International Journal of Law Research, Education and Social Sciences

Open Access Journal – Copyright © 2025 – ISSN 3048-7501
Editor-in-Chief – Prof. (Dr.) Vageshwari Deswal; Publisher – Sakshi Batham

Digital Criminal Procedure in India: A Comprehensive Study of the FIR to Trial Process in District Courts

Pushkar Singh[a]

[a]Gujarat National Law University, Gandhinagar, India

Received 20 November 2025; Accepted 20 December 2025; Published 24 December 2025

India's criminal justice system has long struggled with delays, opacity, and procedural inefficiencies, particularly at the district and subordinate court level, where the bulk of criminal litigation is handled. This article examines the transformation of criminal procedure in India from a paper-driven process to a digitally enabled FIR-to-trial framework. It traces the evolution of digital criminal procedure through initiatives such as the e-Courts Mission Mode Project, CCTNS, ICJS, and statutory reforms under the Bharatiya Nagarik Suraksha Sanhita, 2023. Adopting a doctrinal and empirical approach, the study offers a stage-wise analysis of criminal proceedings, including FIR registration, investigation, chargesheet filing, cognisance, bail and remand, trial, electronic evidence, judgment, and execution. The article highlights how digital systems like CIS and NJDG have enhanced transparency, accountability, inter-agency coordination, and access to justice, while also addressing emerging challenges, including the digital divide, evidentiary compliance under Section 65B of the Evidence Act, cybersecurity risks, and uneven implementation across jurisdictions. It argues that digitalisation, while not a substitute for judicial discretion, has become a critical enabler of fair and speedy trials under Article 21. The study concludes by proposing targeted reforms to strengthen infrastructure, legal clarity, interoperability, and inclusivity in India's digital criminal justice ecosystem."

Keywords: *digital criminal procedure, district courts, trial, e-courts, bnss 2023, electronic evidence, access to justice.*

INTRODUCTION

Board Committees are essential components of corporate governance. Criminal justice is a process, not a singular event, and in India it unfolds from the First Information Report (FIR) to the final judgment. Over 53 million cases were pending nationwide in 2025, with about 47 million of them in district and subordinate courts. Subordinate courts handle the majority of these, and over 80% of pending cases there are criminal in nature.[1] This creates severe delays: decades-long pendency forces victims and accused to wait in limbo, despite the Supreme Court's rulings in *Hussainara Khatoon v State of Bihar* that a speedy trial is part of the right to life under Article 21.[2]

To overcome these challenges, India has embarked on a broad digital modernisation of criminal justice. The e-Courts Mission Mode Project (launched in 2005) has computerised almost every court complex. Under Phase I, over 14,249 district and subordinate courts were computerised. By Phase II, 18,735 courts were on the system, and 99.5% of court complexes were networked via a Wide Area Network.[3] The Criminal Procedure Code (CrPC) of 1973 was updated in 2023 by the new Bharatiya Nagarik Suraksha Sanhita (BNSS).[4] Explicitly mandating e-summons, video conferencing for hearings, strict investigation timelines, and e-FIRs. Real-time data now flows through systems like the Case Information System (CIS) and the National Judicial Data Grid (NJDG), which publishes over 32.19 crore court orders and judgments online. Innovations like e-filing, e-payments, and virtual courts have already streamlined thousands of cases. In short, technology is increasingly enabling transparency, efficiency, and accountability in the FIR-to-trial procedure.

RESEARCH METHODOLOGY

This study employs a doctrinal and empirical research approach. Doctrinal analysis draws from criminal procedure law, constitutional principles, and judicial decisions. The empirical component is based on direct field observation of criminal proceedings in district courts,

[1] Law Commission, *Report on Arrears and Backlog* (Law Com No 245, 2014)
[2] *Hussainara Khatoon & Ors v Home Secretary, State of Bihar* (1980) 1 SCC 98
[3] 'Computerization and Wide Area Network Connectivity under eCourt project' (*Ministry of Law and Justice*, 23 August 2023) <https://www.pib.gov.in/PressReleasePage.aspx?PRID=1951374&reg=3&lang=2> accessed 15 November 2025
[4] Code of Criminal Procedure, 1973; Bharatiya Nagarik Suraksha Sanhita, 2023

including exposure to court files, registry processes, and digital case management practices. These practical insights are supplemented by official data and policy materials, enabling a stage-wise analysis of the FIR-to-trial process and its digital transformation at the grassroots level.

UNDERSTANDING THE CRIMINAL JUSTICE FRAMEWORK IN INDIA

Constitutional and Statutory Foundations: The Indian criminal process is grounded in constitutional rights and statutes. Article 21 guarantees the right to life and liberty.[5] The Supreme Court has interpreted this to include a speedy and fair trial. Statutorily, the CrPC, 1973 has long governed criminal procedure.[6] In 2023, it was overhauled by the BNSS.[7] This codifies new digital procedures. Both laws prescribe each step from FIR to appeal: e.g., registering an FIR, arrest and production rules, chargesheet filing, cognisance, framing of charges, evidence and trial rules, and appeals. Most criminal trials occur in the district judiciary, including Judicial Magistrates, CJM, and Sessions Courts, which handle trials, charge framing, cognisance, and sentencing of most offences. High Courts oversee them on appeal or revision, and the Supreme Court is the court of final appeal.

Traditional Criminal Case Lifecycle (Pre-Digital Revolution): Before digital systems, a criminal case in district courts followed a paper-intensive path. First, upon receiving information about a cognizable offence, the police register an FIR under BNSS §173.[8] If an arrest is made, the accused must be produced before a magistrate within 24 hours (CrPC §57),[9] along with an arrest memo. The police then investigate: recording statements in a station diary, sending injured persons for Medico-Legal Certificates (MLCs), conducting searches, seizures (with panchnamas), and collecting evidence. After investigation (typically within 60-90 days under law), the police prepare a typed or handwritten chargesheet (§193 BNSS) detailing the offences,[10] accused, witnesses, and evidence, along with annexures like witness statements, forensic or medical reports, call data records, etc. The police submit this to the magistrate's court, which reviews it. If the magistrate finds prima facie evidence (BNSS §210),[11] they "take cognisance" and

[5] Constitution of India 1950, art 21
[6] Code of Criminal Procedure, 1973
[7] Bharatiya Nagarik Suraksha Sanhita, 2023
[8] Bharatiya Nagarik Suraksha Sanhita, 2023 s 173
[9] Code of Criminal Procedure, 1973 s 57
[10] Bharatiya Nagarik Suraksha Sanhita, 2023 s 193
[11] Bharatiya Nagarik Suraksha Sanhita, 2023 s 210

formally issue summons or warrants to the accused. The court then frames charges against the accused (CrPC §211) and conducts the trial,[12] the prosecution examines witnesses (cross-examined by the defence), then the defence can present evidence and witnesses, leading to final arguments. The court then reserves judgment; at the verdict, it reads the order in open court. If convicted, the accused is sentenced and has the right to appeal under CrPC §§374-389.[13] At each step, specific roles are assigned: the police investigate, the public prosecutor presents the state's case, and the accused may engage private counsel or a legal-aid lawyer.

