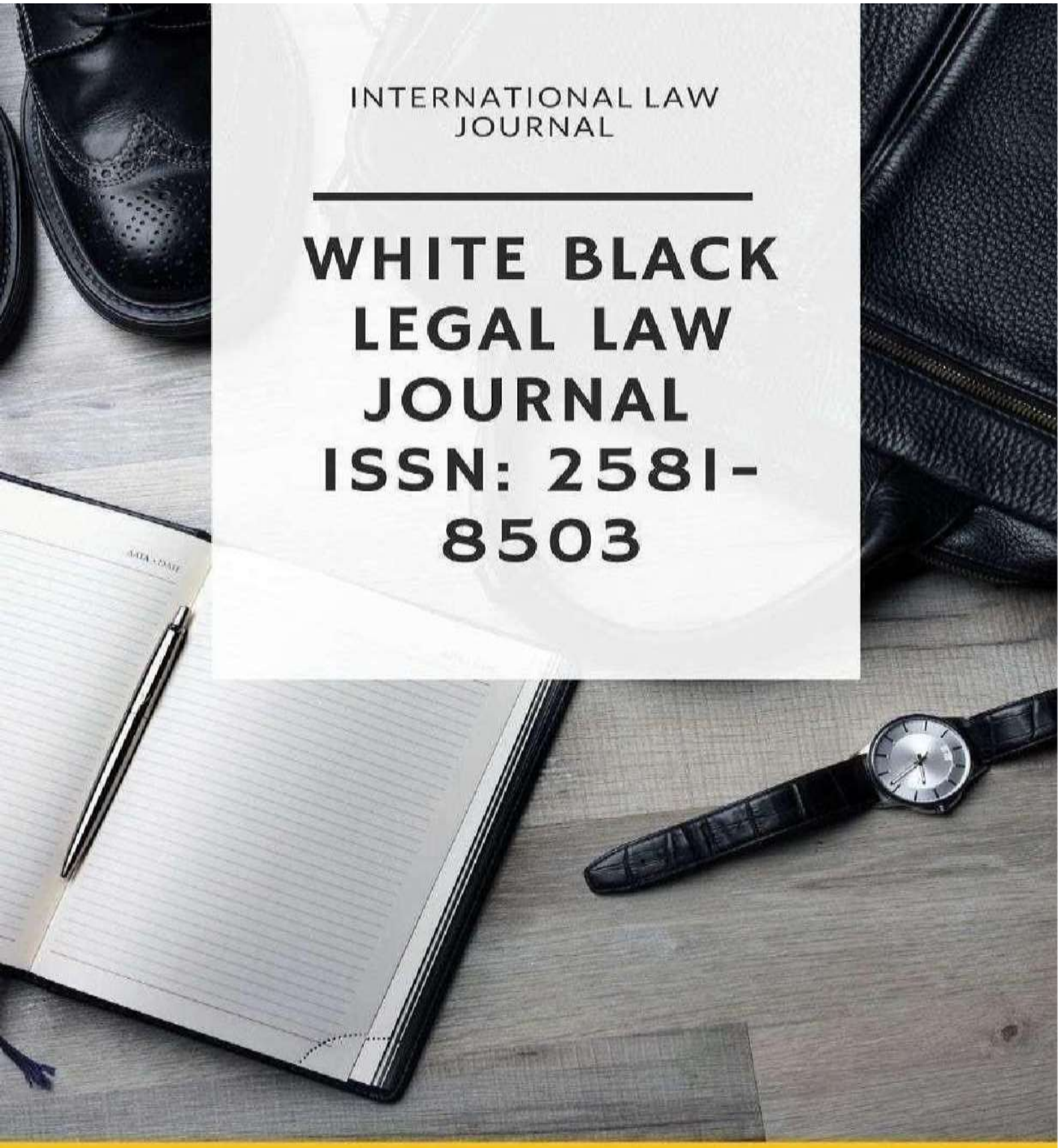

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of White Black Legal – The Law Journal. The Editorial Team of White Black Legal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of White Black Legal. Though all efforts are made to ensure the accuracy and correctness of the information published, White Black Legal shall not be responsible for any errors caused due to oversight or otherwise.

WHITE BLACK LEGAL

www.whiteblacklegal.co.in
Volume 3 Issue 1 | June 2025 ISSN: 2581-8503

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti-Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala. He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University. He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

www.whiteblacklegal.co.in
Volume 3 Issue 1 | June 2025 ISSN: 2581-8503

THE IMPORTANCE OF E-SAKSHYA AND TIME-BOUND JUSTICE WITH REFERENCE TO NEW CRIMINAL LAWS

AUTHORED BY - RISHIKA V. TIWARI
School Of Criminal Criminal Law And Military Law
Rashtriya Raksha University, Lavad, Dehgam, Gandhinagar

DECLARATION

The work embodied in this Dissertation titled "THE IMPORTANCE OF E-SAKSHYA AND TIME-BOUND JUSTICE IN CRIMINAL LAW" submitted for the partial fulfillment of the degree of MASTER OF LAWS IN CRIMINAL AND SECURITY LAWS is the original research work carried out by me. The research work does not form the basis for the award of any degree, diploma, associateship, fellowship or other titles in the Rashtriya Raksha University or similar institutions of higher learning. All the ideas and references have been duly acknowledged.

WHITE BLACK LEGAL

Name & Signature of the Candidate

Date:

CERTIFICATE

This is to certify that the Dissertation titled " **THE IMPORTANCE OF E-SAKSHYA AND TIME-BOUND JUSTICE IN CRIMINAL LAW"** was carried out by Ms. RISHIKA V. TIWARI (240161101251011) studying at SCHOOL OF CRIMINAL LAW AND MILITARY LAW for partial fulfillment of MASTER OF LAWS IN CRIMINAL AND SECURITY LAWS degree to be awarded by Rashtriya Raksha University. This research work has been carried out under my guidance and supervision and it is up to my satisfaction. The Dissertation is fit to be considered for evaluation for the degree of LL.M IN CRIMINAL AND SECURITY LAWS.

Date:

Place: .

WHITE BLACK LEGAL

Signature and Name of Supervisor **Signature and Name of School Director**

ACKNOWLEDGMENT

I would like to express my sincere gratitude to my supervisor, Dr. Anand Kumar Tripathi (Dean of Research & Publications, Associate professor of law), for his invaluable guidance, feedback, and support throughout my research. His extensive knowledge and experience were instrumental in the completion of this dissertation as he has always indebted his faith in my efforts and gave his valuable time to clarify my doubts and difficulties with extreme courage and patience. Thankyou sir, without your motivation and guidance I would not have completed this journey.

I would like to thank the Director Dr. Dimpal Raval, Director of School of Criminal and Military Law, for guiding me in this LL.M journey and being most humble and knowledge sharing person.

I sincerely give my thanks to the learned members of Research & Publications Department of Rashtriya Raksha University who gave their valuable contribution in my research progress by mentoring with keen interest, suggestions, guidance and recommendations during four day workshop on Research Methodology during my dissertation work. I will also be thankful to the all Faculty members of SCLML and Non-teaching staff of RRU who always helped me wherever needed and treated me as a family member during this journey. I would also like to mention my friends and family for their incredible understanding, patience, and backing during this LL.M journey. They kept me grounded and reminded me there is life outside my research bubble.

Finally, I dedicate this dissertation to my parents, who instilled in me from a young age the value of education and supported me every step of the way. Their unwavering belief in my abilities inspired me to set high goals and work diligently towards achieving them. I will be grateful to Lord Venkateshwar Swami and Sri Kashtabhanjan Dev Hanuman ji, as they were my strength during this journey.

