



E-FIR Frameworks and Access to Justice: A Comparative Analysis of India and Nepal

Akshay Chudasama

Unitedworld School of Law

akshaysinhchudasamaphd@gmail.com

<https://orcid.org/0009-0000-7460-2854>

Jim Cherry

Catholic University of America: Washington, District of Columbia

jimcherry1972@gmail.com

<https://orcid.org/0009-0000-2275-6165>

Corresponding Author*

Received: May 22, 2026

Revised & Accepted: July 25, 2026

Copyright: Author(s) (2026)



This work is licensed under a [Creative Commons Attribution-Non Commercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/).

Abstract

Background: The FIR is the first step in criminal justice system, and a crucial path towards justice. Due to the issues of complaints not being lodged with police due to discretion, geographical constraints and time lag in the process, as well as the refusal to lodge complaints in the past, India and Nepal have introduced digital platforms to register complaints and an electronic FIR (e-FIR) system. It's not yet clear whether these reforms have been successful, though.

Data Collection: The method used in collecting data for this research is integrated method of data collection, namely comparative doctrinal method and quantitative method. The doctrinal aspect focuses on the legal frameworks, judicial rulings, law reforms reports and official digital-policing tools in India and Nepal with regards to the registration of e-FIRs. The quantitative part involved a pre-designed Google Form survey of the respondents in Ahmedabad, Dhrangadhra and Gogha to gauge their awareness, accessibility, usability, transparency and public confidence about e-FIR.

Findings: India has a robust constitutional and statutory need to register FIRs but this study suggests that there are gaps in the process – procedural gatekeeping, need for physical verification, lack of single digitized infrastructure and difficulties in electronic complaints being converted into FIRs. While the legal system is less developed in Nepal than in other



countries, digitalization has made the system more citizen-friendly by allowing complaints and complaint tracking to be done electronically, making it more transparent and accessible.

Conclusions: The study finds that an electronic complaint cannot be realized as a "pure" statutory act. Key components of a successful e-FIR system include digital verification, clear procedures, accountability, accessibility, and safeguards for mandatory complaints to be registered. The study is a novel comparative and mixed methods approach that incorporates a doctrinal understanding of the provisions for legal protection but also explores empirical evidence on the perceptions of the public and the impact of digital policing on legal protection and access to justice in India and Nepal.

Keywords: Access to Justice, Accountability, Criminal Procedure, Digital Policing, e-FIR, Transparency.

1. Introduction

1.1 Access to Justice in India

One of the primary stages in South Asian criminal justice system is called the First Information Report (FIR). An FIR is the initial step on the path of the state's investigation and prosecution of a crime and the first time that a citizen can intervene and the first time that the state provides constitutional protection to the complainant. Post-colonialism - both in India and in Nepal - created administrative systems that were highly bureaucratic, with a lot of "gate keeping. Offences in these systems are not being recorded by the police, or 'burking,' as it's known is one of the most chronic issues. In both countries police officers have either deliberately withheld the registration of cognizable offences or postponed it, either to keep the local crime statistics down, to lighten their burden, or to protect allies and government officials. Such a refusal to offer a specific legal remedy has left victims without any means of redress.

1.2 Digitalization of Criminal Justice Systems

Both countries are now making efforts to resolve these challenges by implementing technology and digitizing their criminal justice system, but the paths they have taken technologically and in terms of statutory frameworks differ significantly. The Code of Criminal Procedure, 1973 (CrPC) was repealed by the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) and a digital complaint mechanism was introduced under Section 173 of the BNSS, effective from 1 July 2024. The change, however, added further hurdles to the justice process, such as having to visit a police station in person within three days to sign a document, and a prolonged preliminary-enquiry process which lowered the ease of access to justice for disadvantaged and vulnerable groups.

On the other hand, the National Criminal Procedure (Code) Act, 2017, the incorporation of the Nagarik App and the overall digital-justice system of the Nepal Police has made the digital-justice system in Nepal more user friendly, transparent and legally secure. Through comparative analysis of the statutory, judicial and technological frameworks of the two countries, it is concluded that the introduction of digital FIR system in Nepal is a significant initiative towards enhancing access to justice, providing citizens with a digital platform to track



their FIRs and enable them to communicate directly with the police, thereby minimizing the risk of citizens being denied access to the FIR system.

1.3 Research Problem

Considering the challenges to filing FIRs that exist in traditional methods, including acceptance on police discretion, submission remotely, delay, and outright refusal, countries like India and Nepal have turned to online platforms to address these concerns. But, it is not known how effective these reforms have been. This study shows that India's constitutional and statutory mandate of compulsory registration of the cognizable offence is far from being met, with the procedural, physical-verification, lack of an adequate digital infrastructure, and the question of whether an electronic complaint can be treated as a legally valid FIR being left unanswered. While Nepal's legal framework is relatively less complex, in several significant ways its administrative framework has been more citizen friendly. The research question which this study aims to answer is if the statutory recognition of electronic complaints in each jurisdiction results in citizens having access to justice.

1.4 Significance of the Study

This research aims to compare the e-FIR system in India with that in Nepal by using a doctrinal legal analysis and an empirical study of the public perception which has never been done at the same time in both jurisdictions. The study is interdisciplinary, covers statutory recognition as well as the design of authentication and verification mechanisms, transparency, and citizen trust to shed light on the interplay between digital policing, legal protection and access to justice. The findings are meant to support the policy-reform process on both sides and add to the digital governance and criminal justice literature in South Asia.

2. Research Objectives

2.1 Primary Objectives

The objective of the present study is to have a deep understanding and compare the legal and institutional aspects of e-FIRs in India and Nepal. Explores the statutory requirements of the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) and the National Criminal Procedure (Code) Act, 2017 to comprehend how each jurisdiction will facilitate citizens' access to the criminal justice system using digital means to file complaints.

2.2 Authentication and Verification

The study also compares the various ways in which the complaints have been authenticated and verified under both countries, focusing on the impact of the three-day physical-signature requirement in India and the electronic verification of identity via an integrated system in Nepal on procedural access and effectiveness of legal action.

2.3 Transparency, Accountability and Citizen Engagement

Another goal is to examine the transparency, accountability, and citizen-engagement aspects of digital-policing systems in both jurisdictions (such as acknowledgment systems, complaint-handling systems, communication systems, and other dimensions that influence citizens' trust in their justice system).

2.4 Socio-Legal Dimensions and Reform



Lastly, the paper examines the socio-legal status of vulnerable and marginalised groups and the possible best practices that could enhance digital access to justice using e-FIR. The comparative results help inform recommendations to enhance digital-policing capacity and access to justice in South Asia.

3. Literature Review and Theoretical Framework

3.1 Literature Review

Kuldeep Singh and Shaveta Begra (2020)¹ examine the essence of democracy, its fundamental principles, meaning, and practical implementation, particularly in the context of elections. The authors portray elections as the cornerstone of democratic governance, facilitating the expression of citizens' preferences and the peaceful transfer of power, and they examine the rights and duties of citizens within the electoral process, including voting rights, political participation, and accountability. The work also considers the role of election commissions in upholding the integrity and fairness of elections, underscoring the significance of democratic institutions in shaping inclusive governance.

Raperia (2022)² discusses the Supreme Court's direction on FIR registration in *Lalita Kumari v. State of Uttar Pradesh*, noting that police officers are duty-bound to register an FIR once they encounter evidence of a cognizable offence, while for non-cognizable offences the police retain investigative authority but cannot proceed to trial or arrest without judicial permission. Although the legal structure is well defined, actual implementation is inconsistent: police often decline to register FIRs even where credible evidence of a cognizable offence exists, forcing complainants into repeated visits and significant costs, while courts — already burdened by heavy caseloads — take months to direct police action. Raperia attributes police reluctance to a mix of incentives to keep recorded crime rates low and the political sensitivity of certain cases, and observes that delayed registration can compromise the evidentiary weight of an FIR, since courts have consistently emphasized that FIRs should be filed promptly to preserve the reliability of the complainant's account. The study calls for measures that increase police accountability and expedite FIR registration in order to close the gap between legislative intent and practice.

Anto (2021)³ underscores the fundamental principles of justice and the rule of law, drawing on John Locke's ideas on the protection of individual rights, and stresses the need for a robust judicial system to uphold liberty and justice. The study highlights systemic challenges such as insufficient judicial strength and inconsistent appearance of key witnesses: only 10.5% of surveyed judges reported that police and other key witnesses appeared in all cases, 47.4%

¹ Kuldeep, S., & Shaveta, B. (2020). Police administration: Emerging issues & concerns. Selective and Scientific Books.

² Raperia, S. (2022). Ingredients and law of registration of FIR in India under the Criminal Procedure Code. Available at SSRN: <https://ssrn.com/abstract=4120080>

³ Anto, A. (2021). Analyzing the delay, pendency and backlog of criminal matters in India in the light of COVID-19 with special reference to Kerala: An empirical study (Master's dissertation). National University of Advanced Legal Studies, Kochi.



reported appearances in most cases, 26.3% reported occasional appearances, and 15.8% reported appearances in only a few cases. The police were identified as the second-largest obstacle to the timely disposal of cases, and the study situates these delays within the framework of Locke's social-contract theory, which envisions an effective legal system as essential to protecting individual rights.