Criminal Case Classification in District Courts: District criminal courts sort cases into categories with different procedures. Regular Trials (RT/RCT) handle serious offences under normal procedure. Summary Trials (ST) deal with minor offences under an expedited process. MJCR (Miscellaneous Judicial Criminal) cases cover urgent or interlocutory matters like bail applications, warrants, and petitions, domestic violence cases, etc. Each category has its own rules on procedure and timelines: for example, summary trials proceed faster, and DV cases have special forms and can be heard ex parte. These classifications affect how cases are logged and tracked in court systems, and under digital CIS, they are coded (e.g., Case registration no. code prefixes like RT, ST, MJCR, RCT, EX, etc.).

THE PRE-DIGITAL ERA: CHALLENGES IN PAPER-BASED PROCEDURE

Anatomy of Physical Criminal Files: In the paper era, every criminal case relied on physical paperwork. The FIR was handwritten in a police station register. Police kept Station House Diary entries and an investigation notebook ("rojnamcha") by hand. When the police finished investigating, they collated the chargesheet (on typed or written paper) with dozens of annexures: witness affidavits, lab reports, MLCs, seized documents or CDs, etc. These pages were often bound together with thread or clips. In court, the filing clerk maintained a physical Case File and a daily Order Sheet (roznama) for each case. Exhibits and affidavits were filed as separate papers. Evidence objects (weapons, narcotics, electronics) were listed in a Malkhana register. Any certified copies (for appeal or parties) had to be manually typed or photocopied. So, the entire life of a case existed in tangible paper or objects.

[12] Code of Criminal Procedure, 1973 s 211
[13] Code of Criminal Procedure, 1973 ss 374–389

Physical Movement and File Handling: Because everything was paper or an object, cases involved extensive physical movement. After an FIR, the police investigation file was delivered by hand to the appropriate magistrate's filing counter. After cognisance, the court would physically place the chargesheet before the trial court. At each hearing, the magistrate or judge would order the clerks to fetch the case file from the records and bring it into court for reference. After a decision, the whole file was archived in the disposal records. If there was an appeal, the old file had to be requisitioned and physically sent to the appellate court. Even when a court called for material evidence, the actual document or disc was hand-carried or formally sent. When case records had to move between agencies, for example, if a magistrate remanded an accused to jail or transferred an FIR to another police station, the file box went along. In short, every step depended on the slow, manual transport of papers and exhibits.

SYSTEMIC BOTTLENECKS AND CHALLENGES

This paper-based system created several deep problems:

Delay and Pendency: Transporting and locating files consumed massive amounts of time. Judges would often adjourn hearings just to wait for new documents to be delivered. The physical shuffling of files resulted in court staff and litigants often spending hours tracing files instead of holding hearings.

Opacity: For litigants, the process was opaque. Without visiting the court, parties could not know case updates or even the next hearing date. Courts had no online cause lists or status updates; information was only available via clerk bulletin boards or an in-person lookup of the file. Victims, in particular, often had no way to track police progress on filing a chargesheet or court orders.[14]

Risk of Manipulation and Loss: Paper records can be altered or go missing. Concerns over tampering have long existed, such as erased entries in a diary or a missing FIR sheet that could not be easily checked. Without time stamps or audit trails, it was hard to detect if someone retroactively inserted pages into a chargesheet or re-dated an order register.

[14] Law Commission (n 1)

Accountability Gaps: Tracking deadlines or duties was difficult. There was no automated alert if an investigation dragged past legal limits (e.g., 60-90 days), or if a bail hearing was overdue. Police and magistrates relied on ad hoc reminders. Even statutory requirements (like Section 193's timeline for forwarding the investigation report) were poorly monitored. In sum, the paper regime was slow, opaque, and vulnerable to error.

EVOLUTION OF DIGITAL CRIMINAL PROCEDURE IN INDIA

Genesis and Policy Framework: The shift toward digital courts began in the mid-2000s. In 2005, the Supreme Court's e-Committee issued an ICT Policy for the Judiciary and approved the e-Courts Mission Mode Project to computerise courts nationwide. Phase I (2011–2015) funded basic hardware and software in 14,249 district/subordinate courts, and later phases led to wide-area networks connected 99.5% of court complexes. A historic Phase III (2023–2027) with ₹7,210 crore funding was launched to digitise legacy records and roll out advanced features (AI tools, full e-filing, cloud repositories). These coordinated efforts sit alongside police modernisation. In 2009, the Home Ministry launched CCTNS (Crime and Criminal Tracking Network & Systems) to link all police stations. By July 2021, all 16,276 police stations nationwide were networked under CCTNS, with a centralised crime database of nearly 28 crore records. Together, these projects create a policy environment for integrated digital criminal justice.

Defining Digital Criminal Procedure: It means carrying out every step of the FIR-to-trial process electronically rather than on paper. Key elements include:

Digital FIR Registration: Victims can now lodge many FIRs online via state police portals or mobile apps. Traditional FIRs filed at a station are immediately entered into CCTNS as an "e-FIR." The new BNSS (§173(1)) explicitly recognises e-FIRs and also codifies the concept of a "Zero FIR" – allowing anyone to file an FIR at any police station regardless of jurisdiction,[15] which must then be electronically transferred to the correct station. After an e-FIR is registered, the complainant receives a reference ID and can track progress online. BNSS further requires that the FIR be read over and signed by the complainant, ensuring transparency even in digital entry.

[15] Bharatiya Nagarik Suraksha Sanhita, 2023, s 173

Investigation and Digital Case Diary: The police investigation is also digitised. Standard forms, memos, and reports are increasingly filled out on laptops or tablets and uploaded. CCTV and crime-scene photos are stored digitally. Investigators make daily entries in the case diary within CCTNS (replacing the old rojnamcha), logging recorded witness statements, evidence collected, and arrests. Senior officers can monitor cases on CCTNS dashboards to ensure investigations meet legal deadlines. Meanwhile, courts can immediately see the police chargesheet once filed. In theory, progress reports (IPRs) could be emailed directly to victims.

Chargesheet and E-Submission: Upon completing the investigation, the police prepare a digital chargesheet with scanned annexures. The physical chargesheet (if any) is still submitted at the court's filing counter, but court staff then upload the entire file into CIS. Once uploaded & scanned, the CIS creates a case file and links each scanned document to it. Police-reported data is likewise entered electronically, creating a full digital case diary. Crucially, BNSS now allows the chargesheet and its documents to be served electronically.[16] Supplying the report and annexures to the magistrate via computer is deemed "duly served". This greatly speeds up the handover from police to court.