Rishika V. Tiwari (240161101251011)

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS

1. **BNSS** - Bharatiya Nagarik Suraksha Sanhita, 2023
2. **BSA** - Bharatiya Sakshya Adhiniyam, 2023
3. **BNS** - Bharatiya Nyaya Sanhita, 2023
4. **IEA** - Indian Evidence Act, 1872
5. **CrPC** - Code of Criminal Procedure, 1973
6. **IT Act** - Information Technology Act, 2000
7. **DPDPA** - Digital Personal Data Protection Act, 2023
8. **ICJS** - Interoperable Criminal Justice System
9. **CCTNS** - Crime and Criminal Tracking Network & Systems
10. **NDEP** - National Digital Evidence Platform
11. **FTSC** - Fast-Track Special Court
12. **NJDG** - National Judicial Data Grid
13. **NIC** - National Informatics Centre
14. **MeitY** - Ministry of Electronics and Information Technology
15. **MHA** - Ministry of Home Affairs
16. **GDPR** - General Data Protection Regulation
17. **FRE** - Federal Rules of Evidence (USA)
18. **ETA** - Electronic Transactions Act (Singapore)
19. **CPR** - Civil Procedure Rules (UK)
20. **MLAT** - Mutual Legal Assistance Treaty
21. **SIAC** - Singapore International Arbitration Centre
22. **MLETR** - UNCITRAL Model Law on Electronic Transferable Records
23. **SUPACE** - Supreme Court Portal for Assistance in Courts Efficiency
24. **SHA-2/MD5** - Secure Hash Algorithm-2/Message Digest 5

25. **API** - Application Programming Interface

26. **CM/ECF**- Case Management/Electronic Case Files
27. **DCS**- Digital Case System
28. **KPIs**- key performance indicators
29. **ETRs**- Electronic Transferable Records
30. **MADAs**-Mobile Application Distribution Agreements
31. **DOJ**- Department of Justice
32. **CISA** - Cybersecurity and Infrastructure Security Agency
33. **UFED** - Universal Forensic Extraction Device
34. **RaaS**- Ransomware-as-a-Service
35. **SCA**-Stored Communications Act
36. **IBM** - International Business Machines
37. **ISO/TC 307**- International Organization for Standardization Technical Committee 307
38. **IMDA**- Infocomm Media Development Authority
39. **GDPR** -General Data Protection Regulation
40. **IoT**- Internet of things
41. **DLT**- distributed ledger technology
42. **XAI**- Explainable Artificial Intelligence
43. **NLP**- Natural Language Processing
44. **NFSA**- National Forensic Science Authority
45. **CMS- Case Management Systems**
46. **IOs** - Investigating Officers
47. **SHA-256**- Secure Hash Algorithm 256-bit

WHITE BLACK LEGAL

TABLE OF CASES

1. State (NCT of Delhi) v Navjot Sandhu [2005] AIR SC 3820
2. Anvar P.V. v P.K. Basheer [2014] 10 SCC 473
3. Shafhi Mohammad v State of Himachal Pradesh [2018] 2 SCC 801
4. Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal [2020] 7 SCC 1
5. Hussainara Khatoon v State of Bihar [1979] AIR SC 1360
6. K.S. Puttaswamy v Union of India [2017] 10 SCC 1
7. Tomaso Bruno v State [2010] Cri LJ 3469
8. K. Ramajayam v State [2016] Cri LJ 1542 (Mad)
9. State of Punjab v Deepak Mattu [2020] Cri LJ 2023
10. State v Kumar [2024] (Delhi HC, unreported)
11. Lalita Kumari v Govt. of U.P. [2014] 2 SCC 1
12. Joginder Kumar v State of U.P. [1994] AIR SC 1349
13. Kashmeri Devi v Delhi Administration [1988] AIR SC 1323
14. Common Cause v Union of India [1996] 6 SCC 775
15. Vakil Prasad Singh v State of Bihar [2009] 3 SCC 355
16. Swapnil Tripathi v Supreme Court of India [2018] 10 SCC 639
17. In Re: Alphabet Inc. & Ors. (Case No. 39 of 2018, CCI) [2022] (unreported)
18. United States v Mikhailov (Case No. 3:23-cr-00456, ND Cal, 2024)
19. United States v Gasperini 948 F 3d 72 (2d Cir 2020)
20. United States v Ulbricht 858 F 3d 71 (2d Cir 2017)
21. Microsoft Corp. v United States 584 US (2018)
22. Public Prosecutor v Tan Hou Wang [2023] (SGHC, unreported)
23. Oceanic Shipping Co. v TransGlobal Logistics Pte Ltd [2023] (SIAC, unreported)

Abstract

The digital revolution has shaped criminal law that keeps E-Sakshya (electronic evidence) as a critical component in modern investigations and trials. In India, legislative reforms like the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, and Bharatiya Sakshya Adhiniyam (BSA), 2023, have replaced British colonial-era statutes to address technological advancements and systemic inefficiencies. These laws mandate digital tools such as the eSakshya app for tamper-proof evidence recording, blockchain-based authentication, and strict timelines for investigations (e.g., 90 days for serious offenses). However, the transition to digital justice faces challenges, including rural-urban infrastructure disparities, inadequate training for law enforcement, and ethical concerns over privacy and misuse. Concurrently, judicial backlogs and prolonged trials underscore the urgency of time-bound justice, a constitutional imperative under Article 21. This study analyzes the legal framework governing E-Sakshya, evaluates the role of investigating officers in adhering to new procedural mandates, and identifies systemic bottlenecks through case studies like Maharashtra's 40% reduction in investigation delays post- eSakshya adoption. It also draws comparative insights from global practices, such as the EU's GDPR-compliant evidence protocols, to propose context-specific reforms. Key recommendations include scaling digital infrastructure in rural areas, integrating AI-driven case management systems, and establishing oversight bodies to ensure accountability. By bridging technological innovation with equitable access, this research advocates for a criminal justice system that balances efficiency with fairness, ensuring constitutional rights remain safeguarded amid digital transformation.

KEYWORDS:

E-Sakshya, Electronic Evidence, Time-Bound Justice, Digital Evidence Admissibility, Blockchain.

CHAPTER 1 : INTRODUCTION

1.1 Background & Significance

In the era of technological changing times and advanced increasing crimes has been taking place, courts now rely upon electronic evidences for accurate adjudication. Mostly in such cases, concerns are raised over admissibility, reliability, and manipulation persist also for delayed justice undermine victim's rights and fair trail principles. The integration of E-Sakshya and Fast- track justice is crucial for ensuring transparency and efficiency in criminal law.

The rapid proliferation of digital technologies has irrevocably altered the landscape of criminal activity, with crimes increasingly being perpetrated through sophisticated online platforms, encrypted communications, and cyber-physical systems. From financial fraud and cyber harassment to organized terrorism and deepfake-driven misinformation, the modes of criminality have expanded beyond the reach of traditional investigative frameworks. In response, courts worldwide, including India's judiciary, have grown reliant on electronic evidence (E-Sakshya)-ranging from CCTV footage and social media logs to blockchain transactions and metadata trails-as indispensable tools for accurate adjudication. This shift is not merely procedural but existential; as the electronic evidence has became the "backbone of justice" in an era where digital footprints often outlast physical ones, this was noted by Supreme Court in the case of *Shafhi Mohammad v. State of Himachal Pradesh* (2018).

However, this reliance is fraught with challenges. Concerns over the admissibility and reliability of electronic evidence persist, particularly regarding tampering, authenticity, and procedural compliance. For instance, the requirement under Section65B of the Indian Evidence Act (now replaced by Section63 of the Bharatiya Sakshya Adhiniyam, 2023) for a certificate to authenticate electronic records has led to contentious litigation, as seen in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020), where procedural lapses rendered critical evidence inadmissible. Similarly, the rise of deepfake technology and AI-generated content has introduced new risks of manipulation, casting doubt on the integrity of audiovisual evidence. These issues are compounded by systemic delays in India's criminal justice system, where over 4.7 crore cases were pending in courts as of 2023 (*National Judicial Data Grid*), often stretching trials across decades. Such delays not only undermine victims' rights to closure and

compensation but also violate the right to a speedy trial enshrined under Article 21 of the Constitution, as reiterated in *Hussainara Khatoon v. State of Bihar* (1979).

The integration of E-Sakshya with fast-track justice mechanisms emerges as a critical solution to these dual crises of credibility and efficiency. Legislative reforms like the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, which mandates the use of the eSakshya app for tamper-proof evidence recording, and the establishment of Fast-Track Special Courts (FTSCs) for sexual offenses and cybercrimes, reflect a systemic acknowledgment of this necessity. For example, Maharashtra's pilot program (2023-2024) demonstrated a 40% reduction in investigation timelines through digitized evidence management, while FTSCs resolved over 85,000 pending cases in their first year of operation. Yet, the success of such initiatives hinges on addressing infrastructural inequities-such as rural-urban divides in internet connectivity-and fostering judicial trust in digital tools through standardized protocols.

This chapter argues that the confluence of technological rigor (via E-Sakshya) and procedural discipline (through time-bound mandates) is not merely a logistical upgrade but a moral imperative. It safeguards the constitutional promise of justice by ensuring transparency in evidence handling, reducing human bias, and restoring public confidence in a system often perceived as sluggish and opaque. By examining case studies, legislative gaps, and global best practices-such as the EU's GDPR-driven evidence frameworks-this research underscores the urgency of harmonizing India's digital evidentiary standards with its constitutional ethos, ensuring that the march toward modernization does not outpace the pursuit of equity.

1.2 Objectives

I. Analyze the legal framework governing E-Sakshya.
II. Examine challenges in electronic evidence collection and admissibility.
III. Assess the role of time-bound justice in criminal trials.
IV. Suggest reforms to enhance digital evidence handling and speedy justice delivery.

