluded within seven days. The Court poignantly observed, **"Jurisdictional rigidity often defeated justice at the threshold,"** underscoring how procedural technicalities were overshadowing substantive justice.

The **Nirbhaya gang rape case of 2012** acted as a catalytic tragedy. The Justice J.S. Verma Committee (2013), formed in its aftermath, made sweeping recommendations to reform India's criminal law concerning sexual violence. While focused on substantive law, its spirit emphasized ease of access, victim dignity, and police accountability. It implicitly laid the groundwork for concepts like Zero FIR, recommending that victims should be able to register complaints at any police station, irrespective of jurisdiction, and that refusal should be a punishable offence.

These judicial and socio-legal pressures created the impetus for legislative change. The transition to the BNSS was, therefore, not an abrupt shift but the culmination of decades of judicial activism, civil society advocacy, and technological possibility. The legislative intent behind BNSS Section 173 is clear: to statutorily embed the principles of *Lalita Kumari* and the spirit of the Justice Verma Committee, transforming the FIR from a gatekept document into an accessible right. It represents a conscious move from a model of procedural hindrance to one of facilitative access, setting the stage for the detailed digital mechanisms analyzed in the following chapters.

Legal Framework of E-FIR under BNSS

The **Bharatiya Nagarik Suraksha Sanhita, 2023, Section 173(1)** provides the statutory bedrock for the digital transformation of FIR registration. It states that information about a

cognizable offence can be given orally, in writing, or by electronic communication, to an officer in charge of a police station. This simple yet profound inclusion of "electronic communication" legally sanctifies the concept of E-FIR.

Key Procedural Components under BNSS Section 173:

1. **Mode of Transmission:** The information can be sent via email, dedicated online portals (like the Digital Police Portal), or potentially even structured messaging platforms integrated with official systems.
2. **Signature Verification Mandate:** Recognizing the need to authenticate electronic complaints, the proviso to Section 173(1) mandates that if the information is given electronically, the person must physically sign the recorded information and appear before the police station officer within three days. This creates a hybrid model digital initiation with physical authentication, balancing accessibility with evidentiary integrity.
3. **Preliminary Enquiry Safeguard:** Sub-section (3) of Section 173 incorporates the ***Lalita Kumari*** doctrine. For cognizable offences punishable with imprisonment between three and seven years, the officer *may* conduct a preliminary inquiry to ascertain whether a prima facie case exists. This inquiry must be concluded within fourteen days. This provision aims to prevent frivolous complaints in moderately serious offences while imposing a strict timeline to avoid delays.

Comparative Analysis: E-FIR vs. Traditional FIR

Aspect	**Traditional FIR (CrPC era)**	**e-FIR (BNSS Era)**
Initiation Point	Physically at the jurisdictional police station	Anywhere with internet access, police station portal or national portal
Time of Registration	Subject to officers' availability and discretion, often delayed	Near-instantaneous, 24/7 submission, timestamped electronically
Format & Record	Handwritten/typed in the station register, prone to manual errors	Structured digital form, auto-populated, standardized, and tamper-proof

Victim Trauma	High, requires facing the police station environment, potential intimidation	Reduced initial trauma, complaint can file from a safe, private space
Geographical barrier	Absolutely, must be in the correct jurisdiction	Eliminated at the filing stage, follows the Zero FIR principle for transfer
Tracking and Transparency	Opaque, the complainant must physically visit the station to update	Potential for real-time status tracking via Unique Complaint ID
Data Integration	Siloed, manual entry into CCTNS later	Direct, seamless integration with CCTNS/ICJS, aiding analytics

Safeguards and Penalties: The BNSS framework is reinforced by related provisions. The Bharatiya Nyaya Sanhita, 2023 (BNS), in **Section 199**, prescribes punishment for a public servant who knowingly disobeys any direction of the law with the intent to cause injury to any person. This can be invoked against officers who unjustifiably refuse to register an E-FIR. Furthermore, the IT Act, 2000, and rules thereunder provide the legal validity for electronic records and digital signatures, forming the broader ecosystem for E-FIR's admissibility in court.