Interoperable Criminal Justice System (ICJS): A major innovation is linking all pillars of the criminal justice system. ICJS provides secure data interfaces between police (CCTNS), e-Courts, prisons, forensic labs, and prosecution offices. For example, when a court issues a remand order or warrant, ICJS routes the order digitally to the relevant police station or jail. Similarly, when courts request forensic tests, lab requisitions can be sent over ICJS. Although full end-to-end integration is still being built, ICJS is gradually breaking down complexity by integrating FIR entry from police stations to verifying and integrating the data to the court CIS for registration of criminal cases in courts.[17]

Electronic Evidence Management: With most evidence now digital, courts must handle it accordingly. Electronic exhibits from mobile phone data, CCTV footage, emails/WhatsApp chats, and ATM CCTV clips are standard in cases. The Indian Evidence Act has evolved, and electronic records are admissible under Section 65A/B.[18] Requiring a certificate to confirm

[16] Bharatiya Nagarik Suraksha Sanhita, 2023, ss 193, 210
[17] 'Interoperable Criminal Justice System (ICJS) Overview' (*Ministry of Home Affairs*, 2020) <https://www.mha.gov.in/en/commoncontent/inter-operable-criminal-justice-system-icjs> accessed 15 November 2025
[18] Indian Evidence Act 1872, ss 65A–65B

authenticity. Courts and police have adopted IT tools as seized phones and drives are submitted in forensic labs, where experts provide reports essential for further investigation. A new e-Sakshya system allows deposition of digital evidence into CIS, and the BNSS and Evidence Act 65B certificates are regularly invoked.

Virtual Hearings and e-Summons: The COVID-19 pandemic greatly accelerated video-enabled justice.[19] Courts routinely hold bail and even substantive hearings via video conference (VC). Special applications, such as Nyaya Shruti, allow witnesses or victims to testify remotely from a local court or prison; 17 High Courts have notified rules for this purpose. New platforms, e-Sakshya for digital evidence and e-Summons, have been launched to further paperless procedures. Overall, day-to-day court business with posting cause lists, sending reminders, or recording testimony, etc., has been transformed.

KEY DIGITAL INFRASTRUCTURE COMPONENTS

India's criminal justice digital overhaul rests on major IT projects: e-Courts Services (CIS & NJDG). The Case Information System (CIS) is the core software deployed in all subordinate courts. Every criminal case now gets a unique 16-digit Case Number Record (CNR) when filed. CIS tracks every event of court proceedings against the CNR. The NJDG is a national data repository that continuously pulls case data from CIS. As of August 2025, it holds real-time information from 18,735 courts and makes over 32.19 crore orders and judgments accessible online. Litigants, lawyers, and the public can look up case status, cause lists, and even download judgments via the NJDG portal, eliminating the need to physically inspect court books.

Network Connectivity: Under the e-Courts WAN project, 99.5% of court complexes are now connected by secure high-speed networks. Courts use a mix of fibre net, MPLS, RF, and even VSAT to maintain connectivity. This backbone links CIS servers across the country. It also supports VC facilities, and by late 2025, 3,240 district court halls and 1,272 prisons will be VC-enabled, allowing judges to hear cases or conduct remands across distances.

E-Filing and e-Payments: All district courts now offer online filing portals. Over 92.08 lakh cases were e-filed by September 2025, freeing litigants from daily courtroom visits. Court fees and fines can be paid online. To help citizens, nearly 1,987 e-Sewa Kendras have been established

[19] *In Re: Guidelines for Court Functioning through Video Conferencing* Sou Motu W (Civ) No 05/2020

in court complexes, where clerks assist lawyers and self-represented parties in e-filing and obtaining e-copies.

Virtual Courts and Hybrid Models: The government set up 91 dedicated Virtual Courts (mainly for traffic/challan cases), disposing of millions of petty cases through e-hearings. The Supreme Court and high courts now routinely run hybrid courtrooms. By late 2025, over 3.81 crore online hearings had been conducted. Mobile apps have been released, e.g., the e-Courts Services App, to enable stakeholders to access case information and participate remotely. Live streaming of hearings is active in several High Courts. These advances mean that even in a crisis (e.g., pandemics), criminal trials can continue without crowding courtrooms.

Projects like ICJS &CCTNS: On the police side, the CCTNS project now covers virtually all stations. Its database feeds directly into CIS. The Interoperable Criminal Justice System (ICJS), managed by NCRB & MHA, sits as an integration layer connecting police, courts, prisons, and forensic labs. For example, when a court issues a warrant or orders a scientific examination, ICJS routes that order electronically to the correct agency. While ICJS is still being refined, it is already improving coordination and reducing "lost" cases.[20]

STAGES OF DIGITAL CRIMINAL PROCEDURE

STAGE 1: FIR Registration and Digital Investigation –

A. Digital FIR Registration: The first step in any criminal case is the FIR. Today, FIRs can be lodged online as well as offline. Many states let citizens file e-FIRs via police websites or apps (for example, Delhi Police's e-FIR portal or Uttar Pradesh's COP portal). If a victim goes to a station, the officer enters the FIR details into the CCTNS system on a computer or tablet, effectively creating an e-FIR on the spot. Under the BNSS, this e-FIR mechanism is formalised.[21] The concept of a "Zero FIR" – allowing anyone to file an FIR at any police station irrespective of jurisdiction is now codified.[22] The police are mandated to electronically transfer it to the correct station within 48 hours. In practice, once an e-FIR is registered, the complainant gets a digital acknowledgement and can check the case status online via the police portal or NJDG.

[20] 'Crime and Criminal Tracking Network & Systems (CCTNS)' (*Digital Police*) <https://digitalpolice.gov.in/DigitalPolice/AboutUs> accessed 15 November 2025
[21] Bharatiya Nagarik Suraksha Sanhita 2023, s 173
[22] Bharatiya Nagarik Suraksha Sanhita 2023, s 173(1)

Importantly, BNSS requires the officer to read the FIR back to the complainant and get it signed, ensuring that even though the record is digital, the complainant's voice and consent are captured.

B. Initial Investigation and Medical Examination: Immediately after an FIR, the police begin an investigation. The Station House Officer (SHO) must send any injured person to a hospital for a Medico-Legal Certificate (MLC).[23] The MLC is prepared on a standard form and then scanned or electronically linked to the case file. At the crime scene and upon arrest, officers fill out seizure memos, arrest memos, identification rolls, and panchnamas. These forms now have digital versions: officers often carry tablets to upload a "Crime Details Form" with scene photos. Seized items (weapons, documents, electronics) are photographed and their serial numbers logged electronically. If digital evidence (phones, hard disks, CCTV DVRs) is seized, it is tagged with a case ID and transported to a lab. All this material is scanned or entered into CCTNS so that the investigation has a digital paper trail from the start.

C. Digital Case Diary and Investigation Tracking: In many places, instead of a handwritten diary, investigators log daily progress on CCTNS. Each day's work, including the witnesses recorded, arrests made, and evidence gathered, is entered online. Supervisors can view CCTNS to see how long each case has been pending and whether it is nearing statutory deadlines. Meanwhile, courts monitor progress via CIS: once the chargesheet is filed, the court's CIS file notes it. Under BNSS, the investigating officer must inform the victim of case progress within 90 days,[24] by "any means, including electronic communication". In practice, some states email interim reports or text updates. Even though Investigation Progress Reports are still evolving, the legal mandate promotes timely updates and improves transparency in the investigation process.