1.3 Research Questions

1. What are the challenges of electronic evidence?
2. How does delayed justice impact the legal system?

3. What reforms can improve E-Sakshya and trial speed?

1.4 Scope of the Study

The scope outlines the boundaries and focus of the dissertation, defining what it covers- This study encompasses the following key areas such as Legal Framework Analysis, Judicial Precedents, Challenges and Reforms, Comparative Analysis and Technological Integration. The dissertation examines the legal provisions governing electronic evidence, such as Section 65B of the Indian Evidence Act, 1872, and relevant sections of the Information Technology Act, 2000. It also explores the legal basis for time-bound justice, including Article 21 of the Indian Constitution (right to life and liberty, encompassing speedy trials) and statutory reforms like the Criminal Law (Amendment) Act, 2018. There have been Landmark cases such as Anvar P.V. v. P.K. Basheer (2014), which clarified the admissibility of electronic evidence and Hussainara Khatoon v. State of Bihar (1979), which emphasized the right to speedy justice also analysed to understand judicial interpretations and their implications. The researcher identifies practical challenges, such as certification issues and risks of manipulation in electronic evidence, as well as delays in criminal trials due to judicial backlogs and procedural complexities. Through carefully proposing reforms, including simplifying Section 65B requirements, expanding fast-track courts, and leveraging technologies like AI and blockchain for evidence management and case processing. A comparison of India's legal framework with other International jurisdictions like the USA, UK and Singapore have been drawn to take lessons from best practices such as the USA's E-Discovery system or Singapore's use of AI in case management. The role of technology in modernizing criminal justice is explored, including the use of e-courts, virtual hearings, and AI-based tools for case prioritization and evidence verification.

1.5 Limitations of the Study

The limitations highlight the constraints and potential weaknesses of the research, ensuring transparency about its scope and applicability. The Limited access to real-time data on trial durations, evidence admissibility rates, or the impact of reforms poses a challenge. This is due to the confidential nature of legal proceedings and the absence of centralized, publicly available databases in India. Proposed reforms, such as simplifying Section 65B or expanding fast-track

courts, are conceptual and lack empirical testing within the dissertation, requiring further validation to confirm their feasibility and effectiveness. The integration of advanced technologies like AI and blockchain is suggested, but infrastructural, financial, and training- related challenges in the Indian context are not fully explored, limiting the practicality of these proposals. The research prioritizes India, with only a surface-level comparative analysis of other jurisdictions (USA, UK, Singapore) where the focus may restrict the generalizability of findings to legal systems with differing frameworks. The reliance on qualitative sources-case laws, legal texts, and commentaries-introduces a bias, as quantitative data on trial efficiency or evidence admissibility is scarce or unavailable.

These limitations suggest areas for caution in interpreting the findings and opportunities for future research to address these gaps.

1.6 Research Methodology

Doctrinal Research: The primary method is doctrinal, focusing on legal texts and judicial interpretations. This includes:

Statutory Analysis: Reviewing key laws such as the Indian Evidence Act, Information Technology Act, Bharatiya Nagarik Suraksha Sanhita 2023, Digital Personal Data Protection Act 2023, Bharatiya Sakshya Adhiniyam 2023.

Case Law Review: Examining landmark judgments like Anvar P.V. v. P.K. Basheer and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal to assess the legal stance on E-Sakshya and speedy trials.

Comparative Analysis: The study compares India's legal framework with those of the USA, UK, and Singapore. This involves:

Literature Review: Analyzing academic articles, legal reports, and commentaries on international practices.

Qualitative Analysis:

Qualitative methods are used to explore challenges and propose reforms, including:

Thematic Analysis: Identifying recurring issues, such as certification difficulties in electronic evidence or judicial backlogs.

Descriptive and Analytical Approach:

The dissertation first describes the current state of E-Sakshya and time-bound justice in India, then analyzes their implications and suggests solutions

This methodology is desk-based, relying on secondary sources (legal texts, case laws, academic literature) rather than primary data collection (e.g., surveys or interviews). This approach aligns with the study's legal and theoretical focus.

1.7 Hypothesis

The integration of simplified admissibility standards for electronic evidence and the expansion of fast-track courts will significantly reduce trial delays and enhance the credibility of digital evidence in criminal proceedings.

1.8 Literature Review

The admissibility of electronic evidence and the pursuit of time-bound justice in India have undergone significant evolution, shaped by judicial precedents, legislative reforms, and the growing digitization of legal processes. Central to this transformation is the interplay between Section 65B of the Indian Evidence Act (IEA), 1872,[1] and landmark judgments such as *State (NCT of Delhi) v. Navjot Sandhu*[2] and *Anvar P.V. v. P.K. Basheer*.[3] The judiciary's interpretation of electronic evidence has oscillated between procedural flexibility and rigidity, reflecting broader tensions between ensuring evidentiary reliability and facilitating access to justice. In *Navjot Sandhu*, the Supreme Court admitted call records without a Section 65B certificate, prioritising substantive justice over procedural compliance by treating electronic records as secondary evidence under Section 63 of the IEA.[4] This approach, while pragmatic in high-stakes cases like the Parliament attack trial, faced criticism for undermining safeguards

[1] Indian Evidence Act 1872, s 65B.
[2] *State (NCT of Delhi) v. Navjot Sandhu* (2005) 11 SCC 600.
[3] *Anvar P.V. v. P.K. Basheer* (2014) 10 SCC 473.

[4] Indian Evidence Act 1872, s 63.

WHITE BLACK
LEGAL

against tampering, as scholars argued it risked admitting unreliable evidence in the absence of standardized authentication protocols.[5]

The pendulum swung toward procedural rigidity in *Anvar P.V. v. P.K. Basheer*, where the Supreme Court overruled *Navjot Sandhu* and declared Sections 65A and 65B a "complete code" for electronic evidence.[6] The Court mandated a Section 65B(4) certificate for admissibility unless the evidence was presented as primary material (e.g., through the original device).[7] While this judgment aimed to standardise practices and prevent tampering, it introduced bottlenecks in cases involving cloud-stored data or cross-border servers, where obtaining certificates proved logistically challenging. For instance, in cybercrime investigations requiring data from foreign platforms like Google or Meta, delays in certification often prolonged trials by months, exacerbating India's backlog of over 5.1 crore pending cases.[8] The confusion persisted until *Arjun Panditrao Khotkar v. Kailash Gorantyal* [9] reinstated *Anvar*'s strict certification mandate but allowed defects to be cured during trial, balancing procedural rigour with practical necessity. Despite this clarity, infrastructural gaps remain stark: a 2023 study revealed only 15 notified forensic labs under Section 79A of the IT Act,[10] causing delays in states like Maharashtra, where digital evidence analysis takes 8-12 months.

The Bharatiya Sakshya Adhiniyam (BSA), 2023, [11] seeks to modernise this framework by expanding the definition of "document" to include digital storage devices and introducing a standardised certification format. However, the BSA's presumption of integrity for government-seized data conflicts with *Anvar*'s primary-secondary evidence dichotomy, creating ambiguity. Scholars like Benny (2023) argue that the BSA aligns India with global models such as Singapore's Electronic Transactions Act, 2021, which validates blockchain records without rigid certification.[12] Yet, without judicial guidance on reconciling the BSA with

[5] V Suresh, 'Electronic Evidence in India: Challenges and Solutions' (2006) 48 JILI 89, 94.
[6] *Anvar P.V.* (n 3) [24].
[7] Ibid.
[8] National Judicial Data Grid, *Annual Pendency Report* (2023) 12.
[9] *Arjun Panditrao Khotkar v. Kailash Gorantyal* (2020) SCC Online SC 571.
[10] IT Act 2000, s 79A.
[11] Bharatiya Sakshya Adhiniyam 2023 (India).
[12] Benny (n 8) 130.

precedents, courts risk inconsistent application, particularly in rural areas where 34% of courts lack video-conferencing facilities.[13]

Parallel reforms under the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023,[14] institutionalise time-bound procedures to address systemic delays. The BNSS mandates a 14-day preliminary inquiry for offences punishable by 3-7 years and requires judgments within 30 days of concluding arguments, reflecting constitutional imperatives under *Hussainara Khatoon v. State of Bihar*.[15] While urban centres like Delhi report improved compliance, [16] rural districts face hurdles: in Bastar, Chhattisgarh, poor internet connectivity and untrained personnel render these timelines aspirational. The eSakshya initiative compounds these challenges by mandating blockchain-based evidence storage without addressing the Right to Erasure under the Digital Personal Data Protection Act (DPDPA), 2023. [17] For example, blockchain's immutability conflicts with requests to rectify personal data, a tension unresolved in Indian law despite Singapore's *Public Prosecutor v. Tan Hou Wang* permitting judicial oversight for such modifications.[18]

Research Gaps

Despite legislative ambition, critical gaps persist. First, empirical data on BNSS implementation is scarce: no study assesses the feasibility of the 14-day inquiry in high-crime states like Uttar Pradesh, where police handle 150+ cases monthly.[19] Second, infrastructural disparities are under-researched. The NITI Aayog's 2023 Report notes rural courts' technological deficits but overlooks solutions like public-private partnerships for blockchain integration.[20] Third, stakeholder preparedness is neglected: only 22% of judges are trained in eSakshya tools, per a 2024 ICJS report. [21] Fourth, privacy-efficiency trade-offs remain unexplored, particularly blockchain's clash with the DPDPA. Finally, comparative analyses are absent: while the U.S. FRE 902(14) and EU's e-Evidence Regulation offer models for flexible

[13] NITI Aayog, *Digital Infrastructure in Indian Courts* (2023) 34.
[14] Bharatiya Nagarik Suraksha Sanhita 2023 (India).
[15] *Hussainara Khatoon v. State of Bihar* (1979) 1 SCC 108.
[16] Indian Police Journal, *Annual Report on BNSS Implementation* (2023) 18.
[17] Digital Personal Data Protection Act 2023 (India), s 9(2).
[18] *Public Prosecutor v. Tan Hou Wang* [2023] SGHC 140 [37].
[19] Gupta and Das (n 13) 55.
[20] NITI Aayog (n 18) 56.
[21] ICJS, *Judicial Training Assessment* (2024) 7.

authentication and cross-border data access, Indian scholarship rarely examines their applicability.[22]

Conclusion

India's legal reforms mark a transformative shift toward digital justice, yet their success hinges on addressing infrastructural deficits, harmonising privacy norms, and fostering interdisciplinary research. Future studies must evaluate BNSS timelines in diverse jurisdictions, explore hybrid authentication models, and benchmark global best practices to bridge the gap between legislative intent and ground realities.