The E-FIR mechanism, therefore, is not an unregulated digital free-for-all. It is a carefully structured legal innovation designed to enhance access while embedding verification loops and timelines to maintain the solemnity and integrity of the criminal complaint process

Zero FIR: Concept, Provisions, and Judicial Backing

The **Zero FIR** is a powerful procedural innovation designed to eliminate jurisdictional delays at the very inception of a criminal case. Its core principle is simple: A police station is mandated to register an FIR for a cognizable offence reported to it, irrespective of whether the offence occurred within its territorial limits. The station registers the FIR, assigns it a temporary serial number (hence "Zero"), and then promptly transfers it to the police station having appropriate jurisdiction for investigation.

Codification under BNSS: While the concept gained traction through judicial orders, the BNSS Section 173(2) now provides explicit statutory force to it. It states that if the information relates to an offence committed outside the jurisdiction of the police station where it is reported, the officer shall register the FIR and transfer it to the concerned police station "without any delay." This statutory mandate removes any ambiguity or discretion.

Judicial Evolution and Landmark Backing: Long before its codification, the Supreme Court had been sculpting this principle.

- In ***Satvinder Kaur v. State,*** the Court held that a police officer cannot refuse to register a case merely because the offence was committed outside his jurisdiction.
- The principle was reiterated in ***Ramesh Kumari v. State (NCT of Delhi) (2006)***, emphasizing the duty to register.
- A crucial procedural directive came from the Supreme Court in ***Punati Ramulu v. State of Andhra Pradesh (1993).*** The Court condemned the practice of forwarding a complaint under Section 156(3) instead of registering a Zero FIR, stating it was a "device adopted to slip out of the responsibility."

E-Zero FIR: A Digital Leap for Cybercrime: The Zero FIR concept finds its most potent application in the realm of cybercrime, which is inherently borderless. A victim of online financial fraud in Kerala could be defrauded by servers in Jharkhand and an accused residing in Noida. Recognizing this, the **National Cyber Crime Reporting Portal** operationalizes the concept of **"E-Zero FIR."** When a complaint is filed on this portal, it is automatically routed as a Zero FIR to the appropriate state-level cyber cell based on the information provided (e.g., bank account details, phone number). This system, integrated with the broader CCTNS, ensures that the victim does not need to determine jurisdiction the system does it automatically. The Bureau of Police Research & Development (BPR&D) Standard Operating Procedure on Zero FIR aptly notes, "Zero FIR ensures no victim is turned away from the doorstep of justice."

Operational Procedure:

1. **Registration:** The receiving station registers the FIR in its General Diary, marking it as a "Zero FIR."
2. **Acknowledgement:** An acknowledgement is provided to the complainant immediately.
3. **Transfer:** The FIR, along with any initial evidence, is transferred electronically via CCTNS to the jurisdictional station without delay.

4. **Investigation:** The jurisdictional station re-registers it with its own FIR number and commences investigation.

The judicial backing and now statutory mandate for Zero FIR reflect a victim-centric philosophy: the system must adapt to the victim's need and location, not vice versa. It is a critical tool against police shirking of responsibility and a cornerstone of the accessible justice framework envisioned by the BNSS.

Online Complaint Systems and Digital Portals

The E-FIR and Zero FIR concepts are operationalized through a growing ecosystem of national and state-level digital portals. These platforms serve as the citizen-facing interface of the digital policing transformation.

National Level Portals:

1. **Digital Police Portal:** This is the Government of India's flagship platform under the CCTNS project. It allows citizens to file complaints for certain types of crimes (like theft, loss of property, and cheating) online, which are then converted into E-FIRs at the concerned police station. It also provides services like requesting vehicle theft checks, antecedent verification, and accessing authenticated copies of FIRs.
2. **National Cyber Crime Reporting Portal (cybercrime.gov.in):** Operated by the Indian Cyber Crime Coordination Centre (I4C), this portal is dedicated to reporting all types of cybercrime, with a special focus on **financial fraud and crimes against women/children**. It enables the filing of E-Zero FIRs and has features for reporting lost/stolen mobile phones and blocking fraudulent financial transactions.
3. **UMANG (Unified Mobile Application for New-age Governance):** This integrated app provides access to the Digital Police Portal among hundreds of other government services, bringing complaint filing to citizens' smartphones.