D. Chargesheet Filing: From Police to Court: When the investigation is complete, the police prepare the chargesheet (BNSS §193).[25] In digital practice, this is usually typed on a computer. All annexures with witness statements, MLC reports, forensic analyses, call detail records, etc., are scanned into electronic files. Electronic exhibits (phone memory cards, CCTV DVDs) are noted, and their image outputs are attached digitally. The police then physically

[23] Code of Criminal Procedure 1973, s 53
[24] Bharatiya Nagarik Suraksha Sanhita 2023, s 193(3)
[25] Bharatiya Nagarik Suraksha Sanhita 2023, s 193

submit the chargesheet and exhibit list to the court's filing counter. Crucially, court staff immediately upload the entire chargesheet and annexures into CIS. The CIS links each document to the case CNR. From that point on, judges, prosecutors, and lawyers no longer rely on paper; they download and read the chargesheet and witness affidavits from CIS. The CIS case diary records all entries. The BNSS even permits electronic service: it states that *"supply of the report and other documents by electronic communication shall be considered as duly served"*.[26] This means the police can send the indexed chargesheet by email or portal upload directly to the court, streamlining delivery and creating a digital service record.

E. Safeguards Against False FIRs: As FIR registration becomes easier, safeguards are needed. The Indian Penal Code provides deterrents: Section 182 (providing false information to a public servant) and Section 211 (false charge of offence) punish frivolous or malicious FIRs. In practice,[27] Officers inform complainants of these penalties when registering e-FIRs. Many police apps also have a grievance mechanism: if an e-FIR is wrongfully rejected, a victim can appeal to higher police authorities. Nonetheless, misuse remains a concern that states must address through public awareness and monitoring.

STAGE 2: From Chargesheet to Cognisance in Digital Courts –

A. Digital Case Registration and CNR Generation: Once the court receives the police chargesheet ("challan"), the clerk registers the case in CIS. The clerk enters the parties' names, offences, and police station details into CIS. The system then generates a unique Case Number Record (CNR) – a 16-digit code encapsulating state, district, court, and year (for example, *MP04013645632025*). CIS uses case-type codes (RT, ST, MJCR, EX, RCS, MACT, etc.) and sequential numbers to form this ID. From this point, the case is fully digital; every subsequent entry (bail orders, hearing dates, judgments) is linked to the CNR. The newly registered case immediately appears on the court's digital roster, allowing judges and litigants to see it listed online.

B. Digital Case Allocation: District courts typically use a computerised roster to distribute new cases to judges by random or sequential assignment. In practice, CIS performs this step after registering a case; the system automatically allocates it to an eligible magistrate or sessions

[26] Bharatiya Nagarik Suraksha Sanhita 2023, s 193(5)
[27] Indian Penal Code 1860, ss 182, 211

judge as per the court's roster rules. The assigned judge's CIS dashboard immediately shows the new case. The judge's clerk then fixes the first hearing date in CIS. Because this process is digital, it generates an audit trail (time of allocation, names of officer/judge, etc.) and prevents manual misassignment or bias.

C. Filing Counter and e-Seva Kendra: The court filing counter remains the entry point for the police and parties. The public prosecutor or police personnel submit the printed chargesheet and annexures to the counter. Simultaneously, the clerk uploads scanned copies to CIS. Court fees (if any) can be paid via e-payment kiosks that connect to CIS. Co-located with the filing counter is often an e-Sewa Kendra. There, trained staff assist litigants & parties explaining digital procedures, helping advocates e-file applications through the portal, print certified electronic status reports from CIS, and generate receipts or cause lists. In short, even the act of filing the challan is tracked digitally as CIS logs when and by whom each document was received.

D. Taking Cognisance under Section 210 BNSS: After registration, a magistrate must "take cognisance" of the offences in the chargesheet.[28] In the digital era, the magistrate reviews the scanned chargesheet and annexures on screen, rather than leafing through a file. If satisfied, there is prima facie evidence, and the judge records a cognisance order after scrutiny in CIS. CIS can generate an e-Warrant and transmit it to the police via ICJS. The first hearing date gets set in CIS. The order-sheet entry naming the offences and issuing summons/warrants is typed by the clerk into CIS and digitally signed by the judge, along with a physically printed order sheet.

STAGE 3: Arrest, Bail, and Remand in the Digital System –

A. Arrest and Production Before the Magistrate: When police arrest someone for a cognizable offence, they still must obey the 24-hour rule (CrPC §57) of bringing the accused with a written arrest memo before the magistrate within a day.[29] Digital tools aid this compliance. Modern lock-ups maintain an electronic Arrest Register where details of each arrest (time, grounds, identity) are entered in real time. For the remand hearing, police send the electronic arrest memo to the court through ICJS, and the magistrate can pull it up in CIS as evidence of lawful arrest. If the accused has injuries or health issues, the hospital's report (scanned) is also accessible via CIS. CIS dashboards alert courts if the 24-hour deadline is missed, making late

[28] Bharatiya Nagarik Suraksha Sanhita 2023, s 210
[29] Code of Criminal Procedure 1973, s 57

production obvious. All in all, technology has tightened the coordination between police lock-ups and courts in arrest cases.[30]

B. Digital Bail Proceedings: Bail hearings and orders are now largely conducted and recorded in CIS. An accused or a lawyer can submit a bail application by filing a CIS e-form from jail or by typing it in court. Once a bail application is on record, CIS flags it so the judge sees pending bail cases on his screen. When bail is granted, the surety and PR bonds are often generated from CIS templates, and the judge or clerk prints the bond forms, the accused and his surety sign them, and the CIS records are updated. The bail conditions (personal bond amount, surety details, obligations) are entered into CIS. Crucially, upon granting bail, the CIS instantly notifies the police station and jail through ICJS, so the accused can be released promptly. Attendance of the accused is then tracked via CIS roll-calls. If the accused petitions for exemption from physical appearance (under BNSS §355),[31] that application and the court order on it are processed in CIS as well. Thus, almost all paperwork for bail, from application to printing of bonds to entry of orders, is handled via the digital case files along with physical records.

C. Digital Remand Proceedings: Remand applications (for police or judicial custody extension) are also made digital. When police seek custody of an accused, they file the remand application in CIS. The magistrate can summon the accused on VC (e.g., via "Sakshi" prison video-link) if distance is an issue. The judge enters the remand order into CIS (specifying days of custody, etc.) and electronically sends it back through ICJS to the police and jail. CIS updates the accused's custody status (e.g., "in judicial custody"), which both police and prison can see. Digitally, remand is a seamless, tracked process: the application, the electronic connectivity, and the resulting order all live in the electronic case record.

D. Digital Order Sheets (Roznamas): Throughout these hearings, the judge's notes and interim orders are now recorded in CIS rather than on handwritten sheets. A clerical assistant types a summary of each proceeding of what was decided directly into the CIS Order Sheet. Adjournments and reasons are logged. In many courts, judges can even dictate their orders into an e-filing interface or use speech-to-text. As a result, every court event is time-stamped in the

[30] *Arnesh Kumar v State of Bihar & Anr* AIR 2014 SC 2756
[31] Bharatiya Nagarik Suraksha Sanhita 2023, s 355

digital diary. Litigants can obtain electronic extracts of these order sheets as certified copies. Overall, the digital order sheet dramatically improves accountability as anyone can later review exactly what happened at each hearing, without deciphering heavy notes.