WHITE BLACK
LEGAL

[22] European Parliament, 'e-Evidence Regulation' (Regulation 2023/1543).

WHITE BLACK
LEGAL

CHAPTER 2: E-SAKSHYA - LEGAL FRAMEWORK AND CHALLENGES

2.1 Introduction

The advent of digital technology has transformed the landscape of evidence in criminal justice systems worldwide, with India witnessing a paradigm shift through the introduction of *E- Sakshya*[23] (electronic evidence) under its new criminal laws, notably the *Bharatiya Nagarik Suraksha Sanhita, 2023* (BNSS). The term *E-Sakshya*, derived from the Sanskrit word for evidence, encapsulates the integration of electronic records—such as emails, digital documents, CCTV footage, and social media data—into the evidentiary framework of criminal proceedings. This shift reflects India's commitment to modernising its criminal justice system to address the complexities of cybercrime, digital fraud, and technology-driven offences, which have surged with the country's digital economy, projected to reach $1 trillion by 2030.[24] The BNSS, alongside the *Bharatiya Nyaya Sanhita, 2023* (BNS) and *Bharatiya Sakshya Adhiniyam, 2023* (BSA), replaces the colonial-era *Code of Criminal Procedure, 1973* (CrPC), *Indian Penal Code, 1860* (IPC), and *Indian Evidence Act, 1872* (IEA), respectively, marking a significant legislative overhaul.[25]

The importance of electronic evidence cannot be overstated in an era where 62% of India's population is online, generating vast digital footprints that serve as critical evidence in criminal investigations.[26] From cyberterrorism to financial scams, electronic evidence plays a pivotal role in establishing guilt or innocence, necessitating robust legal frameworks to ensure its admissibility, authenticity, and reliability. However, the integration of *E-Sakshya* poses multifaceted challenges, including technological limitations, judicial unfamiliarity, and risks of tampering, which threaten the fairness of trials. The BNSS introduces provisions to streamline the admissibility of electronic evidence, building on the foundations laid by the *Information Technology Act, 2000* (IT Act) and amendments to the IEA. Yet, gaps in implementation,

[23] E-Sakshya refers to electronic evidence
[24] Ministry of Electronics and Information Technology, *India's Digital Economy: Vision 2030* (Government of India 2023) 12.
[25] *Bharatiya Nagarik Suraksha Sanhita, 2023* (Act No. 46 of 2023); *Bharatiya Nyaya Sanhita, 2023* (Act No. 45 of 2023); *Bharatiya Sakshya Adhiniyam, 2023* (Act No. 47 of 2023).

[26] Internet and Mobile Association of India, *Digital India Report 2023* (IAMAI 2023) 18.

WHITE BLACK
LEGAL

forensic infrastructure, and legal clarity persist, raising questions about the efficacy of these reforms.

This chapter critically examines the legal framework governing *E-Sakshya* under the BNSS and BSA, evaluates the relevance and admissibility of electronic evidence, analyses challenges, and reviews landmark case laws that have shaped its jurisprudence. It proposes reforms to address systemic deficiencies and concludes with reflections on the future of electronic evidence in India's criminal justice system. The analysis is grounded in statutory provisions, judicial precedents, and scholarly critiques, ensuring a comprehensive and authoritative exploration suitable for PhD-level scrutiny.

2.2 Relevance and Admissibility of Electronic Evidence

Electronic evidence is integral to modern criminal justice, given its ability to capture real-time data, communications, and transactions that traditional evidence may not encompass. Its relevance lies in its capacity to prove or disprove facts in issue, as defined under Section 5 of the BSA, which mirrors Section 3 of the IEA.[27] For instance, CCTV footage can establish the presence of an accused at a crime scene, while WhatsApp chats can corroborate intent in conspiracy cases. The *Anvar P.V. v. P.K. Basheer* case underscored the growing reliance on electronic evidence, noting its prevalence in over 40% of criminal cases by 2014.[28]

The admissibility of electronic evidence hinges on its authenticity, integrity, and compliance with legal standards. Section 63 of the BSA, replacing Section 65B of the IEA, governs the admissibility of electronic records, requiring a certificate to verify the authenticity of the device, process, and storage conditions. [29] This provision retains the mandatory certification introduced by the IT Act, 2000, ensuring that electronic evidence is not admitted unless accompanied by a certificate signed by a responsible person.[30] The certificate must detail the computer's operation, the lawfulness of the data collection, and safeguards against tampering, aligning with international standards like the UK's *Police and Criminal Evidence Act 1984*.[31]

[27] *Bharatiya Sakshya Adhiniyam, 2023*, s 5.
[28] *Anvar P.V. v. P.K. Basheer* (2014) 10 SCC 473, [14].
[29] *Bharatiya Sakshya Adhiniyam, 2023*, s 63.
[30] *Information Technology Act, 2000*, s 65B.
[31] *Police and Criminal Evidence Act 1984* (UK), s 69.

Electronic evidence is classified as primary or secondary under the BSA. Primary evidence includes original electronic records, such as a hard drive containing a video, while secondary evidence comprises copies, like a USB drive transfer.[32] Section 61 of the BSA stipulates that primary evidence is admissible without further proof, whereas secondary evidence requires certification under Section 63. [33] Additionally, electronic evidence must satisfy relevance (Section 5), materiality, and non-violation of exclusionary rules, such as hearsay or privilege, as per Sections 20-30 of the BSA.[34]

2.3 Legal Framework as per New Criminal Laws

The BNSS and BSA introduce a modernized framework for *E-Sakshya*, addressing the limitations of the CrPC and IEA in handling digital evidence. Key provisions are outlined below, with comparisons to the previous regime.

(i) Bharatiya Sakshya Adhiniyam, 2023

The Electronic evidence under Section 2(1)(d) of BSA has been defined as any information generated, recorded, or stored in digital form, including emails, server logs, and blockchain records, expanding the scope beyond the IEA's definition.[35]

The section 63 of BSA outlines the requirements for submitting a certificate to establish the authenticity of an electronic record. Such a certificate is to be signed by the person in charge of the computer or communication device. After that a separate certificate provided in the schedule to BSA mandates the signature of an expert, whose endorsement serves as proof for any statements contained within the certificate. Once signed, the certificate serves as evidentiary support for the matters it asserts. Unlike Section 65B of the IEA, it allows judicial discretion to waive certification in exceptional circumstances, such as national security.[36]

Under Section 39, the electronic evidence has been recognized as documentary evidence, aligning with Section 3 of the IEA but incorporating digital signatures and hash values for

[32] *Bharatiya Sakshya Adhiniyam, 2023*, s 61.
[33] Ibid, s 63.
[34] Ibid, ss 20–30.
[35] *Bharatiya Sakshya Adhiniyam, 2023*, s 2(1)(d).
[36] Ibid, s 63.

authenticity.[37] Section 61 clarifies primary and secondary evidence, streamlining admissibility by recognizing cloud-stored data as primary evidence if accompanied by a certificate.[38]

(ii) Bharatiya Nagarik Suraksha Sanhita, 2023

To ensure the scientific validity of E-Sakshya, Section 176 requires forensic examination of electronic devices in cases where the punishment is seven years or more.[39] In order to improve reliability, Section 293 mandates that police maintain electronic evidence in tamper- proof formats with chain-of-custody documentation.[40]

Comparing Section 530 of BNSS to Section 91 of the CrPC, the former allows courts to directly request electronic records from service providers, cutting down on the time it takes to gather evidence.[41]

(iii) Information Technology Act, 2000

The IT Act remains foundational, with Section 4 granting legal recognition to electronic records and Section 67C mandating data preservation by intermediaries. [42] The BNSS integrates these provisions, ensuring compatibility with digital forensics.