The Role of CCTNS and the 100% Digital Vision: The Crime and Criminal Tracking Network & Systems (CCTNS), launched in 2009 under the National e-Governance Plan, is the central nervous system enabling all these portals. It digitally links over 16,000 police stations, creating a unified national database. The government's vision, as reiterated in various policy documents, is to achieve 100% digital FIR registration via CCTNS by 2025. This does not necessarily mean 100% E-FIR from the public, but that every FIR, whether initiated online

or at the station, is digitally recorded and processed in the CCTNS ecosystem, eliminating manual registers.

Escalation for Non-Cognizable Offences: For non-cognizable offences (NCs), where police cannot investigate without a magistrate's order, online systems play a different but vital role. Citizens can file Non-Cognizable Complaints (NCs) online. While this doesn't initiate an investigation, it creates an official, timestamped record. This digital trail can be crucial for the complainant to approach the magistrate under Section 174(2) of the BNSS (equivalent to old CrPC) for an order to investigate, or for establishing a pattern of harassment in cases like cyberstalking or defamation.

These portals, therefore, are not just technological tools but symbols of a shifting power dynamic, placing the initiative and a degree of control back into the hands of the citizen, making the first interaction with the justice system less daunting and more accountable.

Technological Infrastructure and Integration

The ambitious vision of digital policing rests on a complex and evolving technological infrastructure. The journey began with the CCTNS project in 2009, aimed at creating a nationwide, integrated platform for crime tracking. Over the past decade, CCTNS has evolved from a basic digitization project to the backbone for advanced applications, such as E-FIR portals and analytics.

Core Technological Pillars:

1. **CCTNS & ICJS:** While CCTNS links police stations, the Interoperable Criminal Justice System (ICJS) is a broader framework to interconnect CCTNS seamlessly with the e-Courts, e-Prisons, and Forensics databases. This horizontal integration is crucial for E-FIR data to flow smoothly to prosecutors and courts.
2. **Artificial Intelligence & Machine Learning:** AI/ML is being piloted for predictive policing, fraud detection in online complaints, and cyber threat analysis. For instance, AI can flag patterns in online financial fraud complaints to identify syndicates. However, this raises significant ethical and legal questions. The Supreme Court, in hearings related to "digital arrests" and privacy, has cautioned against unregulated technological overreach. A

bench observed, "Technology must serve justice, not supplant human judgment," warning against over-reliance on automated systems that may embed biases.

3. **BNSS Mandates for Digital Evidence:** The BNSS itself pushes technological adoption**.** Section 180 makes video recording of search and seizure proceedings mandatory in certain cases. Section 530 allows for e-trials, the recording of evidence via video-conferencing. This creates a natural demand for the digital chain of custody, starting with an E-FIR.
4. **Cloud Infrastructure and Cybersecurity:** The massive volume of sensitive data from E-FIRs and portals necessitates secure, scalable cloud storage and robust cybersecurity protocols to prevent breaches that could compromise investigations and victim identities.

Critical Integration Challenges:

- **Interoperability Gaps:** Despite ICJS, full seamless data exchange between police, courts, and forensic labs remains a work in progress. An E-FIR's digital evidence packet must be compatible with court case management systems.
- **Legacy System Inertia:** Many police stations, especially in rural areas, still operate with older versions of CCTNS software or rely on parallel manual systems, creating data silos.
- **Skill Gaps:** The technological shift demands a digitally literate police force. Training constables and officers to proficiently handle E-FIR verification, digital evidence management, and portal interfaces is a massive human resource challenge.
- **Standardization:** The plethora of state-level portals, while innovative, can lead to a lack of uniform standards for data fields, security protocols, and user experience, complicating national-level analytics and coordination.

The technological infrastructure is thus both the enabler and a potential bottleneck. Its success depends not just on hardware and software, but on systemic integration, capacity building, and a strong legal-ethical framework governing the use of emerging technologies like AI in policing.