STAGE 4: Digital Trial and Evidence Recording –

A. Framing of Charges: Once cognisance is taken, the first act of trial is framing charges.[32] In court, the magistrate reads the formal charges to the accused. In a digital court, the charges are prepared. The clerk or judge enters the charges into the CIS template, which generates a formal charge sheet. The judge ensures the accused understands and asks him to plead. That exchange is noted in CIS. If the accused pleads not guilty, the case proceeds to evidence. (If he pleads guilty, the court may convict summarily.) The final framed charges document is saved in CIS, and a certified copy can be printed for the defence at once.

B. Statement of the Accused (under §313 CrPC): After the prosecution's evidence, the judge must record the accused's statements on the prosecution's case.[33] In a digital trial, the judge consults the CIS file (witness testimony, entries) while questioning the accused. The accused's answers are typed directly into CIS as part of the case record. If the accused submits a written explanation of non-guilty, it is scanned and uploaded to CIS. Thus, the accused's own statement and its discussion remain in the searchable digital file. The court ensures that whatever the accused says is promptly logged in the system.

C. Prosecution Evidence: The Public Prosecutor (State) examines witnesses (e.g., PW-1, PW-2, etc.). In most modern courts, this examination-in-chief is recorded live in CIS: a court stenographer or operator types the questions and answers as they happen. In some places, audio of the session is recorded, and software transcribes it. After each direct examination, defence counsel cross-examines, which is likewise entered into CIS in real time. When an exhibit (e.g., a document or photo) is presented, the clerk quickly scans it (if not already uploaded) and tags it in CIS, linking it to the witness who identified it. Witnesses now digitally sign their deposition on an e-pad or provide fingerprints, after which the CIS marks their testimony as complete. This way, at any moment, anyone can open CIS and see exactly what PW-1 said on examination, what he was asked on cross, and what exhibits were proved through him. All depositions become text

[32] Code of Criminal Procedure 1973, ss 211–214
[33] Code of Criminal Procedure 1973, s 313

within CIS, searchable by keyword. The digital recording greatly increases accuracy (no illegible handwriting) and speeds up the preparation of certified transcripts.

D. Defence Evidence: If the accused elects to call defence witnesses (DW-1, DW-2, etc.),[34] the process is symmetric. The court enters the direct examination of defence witnesses and any prosecution cross-examination into CIS live. Any documents the defence tries to mark (e.g., character references, alibi proofs) are scanned and indexed. If the accused himself gives evidence or makes a statement, that is typed in. CIS treats defence materials the same way as prosecution evidence. This ensures the defence case is equally well-documented and integrated in the digital record.

E. Final Arguments and Judgment Reserved: After the evidence, both sides make final submissions. Many courts now encourage written arguments so the judge can review them. If arguments are oral, the gist is logged in the CIS order sheet by the clerk. Once arguments end, the judge formally "reserves judgment" and marks the case as such in CIS. At this stage, CIS may "lock" the file to prevent further changes. When the judge is ready to pronounce judgment, the final order is typed into CIS as an official judgment or order. This document is digitally signed by the judge and added to the case record. Instantaneously, the system can issue certified copies of the judgment to the parties. The court also uploads the judgment text to e-courts or NJDG. In summary, from framing charges through the verdict, every question, answer, and ruling is systematically captured in CIS.

ELECTRONIC EVIDENCE AND SECTION 65B OF THE EVIDENCE ACT

A. Nature and Types of Electronic Evidence: Modern trials routinely involve electronic evidence. Examples include: text and instant messages like WhatsApp chats, SMS logs, emails, social media posts, call detail records, and location (GPS) logs from telecom providers, CCTV and dashcam videos, voice recordings, and data from seized devices (smartphones, laptops, SIM cards). Investigators often extract digital data using forensic labs (e.g., recovering chat logs from a phone). Even things like online bank statements or computer-generated documents are produced. All these are "electronic records" as defined in the Evidence Act. Recognising this, Sections 65A and 65B of the Indian Evidence Act (introduced in 2000) establish rules for

[34] Code of Criminal Procedure 1973, s 233

admitting computer-generated evidence. In effect, almost any fact that can be proved by digital data, from a photo to an email to a database entry, is now admissible if properly certified.[35]

B. Admissibility of Section 65B Certificate: It generally governs the admissibility of electronic records. It mandates that secondary electronic evidence must be accompanied by a 65B certificate attesting to its authenticity. The Supreme Court has emphasised that 65A/65B "fully governs" electronic evidence. In *Arjun Panditrao Khotkar v State of Maharashtra* (2020),[36] the Court held that Sections 65A and 65B override other Evidence Act provisions for digital records, and a 65B(4) certificate is mandatory whenever the original electronic device (computer, phone, DVR) cannot be produced.[37] In practice, this means that whenever police submit, say, a pen-drive extract or a CCTV DVD, they must also submit a signed certificate confirming that the device was working and the data is genuine. Thus, for digital trials to succeed, police and lawyers must meticulously follow these technical rules.

C. Challenges in Electronic Evidence: Electronic evidence also brings new challenges. The court scrutinises the chain of custody closely, so that it must see exactly how each digital device was seized, transported, forensically imaged, and stored, to guard against tampering. Forensic labs typically use methods (hashing, write-blockers) to prove a copy is identical to the original, but defence lawyers sometimes still question these procedures. The volume of data is another issue, as judges must decide which parts of a long video or thousands of messages are relevant. Moreover, awareness of technical pitfalls is uneven. For instance, mistakes in a 65B certificate can render key evidence inadmissible. Finally, digital records raise privacy concerns. Hacking incidents such as the July 2025 NCLT disruption, where a hacker broadcast obscene content during a hearing, show that video links and databases can be vulnerable.[38] Courts must therefore balance the use of digital technology with the protection of confidentiality; secure networks, encrypted evidence files, and strict access protocols are essential.

[35] Indian Evidence Act 1872, ss 65A–65B
[36] *Arjun Panditrao Khotkar v State of Maharashtra* AIR 2020 SC 4908
[37] Indian Evidence Act 1872, s 65B(4)
[38] Dwaipayan Ghosh, 'Breach in cyber security disrupts NCLT hearing' *Times of India* (04 August 2025) <https://timesofindia.indiatimes.com/city/kolkata/breach-in-cyber-security-disrupts-nclt-hearing/articleshow/123081457.cms> accessed 19 November 2025

DIGITAL INFRASTRUCTURE AND SUPPORTING DEPARTMENTS IN DISTRICT COURTS

A. Computer Section: Every district court complex now has an IT Cell or Computer Department. Its staff maintains the core infrastructure: servers, network switches, desktop PCs, printers, scanners, and the CIS software. They provide technical support day-to-day, for eg, if the CIS server goes down or a judge's digital signature token expires, the IT cell troubleshoots it. They also set up and run the court's video-conferencing hardware (cameras, mics, VC software), for instance, enabling Nyaya Shruti rooms for witness testimony. Clerks from IT update the court's website: uploading daily cause lists, filing digital judgments, and sending email/SMS notices. The Computer Department manages (accounts, passwords, security) of domains and accounts used for coordination in courts. In short, without this team, the digital systems would collapse. They are the backbone that keeps CIS, e-filing, and VC running reliably in every court.