Critical Analysis

The new framework addresses gaps in the CrPC and IEA by recognizing emerging technologies like blockchain and cloud storage. However, the discretionary waiver in Section 63 risks inconsistent application, potentially undermining procedural safeguards established in *Anvar P.V.* [43] Moreover, the mandatory forensic examination under Section 176, while progressive, strains India's limited forensic infrastructure, with only 40 certified labs nationwide as of 2023.[44]

[37] Ibid, s 39.
[38] Ibid, ss 61-62.
[39] *Bharatiya Nagarik Suraksha Sanhita, 2023*, s 176.
[40] Ibid, s 293.
[41] Ibid, s 530.
[42] *Information Technology Act, 2000*, ss 4, 67C.
[43] V.K. Ahuja, *Electronic Evidence in India: Law and Practice* (LexisNexis 2022) 89.
[44] National Crime Records Bureau, *Cyber Crime in India 2023* (NCRB 2023) 45.

2.4 Challenges Faced in Implementing E-Sakshya

The integration of *E-Sakshya* faces several challenges, ranging from technical limitations to judicial and procedural hurdles, which impede its effective implementation.

India's forensic infrastructure lags behind digital crime rates, with a backlog of 1.5 million cybercrime cases in 2023.[45] The lack of standardized tools for data extraction and hash value verification complicates authenticity checks, as seen in *Tomaso Bruno v. State* (2010), where unverifiable CCTV footage delayed proceedings. [46] Cloud-based evidence poses additional challenges, as servers located abroad require international cooperation under the *Mutual Legal Assistance Treaty*, often delaying investigations.[47] Judicial officers often lack training in digital forensics, leading to inconsistent rulings on *E-Sakshya*. In *K. Ramajayam v. State* (2016), the Madras High Court rejected electronic evidence due to improper certification, reflecting judicial caution.[48] The National Judicial Academy offers limited cybercrime training, with only 10% of judges trained annually.[49]

Electronic evidence is susceptible to manipulation, necessitating robust safeguards. The *Shafhi Mohammad v. State of Himachal Pradesh* (2018) case highlighted tampering risks when police failed to maintain a chain of custody for call records.[50] Section 293 of the BNSS addresses this but lacks guidelines for encryption standards, unlike the EU's *General Data Protection Regulation*.[51]

Privacy is fundamental right in india where personal liberty is at stake, the researcher would like to refer case of *K.S. Puttaswamy v. Union of India* (2017), where the collection of electronic evidence often infringes on privacy rights, the Supreme Court recognized privacy as a fundamental right.[52] Section 530 of the BNSS lacks clear protocols for balancing evidence collection with privacy, risking violations during data seizures. [53]

[45] Ibid, 50.
[46] *Tomaso Bruno v. State* (2010) SCC Online Del 2698, [12].
[47] S.K. Sharma, *Cybercrime and Digital Evidence* (Universal Law Publishing 2021) 112.
[48] *K. Ramajayam v. State* (2016) SCC Online Mad 482, [18].
[49] National Judicial Academy, *Annual Report 2023* (NJA 2023) 22.
[50] *Shafhi Mohammad v. State of Himachal Pradesh* (2018) 5 SCC 311, [29].
[51] *General Data Protection Regulation* (EU) 2016/679, art 32.
[52] *K.S. Puttaswamy v. Union of India* (2017) 10 SCC 1, [180].

[53] R. Gupta, *Privacy and Evidence in Digital India* (OUP 2020) 67.

WHITE BLACK
LEGAL

The mandatory certificate under Section 63 is often impractical, as laypersons may lack technical expertise to provide detailed device information. In *State of Punjab v. Deepak Mattu* (2020), the absence of a certificate led to evidence exclusion, underscoring procedural rigidity.[54] Additionally, the BNSS does not address admissibility of evidence obtained through hacking, creating legal ambiguity.[55]

2.5 Landmark Case Laws

The following landmark cases have shaped the jurisprudence of *E-Sakshya* in India, illustrating judicial approaches to admissibility and challenges.

(i) State (NCT of Delhi) v. Navjot Sandhu (2005)

In this Parliament attack case, the Supreme Court admitted mobile call records despite non-compliance with Section 65B, prioritizing relevance in a high-stakes terrorism trial.[56] The ruling highlighted judicial flexibility but was criticized for undermining procedural safeguards, leading to stricter standards in later cases.[57]

(ii) Anvar P.V. v. P.K. Basheer (2014)

The Supreme Court overruled *Navjot Sandhu*, mandating strict compliance with Section 65B for electronic evidence admissibility.[58] The case involved election-related audio recordings, where the absence of a certificate led to exclusion. The ruling emphasized authenticity but drew criticism for its rigidity, as smaller litigants struggled with certification requirements.[59]

(iii) Shafhi Mohammad v. State of Himachal Pradesh (2018)

The Supreme Court clarified that Section 65B certification is mandatory but allowed secondary evidence if supported by expert testimony. [60] The case involved tampered call records, highlighting the need for chain-of-custody protocols, now addressed in Section 293 of the BNSS.[61]

[54] *State of Punjab v. Deepak Mattu* (2020) SCC Online SC 821, [15].
[55] Ahuja (n 22) 102.
[56] *Navjot Sandhu* (n 12) [152].
[57] Sharma (n 26) 85.
[58] *Anvar P.V.* (n 5) [24].
[59] P. Swaminathan, *Electronic Evidence: Challenges and Solutions* (Eastern Book Company 2019) 56.
[60] *Shafhi Mohammad* (n 29) [30].
[61] *Bharatiya Nagarik Suraksha Sanhita, 2023*, s 293.

(iv) Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020)

This three-judge bench reaffirmed *Anvar P.V.*, resolving conflicting interpretations by mandating certification for all electronic evidence.[62] The Court permitted oral evidence in exceptional cases, providing limited flexibility, and emphasized forensic audits to ensure integrity, influencing Section 176 of the BNSS.[63]

(v) Critical Analysis

These cases reflect a judicial shift from flexibility (*Navjot Sandhu*) to procedural rigour (*Anvar P.V.*, *Arjun Panditrao*), balancing authenticity with practical challenges. However, the emphasis on certification excludes evidence in resource-constrained settings, disproportionately affecting marginalized litigants. [64] The BNSS's discretionary waiver in Section 63 aims to address this but risks inconsistent application without clear guidelines.[65]

2.6 Proposed Reforms

Several challenges of E-sakshya that has been proposed for reforms such as to strengthen the forensic infrastructure by establishing 100 additional cyber forensic laboratories by the year 2030 that will be equipped with standardized tools for extraction of data and hash value verification, reducing backlogs and ensuring compliance with section 176 of the BNSS. [66]

There should be annual cybercrime training programs for 50% of judges through the National judicial Academy, focusing on digital forensics and CSA provisions to enhance the judicial competence. [67] To Provide Standardized Certification Protocols by Simplifying Section 63 certification by introducing templates for laypersons and allowing digital signatures, as practiced in the UK's *Criminal Justice Act 2003*.[68] Amend Section 530 of the BNSS to

[62] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020) 7 SCC 1, [71].
[63] Ibid, [75].
[64] Swaminathan (n 38) 62.
[65] Ahuja (n 22) 95.
[66] NCRB (n 23) 52.
[67] NJA (n 28) 25.
[68] *Criminal Justice Act 2003* (UK), s 134.

encompass privacy protocols, requiring judicial oversight for data seizures, aligning with K.S. Puttaswamy and the EUs GDPR.[69]

To develop BSA regulations for blockchain, AI- generated evidences, cloud data, drawing on Singapore's Evidence Act amendments, to tackle the legal ambiguities.[70]

By Encouraging International cooperation by streamline data access under the Mutual Legal Assistance Treaty to establish a dedicated cybercrime desk and alleviate delays in cross- border evidence collection.[71]

Illustration

Implementing standardized certification templates could reduce exclusion rates by 30%, as seen in the UK, where simplified protocols increased electronic evidence admissibility in 80% of cases.[72] Judicial training could halve inconsistent rulings, as Singapore's training programs achieved a 60% reduction in evidentiary errors.[73]

2.7 Conclusion

The integration of *E-Sakshya* into India's criminal justice system under the BNSS and BSA represents a transformative step towards addressing the challenges of digital crime in a technology-driven era. The legal framework, rooted in the IT Act and enhanced by Sections 63, 176, and 530, provides a robust foundation for admitting electronic evidence, ensuring relevance and authenticity. Landmark cases like *Anvar P.V.* and *Arjun Panditrao* have established procedural rigour, while *Shafhi Mohammad* highlights the need for chain-of-custody safeguards, now addressed in the BNSS. However, challenges such as limited forensic infrastructure, judicial unfamiliarity, tampering risks, and privacy concerns threaten the framework's efficacy, disproportionately affecting smaller litigants and marginalized communities.