Benefits, Impacts, and Empirical Evidence

The transition to digital investigation mechanisms promises and, in many instances, is already delivering tangible benefits. These can be assessed through quantitative data, qualitative improvements, and specific case studies.

Quantitative Benefits & NCRB Data: The National Crime Records Bureau (NCRB), through CCTNS, now generates more granular data. While pre-/post-BNSS longitudinal studies will take time, early trends from states that pioneered E-FIR are instructive.

- **Registration Speed:** In Uttar Pradesh, after the launch of UP COP, the time for FIR registration for eligible crimes reduced from an average of 24-48 hours (including travel and station procedures) to under 60 minutes for a digitally filed complaint.
- **Increased Reporting:** The NCRB's "Crime in India" report shows a consistent year-on-year increase in the registration of cybercrime and crimes against women. While this reflects an actual rise in crime, it also indicates reduced under-reporting due to easier, less intimidating online and Zero FIR options. For instance, the national cybercrime portal received over 10 lakh complaints in its first few years of operation, a volume unimaginable through traditional channels.

Qualitative Impacts:

1. **Victim Empowerment:** The digital shift is profoundly empowering for women, LGBTQ+ individuals, and rural complainants. A survivor of online harassment can file a complaint without facing potentially insensitive questioning at a police station first. A farmer who cheated in an online scheme can register an E-FIR from a Common Service Centre in his village.
2. **Transparency and Accountability:** The unique complaint ID generated for every online submission allows citizens to track the status of their complaint, reducing the "black box" of police procedures. This creates a passive audit trail, making it harder for officers to ignore or misplace complaints.
3. **Systemic Efficiency:** Digital FIRs eliminate manual data entry errors, auto-populate fields, and enable instant sharing across jurisdictions for Zero FIRs. This saves thousands of man-hours and accelerates the initial phase of investigation.

Pre/Post-BNSS Comparative Metrics

Metric	**Pre-BNSS (CrPC Era) Typical Scenario**	**Post- BNSS (Digital Mechanisms) Target/outcome**

FIR Registration Time	1-3 days (often longer with delays)	24 hours for E-FIR; minutes for the portal's submission.
Jurisdiction Transfer Time	Weeks for zero FIR physical transfer	48 hours via digital CCTNS transfer
Complaint Travel	Often required to go to a jurisdictional station	Minimal, Possible zero travel for e-FIR initiation
Data Accuracy	Low, dependent on the officer's willingness	Medium, High potential for portal-based training

Challenges, Criticisms, and Safeguards

The digital leap, while transformative, encounters formidable obstacles rooted in India's socio-economic diversity, institutional culture, and the inherent risks of technology.

1. The Digital Divide and Access Inequality: The promise of "anywhere, anytime" justice presumes digital literacy and access. This creates a new form of marginalization. Rural populations, the elderly, the urban poor, and those with disabilities may find online portals as intimidating as physical police stations. The requirement to appear for signature verification within three days, while a safeguard, can be an insurmountable barrier for a daily wage earner from a remote area who filed an E-FIR. The solution lies not in rolling back digitalization, but in complementing it with human intermediaries**,** like making police station aides or Common Service Centre operators available to assist in filing digital complaints.

2. Misuse and Verification Challenges: The ease of filing can lead to frivolous, false, or malicious complaints. While the preliminary inquiry clause in BNSS Section 173(3) for mid-level offences is a check, it may not suffice for all cases. The police must develop robust but quick verification protocols for digital complaints to prevent harassment and wasting investigative resources. The Law Commission of India, in its reports, has cautioned against a blanket e-FIR system for all offences, warning of potential misuse. A graded approach, where

E-FIR is initially permitted for a defined list of crimes (as most states do), is a prudent safeguard.

3. Institutional and Cultural Resistance: A significant barrier is police resistance to the transparency and accountability that digital systems bring. The "chowki culture" of informal dispute resolution and discretionary power is disrupted by time-stamped, centrally recorded digital complaints. There is often a lack of ownership and training, leading to scenarios where an E-FIR is registered but not promptly acted upon, defeating its purpose. Changing this mindset requires leadership commitment, performance metrics linked to digital response times, and continuous training.