Saud (2025),⁴ drawing on data from the Nepal Police Cyber Bureau and the Nepal Telecommunications Authority, analyzes the trends and status of cybercrime in Nepal between 2018 and 2024. The study identifies major categories of cybercrime — including social-media misuse, online financial fraud, and data breaches — and finds that reported incidents, particularly on platforms such as Facebook/Messenger and TikTok, have grown significantly over the period. It also highlights the disproportionate impact of cybercrime on women and marginalized groups, and institutional challenges including limited technical capacity, low public awareness, and inadequate legislation. While the study does not directly address digital access to justice or electronic complaint registration, it offers a useful account of the evolution of digital governance in Nepal and the growing need for legal responses to cyber offences.

Bhandari, Bhatta, Sharma, and Poudyal (2026)⁵ analyze the use of digital-governance mechanisms at the local level in Nepal, using semi-structured interviews and document analysis. The study finds that e-governance projects have improved administrative efficiency, transparency, accountability, and accessibility, particularly in revenue collection, taxation, and permit management, while identifying persistent challenges including limited technical skills, inadequate digital infrastructure, cybersecurity gaps, weak regulation, financing constraints, and an urban-rural digital divide. The authors argue that digital transformation must be accompanied by investment in infrastructure, capacity building, data-protection measures, and governance structures. Although the article does not address criminal-justice administration directly, its findings on transparency, accessibility, and infrastructure are directly relevant to the functioning of e-FIR mechanisms in Nepal.

Maharjan (2025)⁶ studies the factors affecting citizens' independent use of electronic government forms in Itahari Sub-Metropolitan City, Nepal, applying the Unified Theory of Acceptance and Use of Technology (UTAUT) to model the influence of social influence, facilitating conditions, trust in e-government, and effort expectancy. The study finds that social influence was the most significant driver of adoption, while limited digital competence, inadequate ICT infrastructure, and low public awareness remained obstacles; it also finds that some citizens, despite having access to online procedures, still relied on third-party intermediaries. Although the study does not focus on e-FIR registration specifically, its

⁴ Saud, Chandra. (2025). Cyber Crime in Nepal: An Analysis of Case Status and Trends.

⁵ Bhandari, R. B., Bhatta, N., Sharma, G., & Poudyal, Y. R. (2026). *e-Governance practices in Nepal: Opportunities, challenges, and strategies from the local level*. Journal of Computer Science, 22(3), 367–377. <https://doi.org/10.3844/jcssp.2026.367.377>

⁶ Maharjan, G. (2025). *Examining the factors influencing the use of e-forms in government services in Itahari Sub-Metropolitan City*. Journal of Vishwa Adarsha College (JOVAC), 2(1), 157–178. <https://doi.org/10.3126/jovac.v2i1.83884>



findings — that digital public services are effective only when citizens trust them, engage with them, and can use them independently — provide a useful context for evaluating Nepal's e-FIR and digital complaint-registration systems. This finding is consistent with the broader e-government adoption literature, which identifies perceived usefulness, trust in government, and facilitating conditions as the dominant predictors of citizens' willingness to use digital public services.⁷

Islam and Rahman (2022)⁸ trace Bangladesh's progress toward digital governance to enhance public-service delivery, transparency, and citizen participation, documenting the growth of online platforms, mobile applications, and electronic service-delivery systems. While digitalization has improved access and administrative effectiveness, the authors find that infrastructure gaps, low digital literacy, and limited institutional capacity continue to hinder implementation. These findings are directly relevant to Bangladesh's online General Diary (GD) platform and complaint-tracking mechanisms, which represent early steps toward citizen-centric digital justice, though — as discussed in Section 7 — Bangladesh has not yet adopted a full e-FIR system comparable to those of India or Nepal.

Access-to-Justice Scholarship

This review is further strengthened by engagement with the broader access-to-justice literature. Upendra Baxi's work on legal access in India — including his influential analysis of panchayat justice and the structural barriers facing rural and marginalized litigants — remains foundational to understanding why formal legal entitlements often fail to translate into substantive access, a dynamic that this study finds mirrored in India's e-FIR framework (Baxi, 1976). Martha Minow's scholarship on access to justice for marginalized populations similarly cautions that procedural reforms which are facially neutral can nonetheless reproduce existing inequalities if they are not designed around the lived circumstances of the people they are meant to serve (Minow, 2014). At the international level, the UNDP's access-to-justice framework identifies legal awareness, legal aid, adjudication, and enforcement as interdependent pillars of a functioning system (UNDP, 2004), while the Asian Development Bank's studies on legal empowerment in South Asia emphasize that digital-governance reforms deliver access-to-justice gains only when paired with legal literacy and institutional accountability (Asian Development Bank, 2019). Read together, this literature supports the study's central claim that statutory recognition of electronic complaints is a necessary but not sufficient condition for meaningful access to justice.⁹

International Digital-Justice and Digital-Policing Scholarship

⁷ Gupta, K. P., Singh, S., & Bhaskar, P. (2022). Citizen adoption of e-government: A literature review and conceptual framework. *Electronic Government, an International Journal*, 18(1), 1–25. <https://doi.org/10.1504/EG.2022.119377>

⁸ Islam, M. S., & Rahman, M. M. (2022). Digital transformation of public service delivery in Bangladesh: Challenges and opportunities of e-governance. *International Journal of Public Administration in the Digital Age*, 9(1), 1–17. <https://doi.org/10.4018/IJPADA.290001>

⁹ Wei, K. K., Teo, H. H., Chan, H. C., & Tan, B. C. Y. (2011). Conceptualizing and testing a social cognitive model of the digital divide. *Information Systems Research*, 22(1), 170–187. <https://doi.org/10.1287/isre.1090.0273>



Scholarship on digital-justice reform outside South Asia further situates this study's findings. Susskind (2019)¹⁰ argues that the shift toward online courts and digital dispute-resolution mechanisms is best understood as a structural reimagining of how justice is delivered rather than mere automation of existing procedure, and cautions that such systems expand access to justice only when procedural safeguards and support for digital literacy are built into their design from the outset — a caution borne out by this study's findings on India's e-FIR system in Section 9. Brown (2014)¹¹ examines the digitisation of policing in comparative perspective, finding that digitising police records and reporting channels can improve administrative efficiency and record-keeping but does not, by itself, resolve the discretionary and cultural barriers — such as reluctance to register complaints — that determine whether citizens actually obtain a remedy, a finding directly relevant to the 'burking' practices discussed in Section 1.1. Contini and Cordella (2015; updated 2020)¹² similarly argue that digital technologies for justice systems function as a toolkit whose benefits depend on the institutional and procedural choices made in implementation, rather than being an inherent property of the technology itself, reinforcing this study's central claim that statutory recognition of electronic complaints is necessary but not sufficient for meaningful access to justice.

3.2 Digital Governance and the Digital Divide

3.2.1 Evolution of the Digital Divide

The concept of the digital divide arose in the early 1990s, when the uptake of computing and internet technologies across developed economies was markedly uneven. At the time, the term referred to a binary condition — some people had computers and internet access, and others did not. The U.S. Department of Commerce's 'Falling Through the Net' series (1995–2000) was among the first efforts to formally quantify differences in access to technology across income, race, geography, and education.

In the late 1990s and early 2000s, researchers moved beyond simple measures of access and began identifying deeper structural dimensions of the divide. Helsper (2021), in *The Digital Disconnect*, argues that digital inequalities are not merely a technical gap but the product of entrenched social, economic, and cultural inequalities, such that groups already excluded from education, employment, or income are more likely to also be digitally excluded.

The digital divide in developing countries followed a related but distinct trajectory. International organizations such as the International Telecommunication Union (ITU) and the United Nations Development Programme (UNDP) began measuring access and linking the digital divide to broader development outcomes, while the World Summits on the Information Society (2003 and 2005) placed the digital divide on the international development-policy

¹⁰ Susskind, R. (2019). Online courts and the future of justice. *Computer Law & Security Review*, 35(1), 1–11. <https://doi.org/10.1016/j.clsr.2018.11.005>

¹¹ Brown, K. (2014). The promise and perils of digitising the police. *Policing and Society*, 24(2), 131–144. <https://doi.org/10.1080/10439463.2013.784309>

¹² Contini, F., & Cordella, A. (2015). Digital technologies for better justice: A toolkit for action. *Government Information Quarterly*, 32(4), 380–390. <https://doi.org/10.1016/j.giq.2015.09.005>; see also the updated version, Cordella, A., & Contini, F. (2020), *Government Information Quarterly*, 37(4), 101466. <https://doi.org/10.1016/j.giq.2020.101466>



agenda. Nepal entered this global narrative from a position of significant disadvantage — landlocked, largely rural and agrarian, and constrained by limited infrastructure in roads, electricity, and telecommunications. In the early 2000s, internet connectivity in Nepal remained below two percent and was concentrated almost exclusively in the Kathmandu Valley and a small number of major cities.¹³

3.2.2 Three Levels of the Digital Divide

In the mid-2000s, a 'second-level' divide emerged in the academic literature, focused not on access itself but on the skills and capacities required to use technology effectively; researchers found that as low-income or rural populations gained internet access, they often used it less effectively than wealthier counterparts. In the 2010s, a 'third-level' divide emerged, concerned with outcomes — the actual economic, social, and civic gains that different users derive from digital engagement. Van Deursen's (2024) recent review of developments in digital inequality and inclusion finds that these multi-layered inequalities persist, and are being compounded by the growth of artificial intelligence, the platform economy, and algorithmic governance.¹⁴