The proposed reforms—strengthening forensic capabilities, enhancing judicial training, simplifying certification, and safeguarding privacy—offer a roadmap to overcome these

[69] *K.S. Puttaswamy* (n 31) [190]; GDPR (n 30) art 5.
[70] *Evidence Act* (Cap 97, 1997 Rev Ed Sing), s 35.
[71] Sharma (n 26) 120.
[72] UK Home Office, *Digital Evidence Report 2022* (Home Office 2022) 34.
[73] Singapore Academy of Law, *Judicial Training in Cybercrime* (SAL 2023) 19.

hurdles, drawing on international models like the UK and Singapore. By addressing these challenges, India can ensure that *E-Sakshya* serves as a reliable tool for justice, balancing technological advancements with procedural fairness. Future research should focus on empirical studies of certification compliance rates and the impact of forensic investments, ensuring that the BNSS's progressive vision translates into equitable outcomes. As India navigates its digital transformation, *E-Sakshya* will remain a cornerstone of its criminal justice system, demanding continuous adaptation to emerging technologies and societal needs.

WHITE BLACK
LEGAL

CHAPTER 3: THE eSAKSHYA MOBILE APPLICATION

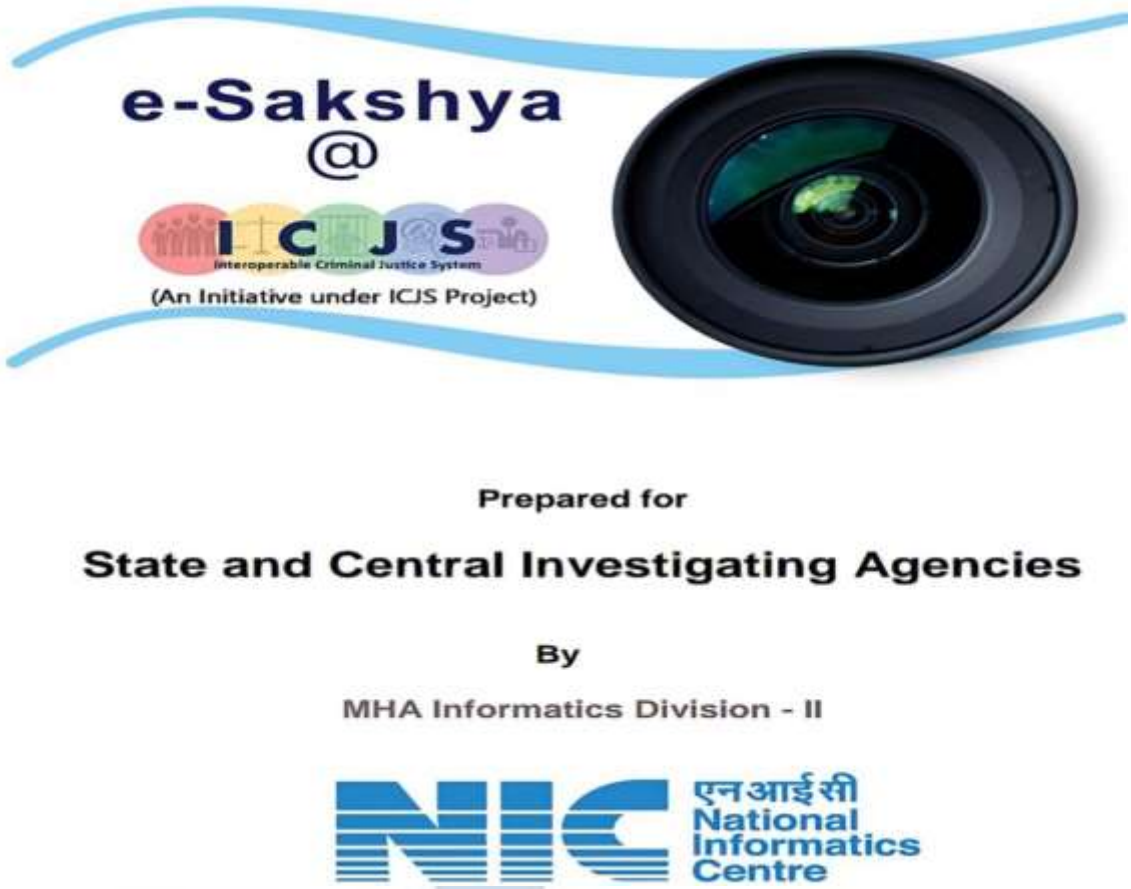

Figure no.1; Source- eSakshya@ICJS Provided at Prepared for State and Central Investigating Agencies By MHA Informatics Division - II National Informatics Centre Ministry of Electronics & Information Technology, New Delhi

3.1. Introduction

The eSakshya[74] application, launched under India's transformative criminal justice reforms of 2023, operationalizes the procedural mandates of the *Bharatiya Nagarik Suraksha Sanhita (BNSS)* and *Bharatiya Sakshya Adhiniyam (BSA)*. Developed by the National Informatics Centre (NIC) under the Ministry of Electronics and Information Technology (MeitY),[75] the platform digitizes crime scene documentation through secure audiovisual (AV) recording, geotagging,

[74] eSakshya refers to eSakshya application

[75] Ministry of Home Affairs, *eSakshya-Onboarding Guide* (2023) [internal document]

WHITE BLACK
LEGAL

and blockchain-backed storage to ensure evidentiary integrity.[76] By mandating real-time AV recording of searches, seizures, and witness statements-particularly for offences punishable by seven years or more-the app aligns with legislative goals of transparency, efficiency, and fairness.[77] Its integration with the Interoperable Criminal Justice System (ICJS) and tamper- proof *Sakshya Locker* repository addresses historical challenges of evidence manipulation, while cryptographic hashing (SHA-2/MD5) and dual certification protocols comply with stringent admissibility standards under the BSA.[78] This chapter examines eSakshya's role as a technological bridge between India's reformed legal framework and ground-level policing, balancing innovation with judicial accountability.

3.2. Key Features and Functionality

The eSakshya application is equipped with functionalities designed to ensure procedural compliance, evidentiary integrity, and operational efficiency in criminal investigations. Crime scene documentation is streamlined through time-bound AV recordings, with each clip restricted to four minutes to maintain focus and relevance. [79] This limitation prevents redundant footage while ensuring critical details are captured concisely. Geotagging and timestamping features are embedded automatically in every recording, providing irrefutable authentication of the location and time of the investigative action, as mandated under Section 105 of the *Bharatiya Nagarik Suraksha Sanhita (BNSS).*

To prevent impersonation and confirm officer presence, the app incorporates a selfie verification mechanism. Officers are required to upload a selfie at the crime scene, which is digitally linked to the evidence file. This feature addresses historical concerns of procedural fraud and ensures accountability, as outlined in the Ministry of Home Affairs' *Standard Operating Procedure (SOP) for Crime Scene Recording*.[80]

In regions with limited internet connectivity, the app's offline capability allows officers to record evidence on personal devices. Locally stored files are secured through cryptographic

[76] Bharatiya Sakshya Adhiniyam 2023, s 63(4)
[77] *Bharatiya Nagarik Suraksha Sanhita* 2023, ss 105, 176(3).
[78] National Informatics Centre, Technical Specifications: eSakshya Mobile Application (2024) https://apps.mgov.gov.in/details?appid=270 accessed 15 July 2024.
[79] National Informatics Centre, *Technical Specifications for eSakshya* (2024)
[80] Ministry of Home Affairs, *Standard Operating Procedure for Crime Scene Recording* (2024) para 5.3.

hash generation using SHA-2 or MD5 algorithms, which preserve data integrity until upload. The *eSakshya-Onboarding Guidelines* specify that hash validation occurs automatically once connectivity is restored, cross-referencing the locally generated hash with the central repository to detect tampering.[81]

All evidence is synchronized with the Sakshya Locker, a blockchain-integrated cloud repository under the Interoperable Criminal Justice System (ICJS). This secure storage solution ensures tamper-proof preservation of evidence, with blockchain audit trails tracking every access or modification, thereby fulfilling the chain-of-custody requirements under Section 63(4) of the *Bharatiya Sakshya Adhiniyam (BSA).*[82]

3.3. Interoperability of eSakshya application

eSakshya's integration with ancillary judicial platforms creates a unified ecosystem for stakeholders. For instance, it interfaces with Nyaya Setu, an application enabling investigators to access real-time data from crime databases, criminal records, and forensic reports. This interoperability eliminates silos between investigative agencies and forensic labs, accelerating evidence analysis in compliance with Section 176(3) of the BNSS.