4. Privacy and Data Security Risks: An E-FIR contains highly sensitive personal data—victim details, allegations, and potentially intimate facts. The storage and transmission of this data across CCTNS/ICJS creates massive cybersecurity vulnerabilities. A data breach could be catastrophic. The newly enacted **Digital Personal Data Protection Act (DPDPA), 2023,** will have a critical interplay here. Police, as "Data Fiduciaries," will have legal obligations to ensure lawful processing, purpose limitation, and strong security safeguards for the personal data collected through E-FIRs. Non-compliance could invite penalties and erode public trust.

5. Judicial Caution and Ethical Boundaries: The judiciary has welcomed efficiency but remains wary of technological overreach. The Supreme Court's observation, "Technology must serve justice, not supplant human judgment," is a guiding principle. Over-dependence on AI for profiling or predictive policing risks algorithmic bias and erosion of civil liberties. The human element of policing, empathy, discretion in sensitive situations, and understanding context cannot be fully automated. Digital tools must be assistants, not replacements, for investigative reasoning.

Addressing these challenges requires a multi-pronged strategy of infrastructure development, legal safeguards (like the DPDPA), intensive training, and a strong ethical charter for police technology use.

Comparative Analysis and Global Perspectives

India’s digital journey is part of a global trend. Examining international models provides valuable benchmarks and lessons.

United Kingdom: The UK police have a mature **"Online Crime Reporting"** system for non-emergency incidents. Citizens can report crimes like theft, criminal damage, or hate crimes online. The system is integrated with the National Police National Computer. A key lesson is their clear triage the portal clearly states which crime types are suitable for online reporting and which require an emergency call. This manages public expectations and prevents system overload.

United States: There is no single federal system; practices vary by state and county. Many large departments, like the Los Angeles Police Department (LAPD) and the New York Police Department (NYPD), offer online incident reporting for non-violent crimes. The US also has specialized portals for reporting cybercrime to federal agencies like the FBI's Internet Crime Complaint Centre (IC3). The US experience highlights the challenge of fragmentation in a federal system, a challenge India is overcoming through centralized platforms like CCTNS.

Singapore: Known for its tech-enabled governance, Singapore's police force allows e-Services for reporting minor crimes, lodging police certificates, and providing feedback. Its integration with the national digital identity system (SingPass) simplifies authentication, a step India is moving towards with Aadhaar-based verification (with due privacy safeguards).

Comparative Efficiency Benchmarks:

- **Registration Time:** In the UK, an online report is typically acknowledged instantly, and a reference number is provided. India's E-FIR systems are achieving similar benchmarks.
- **Integration:** The UK's system is deeply integrated with national databases, similar to India's CCTNS vision.
- **Scope:** India's ambition to expand E-FIR to more serious offences is bolder than many Western systems, which often restrict online reporting to minor, non-violent crimes.

Lessons for India:

1. **Phased Expansion:** Like the UK, India should continue a phased, crime-type specific expansion of E-FIR, building police capacity and public trust gradually.
2. **Public Awareness:** Global models invest significantly in public campaigns to educate citizens on how and when to use online systems.
3. **Inter-Agency Integration:** The seamless flow of information between police, prosecutors, and courts in some European countries is an aspirational model for India's ICJS.

4. **Balancing Act:** All systems grapple with the balance between accessibility and preventing misuse. India's hybrid model (digital filing + physical verification) is a reasonable middle path, but the 3-day verification window needs flexibility for genuine hardship cases.

India's digital investigation framework, while learning from others, is uniquely positioned due to its scale, the boldness of BNSS codification, and the direct attempt to solve deep-seated access issues through technology.