3.2.3 Digital Governance: Concept and Principles

Digital governance concerns the ways digital technologies are used to reimagine and enhance the decision-making, service provision, and citizen-engagement processes of public institutions. Lythreath, Singh, and El-Kassar (2022) argue that aggregate connectivity statistics systematically obscure the heterogeneity of digital experience within populations, and that digital-governance schemes which fail to account for the access preconditions of their intended beneficiaries may exacerbate the digital divide rather than reduce it, by extending services to more people while leaving the most marginalized behind.¹⁵

3.3 Digital Governance in Nepal

3.3.1 Development of ICT Policy in Nepal

Digital governance in Nepal has developed through a series of overlapping policy frameworks, institutional reforms, and technology projects. Nepal's first systematic articulation of a national vision for ICT was the Information Technology Policy 2000, followed by the National ICT Policy 2015. The Ministry of Communication and Information Technology (MoCIT) coordinates these activities, though inter-ministerial coordination and implementation capacity remain areas requiring further development. This is consistent with Mensah's (2020) finding

¹³ Bhandari, R. B., Bhatta, N., Sharma, G., & Poudyal, Y. R. (2026). *e-Governance practices in Nepal: Opportunities, challenges, and strategies from the local level*. Journal of Computer Science, 22(3), 367–377. <https://doi.org/10.3844/jcssp.2026.367.377>

¹⁴ Scheerder, A., van Deursen, A. J. A. M., & van Dijk, J. A. G. M. (2017). Determinants of Internet skills, uses and outcomes: A systematic review of the second- and third-level digital divide. *Telematics and Informatics*, 34(8), 1607–1624. <https://doi.org/10.1016/j.tele.2017.07.007>

¹⁵ van Deursen, A. J. A. M., & Helsper, E. J. (2015). The third-level digital divide: Who benefits most from being online? In *Communication and Information Technologies Annual* (Vol. 10, pp. 29–52). Emerald Publishing. <https://doi.org/10.1108/S2050-206020150000010002>



that government capacity — rather than infrastructure alone — is a decisive determinant of e-government performance and citizen adoption of digital-government services.¹⁶¹⁷

3.3.2 Digital Nepal Framework 2019

The Digital Nepal Framework, launched in 2019, is Nepal's most ambitious digital-governance initiative to date. It establishes eight digital pillars — digital infrastructure, digital economy, digital government, digital citizen, digital tourism, digital agriculture, digital health, and digital education — and sets targets for digital-service delivery across all levels of government.¹⁸

3.3.3 Nagarik App and National Digital Identity

Programs implemented under this framework include the National ID Management Center (NIDMC), which manages a biometric national-identification program aimed at giving every citizen a verifiable digital identity, and the Integrated Property Tax Administration System (IPTAS), which has digitized property registration in some municipalities. The government has also begun developing interoperability frameworks to enable data-sharing between government systems, without which digital governance risks creating digital silos that mirror the fragmentation of pre-digital bureaucracy.

Digital inclusion remains the central challenge facing Nepal's digital-governance agenda. Nepal's connectivity landscape is paradoxical in several respects: while access has grown rapidly — over 80% of the population had mobile internet access as of 2023 — deep inequalities in the quality of participation persist along multiple axes: urban-rural (with rural areas faring markedly worse); gender (with women statistically less likely to access and use digital services, owing to cultural norms, economic dependence, and digital-literacy gaps); caste and ethnicity (with Dalit, Janajati, and some Madhesi communities underserved relative to other communities); and generational (with elderly citizens less likely to access and use digital services).

Infrastructure remains a further obstacle: many local (palika) government offices face unstable internet connectivity, inadequate IT resources, and insufficient staffing with qualified IT professionals, creating a risk of 'isomorphic mimicry' — adopting the form of digital governance without its substance. Digital inclusion is not only a matter of device access but also of developing the operational, informational, communicative, and strategic skills needed to use the internet effectively, a gap that is especially pronounced among sub-national government employees, women, and elderly citizens, who often rely on intermediaries for internet use. Legally, the Electronic Transactions Act (2008) was the first to grant legal

¹⁶ Lythreathis, S., Singh, S. K., & El-Kassar, A. N. (2022). The digital divide: A review and future research agenda. *Technological Forecasting and Social Change*, 175, 121359. <https://doi.org/10.1016/j.techfore.2021.121359>

¹⁷ Mensah, I. K. (2020). Impact of government capacity and e-government performance on the adoption of e-government services. *International Journal of Public Administration*, 43(4), 303–311. <https://doi.org/10.1080/01900692.2019.1628059>

¹⁸ Janowski, T. (2015). Digital government evolution: From transformation to contextualization. *Government Information Quarterly*, 32(3), 221–236. <https://doi.org/10.1016/j.giq.2015.07.001>



recognition to electronic signatures and digital records, while the Privacy Act (2018) aims to protect personal data, though its application remains incomplete and uneven.

3.4 Digital Governance and Access to Justice

3.4.1 Digital Policing and Citizen Participation

The eFIR — Electronic First Information Report — is one of the most socially consequential digital-governance programs implemented within Nepal's law-enforcement community, and it is integrated into the broader Digital Nepal Framework. Under the previous system, complainants were required to appear in person at a police station, which posed particular difficulties for women victims of gender-based violence, people in remote areas, economically weaker sections of society, and others apprehensive about intimidation at police stations. The eFIR system enables citizens to register complaints online, reducing friction, cost, and social barriers in the physical reporting process, and provides an acknowledgment number that allows complainants to follow the status of an investigation.

3.4.2 The Digital Divide and Accessibility of the eFIR

The eFIR system has significant potential, but it faces implementation challenges similar to those confronting digital governance more broadly in Nepal. Digital-literacy barriers mean that many potential users — including rural women who are victims of domestic violence or trafficking, precisely the population the system is meant to serve — are unable to use the online portal without assistance. Connectivity gaps in areas with high crime-reporting needs but poor internet infrastructure compound the problem, and institutional culture within the Nepal Police — where the shift to online filing removes a gatekeeping role traditionally held by officers — together with incomplete data-protection measures, raises reasonable concerns among survivors of gender-based violence.

3.4.3 Theoretical Relationships Between Digital Governance and the eFIR System

Despite these obstacles, pilot initiatives — particularly in Bagmati Province — have demonstrated the potential of digital complaint registration to increase overall registration rates and shorten the time between an incident and case initiation. Civil-society organizations supporting survivors of gender-based violence have adopted assisted digital reporting as an advocacy tool, with trained paralegal workers acting as 'digital intermediaries' between citizens and the digitized government system. Van Deursen (2024) maintains that such intermediation, if well designed, can be a legitimate element of a digital-inclusion strategy, provided it is intended over time to build citizens' own digital capabilities. Together, the findings of Van Deursen (2024), Helsper (2021), and Lythreath et al. (2022) suggest several guiding principles for the design of digital governance and eFIR systems: a multi-faceted approach addressing access, skills, usage, and outcomes; social equity as the central evaluative framework; participatory design involving marginalized communities; robust and rights-respecting legal frameworks; sustained investment in human capital and digital literacy; and independent monitoring and accountability mechanisms. These principles, and in particular the three-level digital-divide framework (access, skills, outcomes) introduced in Section 3.2.2, provide the



analytical lens applied throughout Sections 8 and 9 of this study to the comparative and reform analysis of India's and Nepal's e-FIR systems.¹⁹

4. Research Methodology

4.1 Research Design

The study used an integrated, mixed-methods research design, combining qualitative (doctrinal comparative) and quantitative (empirical) methods. The design tests claims made in India and Nepal about the ease of access of e-FIR systems against citizens' lived experiences of engaging, or attempting to engage, with those systems.

4.2 Doctrinal Legal Analysis

The doctrinal component examines the legislation governing e-FIR registration in the Indian context, judicial rulings, and the law-reform proposals of the 22nd Law Commission of India (Report No. 269), alongside the official digital-policing tools that implement these provisions.

4.3 Comparative Method

The comparative method operates at two levels: first, comparing India and Nepal to understand differences in statutory recognition, authentication design, and citizen engagement; and second, comparing both jurisdictions against four illustrative international benchmarks — the United Kingdom, Hong Kong, Saudi Arabia, and Canada — whose online crime-reporting systems illustrate a range of approaches to authentication, acknowledgment, offence coverage, and institutional integration. These four jurisdictions were selected because each represents a distinct institutional design choice relevant to the reforms discussed in Section 10: the UK for its guided, verification-based reporting model; Hong Kong for its time-bound acknowledgment standard; Saudi Arabia for its anonymous-reporting option; and Canada for its federal-provincial interoperability model. The rationale for this selection, together with its methodological limitations, is discussed further in Section 7.5.

4.4 Empirical Survey Method and Results

The quantitative component involved a pre-designed Google Form survey administered to respondents in Ahmedabad, Dhrangadhra, and Gogha. The survey instrument was designed to capture respondents' awareness, accessibility, usability, transparency, and confidence in relation to the e-FIR system, in order to provide empirical support for the doctrinal and comparative findings of the study. A copy of the survey instrument, together with the item wording used for each construct, is provided in Appendix A.