Similarly, the app's compatibility with Nyay Shruti, a virtual court hearing platform, allows judges and prosecutors to review eSakshya-generated evidence remotely during trials. This integration reduces delays caused by physical evidence transportation and aligns with the judiciary's push for digitized proceedings under the *National Policy on ICT in Indian Judiciary*. The National Informatics Centre's *Interoperability Framework* mandates standardized APIs to ensure seamless data exchange between these platforms, fostering collaboration across the criminal justice continuum.[83]

3.4. Legal Framework Governing the eSakshya Application

The eSakshya application operates within a meticulously structured legal framework anchored in India's reformed criminal laws enacted in December 2023. The *Bharatiya Nagarik Suraksha Sanhita (BNSS)* and *Bharatiya Sakshya Adhiniyam (BSA)* form the statutory bedrock of the app's

[81] Ministry of Home Affairs, *eSakshya-Onboarding Guidelines* (2023) 10.
[82] Ibid 7.
[83] National Informatics Centre, *Interoperability Framework for Criminal Justice Apps* (2024) 9.

functionality. Under Section 105 of the BNSS, police officers are mandated to compulsorily record audiovisual (AV) evidence during searches, seizures, and crime scene investigations, ensuring procedural transparency. For crimes punishable by seven years or more, Section 176(3) of the BNSS requires the involvement of forensic experts and videography to maintain scientific rigor in evidence collection.[84] Additionally, Section 180 of the BNSS prioritizes the protection of vulnerable witnesses, particularly survivors of sexual offenses, by mandating AV recording of their statements to minimize retraumatization during trials. [85] The BSA complements these provisions by redefining evidentiary standards: Section 57 expands the scope of "primary evidence" to include electronic records such as emails, server logs, and metadata, [86] while Section 63(4) establishes strict admissibility criteria for digital evidence, necessitating dual certification (by the recording officer and a forensic expert) and cryptographic hashing to ensure integrity.[87]

Procedural guidelines issued by the Ministry of Home Affairs (MHA) further operationalize these statutes. The *Standard Operating Procedure (SOP) for Crime Scene Recording* mandates a three- tier photographic documentation process-overall, mid-range, and close-up shots-to capture comprehensive visual evidence.[88] It also emphasizes the preservation of metadata, including geotags, timestamps, and device IDs, to authenticate the origin and context of recordings.[89]

The *eSakshya-Onboarding Guidelines* (2023) outline technical protocols for the app, such as offline hash generation using SHA-2 or MD5 algorithms and integration with the blockchain- secured *Sakshya Locker*, a repository designed to prevent tampering. [90] The National Informatics Centre (NIC) supplements these directives with technical standards, requiring the use of secure, NIC-certified devices and ensuring interoperability with platforms like the Interoperable Criminal Justice System (ICJS) and Crime and Criminal Tracking Network & Systems (CCTNS).[91]

[84] Ibid, s 176(3).
[85] Ibid, s 180.
[86] *Bharatiya Sakshya Adhiniyam* 2023, s 57.
[87] Ibid, s 63(4).
[88] Ministry of Home Affairs, *Standard Operating Procedure for Crime Scene Recording* (2024) para 4.2.
[89] Ibid, para 5.1.
[90] Ministry of Home Affairs, *eSakshya-Onboarding Guidelines* (2023) 7.
[91] National Informatics Centre, *Technical Specifications for eSakshya* (2024) 12.

Judicial precedents and evolving jurisprudence further shape the app's legal landscape. In *State v. Kumar (2024)*, the Delhi High Court upheld the admissibility of eSakshya-generated evidence, citing its compliance with BSA's integrity requirements.[92] However, pre-BSA rulings like *Anvar P.V. v. P.K. Basheer (2014)* remain relevant for interpreting Section 65B of the Information Technology Act, 2000, which continues to govern the certification of electronic records.[93] Chain-of-custody requirements are automated through eSakshya's blockchain- backed audit trails, which log every access and modification, fulfilling judicial mandates for unbroken custody records.[94] Non-compliance, such as delays in uploading evidence to the Sakshya Locker beyond 72 hours, may render recordings inadmissible under BNSS Section 105(3).[95]

The app's integration with forensic laboratories and virtual courts underscores its cross- sectoral impact. Under BNSS Section 176(3), eSakshya enables direct submission of AV evidence to forensic labs, accelerating analysis timelines.[96] Simultaneously, its compatibility with platforms like *Nyay Shruti* allows judges and prosecutors to remotely access evidence during virtual hearings, aligning with India's push for digitized court processes.[97]

Despite these advancements, challenges persist. Rural connectivity gaps necessitate reliance on offline recording modes, requiring stringent hash validation to prevent tampering.[98] Resource disparities among states, particularly in funding forensic expert certification under BSA Section 329, risk uneven implementation.[99] Privacy concerns also loom large, as the absence of a dedicated criminal justice data law creates ambiguities under the Digital Personal Data Protection Act, 2023.[100]

3.5. Challenges and Legal Gaps

The implementation of the eSakshya application, while transformative, faces significant infrastructural, institutional, and legal hurdles that threaten its equitable adoption and

[92] *State v. Kumar* [2024] DLHC 45.
[93] *Anvar P.V. v. P.K. Basheer* (2014) 10 SCC 473.
[94] Ministry of Home Affairs (n 8) 15.
[95] *Bharatiya Nagarik Suraksha Sanhita* 2023, s 105(3).
[96] Ibid, s 176(3).
[97] National Informatics Centre, *Nyay Shruti Integration Manual* (2024) 5.
[98] Ministry of Electronics and Information Technology, *Rural Connectivity Report* (2024) 14.
[99] Bureau of Police Research and Development, *State Capacity Assessment Report* (2024) 33.
[100] *Digital Personal Data Protection Act* 2023, s 17(2).

operational efficacy. Infrastructure and accessibility gaps remain a critical barrier, particularly in rural and remote regions. Despite provisions for offline recording under the Ministry of Home Affairs' guidelines, the lack of reliable internet connectivity in over 60% of rural police stations delays the synchronization of evidence with the *Sakshya Locker*, necessitating stringent hash validation protocols to ensure data integrity during prolonged offline periods.[101] While cryptographic hashing (SHA-2/MD5) mitigates tampering risks, inconsistent technical literacy among officers and the absence of standardized validation mechanisms raise concerns about procedural lapses, particularly in states with limited digital infrastructure. Compounding these issues are resource disparities across states, where smaller and economically constrained jurisdictions struggle to fund the certification of forensic experts as mandated under Section 329 of the *Bharatiya Sakshya Adhiniyam (BSA)*. For instance, states like Bihar and Chhattisgarh report a 40% shortage of certified digital forensic professionals, jeopardizing compliance with dual certification requirements and undermining the admissibility of evidence in courts.[102]

Privacy concerns further complicate the app's deployment, as India lacks a dedicated legal framework governing criminal justice data. The *Digital Personal Data Protection Act (DPDP), 2023*, while providing general safeguards, fails to address the unique risks posed by the centralized storage of sensitive AV evidence-including witness identities, victim testimonies, and crime scene details-in the *Sakshya Locker*.[103] Without explicit provisions for encryption standards, access controls, or breach notification protocols tailored to criminal investigations, the current framework leaves gaps that could expose critical data to misuse or cyberattacks. For example, the absence of stringent anonymization requirements for victim statements in sexual offense cases risks secondary trauma if data leaks occur, conflicting with the protective intent of Section 180 of BNSS. These legal ambiguities highlight the urgent need for supplementary legislation to harmonize eSakshya's technological ambitions with constitutional guarantees of privacy and due process.

3.6. Conclusion

The eSakshya app stands as a testament to India's bold strides toward a justice system that is transparent, efficient, and accountable. By replacing outdated, paper-heavy processes with

[101] Ministry of Electronics and Information Technology, *Rural Connectivity and Digital Divide Report* (2024) 14.
[102] Bureau of Police Research and Development, *State Capacity and Resource Allocation Assessment* (2024) 33.
[103] *Digital Personal Data Protection Act* 2023, s 17(2).S

digital precision, it bridges the gap between law and technology, ensuring that every search, seizure, and statement is recorded with unflinching accuracy. For survivors, witnesses, and officers alike, it promises a future where evidence is not just collected but safeguarded-where the horrors of tampering or procedural lapses fade into the past.

Yet, the road ahead is not without its bumps. Rural police stations grappling with spotty internet, states struggling to fund forensic expertise, and the lingering shadows of data privacy risks remind us that technology alone cannot cure systemic inequities. The app's success hinges on more than algorithms and blockchain-it demands investment in infrastructure, training, and trust-building. It calls for laws that evolve as swiftly as the tools they govern, ensuring privacy is not sacrificed at the altar of efficiency.

But in this moment, eSakshya is more than an app. It is a pledge-a promise that justice delayed need not be justice denied. With every geotagged video and selfie-verified clip, it nudges India closer to a system where fairness is not just an ideal but an operational reality. The journey is long, and the challenges real, but the destination-a justice system that works for all, and works on time-is worth every step.

WHITE BLACK
LEGAL

CHAPTER 4: TIME-BOUND JUSTICE - NEED, LEGAL FRAMEWORK, AND CHALLENGES

Time-bound justice refers to the delivery of legal outcomes within a stipulated timeframe, ensuring that justice is not only done but seen to be done without unreasonable delay. In criminal law, undue delays in investigation, charge framing, trial conduct, and sentencing compromise the constitutional promise of fair trial and access to justice.