B. Copying Section: It has traditionally handled all applications for certified copies of case documents. In the digital era, its work is simplified but still vital. Since every order and judgment is digitised in CIS, clerks in the copying section simply retrieve the requested documents from the CIS archive rather than searching physical files. Copy requests can be queued and tracked in CIS. Applicants can pay copy fees online, and the system generates electronic receipts. When a judgment is pronounced, its text is already in CIS, so copies can be printed immediately. Many copying sections now send SMS alerts when copies are ready. Even for RTI or appeal purposes, copy clerks search the CIS to find case data. Thus, digitisation has sped up the supply of certified copies and reduced transcription errors.

C. Malkhana: It is the evidence locker that holds all physical exhibits in criminal cases, like weapons, narcotics, mobile phones, cash, etc. Traditionally, every deposit or withdrawal had to be noted by hand. Now, many courts maintain a digital malkhana register (often integrated into CIS). When items are seized, the police or court label them and enter key details (type, value, serial no.) into the digital record. High-value or sensitive items (pistols, large cash sums) are kept in double-locked vaults and also logged electronically. Electronic items meant for forensic analysis are noted by their device IDs, IMEI no, and chains of custody are tracked in the system. When a judge orders a material to be produced as evidence, the malkhana officer can quickly

identify and retrieve it using the digital index. Releases of exhibits (e.g., returning property to owners after trial) are also recorded with dates in CIS.[39]

D. Record Room: After a case is disposed of, its paper case file is sent to the court's Record Room. Final orders and judgments are scanned into the digital archive before filing away the file. CIS automatically indexes disposed cases (with file number, parties, judge, disposal date). If an appeal is filed, the appellate court clerk can send an e-request via CIS to requisition the lower court's file. The record-room staff then fetches the physical file number from CIS and delivers it. Courts are increasingly allowing searches of disposed case indexes via the NJDG. Thus, although the stored files remain physical, their existence and contents are reflected digitally. This hybrid setup means that retrieving an old file requires less manual searching.

E. Nazarat Section: The process-service section issues and serves all court processes: summons, warrants, attachments, notices, etc. In the digital system, many of these tasks are automated by CIS.[40] For example, when the judge directs a summons to an accused, CIS creates an e-summons and dispatches it via email or SMS; it also prints a summons slip for the police to serve to the parties. CIS tracks who was served or not. If a non-bailable warrant is issued, the court sends it electronically through ICJS to the relevant police station, and the police updates CIS on its execution (arrest made or not). Court bailiffs use CIS to know which documents or attachments need dispatch (e.g., sending a forensic report to a medical board). In short, the Nazarat wing now uses CIS schedules and alerts to know which processes are due. This significantly cuts down the old "paper chase" of manually sending memos to station houses.

DIGITAL PROCEDURE IN SPECIAL CRIMINAL CASES

A. Domestic Violence Cases: Cases under the Protection of Women from Domestic Violence Act (2005) are handled via special summary procedures,[41] often in courts labelled MJCR-DV. These hybrid cases have both civil and criminal aspects. A DV case can begin when an aggrieved person (usually a woman) files a written application or Domestic Incident Report (DIR) alleging violence.[42] Police now allow registration of DIRs electronically in some states. Protection Officers (government-designated), NGOs, or relatives can assist in drafting the complaint in the

[39] *Sunderbhai Ambalal Desai v State of Gujarat* AIR 2003 SC 638
[40] Code of Criminal Procedure 1973, ss 61–90
[41] Protection of Women from Domestic Violence Act 2005
[42] Protection of Women from Domestic Violence Rules 2006, r 5

prescribed format. Upon receiving a DIR, a magistrate must issue notice to the respondent (abuser) immediately. In practice, the court registers DV cases in CIS as "MJCR" Orders (interim protection, residence, or maintenance orders) that are drafted electronically. Because DV proceedings allow rapid relief (even ex parte protection orders), courts often expedite them digitally: CIS triggers fast hearings. Video conferencing is sometimes used so that vulnerable victims need not face the abuser in court. Crucially, DV victims can track their case status online and receive digital copies of orders, which helps enforce these sensitive proceedings.

B. Compounding of Offences: Certain offences (e.g., simple assault, defamation, certain property disputes) are compoundable by agreement of parties.[43] When a victim and the accused decide to reconcile, they submit a written compromise deed to the court. Today, this deed is usually prepared electronically and uploaded to CIS. The judge, upon reviewing it, compels the accused to plead to the compounding as per the law. If accepted, the court passes an order discharging the accused and closing the case. CIS immediately marks the case as disposed of by compounding. If the accused had been in custody, CIS notifies jail authorities for immediate release. The digital record now clearly shows the date of compounding. This transparency prevents confusion later about whether the case was truly settled or incorrectly thought to be dismissed. The ease of electronic filing makes mutual settlements smoother, and summary compounding orders can be issued within hours in some instances.

C. Lok Adalats in Criminal Matters: They offer an alternate dispute resolution route for compoundable criminal cases. In recent years, e-Lok Adalats have been launched.[44] Here, courts or legal services authorities upload lists of pending compoundable cases onto an online portal before the Lok Adalat session. During a Lok Adalat, which can occur either physically or virtually, parties negotiate and settle their disputes. If a settlement is reached, the terms are entered into a digital Lok Adalat award form, which the officers then upload to the NJDG system as a final judgment. Even fines or compensation agreed in Lok Adalat are collected via e-payment and reflected in the digital record. By integrating Lok Adalat settlements into the ICT system, cases get disposed of in a paperless manner and are immediately transparent to all stakeholders.

[43] Code of Criminal Procedure 1973, s 320
[44] Legal Services Authorities Act 1987, ss 19–21

ACCESS TO JUSTICE: LEGAL AID AND VICTIM SUPPORT

A. District Legal Services Authority (DLSA): The state-funded DLSA provides free legal aid and victim compensation.[45] DLSAs increasingly use digital tools to reach beneficiaries. Many DLSAs have online portals or social media hotlines to register complaints and guide the poor. In some districts, a victim or accused can apply for aid by filling out an online form; the DLSA then assigns an advocate from its panel through CIS. Web conferencing rooms in court premises are often reserved for legal-aid clients to confer with their lawyers remotely. The DLSA also uses messaging apps to disseminate information on legal rights. Each legal-aid case is tracked in CIS so that the court can automatically compute free copies or fee waivers.

B. Legal Aid Defence Counsel (LADC) System: Under Article 39A and relevant schemes,[46] states must provide lawyers for indigent accused. Digital systems have streamlined this, too. Advocates register on National/State Legal Services Authority (NALSA/SLSA) portals. Once a court deems an accused eligible for free counsel, CIS pulls from that panel and assigns a specific LADC to the case, only entitled to give aid in criminal cases introduced in the NALSA(Legal aid defence counsel) Scheme, 2022.[47] It highlights the LADC board comprising the Chief LADC, 3 Deputy LADCs, and 8 Assistant LADCs in every DLSA. (or as prescribed by the concerned High Court). The assigned counsel receives the case CNR and can access the digital file online, enabling them to prepare effectively. This automation helps ensure no eligible accused is deprived of representation, since CIS will flag unrepresented indigents.