Respondents were drawn from Gujarat, selected as the study site because it is one of the earlier-adopting states for state-level e-FIR implementation (see Section 5.3) and because it offers meaningful internal variation — urban, semi-urban, and rural — within a single state-level

¹⁹ Mergel, I., Edelmann, N., & Haug, N. (2019). Defining digital transformation: Results from expert interviews. *Government Information Quarterly*, 36(4), 101385. <https://doi.org/10.1016/j.giq.2019.06.002>

legal and administrative framework, allowing the survey to hold the applicable state police infrastructure constant while varying geography and connectivity. Gujarat's position as a comparatively high digital-infrastructure state means these findings should be read as indicative of best-case conditions within India's federal police system rather than as representative of the country as a whole; state police forces vary widely in e-FIR maturity (see Section 5.3), and future research extending this survey to lower-infrastructure states would materially strengthen the generalizability of the findings.

A cluster-sampling method was used, covering Ahmedabad (urban), Dhrangadhra/Bahnagar (semi-urban), and Gogha (rural). A structured questionnaire was administered to 50 respondents over a ten-day period. The sample size of 50 was set with the study's exploratory, hypothesis-generating purpose in mind: the survey is designed to identify the range and salience of concerns around awareness, accessibility, usability, transparency, and confidence — sufficient for that descriptive purpose — rather than to produce point estimates that are statistically generalizable to the population of Gujarat or India as a whole. The findings should accordingly be read as preliminary and indicative; Section 12 (Future Research Agenda) recommends a larger, stratified sample as a next step.

The results show strong public interest in digital complaint registration. Approximately 56% of respondents did not prefer visiting a police station to file an e-FIR. A further 65% endorsed an authentication system to enable the timely reporting of complaints, while 50% felt the current system was not transparent. Twenty percent of respondents were unaware of the concept of e-FIR, and a further 12% wanted to know more about it — a finding that, read through Helsper's (2021) account of digital exclusion, suggests that awareness gaps in the sample track the same underlying social and economic inequalities that produce access and skills gaps in the broader digital-divide literature discussed in Section 3.2. Seventy-five percent supported expanding the number of offences reportable online, and, as shown in Figure 4.1, 70% felt the existing reporting system was inadequate and needed to be strengthened. Together, these findings point to a high level of demand for greater transparency, accountability, awareness, and inclusiveness in the implementation of the BNSS e-FIR framework.

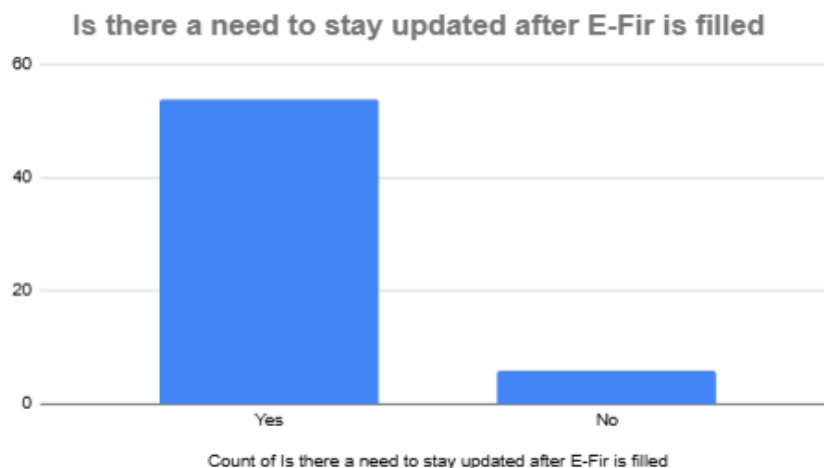


Figure 4.1 need of authentication and follow-up mechanism.

Among the six jurisdictions presented to respondents, the United Kingdom's system was the most preferred, at 30% of responses, followed by Hong Kong (25%), Saudi Arabia (10%), Canada (10%), Bangladesh (10%), and Nepal (5%), with the remaining 10% either preferring another option or undecided. As shown in Figure 4.2, this ranking broadly favors jurisdictions offering both structured, guided reporting (the UK) and rapid formal acknowledgment (Hong Kong) — the two features most consistently identified as absent from India's current framework in Sections 7 and 9.

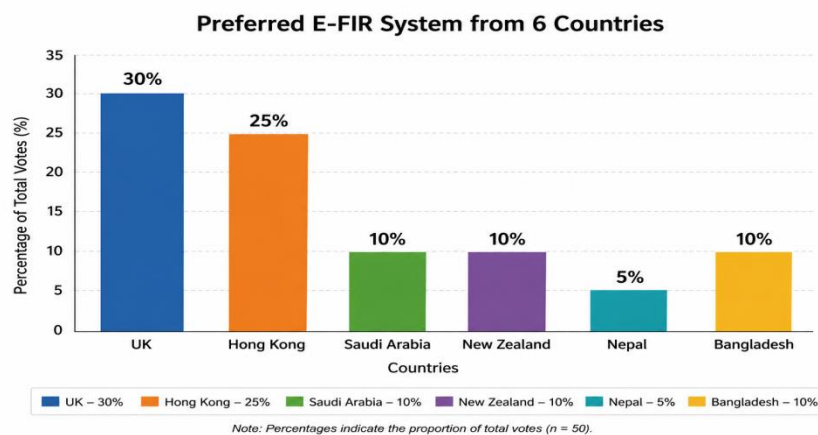


Figure 4.2 Shows most favored mechanisms

5. Status and Implementation of India's E-FIR Framework

5.1 Evolution of Digital FIR Registration in India

The Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) repealed the Code of Criminal Procedure, 1973 (CrPC) from 1 July 2024, and added a digital complaint procedure in Section 173 of BNSS. This institutional change was in line with a legislative change introduced almost a decade ago, by the 22nd Law Commission of India, which had recommended for enabling the online filing of FIRs under Section 154 of the CrPC. The Law Commission noted that electronic filing would be a boon for those who could not safely and practically visit a police station and would help solve the problem of the recorded practice of police officers not registering FIRs for petty offences.²⁰

This legislative work led to the establishment of the Crime and Criminal Tracking Network and Systems (CCTNS), the largest IT enabled policing initiative of India, which was a Mission Mode Project under the National e-Governance Plan and was implemented by the National Crime Records Bureau (NCRB). In June 2009, CCTNS was approved by the Cabinet Committee on Economic Affairs with a budget of ₹2,000 crore to establish a national e-governance enabled system for policing, tracking of crime and digital record management. The foundation laid by CCTNS is now being used for the registration of FIRs under Section 173 of the BNSS, both on paper and electronically.

²⁰ Mishra, A., & Kaushik, A. (2023). Digital governance and public service delivery in India: Opportunities and challenges. *Journal of Public Affairs*, 23(4), e2901. <https://doi.org/10.1002/pa.2901>



Section 173(1)(ii) of the BNSS prescribes that the electronically filed FIR shall be signed in person at the police station within 3 days of filing or else the FIR shall not be legally valid and the duty of police to register the FIR and/or carry out an inquiry shall not be deemed to be discharged. This requirement is supposed to encourage authenticity, but in practice makes formal registration more difficult — even for cognizable offences — as complainants are required to make a trip to a police station after filing online, which is counterproductive to the purpose of an online system and disproportionately places a burden on those who cannot travel because of geographic, social or economic constraints.²¹

5.2 State-Level E-FIR Implementation

There are some state-level partial and fragmented registration of e-FIRs. The police departments in Delhi, Gujarat, Karnataka, Madhya Pradesh, Odisha, Rajasthan, Uttar Pradesh and Uttarakhand have implemented e-FIR systems, although most of the time, they are used for non-heinous offenses, most frequently vehicle theft cases and reports of property being stolen or missing. There are a number of state police portals, but no such portal offers end-to-end digital FIR registration and tracking system. This fragmentation is a reflection of policing being a state subject in India — although it is an oversight function that the Ministry of Home Affairs has, it does not have operational control and this leads to a wide variation in the availability, effectiveness and enforceability of the e-FIR mechanism throughout the country.²²

5.3 Practical Issues in E-FIR System in India.

These are the effects of a segmented and closed system. The Mumbai police reported that only about 5% of the hundreds of complaints of online banking fraud and cybercrime are registered as FIRs, mostly after a physical visit to the police station by the complainant. This is a classic systemic flaw in the system: it receives digital inputs but does not work digitally, which is what e-FIR was designed to fix. These practical problems, and the structural deficiencies that lead to them, are explored in detail in Section 9.²³

6. Nepal's E-FIR Framework and Digital Justice Ecosystem

6.1 Legal Framework under the National Criminal Procedure (Code) Act, 2017

The FIR is the most crucial document in the criminal justice process under the National Criminal Procedure (Code) Act, 2017, and it is a formal record of a complaint made by a person to the police which starts the criminal case and investigation. Traditionally, the first step of an FIR was to go to a police station, which made filing a difficult task for women victims of gender-based violence, people in remote areas, and economically vulnerable and/or intimidated

²¹ ²¹ Mergel, I., Edelmann, N., & Haug, N. (2019). Defining digital transformation: Results from expert interviews. *Government Information Quarterly*, 36(4), 101385. <https://doi.org/10.1016/j.giq.2019.06.002>

²² Gupta, K. P., Singh, S., & Bhaskar, P. (2022). Citizen adoption of e-government: A literature review and conceptual framework. *Electronic Government, an International Journal*, 18(1), 1–25. <https://doi.org/10.1504/EG.2022.119377>

²³ Janowski, T. (2015). Digital government evolution: From transformation to contextualization. *Government Information Quarterly*, 32(3), 221–236. <https://doi.org/10.1016/j.giq.2015.07.001>



citizens. The eFIR system was introduced as part of the ongoing digital modernization of the Nepal Police to allow citizens to report police complaints online, thus minimising the hassles, costs and social inconvenience of going in person to register police complaints.