Recommendations and Future Roadmap

To realize the full potential of the BNSS's digital vision and overcome existing challenges, a concerted, multi-stakeholder effort is required. The following recommendations outline a future roadmap:

A. Policy and Administrative Reforms:

1. **National Digital Literacy Drive for Policing:** Mandate and fund continuous, certified training programs for police personnel at all levels on E-FIR procedures, digital evidence handling, and cybersecurity. Performance appraisals should include digital competency metrics.
2. **Bridging the Access Divide:**

   i. Establish "Digital *Sahyog*" kiosks at every police station and post office, staffed by trained facilitators.
   ii. Integrate voice-based or vernacular language interfaces in online portals for greater inclusivity.
   iii. Allow for extended or flexible timelines for physical signature verification in documented cases of genuine distance or hardship.

3. **Standardization and Interoperability:** The Ministry of Home Affairs should enforce strict data and API standards for all state portals to ensure seamless national interoperability and analytics.

B. Legislative and Procedural Tweaks:

1. **Amend BNSS for Flexibility:** Consider amending the 3-day verification rule to a more flexible "as soon as reasonably practicable, not exceeding 7 days," with provisions for remote verification via verified video link in exceptional circumstances.
2. **Strengthen DPDPA Implementation:** Develop clear, police-specific guidelines under the DPDPA, 2023, for processing E-FIR data. Appoint dedicated Data Protection Officers in state police headquarters.
3. **Mandatory Timelines in SOPs:** The BPR&D should issue model SOPs with mandatory timelines for each step: E-FIR acknowledgement (instant), transfer of Zero FIR (within 24 hours), preliminary enquiry conclusion (strictly within 14 days).

C. Technological and Ethical Advancements:

1. **AI Ethics Framework:** Develop and publish a national "AI in Policing" ethics charter, prohibiting its use for mass surveillance or predictive profiling that targets communities. AI should be limited to pattern analysis in specific crime types (e.g., financial fraud, cyber-attack sources).
2. **Enhanced Cybersecurity for CCTNS/ICJS:** Conduct regular white-hat hacking audits, implement end-to-end encryption for sensitive data fields, and establish a dedicated cybersecurity wing within the NCRB.
3. **Blockchain for Evidence Chain-of-Custody:** Pilot the use of blockchain technology to create an immutable audit trail for digital evidence collected from the point of E-FIR registration through to the courtroom.

Vision for an Integrated E-Justice Ecosystem: The ultimate goal is a fully integrated e-justice ecosystem. In this vision:

- An **E-FIR** seamlessly populates a digital case file.
- Investigative updates, **e-charge sheets**, and forensic reports are added digitally.
- The case file is electronically transmitted to the **e-Court**.
- **E-trials** (BNSS Section 530) are conducted, with evidence presented digitally.
- The entire lifecycle, from complaint to judgment, is trackable by the victim (within privacy limits) through a secure portal.

This ecosystem would dramatically reduce delays, minimize human interface-related corruption, and create a transparent, efficient, and truly citizen-centric criminal justice process.

CONCLUSION

The digital transformation of India's criminal investigation landscape, crystallized in the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, represents a historic pivot. By statutorily embracing E-FIR, Zero FIR, and online complaint systems, India has taken a decisive step from a rigid, jurisdiction-bound model to a fluid, victim-empowering paradigm. This shift addresses core flaws highlighted by the judiciary over decades and demanded by a changing society.

The analysis confirms that these mechanisms are indeed bridging critical accessibility gaps, particularly for women, cybercrime victims, and those distant from jurisdictional police stations. They are injecting efficiency and transparency into the system's first and most crucial gate. Empirical evidence from early-adopter states and national portals demonstrates increased reporting, faster registration, and the potential for data-driven policing.

However, the journey is far from complete. The digital divide, institutional resistance, risks of misuse, and formidable privacy challenges pose real threats to the inclusive and just implementation of this vision. Technology is not a panacea. As the Supreme Court wisely cautioned, it must be a servant to justice, not its master.