C. Victim Compensation Scheme: Criminal law mandates state compensation for victims (BNSS §396).[48] Today, most states operate online compensation portals. A victim (or guardian) submits a claim form digitally, attaching scanned FIRs, MLCs, and bills. The district compensation board processes it, and once approved, the funds are released via DBT to the victim's bank account. All filings and sanctions are tracked on the portal. Emergency relief (for rape or acid attacks) can be sanctioned very quickly,[49] As courts can direct interim relief by emailing the state's legal services authority. Digital disbursement ensures victims get prompt

[45] Legal Services Authorities Act 1987, ss 6–10
[46] Constitution of India 1950, art 39A
[47] National Legal Services Authority, *Legal Aid Defence Counsel Scheme 2022* (2022)
[48] Bharatiya Nagarik Suraksha Sanhita 2023, s 396
[49] *Laxmi & Ors v Union of India & Ors* (2014) 4 SCC 427

financial aid without chasing cheques, and they can monitor payment status online. In short, ICT has made it easier for victims to access their entitled compensation.

POST-TRIAL PROCESS: JUDGMENT, APPEALS, AND EXECUTION

A. Judgment and Sentencing: After the verdict is pronounced, the judge prepares the final judgment text digitally. The court's decision (acquittal or conviction with sentence) is entered as the final order in the CIS diary. The judgment is then uploaded to CIS and often to the state's e-Court website. CIS can automatically send SMS/email notifications to the lawyers and parties (if their contacts are in the record). Simultaneously, the system generates a certified copy of the judgment for distribution. In many courts, judges use digital templates that auto-fill legal citations and standard sentencing language, reducing typos. Once finalised, the judgment is immediately accessible on NJDG. Litigants and lawyers can download or print it on demand, eliminating delays from manual transcription.

B. Appellate Hierarchy: If the verdict is appealed, digital procedures ease the process. From a magistrate's trial, a conviction appeal is filed in the Sessions Court via CIS e-filing (if available). The subordinate court's digitised record can be transferred electronically to the High Court under the E-CRBA (E-Court Records and Books Archive) project. In high courts, appeals from sessions or from high court convictions can often be e-filed on the state or national portal, and hearing notices are sent digitally. Likewise, the Supreme Court's Special Leave Petitions (SLPs) can now be filed online. Some appeals hearings proceed by video link, especially during emergencies. Overall, lower court records now feed into a digital chain: appellate judges often receive scanned trial documents on their terminals before arguments, speeding up case transfer.

C. Free Supply of Documents: The law entitles an accused convicted and seeking an appeal to free certified copies of relevant documents.[50] Digitalisation has made compliance easier. CIS can generate the exact set of documents (chargesheet, depositions, exhibits, etc.) electronically for the accused at no cost. In many courts, there is a "free copy" portal linked to CIS: an accused or his lawyer logs in, and CIS immediately provides password-protected downloads of the case

[50] Bharatiya Nagarik Suraksha Sanhita 2023, s 230

file. There have been no more complaints of missing pages in free copies, since the entire record is the same digital master file.

D. Execution of Sentences: Once a conviction is final, courts issue a warrant of conviction, which is digitally signed in CIS. This order goes via ICJS to prison authorities, who update their jail database with the inmate's new status. The sentencing entry is automatically added to the person's prison record. For fines or compensation orders, the court's e-pay module can process the transactions and track them. If an accused is sentenced to imprisonment, CIS can update the period and location (e.g., District Jail, Prison) to the national prison database. Subsequent parole or remission applications are now often filed online, and prison records on good behaviour can be electronically verified. Even probation or bond conditions are entered in CIS, and notification is sent to the probation office. In essence, from convict to jailor, the outcome flows, reducing errors in enforcement.

CRITICAL ANALYSIS: ACHIEVEMENTS AND GAPS

A. Key Achievements of Digitalisation: India's digital FIR-to-trial overhaul has delivered palpable gains. Transparency has vastly improved. The NJDG's public portal lets parties check case status at any time. A victim can now log in and see that the chargesheet is filed, or that a hearing is scheduled, instead of wandering court halls. This audit trail across agencies has strengthened accountability, as any official can see timestamps of FIR entry, chargesheet submission, remand orders, etc. Risk of tampering has fallen. Every police report and court order carries a date-and-time stamp in the digital record; altering it later would leave a visible trace. The speed of communication has soared, summons and warrants zip to the police in seconds via ICJS rather than days by courier. Judicial management is more data-driven, and administrators use e-Courts dashboards to spot judges with high pendency or cases nearing time norms. Importantly, the pandemic-proven resilience with over 3.8 crore virtual hearings held by late 2025 demonstrates that justice can proceed even under lockdowns. Coordination among agencies has improved, too: police, courts, and prisons see shared data, so fewer cases "fall through the cracks." The World Bank even praised India's NJDG in its Ease of Doing Business report for making case records more accessible. In short, what was once an opaque paper maze is now largely a visible, networked workflow, delivering a more accessible and timely justice system.

B. Emerging Technologies in Criminal Justice: In addition to core digitalisation of court processes, recent legal scholarship highlights the growing use of emerging technologies such as artificial intelligence, facial recognition systems, and secure digital evidence management tools within the criminal justice framework. These technologies function primarily as procedural enablers, assisting investigation, legal research, translation, and evidence handling, without displacing judicial discretion.

Artificial intelligence tools are increasingly used for data aggregation, legal research support, and language translation, while facial recognition systems are being explored by law enforcement agencies for identification and investigative purposes. Similarly, scholarly discourse has examined the potential of tamper-resistant digital audit mechanisms, such as blockchain-based evidence logs, to strengthen chain-of-custody compliance and electronic evidence integrity under Section 65B of the Indian Evidence Act.[51]

PERSISTENT CHALLENGES

Despite progress, significant gaps remain. Digital Divide: Many rural or small-town courts still struggle with weak infrastructure. Even with 99.5% connectivity, the remaining unconnected or intermittently connected courts (100s of complexes) face disruptions. Outdated PCs or printers can halt proceedings. On the user side, a digital divide persists: many lawyers, parties, and witnesses lack familiarity with CIS or do not have personal internet access. Language barriers exist since much software is in English or Hindi by default, disadvantaging speakers of other regional languages. Marginalised litigants (the poor, elderly, and disabled) may depend on e-Seva kiosks or law-help desks to navigate the system.

A. Legal and Procedural Issues: The procedural code has only recently begun to accommodate e-justice. For example, there is no comprehensive law explicitly defining how an e-summons is served, or how exactly digital signatures should be treated in every context. Some courts still hesitate to fully accept e-documents without paper backups. Electronic evidence rules remain in flux as many police are still uncertain about 65B certificates, leading to occasional rejections of critical digital evidence. Training has lagged as some judges and clerks use old

[51] Kamakshi Tiwari, 'Digital Revolution in Criminal Procedure of India: An In-depth Examination of the Impact of Emerging Technologies' (2025) 6(6) International Journal of Law Management & Humanities <https://ijlmh.com/wp-content/uploads/Digital-Revolution-in-Criminal-Procedure-of-India.pdf> accessed 19 November 2025; Indian Evidence Act 1872, s 65B

habits (e.g., insisting on physical files when CIS is available) due to a lack of comfort with the new tools.