6.2 Digital Governance Platforms (DGP)

The eFIR system was inspired by earlier eFIR systems in Indian states that were brought up in the early 2010s and other international ePolice Complaint systems. It has a multilingual interface (Nepali and now more local languages), a mobile-first application because most internet users in Nepal use mobile devices, integration with national ID system for complainant verification and a case-tracking dashboard, making the eFIR a part of a wider Digital Nepal Framework and the supporting digital-identity infrastructure.

6.3 Nagarik App and Digital Authentication

Nepal's answer to the authentication issue is the Nagarik App, a centralized digital-identity-verification system that is connected to government databases. Electronic complaints are legally binding from the time they are filed, and a digital acknowledgment receipt is issued by the police authorities when the complaint is filed, thus removing the need to verify it later.

6.4 Complaint Tracking and Citizen Engagement

A complaint identifier is provided to the complainant, enabling a real-time tracking of a complaint through the Nagarik App and a dedicated Online Police Clearance Report (OPCR) portal. Citizens can access the status of their complaints, submit pictures, videos, and other pieces of evidence and connect directly with investigators via digital channels.

6.5 Transparency and Accountability Mechanisms

These tracking and communications tools enhance accountability, minimize uncertainty and foster trust in the justice system. They, alongside secure authentication, illustrate a vision of digital justice, one that goes beyond identity verification and evidence submission to the status monitoring and direct communication through a single system, not simply an administrative process.

6.6 Challenges and Limitations

Implementing the eFIR system in Nepal has numerous challenges, even in this relatively citizen-driven design. Many users, including women from rural communities reporting domestic violence and trafficking, cannot use the online system without support due to digital-literacy issues. Lack of connectivity also limits access in high crime-reporting areas including areas affected by the legacies of the insurgency, trafficking corridors, and gender-based-violence hotspots. The quest for institutional culture within the Nepal Police compound another challenge, as the digital filing has eliminated a barrier that was previously being leveraged by officers (not always necessarily in the right way); a few officers have not yet adapted to the system's inherent lack of control over how complaints are filed; and limited trainings on digital case management have delayed the system's incorporation into the routine of the police. Lastly, strong protections are required for data security and privacy, especially regarding survivors of gender-based and sexual violence and their assurance that no one can access their personal data except themselves, without other parties or perpetrators. Nepal's data-protection laws are still



in their infancy in this regard. Due to these literacy and trust issues, the use of trained civil-society-based 'digital workers' to fill in the eFIRs is now a viable option, especially with the pilot projects in Bagmati Province.

6.7 Non-Cognizable Offences: A Balanced Assessment

In the case of non-cognizable offences, the National Criminal Procedure (Code) Act, 2017 maintains a distinction between cognizable and non-cognizable offences, similar to that India contains in its Section 173(3) preliminary-enquiry requirement, with the eFIR portal accepting the complaint and generating a case reference, but investigation being launched only after the matter is referred to a magistrate for authorization. But Nepal's system is more citizen-centred merely because it operates after, not as a precondition for, the legal recognition of the complaint, whereas India's three-day physical-signature rule is kept in place for the reason of gatekeeping non-cognizable matters.

However, in the context of what was discussed in Nepal above, and in the light of the documented challenges in India as discussed in Section 9, Nepal's implementation challenges are, on the evidence reviewed in Section 6.6, comparable in kind – if not always in degree. This study does not suggest that the Nepalese legal design of electronic complaints is free of the access barriers that affect the Indian system, but only that this is the case in Nepal.²⁴

7. Comparative Analysis of International E-Reporting Models

This section puts the e-FIR systems of India and Nepal within the context of four illustrative models from around the world. The comparative study of these systems shows that there are significant differences between the current e-FIR system in India and the jurisdictions surveyed below, on four areas of focus – authentication, acknowledgment and coverage of offences, and institutional integration.

7.1 United Kingdom

The UK has one of the most advanced online crime reporting systems in common law countries, which is a guided reporting system with verification. Complainants are asked a series of structured questions to ensure the report is followed up correctly and reaches the appropriate police force and offence category, anonymous reporting can be via Crimestoppers UK in addition to online forms, by telephone, by fax or by postal mail. Pre-reporting means the identification of which police agency would be appropriate, for example, the British Transport Police would have jurisdiction over offences on the railway network while a territorial force would not. A complaint, once filed, is reviewed in relation to four factors: the reasonableness of a resolution, the nature of the offense, the vulnerability of the victim and the allocation of police resources. Cases are allocated a case-reference number, with an investigating officer assigned where a case goes to investigation, and complainants where cases are referred to court are referred to the Witness Care Unit.²⁵

²⁴ Mensah, I. K. (2020). Impact of government capacity and e-government performance on the adoption of e-government services. *International Journal of Public Administration*, 43(4), 303–311.
<https://doi.org/10.1080/01900692.2019.1628059>

²⁵ Brown, K. (2014). The promise and perils of digitising the police. *Policing and Society*, 24(2), 131–144.
<https://doi.org/10.1080/10439463.2013.784309>



7.2 Hong Kong

The Hong Kong Police Force has an e-Report Centre for non-emergency and non-urgent incidents to report, which provides a reference number which is carried on the internet and a formal acknowledgment of receipt is sent by email to the reporter within approximately 15 minutes of the report's submission. The system is for written, audio and video evidence, and provides an SMS emergency hotline and fax as alternative reporting options, and full contact details for all Police Station Report Rooms are available on the force website. This reference and acknowledgment with time limits provide accountability and helps a complainant to keep track and follow up a complaint, which is not available in the current Indian system.

7.3 Saudi Arabia

The e-Cops system, which operates in Riyadh, allows citizens to report crimes online without the requirement to provide their identity to the police, thus helping to alleviate the difficulties for those citizens who might not feel comfortable revealing their identity to the police. It features complaint submission, follow-up and case management capabilities and structured data fields to help identify perpetrators and identify patterns.

7.4 Canada

The Royal Canadian Mounted Police (RCMP) has an integrated online reporting system, with a clear focus on accessibility for complainants in rural, remote and linguistically diverse communities. The Canadian model focuses on the interoperability of federal and provincial law-enforcement information systems, and not just on the integration of complaints into force-level information systems—online complaints are also incorporated into the national crime-data system.²⁶

7.5 The rationale for the selection of jurisdiction and methodological caveats

The United Kingdom, Hong Kong, Saudi Arabia and Canada were chosen as comparators because, taken together, they provide a range of institutional design options along the four design dimensions that are explored in this study: authentication, acknowledgment, offence coverage and institutional integration; not because they share India's or Nepal's legal heritage. The UK, Canada, and every other system discussed is a federal or common-law system with a police architecture similar to that of India; the civil law system of Saudi Arabia was selected for comparison because it included a structure with Sharia influence; the Hong Kong system is common-law and has a structure that was compact and centralized, features that were absent from the other jurisdictions examined, and in which anonymous reporting was a feature of the system. This combination almost always generates the criticism that there is no direct comparison in criminal procedure to be made between common-law and civil-law systems and between federal and unitary systems as far as the underlying doctrinal structure of criminal procedure is concerned. This study does not compare underlying theories of criminal procedure or evidence, which can vary significantly between traditions, as these are also not

²⁶ Cordella, A., & Contini, F. (2020). Digital technologies for better justice: A toolkit for action. *Government Information Quarterly*, 37(4), 101466. <https://doi.org/10.1016/j.giq.2020.101466>

interchangeable; instead, it merely compares the operational design of the reporting interface — authentication, acknowledgment, tracking and offence coverage.

7.6 Comparative Lessons for India and Nepal

The four jurisdictions share the following features which are not a feature of the Indian e-FIR framework: formal acknowledgment of the digital format; unique case reference systems; prereading guidance for complaints; authentication systems; anonymity options; and time limits for complaint processing. These are not ‘extras’ but essential parts of the legitimacy and effectiveness of any digital crime-reporting system and are the common features used to contrast India's and Nepal's systems developed in the next sections.

7.7 Comparative Table: India, Nepal, and Six Benchmark Jurisdictions

Table 1 below summarizes the comparative position of India, Nepal, and six benchmark jurisdictions — including Bangladesh — across the operational dimensions discussed above.