The success of this reform, therefore, will not be measured by the sophistication of the software but by its on-the-ground impact on the most vulnerable citizen seeking justice. It hinges on a holistic approach that couples digital tools with human sensitivity, bridges access gaps, fortifies data protections, and continuously adapts based on feedback. The BNSS has provided the legal framework; it now falls upon the police leadership, the judiciary, civil society, and the technology community to collaboratively build the infrastructure, culture, and trust needed to realize its promise. If done right, India can set a global benchmark for a rights-respecting, efficient, and truly digital-era criminal justice system that lives up to the ethos of the *Nagarik Suraksha Sanhita*, a code for the security and dignity of every citizen.

REFERENCES

Statutes

1. The Bharatiya Nagarik Suraksha Sanhita, 2023 (No. 46 of 2023).
2. The Bharatiya Nyaya Sanhita, 2023 (No. 45 of 2023).
3. The Code of Criminal Procedure, 1973 (Repealed).

4. The Digital Personal Data Protection Act, 2023.
5. The Information Technology Act, 2000.

Cases

1. Lalita Kumari v. Govt. of Uttar Pradesh, (2014) 2 SCC 1.
2. Ramesh Kumari v. State (NCT of Delhi), (2006) 2 SCC 677.
3. Satvinder Kaur v. State (Govt. of NCT of Delhi), (1999) 8 SCC 728.
4. Punati Ramulu v State of Andhra Pradesh 1993 SCC (Cri) 1024.

Reports & Official Documents

1. Bureau of Police Research & Development (BPR&D). (2021). *Standard Operating Procedure (SOP) on Zero FIR*.
2. Government of India, Ministry of Home Affairs. (2023). *Crime and Criminal Tracking Network & Systems (CCTNS): Project Status Report*.
3. Justice J.S. Verma Committee. (2013). *Report of the Committee on Amendments to Criminal Law*.
4. National Crime Records Bureau (NCRB). (2022). *Crime in India – 2021*.

Articles & Journals

1. Singh, M. P. (2020). *Digital Policing in India: The CCTNS Experience*. Indian Journal of Public Administration, 66(2), 245–260.
2. Suman, D. (2023). *E-FIR and Zero FIR under the New Criminal Laws: A Critical Analysis*. Journal of the Indian Law Institute, 65(3).

Web Resources

1. Digital Police Portal**.** **https://digitalpolice.gov.in**
2. National Cyber Crime Reporting Portal**.** **https://cybercrime.gov.in**
3. UMANG App**.** **https://web.umang.gov.in**

ABOUT LEX SCRIPTA JOURNAL

Lex Scripta Magazine is a premier peer-reviewed online and print journal dedicated to advancing scholarly research in law, policy, and social sciences. With the vision of promoting academic excellence and fostering a culture of intellectual exchange, the magazine provides a distinguished platform for academicians, researchers, legal professionals, and students to publish their original work and contribute to contemporary legal discourse.

Each submission undergoes a rigorous double-blind review process conducted by a panel of eminent national and international professors, ensuring the highest standards of quality and academic integrity. Lex Scripta not only encourages original and innovative research but also strives to bridge the gap between theoretical insights and real-world applications in the legal domain.

Contributors and editorial members receive global recognition through certificates and publication opportunities, while readers gain access to insightful, authoritative, and thought-provoking content across diverse areas of law and policy.

Now managed by Integrity Education India, Lex Scripta Magazine is committed to expanding its academic footprint through enhanced digital presence, global collaborations, and university partnerships. Upholding its ISSN identity, Lex Scripta continues to evolve as one of India's most trusted and respected journals in the field of legal research and education.

KEY FEATURES

- **Scholarly Insights** – Access in-depth, peer-reviewed research articles written by distinguished academicians and legal experts.
- **Global Perspectives** – Explore diverse viewpoints on law, policy, and governance from national and international scholars.
- **Authentic Content** – Read verified and academically sound articles that uphold the highest standards of research quality.
- **Knowledge Enhancement** – Stay updated with emerging trends, case studies, and policy developments across multiple legal domains.
- **Easy Accessibility** – Enjoy seamless access to online editions and exclusive hardcover issues for academic and professional use.

LEX SCRIPTA JOURNAL
JOURNAL MAGAZINE BY INTEGRITY EDUCATION INDIA

CONNECT WITH US 9811 666 216
7011 605 618