B. Security and Privacy: Cyber threats are real. High-profile breaches have exposed vulnerabilities. For instance, in July 2025, hackers infiltrated a video hearing of the NCLT (Kolkata) and broadcast obscene content, forcing the tribunal to suspend all virtual sessions.[52] Similar intrusions have occurred in other courts. These incidents highlight that many court networks lack robust encryption and access controls. Data privacy is another concern as sensitive information (witness statements, medical details, personal data) stored in CIS must be protected under India's new Digital Personal Data Protection Act.[53] But standard cybersecurity protocols (regular audits, two-factor login, intrusion detection) are not uniformly enforced across states.

C. Interoperability Shortfalls: The ideal of a seamless ICJS is not yet fully realised. State police databases and court CIS systems sometimes use differing software versions or formats, requiring manual reconciliation. For example, a chargesheet filed on one police software may not auto-populate the court's CIS until clerks manually upload it. Legacy data migration is incomplete as older cases (filed before e-Courts) are not fully digitised in many regions, meaning the NJDG may lack historical data. Likewise, prison management systems are variably digital. Until truly "single sign-on" integration is achieved, some silos will remain.

In sum, while technology has transformed processes, uneven implementation and policy gaps mean its benefits are not yet universal. The promise of e-justice, faster, fairer trials, will only be fully realised when every stakeholder, from rural litigants to senior judges, is on board and protected by sound rules and infrastructure.

RECOMMENDATIONS FOR STRENGTHENING DIGITAL CRIMINAL PROCEDURE

A. Legislative and Policy Reforms: India should update its laws for the digital age. For example, a *Digital Criminal Procedure Code* could explicitly authorise e-services of summons/notices, define valid electronic signatures, and lay out how e-filing works. Section 65B of the Evidence Act could be clarified or relaxed.[54] For instance, a provision to accept digital evidence without a certificate if strong metadata or a forensic hash proves authenticity. Laws

[52] Ghosh (n 38)
[53] Digital Personal Data Protection Act 2023
[54] Indian Evidence Act 1872, s 65B

should officially sanction practices accelerated by COVID (e.g., video conferencing for all bail and remand hearings, e-appeals). A national policy or a Model Court Rule could mandate uniform e-Courts standards and data protection across all states. Importantly, the integration of systems (ICJS) should have a legal mandate so that police, courts, prisons, and labs are required by law to interlink their databases.

B. Infrastructure Development: Every district court must be fully equipped to go digital. This means reliable high-speed internet (fibre or satellite as backup) and uninterrupted power (UPS and generators) in all courts, including rural outposts. Hardware systems like PCs, servers, and cameras should be regularly refreshed; no courtroom should rely on a single server or an old 32-bit computer. Each courtroom needs a stable video conferencing setup (cameras, mics, a large screen) and at least two terminals for judges or parties. Crucially, there must be round-the-clock IT support, and every circuit or cluster of courts should have dedicated technicians to fix problems immediately. For litigants, courts should provide public terminals or kiosks (e.g., through e-Mitra booths) where one can check case status or file simple forms. The e-Courts project can assist by bulk-procuring and distributing hardware to under-resourced courts. In short, digital mode must be as robust as physical without solid infrastructure; even the best software will fail.

C. Capacity Building: Human capacity is the linchpin of success. All judges, clerks, and lawyers must be trained to use the new systems. This requires regular, hands-on workshops at the district level. Every new judicial officer should have an induction program on CIS and e-justice before taking charge. Existing judges and staff need periodic refresher courses and helpdesks. Training should be practical (e.g., how to upload an order in CIS, how to extract witness transcripts) and ongoing, not one-off. Digital "champions" or e-court coordinators at each court can mentor others. The e-Committee's training with 322,740 participants by 2024 is a start,[55] but local mentoring will ensure continuous support. For lawyers and litigants, governments and bar councils can run awareness camps (also in local languages) on e-services, cause-list apps, and e-filing. User manuals, FAQs, and helplines should be prominently available on court websites. Finally, all system interfaces must be multilingual and accessible for screen-readers for the visually impaired, etc., so that no one is disenfranchised by technology.

[55] Supreme Court of India e-Committee, *Training and Capacity Building Statistics* (2024)

D. Access and Inclusivity: To truly serve "justice for all," digital courts must include everyone.[56] Websites and apps should be translated into major regional languages and designed for low literacy (with icons or audio prompts). For litigants without personal devices, courts can station volunteer advocates or law students in courthouses to help file e-FIRs or e-appeals on behalf of the needy. DLSAs and NGOs should equip community centres with internet kiosks for victims to check case status.[57] The Saksham e-Courts helpdesk should be widely publicised so that anyone confused by e-filing can get prompt guidance. Courts can also allow assisted e-filing, for example, physically taking an e-form template from a party and filing it online on their behalf. Ultimately, technology should amplify access, not become a new barrier for the marginalised.

E. Integration and Interoperability: Full end-to-end integration is the goal. All states should standardise on compatible software stacks or at least APIs so that a police charge automatically populates the court CIS case entry. A nationwide case ID (beyond the CNR) could be introduced to link police FIRs, court cases, and prison files. Prison management systems, forensic lab trackers, and prosecution portals should likewise feed into CIS through ICJS. Eventually, one should be able to pull up the entire history of a crime from FIR, chargesheet, bail history, judgment on one portal via the case ID. Achieving this requires state and central coordination so that interoperability does not get bogged down in technical silos.

F. Security and Accountability: As justice goes digital, it must be made secure. Court data should be encrypted at rest and in transit. System logins should use strong multi-factor authentication for officials (e.g., passwords). Each access to case records should be logged, preventing unauthorised lookups. Courts should establish routine cybersecurity audits to patch vulnerabilities. Special care is needed for VC links with encryption, and waiting rooms must be enabled so that only authorised persons enter hearings. New technologies might help, for example, blockchain-based audit trails for evidence chains could make tampering virtually impossible. The government should also finalise a uniform data retention and deletion policy (e.g., expunging judicial records in acquittal cases as mandated, and ensuring the expungement is done in CIS/NJDG). Finally, all court staff must follow clear privacy protocols, and personal devices should not store case data outside the secured network; official data-sharing must

[56] Constitution of India 1950, art 39A
[57] Legal Services Authorities Act 1987

comply with the Digital Personal Data Protection Act. In the end, as courtrooms become virtual, building trust and safeguarding rights must remain paramount.

CONCLUSION

India's move from a paper-based criminal justice system to a digitally driven FIR-to-trial process is a major step toward improving justice delivery. As this study shows, digital tools have changed how criminal cases are handled at every stage, from FIR registration to judgment. Systems like CIS, NJDG, CCTNS, and ICJS have made court processes more transparent, easier to track, and better coordinated. This impact is most visible in district courts, where the majority of criminal cases are decided. By reducing delays and increasing accountability, digitalisation has begun to support the constitutional promise of a fair and speedy trial under Article 21.

At the same time, digital criminal procedure is still evolving. Problems such as uneven infrastructure, limited technical training, mistakes in handling electronic evidence, and cybersecurity risks remain. Addressing these challenges requires clearer legal rules, better training for court staff and lawyers, and systems that are accessible to all litigants. If technology is used carefully and supported by strong safeguards, it can strengthen trust in the justice system and help ensure that criminal justice in India becomes faster, fairer, and more accessible for everyone.