Feature	India (CCTNS & E-FIR)	United Kingdom	Hong Kong	Saudi Arabia	Canada	Nepal	Bangladesh
Legal Basis	Section 173, BNSS 2023; CCTNS Framework	Police Online Reporting Framework	Hong Kong Police e-Report Centre	e-Cops System	RCMP Online Reporting System	National Criminal Procedure (Code) Act, 2017; Nagarik App	Code of Criminal Procedure, 1898; Online GD System
Online Reporting of Complaints	Limited e-FIR for selected offences	Yes	Yes	Yes	Yes	Yes	Online GD only
Registration of Cognizable Offences Online	Restricted; subject to preliminary enquiry under	Yes	Yes	Yes	Yes	Yes	No; requires formal FIR procedure

Feature	India (CCTNS & E- FIR)	United Kingdo m	Hong Kong	Saudi Arabia	Canada	Nepal	Bangla desh
	Section 173(3), BNSS						
Identity Verification	Often requires later physical verification and signature	Guided verification process	Electronic acknowledgment and verification	Anonymous reporting possible	Standard identity verification	Digital identity authentication through Nagarik App	OTP-based verification
Immediate Acknowledgment	Not consistently provided	Case reference number issued	Electronic reference number and email acknowledgment within minutes	Complaint receipt generated	Reference number provided	Digital acknowledgment receipt issued	Tracking number generated
Complaint Tracking Facility	Limited; tracking not available for all complaints	Case reference tracking	Reference-based follow-up	Case management and tracking	Integrated tracking mechanisms	Real-time tracking through app and portal	Complaint status tracking available
Evidence Upload Facility	Limited	Varies by police force	Audio, video and document uploads	Structured digital evidence submission	Available in many jurisdictions	Upload photos, videos and documents	Upload digital documents

Feature	India (CCTNS & E-FIR)	United Kingdom	Hong Kong	Saudi Arabia	Canada	Nepal	Bangladesh
Communication with Investigating Officer	Generally unavailable	Investigating officer assigned	Follow-up through police channels	Integrated case management	Available through reporting systems	Direct digital communication channels	Limited
Anonymously Reporting	Not generally available	Through Crimestoppers UK	No	Yes	Limited	No	No
Integrated National Platform	CCTNS and National Digital Police Portal	Multiple police force systems linked	Centralized Police e-Report Centre	Integrated city-level system	Federal-provincial interoperability	Single national digital-identity-based platform	Centralized Online GD platform
Accessibility Features	Web portal and mobile access	Online forms, telephone, fax and mail	Online reporting and emergency hotline	Mobile-based reporting	Focus on rural and multilingual accessibility	Mobile application and web portal	Mobile app and web portal
Citizen Participation & Transparency	Relatively low; complainants often receive no updates	Moderate to high	High, due to acknowledgment and tracking	Moderate	High	Very high, through tracking and communication features	Moderate
Overall Assessment	Administrative digitization	Mature guided-	Strong accountability and	Integrated reporting	Accessibility-focused	Most comprehensive	Advanced digital

Feature	India (CCTNS & E-FIR)	United Kingdom	Hong Kong	Saudi Arabia	Canada	Nepal	Bangladesh
	on with limited citizen engagement	reporting model	acknowledgment model	g and case-management model	integrated model	citizen-centric digital-justice model	complaint registration, but not a full e-FIR system

Table 1: Comparative Overview of Online/Electronic Complaint-Reporting Systems.

Bangladesh is included in Table 1 because its online General Diary (GD) system represents an early and instructive stage of digital complaint intake — citizens may lodge an online GD with OTP-based verification, but, unlike India's and Nepal's e-FIR systems, an online GD does not itself constitute an FIR and cognizable offences still require the complainant to pursue the formal FIR procedure in person (Islam & Rahman, 2022). Bangladesh's experience is therefore a useful negative benchmark: it demonstrates that digital intake alone, without a corresponding legal mechanism converting the digital complaint into a legally binding document, reproduces the same 'notice document' problem this study identifies in India's three-day signature requirement (Section 9.1), rather than resolving it.

8. Comparative Analysis of Legal Frameworks and Implementation

8.1 Legal Recognition of Electronic Complaints

Both states have laws that acknowledge e-complaints which are based on digital-identity infrastructure in the Nagarik App in Nepal and Section 173 of the BNSS in India. The difference is not so much on the recognition of the document but the legal completeness; while an e-complaint in India waits for signature, and gains legal strength within 3 days of the actual signing, an e-complaint in Nepal is legally valid as soon as it is filed.

8.2 The authentication and verification mechanisms

This leaves an open question about how Indian courts would be able to reconcile the three day rule without legislative changes. The term 'sign' in Section 173(1)(ii) does not preclude electronic signatures and India already has the Information Technology Act, 2000 which recognizes electronic signature in various other situations without mandating a physical presence. On the face of it, there is scope for a court to conclude that a secure electronic signature or an OTP based authentication satisfies the requirement of signing without physical presence. The Jammu and Kashmir and Ladakh High Court ruled on this question in September 2023 in deciding whether a WhatsApp complaint was a 'substantial compliance' with the requirement for an FIR to be filed in accordance with law, but the judgment did not answer this



question and for now it seems that the three-day physical requirement will continue to apply for complainants and police alike until resolved by the Supreme Court or by the legislature. The direction of this study's reform recommendation, provided in Section 10.1, as legislative removal of the physical-signature requirement, should then be understood to be the more likely means of reform, and judicial reinterpretation as a potential but as yet unconfirmed means of reform.

The difference between cognizable and non-cognizable offences also impacts the working of each of the electronic systems mentioned. In India, the initial argument in the registration of an FIR under Section 173(3) of the BNSS is that the officer concerned has to give preliminary enquiry permission to the officer, not below Deputy Superintendent of Police, before registering an FIR in offenses punishable by 3-7 years imprisonment, to screen out complaints where adequate investigation is not warranted at that stage. The rationale is not entirely without foundation: unchecked registration of all complaints has its own costs, but as explained in Section 9.1, the enquiry period does not replace the 3-day signature period: there are two back-to-back periods of gatekeeping for complainants. The Nepalese system, as outlined in Section 6.7, requires a similarly comparable authorization step by a magistrate for non-cognizable offences, but only once the complaint is already legally valid, resulting in a less practical burden for complainants as compared to the Indian system.

The citizen engagement, transparency and accessibility of the Crime and Criminal Tracking Network and Systems (CCTNS) in India and Nepal's digital complaint system are quite different. On the other hand, while both are implementing online complaint registration, Nepal's approach is more holistic and citizen-centric, featuring secure authentication, real-time tracking, and direct communication, whereas India's focus is on administrative processing. While Nepal has a centralized database driven verification system with the Nagarik App which verifies the identity of the complainant at the time of filing, India has no systematic mechanism for digital-authentication and neither the BNSS nor state-level e-FIR systems check the complainant's identity prior to the filing of a complaint.²⁷

8.3 Accessibility and Inclusion

The three-level digital-divide model outlined in Section 3.2.2 (access, skills, outcomes) highlights the different areas of friction for the two jurisdictions at each of these levels in the context of accessibility. Nepal's system is also removing the second physical barrier that India's Section 173(1)(ii) signature requirement brings at access, by digitally verifying the complainant when submitting the complaint, but Nepal's own access barriers, stemming from rural connectivity and infrastructure gaps (Section 6.6), are still significant. Both systems rely on complainants having a degree of digital literacy that enables them to make their way through an online form, which disproportionately disadvantages the same groups – rural, elderly and economically marginalised – in both countries (Section 3.3.3), and which is not currently compensated for by built-in features of either system other than informal or civil-society

²⁷²⁷ anowski, T. (2015). Digital government evolution: From transformation to contextualization. *Government Information Quarterly*, 32(3), 221–236. <https://doi.org/10.1016/j.giq.2015.07.001>



provided digital intermediation (Section 6.6). At the level of outcomes, the requirement to sign the document in the physical presence of the complainant within three days of filing the complaint (Section 173(1)(ii), BNSS) is likely to impact those who are unable to travel to sign the document because they are emotionally unavailable or are unable to afford the process due to economic constraints, and can even impact those who are physically able to travel to sign the document but are uncomfortable doing so.²⁸

8.4 Complaint Tracking and Transparency

In India, CCTNS and National Digital Police Portal are administrative databases and offer various services including FIR status, tenant verification and vehicle clearance, but do not have high levels of citizen engagement – citizens do not receive proactive updates when their complaints are referred for an enquiry under Section 173(3) of the BNSS and they do not get notified on the status of their complaints, such as whether they are pending, delayed or closed without follow-up. In contrast, Nepal's Nagarik App and OPCR portal provide a reference number that enables the complainant to constantly monitor the case and directly connect with the investigating officer, which India's system currently does not have.²⁹

8.5 Inclusive citizen participation and trust

India's deficiency in establishing formal channels of communication between complainants and investigating officials can hinder transparency, as it can reduce the impact of citizen participation and undermine the trust of the public in the system. Nepal's integrated platform (authentication, tracking, evidence collection and direct communication) is intended to foster exactly this level of trust, while, limited trust among citizens, especially vulnerable complainants, is due to institutional reluctance in the Nepal Police and incomplete data-protection measures.³⁰

8.6 The impact on access to justice

In sum, these findings suggest that there is now a more holistic understanding in Nepal of how to work towards digital justice, including authentication, status tracking, evidence submission, and direct communication, all on one platform. Though significant technology has been invested, the system of processes and institutions are still relatively opaque and inaccessible in India. In this particular aspect — the design of the digital-complaint interface and the accountability mechanisms that go with it— Nepal does better than India in ensuring that the system is accessible, accountable and trustworthy to citizens who file complaints, even if Nepal's constitutional and statutory underpinnings for compulsory FIR registration are comparatively weaker than India's (Section 1.2).³¹

9. Structural Loopholes and Systemic Deficits

²⁸ Mergel, I., Edelmann, N., & Haug, N. (2019). Defining digital transformation: Results from expert interviews. *Government Information Quarterly*, 36(4), 101385. <https://doi.org/10.1016/j.giq.2019.06.002>

²⁹ Contini, F., & Cordella, A. (2015). Digital technologies for better justice: A toolkit for action. *Government Information Quarterly*, 32(4), 380–390. <https://doi.org/10.1016/j.giq.2015.09.005>

³⁰ Susskind, R. (2019). Online courts and the future of justice. *Computer Law & Security Review*, 35(1), 1–11. <https://doi.org/10.1016/j.clsr.2018.11.005>

³¹ Contini, F., & Cordella, A. (2015). Digital technologies for better justice: A toolkit for action. *Government Information Quarterly*, 32(4), 380–390. <https://doi.org/10.1016/j.giq.2015.09.005>



9.1 Physical Presence Requirement under BNSS

The central paradox of the e-FIR provisions in the BNSS 2023 is the physical-presence requirement embedded in Section 173(1): information may be submitted electronically, but must be signed in person at the police station within three days of submission. This converts the e-FIR into a notice document rather than a standalone electronic legal instrument, defeating much of the purpose of electronic reporting. The consequences are serious for complainants who are geographically isolated from a police station, physically disabled, in a security-compromised environment, or otherwise unable to travel — precisely the population the 22nd Law Commission identified as most in need of an electronic filing option. The BNSS increases the number of digital steps preceding the physical barrier, but does not remove the barrier itself.

9.2 Limited Scope of Electronic Reporting

The BNSS introduces a deliberately broad definition of 'electronic communication' in Section 2(1)(i), encompassing, for example, WhatsApp messages, emails, video calls, and social-media transmissions — but this breadth has produced institutional confusion rather than clarity. Police stations in Mumbai receive hundreds of complaints of digital-banking fraud daily across various platforms, yet only a fraction are entered as FIRs, and complainant follow-up in person is still typically required. The Jammu and Kashmir and Ladakh High Court's September 2023 decision on whether a WhatsApp complaint constitutes 'substantial compliance' with FIR-filing requirements did not resolve this uncertainty (see Section 8.1). In practice, state-level e-FIR implementation remains confined to non-heinous offences — those punishable by no more than three years' imprisonment — leaving unresolved whether an electronically submitted report of a more serious offence should be treated as an FIR or merely as information, a jurisdictional gap that materially affects complainants' rights and the integrity of the criminal-justice process.

9.3 Deficits in Authentication and Acknowledgment

India's e-FIR system lacks an integrated authentication mechanism at either the BNSS or the state e-FIR portal level: complainants are not required to authenticate their identity before filing. This stands in contrast to Hong Kong's email confirmation within 15 minutes and unique reference number, and the United Kingdom's provision of a case number and assigned investigating officer. The absence of a matching acknowledgment system in India creates an informational gap that undermines public confidence and facilitates systemic non-registration.

9.4 Infrastructure and Technology Challenges

Despite an outlay of ₹2,000 crore on CCTNS, implementation of digital policing has been delayed and adopted unevenly across states, without a consistent institutional commitment to cloud-based infrastructure. This hesitation appears to reflect institutional risk perception more than an objective risk assessment, since well-configured cloud platforms are generally more secure than comparable on-premise state systems. Funding instability compounds the problem: the programme is funded through annual budget appropriations and has been suspended on several occasions owing to budget shortfalls.

9.5 Data Transparency and Accountability Gaps



A further significant gap is the absence of published data on the use, processing, and disposal of e-FIRs. Neither the National Crime Records Bureau (NCRB) nor state police maintain accessible records of the number of digital complaints received, the proportion that result in registered FIRs, or the eventual disposition of digitally reported crimes. This information vacuum makes policy evaluation difficult and insulates institutional non-performance from public and judicial scrutiny — a gap the BNSS does not address. Read through the three-level digital-divide framework applied in Section 8.3, this data gap is itself an outcomes-level failure: without published disaggregated data, it is not possible to determine whether the access and skills gaps documented for rural, female, elderly, and economically marginalized complainants are translating into worse registration and investigation outcomes, which is precisely the empirical question the reform proposed in Section 10.7 is designed to make answerable. This accountability gap mirrors the broader pattern identified in the literature on digital governance in India, which finds that opportunities and challenges of digital public-service delivery are frequently shaped as much by institutional transparency and accountability practices as by the underlying technology itself.³²

10. Reform Recommendations

The foregoing analysis identifies specific legislative, administrative, and technological reforms needed to make India's e-FIR system genuinely citizen-friendly. These recommendations draw on the comparative international evidence presented in Section 7 and respond directly to the structural deficits identified in Section 9.

10.1 Removing the Mandatory Physical-Signature Requirement

The first priority is removing the mandatory physical-signature requirement in Section 173(1) of the BNSS. The provision should be amended to allow e-FIRs to be submitted entirely through electronic means, supported by Aadhaar-based biometric verification, One-Time Password (OTP) authentication, or another digital-authentication mechanism notified by the Central Government. This would collapse the current two-stage process — digital followed by physical — into a single digital stage.

10.2 Secure Digital Authentication Framework

India should establish a secure digital-authentication system providing at least biometric-based verification of complainant identity at the point of filing (via the Aadhaar platform, OTP, or similar means), ensuring that the legal validity of a complaint is embedded in the electronic filing itself rather than in a subsequent physical process.

10.3 Unified National E-FIR Portal

All state e-FIR portals should incorporate a structured, guided complaint-lodging procedure that classifies offence category, severity, and jurisdiction; determines complainant eligibility; informs complainants of the applicable complaint and investigation procedure; and identifies the investigating authority. This would help minimize misclassification and institutional triage,

³² Mishra, A., & Kaushik, A. (2023). Digital governance and public service delivery in India: Opportunities and challenges. *Journal of Public Affairs*, 23(4), e2901. <https://doi.org/10.1002/pa.2901>



and would provide clarity to complainants, ideally through a single, uniform national e-FIR portal rather than the current fragmented array of state-level systems.

10.4 Mandatory Acknowledgment and Tracking Mechanisms

India should legislate a mandatory acknowledgment system modeled on Hong Kong's practice, generating an e-acknowledgment with a unique reference number sent to the complainant within a fixed period — for example, within half an hour of electronic filing. This reference number should enable real-time case tracking through a publicly accessible, authenticated portal developed by the Ministry of Home Affairs, and should be mandatory for all state police forces.

10.5 Expanding Electronic Reporting to More Serious Offences

Restricting e-FIR registration to offences punishable by less than three years' imprisonment is arbitrary and undermines the objectives of digital-justice reform. The BNSS should be amended, or rules framed under it, to permit electronic filing of FIRs for more serious offences, subject to appropriate safeguards such as Aadhaar-based verification and mandatory attachment of electronic evidence, together with a streamlined preliminary-enquiry procedure for such offences.

10.6 Digital Inclusion Strategies

Legal reform must be paired with sustained investment in digital inclusion, guided by the principles outlined in Section 3.4.3: a multi-faceted approach addressing access, skills, usage, and outcomes rather than infrastructure alone; social equity as the central criterion for evaluating digital-governance initiatives; participatory engagement with marginalized communities in shaping digital-government services; and scaled digital-literacy programmes, civil-servant training, and community digital-skills development to ensure that infrastructure investment translates into tangible benefits for rural, female, elderly, and economically marginalized citizens in both India and Nepal.

10.7 Data Publication and Accountability Standards

The NCRB should be placed under a statutory duty to collect, validate, and publish quarterly disaggregated data on e-FIR inputs, the rate of conversion from e-FIR to registered FIR, the rate of investigation initiation following e-FIR, and average investigation and disposal times. This requirement would create the accountability infrastructure necessary for evidence-based policy evaluation and judicial review of systemic non-registration. In parallel, the Ministry of Home Affairs should approve a defined timeframe and budget for transitioning CCTNS to cloud infrastructure, subject to security protocols approved by MEITY, and should establish a dedicated technology-modernization fund, separate from the annual budget cycle, to ensure stable multi-year funding for digital-policing infrastructure. Nepal's eFIR system should likewise be subject to independent monitoring, with results shared publicly, consistent with the comparative literature reviewed in Section 3.

11. Conclusion



This comparative analysis shows that the effectiveness of an e-FIR system depends not merely on the statutory recognition of an electronic complaint, but on the capacity of the surrounding digital mechanisms to enhance access, transparency, accountability, and citizen participation. India possesses a stronger institutional and judicial framework safeguarding the mandatory registration of cognizable offences, yet substantial procedural hurdles remain: administrative gatekeeping under Section 173(1)(ii) of the BNSS, combined with the extended preliminary-enquiry procedure under Section 173(3), creates opportunities for delay even as it formally enables digital filing. Nepal, by contrast, has built a more citizen-centred digital system combining secure digital-identity verification, mandatory electronic acknowledgment, complaint-tracking mechanisms, and direct channels between complainant and investigating authority — while facing implementation challenges of its own, discussed in Sections 6.6 and 6.7, that qualify but do not eliminate this comparative advantage.

This study extends existing scholarship by demonstrating, through a comparative case study, that technological innovation alone is not sufficient to secure access to justice. Digital-justice mechanisms must be paired with legal protection, ensuring that citizens can lodge complaints without being subject to police discretion, and that clear digital procedures allow citizens to follow their complaints through to resolution. The comparative findings suggest lessons that other South Asian jurisdictions seeking to modernize criminal-justice governance might draw from Nepal's experience — in particular, that secure digital authentication combined with real-time tracking and communication capability demonstrates how technology can serve both procedural integrity and citizen trust.

This study recommends that India revise the three-day physical-signature rule in favour of secure electronic-signature verification, such as OTP-based or biometric e-signature systems, and that the scope of preliminary enquiries be kept to the minimum necessary, consistent with the principles laid down in *Lalita Kumari v. State of Uttar Pradesh*, to prevent unnecessary delay in FIR filing. It further recommends the creation of a unified national digital-policing system to replace the current fragmented array of state-level systems, providing citizens with real-time complaint tracking and communication facilities. Finally, both India and Nepal must invest in digital-inclusion programmes — particularly for the rural poor, women, and other marginalized communities — to ensure that the benefits of digital justice are available to all citizens. Reforms of this kind would make the criminal-justice systems of both countries fairer, more open, and more transparent.

12. Implications for Policy and Practice

For India, the findings in Sections 9 and 10 point toward an immediate legislative priority: amending Section 173(1)(ii) of the BNSS to remove the physical-signature requirement, paired with a Ministry of Home Affairs-led rollout of a unified, authenticated national e-FIR portal. Because policing is a state subject, the Ministry's practical leverage lies in conditioning CCTNS funding and MEITY-approved cloud migration (Section 9.4) on state adoption of common authentication and acknowledgment standards, rather than in direct legislative harmonization across states.



For Nepal, the priority is less legislative than institutional: consolidating the data-protection safeguards flagged in Sections 6.6 and 6.7, and formalizing the currently informal digital-intermediation model (trained civil-society 'digital workers') into a funded, monitored component of the Digital Nepal Framework, so that the accessibility gains documented in this study are not dependent on the continued availability of pilot-programme funding in Bagmati Province alone.

For both countries, the comparative evidence in Section 7 suggests that a mandatory, time-bound acknowledgment obligation — modeled on Hong Kong's 15-minute standard — is among the lowest-cost, highest-impact reforms available, since it requires no change to underlying investigative procedure and directly addresses the transparency gap identified as the most consistent complaint across the doctrinal and survey evidence in this study.

13. Future Research Agenda

This study opens several avenues for further research. First, longitudinal studies tracking e-FIR adoption and outcomes over time, particularly following any legislative amendment to Section 173(1)(ii), would allow researchers to assess whether removing the physical-signature requirement in fact increases registration rates, rather than relying on the cross-sectional comparison this study provides. Second, comparative studies of police attitudes toward digital complaint registration — extending the institutional-culture findings noted for Nepal in Section 6.6 to India's state police forces — would help identify where institutional resistance, rather than legal or infrastructural constraints, is the binding barrier to reform. Third, studies of e-FIR effectiveness disaggregated by offence type would test whether the benefits of digital filing documented here for non-heinous offences extend to the more serious offence categories this study recommends including in Section 10.5. Finally, extending the survey instrument used in this study (Appendix A) to a larger, stratified sample across additional Indian states with lower digital-infrastructure maturity than Gujarat (Section 4.4) would materially strengthen the generalizability of the empirical findings reported here.

Transparency Statement: The authors confirm that this study has been conducted with honesty and in full adherence to ethical guidelines.

Funding: The study received no external funding.

Conflict of Interest: The authors declare there is no conflict of interest.



References

- Anto, A. (2021). Analyzing the delay, pendency and backlog of criminal matters in India in the light of COVID-19 with special reference to Kerala: An empirical study (Master's dissertation). National University of Advanced Legal Studies, Kochi.
- Asian Development Bank. (2019). Legal empowerment for women and disadvantaged groups: South Asia studies. Asian Development Bank.
- Baxi, U. (1976). Access, development and distributive justice: Access problems of the 'rural' population. *Journal of the Indian Law Institute*, 18(3), 375–401.
- Bhandari, R. B., Bhatta, N., Sharma, G., & Poudyal, Y. R. (2026). E-governance practices in Nepal: Opportunities, challenges, and strategies from the local level. *Journal of Computer Science*, 22(3), 367–377. <https://doi.org/10.3844/jcssp.2026.367.377>
- Brown, K. (2014). The promise and perils of digitising the police. *Policing and Society*, 24(2), 131–144. <https://doi.org/10.1080/10439463.2013.784309>
- Contini, F., & Cordella, A. (2015). Digital technologies for better justice: A toolkit for action. *Government Information Quarterly*, 32(4), 380–390. <https://doi.org/10.1016/j.giq.2015.09.005>
- Cordella, A., & Contini, F. (2020). Digital technologies for better justice: A toolkit for action. *Government Information Quarterly*, 37(4), 101466. <https://doi.org/10.1016/j.giq.2020.101466>
- Gupta, K. P., Singh, S., & Bhaskar, P. (2022). Citizen adoption of e-government: A literature review and conceptual framework. *Electronic Government, an International Journal*, 18(1), 1–25. <https://doi.org/10.1504/EG.2022.119377>
- Helsper, E. J. (2021). *The digital disconnect: The social causes and consequences of digital inequalities*. SAGE Publications.
- Islam, M. S., & Rahman, M. M. (2022). Digital transformation of public service delivery in Bangladesh: Challenges and opportunities of e-governance. *International Journal of Public Administration in the Digital Age*, 9(1), 1–17. <https://doi.org/10.4018/IJPADA.290001>
- Janowski, T. (2015). Digital government evolution: From transformation to contextualization. *Government Information Quarterly*, 32(3), 221–236. <https://doi.org/10.1016/j.giq.2015.07.001>
- Kuldeep, S., & Shaveta, B. (2020). *Police administration: Emerging issues & concerns*. Selective and Scientific Books.
- Lythreathis, S., Singh, S. K., & El-Kassar, A. N. (2022). The digital divide: A review and future research agenda. *Technological Forecasting and Social Change*, 175, 121359. <https://doi.org/10.1016/j.techfore.2021.121359>
- Maharjan, G. (2025). Examining the factors influencing the use of e-forms in government services in Itahari Sub-Metropolitan City. *Journal of Vishwa Adarsha College (JOVAC)*, 2(1), 157–178. <https://doi.org/10.3126/jovac.v2i1.83884>
- Mensah, I. K. (2020). Impact of government capacity and e-government performance on the adoption of e-government services. *International Journal of Public Administration*, 43(4), 303–311. <https://doi.org/10.1080/01900692.2019.1628059>



- Mergel, I., Edelmann, N., & Haug, N. (2019). Defining digital transformation: Results from expert interviews. *Government Information Quarterly*, 36(4), 101385. <https://doi.org/10.1016/j.giq.2019.06.002>
- Minow, M. (2014). Access to justice: Perspectives on the crisis and opportunities for reform. *Daedalus*, 143(3), 5–13.
- Mishra, A., & Kaushik, A. (2023). Digital governance and public service delivery in India: Opportunities and challenges. *Journal of Public Affairs*, 23(4), e2901. <https://doi.org/10.1002/pa.2901>
- Raperia, S. (2022). Ingredients and law of registration of FIR in India under the Criminal Procedure Code. SSRN. <https://ssrn.com/abstract=4120080>
- Saud, C. (2025). Cyber crime in Nepal: An analysis of case status and trends. Nepal Police Cyber Bureau.
- Scheerder, A., van Deursen, A. J. A. M., & van Dijk, J. A. G. M. (2017). Determinants of Internet skills, uses and outcomes: A systematic review of the second- and third-level digital divide. *Telematics and Informatics*, 34(8), 1607–1624. <https://doi.org/10.1016/j.tele.2017.07.007>
- Susskind, R. (2019). Online courts and the future of justice. *Computer Law & Security Review*, 35(1), 1–11. <https://doi.org/10.1016/j.clsr.2018.11.005>
- United Nations Development Programme. (2004). Access to justice: Practice note. UNDP.
- Van Deursen, A. J. A. M. (2024). Digital inequality during a pandemic: Update of the second- and third-level digital divide framework. In *Communication and Information Technologies Annual*. Emerald Publishing.
- van Deursen, A. J. A. M., & Helsper, E. J. (2015). The third-level digital divide: Who benefits most from being online? In *Communication and Information Technologies Annual* (Vol. 10, pp. 29–52). Emerald Publishing. <https://doi.org/10.1108/S2050-206020150000010002>
- Wei, K. K., Teo, H. H., Chan, H. C., & Tan, B. C. Y. (2011). Conceptualizing and testing a social cognitive model of the digital divide. *Information Systems Research*, 22(1), 170–187. <https://doi.org/10.1287/isre.1090.0273>

Views and opinions expressed in this article are the views and opinions of the author(s), *NPRC Journal of Multidisciplinary Research* shall not be responsible or answerable for any loss, damage or liability etc. caused in relation to/arising out of the use of the content.



Appendix A: Survey Instrument

Section 1: Demographic and Location Information

1. Location cluster (Ahmedabad / Dhrangadhra–Bahnagar / Gogha)
2. Age group
3. Gender
4. Prior experience filing a police complaint or FIR (Yes / No)

Section 2: Awareness

5. Are you aware of the e-FIR / online complaint-filing system? (Yes / No / Somewhat)
6. I would like to know more about how the e-FIR system works. (Likert: Strongly Disagree – Strongly Agree)

Section 3: Accessibility and Usability

7. I would prefer to file a complaint online rather than visit a police station in person. (Likert scale)
8. The current process for filing an e-FIR is easy to use. (Likert scale)
9. The categories of offences that can currently be reported online should be expanded. (Likert scale)

Section 4: Authentication and Transparency

10. A secure authentication system (e.g., OTP or biometric verification) would improve the reliability of the e-FIR process. (Likert scale)
11. The current e-FIR system is transparent about the status of my complaint. (Likert scale)