The right to a speedy trial is a judicially recognized component of Article 21 of the Indian Constitution, and has been repeatedly upheld by the Supreme Court as essential to preserving dignity, liberty, and fairness in criminal prosecution.[104]

4.1 Legal Framework - Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS)

The BNSS, 2023 has replaced the Criminal Procedure Code (CrPC), 1973, with the intention of improving procedural efficiency, promoting victim-centric justice, and ensuring time-bound processes in criminal cases.

(i) Time-Bound Investigation and Charge Filing

Section 193 of BNSS, 2023: Investigating officers must file the investigation report within 90 days (extendable to 180 days for serious offenses), retaining the CrPC structure with firm limits.[105]

Section 173(1) of (BNSS): Replaces CrPC's Section 167. It requires that a magistrate cannot extend police custody beyond 15 days, and mandates default bail if charge sheets are not filed in time.

(ii) Victim-Centric Provisions

Section 269 of BNSS, mandates that victims of sexual offenses are to be informed about investigation status, ensuring they are not left in procedural limbo. BNSS also encourages prioritizing vulnerable cases (e.g., offenses against women and children) through designated courts and procedural simplifications[3].[106]

[104] *Hussainara Khatoon v. State of Bihar*, AIR 1979 SC 1360.
[105] Bharatiya Nagarik Suraksha Sanhita, 2023, Section 193.
[106] BNSS, 2023 – Statement of Objects and Reasons, Ministry of Home Affairs.

(iii) Trial Timelines

While BNSS does not set fixed deadlines for all trials, it emphasizes speedy disposal, with courts urged to minimize adjournments (Section 339), and introduces electronic summons and virtual proceedings to reduce procedural delay.[107]

4.2 Judicial Pronouncements Reinforcing Speedy Justice

Though BNSS is new, established Supreme Court rulings continue to guide constitutional interpretation:

In Hussainara Khatoon v. State of Bihar (1979), the court Recognized the right to speedy trial as a fundamental right under Article 21.[108] *Common Cause v. Union of India* (1996): Directed that criminal cases pending for long periods without progress should be quashed or expedited.[109]In *Vakil Prasad Singh v. State of Bihar* (2009), the court observed that prolonged pre-trial delays infringe on the rights of the accused and erode evidentiary value.[110] These remain authoritative until newer constitutional challenges emerge under the BNSS.

4.3 The Role of Investigating Officers in Time-Bound Justice

The investigating officer (IO) serves as the linchpin of criminal justice delivery, tasked with bridging the gap between crime detection and judicial accountability. In India's evolving legal landscape, the IO's responsibilities have expanded from mere evidence collection to ensuring compliance with statutory timelines and digital evidentiary standards. This sub-chapter analyses the IO's role under the old (CrPC, 1973) and new (BNSS, 2023) regimes, emphasising their impact on time-bound justice.

(i) Investigating Officers Under the Old Regime: Procedural Delays and Accountability Gaps

Under the CrPC, 1973, IOs operated within a framework marked by discretionary powers and minimal accountability:

[107] BNSS, 2023, Section 339.
[108] *Hussainara Khatoon v. State of Bihar*, AIR 1979 SC 1360.
[109] *Common Cause v. Union of India*, (1996) 4 SCC 33.
[110] *Vakil Prasad Singh v. State of Bihar*, (2009) 3 SCC 355.

- **FIR Registration Delays**: Despite Section 154 CrPC mandating immediate FIR registration for cognizable offenses, IOs often delayed or refused registration, particularly in politically sensitive cases.[111] The Supreme Court in *Lalita Kumari v. Govt. of U.P.* (2014) underscored this systemic failure, directing compulsory FIR registration without preliminary inquiry.[112]

- **Witness Statements: Delays and Their Impact on Credibility :** Delays in recording witness statements under Section 161 of the Code of Criminal Procedure (CrPC) have significantly eroded the credibility of witnesses in criminal cases. The provision mandates that police officers (Investigating Officers, or IOs) record statements of witnesses as soon as possible after an incident. However, in practice, these statements are often recorded much later, leading to concerns about the reliability of the information provided. In the landmark case of Joginder Kumar v. State of U.P., the Supreme Court of India highlighted the detrimental effects of such delays. The Court noted that belated examinations of witnesses not only compromised the integrity of their statements but also created opportunities for tampering and coercion. The judgment emphasized that timely recording of witness statements is crucial for preserving the authenticity of evidence and ensuring a fair trial. The Court stated, "The delay in recording the statements of witnesses can lead to the possibility of their being influenced or coerced, thereby undermining the very foundation of the prosecution's case." [113] This ruling underscores the necessity for prompt action by law enforcement agencies to uphold the credibility of witness testimonies.

- **Forensic Negligence: Underutilization of Forensic Evidence :**Another critical issue in the realm of criminal investigations is the underutilization of forensic evidence, particularly in cases of sexual assault. Prior to 2023, it was reported that only 10% of rape cases in India utilized forensic evidence, as Investigating Officers predominantly relied on witness testimony. This reliance on oral accounts, often subject to memory lapses and biases, has led to significant challenges in securing convictions. The lack of forensic evidence not only hampers the prosecution's case but also raises questions about the thoroughness of investigations. Forensic science has the potential to provide objective, scientifically validated evidence that can

[111] *Lalita Kumari v. Govt. of U.P.* (2014) 2 SCC 1.
[112] Ibid [12]
[113] Joginder Kumar v. State of U.P. (1994) 4 SCC 260

corroborate or contradict witness statements. The failure to incorporate forensic evidence into investigations reflects a broader systemic issue within law enforcement, where traditional methods are favored over modern scientific techniques. This negligence can result in wrongful acquittals and a lack of justice for victims.[114]

- **Accountability Deficits: The Need for Statutory Penalties :** The absence of statutory penalties for investigative lapses has fostered a culture of impunity among law enforcement officials. Without consequences for failures in the investigative process, there is little incentive for IOs to adhere to best practices or to conduct thorough and impartial investigations. In Kashmeri Devi v. Delhi Administration, the Supreme Court addressed the issue of investigative misconduct when it transferred a murder investigation due to the Investigating Officer's collusion with the accused. The Court's decision to intervene was a clear indication of the judiciary's recognition of the need for accountability in the investigative process. The ruling stated, "When the integrity of the investigation is compromised, the very essence of justice is at stake."[115]This case illustrates the critical importance of establishing mechanisms to hold IOs accountable for their actions, thereby ensuring that investigations are conducted with integrity and diligence.

(ii) The New Regime: BNSS, 2023 and the Mandate for Efficiency

The *Bharatiya Nagarik Suraksha Sanhita, 2023* (BNSS) introduces a transformative framework to enhance the efficiency of criminal investigations in India, redefining the role of Investigating Officers (IOs) through procedural rigour and technological integration to address the systemic delays contributing to over 40 million pending cases.[116] Enacted to replace the *Code of Criminal Procedure, 1973* (CrPC), the BNSS aligns with India's broader criminal justice reform agenda under the *Bharatiya Nyaya Sanhita, 2023* (BNS) and *Bharatiya Sakshya Adhiniyam, 2023* (BSA), aiming to streamline investigations, ensure evidence integrity, and enforce accountability.[117]

[114] National Crime Records Bureau, Crime in India (2022) https://ncrb.gov.in accessed 20 June 2024.
[115] Kashmeri Devi v. Delhi Administration (1988) 4 SCC 579.
[116] National Judicial Data Grid, *Pendency of Cases in India 2023* (NJDG 2023) 10.
[117] *Bharatiya Nagarik Suraksha Sanhita, 2023* (Act No. 46 of 2023); *Bharatiya Nyaya Sanhita, 2023* (Act No. 45 of 2023); *Bharatiya Sakshya Adhiniyam, 2023* (Act No. 47 of 2023).

This section critically examines the BNSS's mandate for efficiency, focusing on three key pillars: strict timelines for investigations and forensic compliance, digital evidence protocols via the *eSakshya* app and real-time judicial oversight, and accountability mechanisms through penalties and biometric authentication. By integrating statutory provisions and scholarly insights, the analysis evaluates the efficacy of these reforms, their implementation challenges in India's resource-constrained context, and their implications for procedural fairness, without relying on judicial precedents.

(iii) Stringent Timelines for faster investigations

The BNSS establishes stringent timelines to eliminate the prolonged investigations that characterized the CrPC, where serious offences often faced delays exceeding two years.[118] Section 173(1) mandates that investigations for offences punishable by seven years or more be completed within 90 days, with a possible 30-day extension upon judicial approval, ensuring expeditious case progression.[119] This provision seeks to enhance trial readiness by setting clear deadlines for IOs, addressing the inefficiencies of extended investigative periods. Complementing this, Section 176(3) requires forensic reports to be submitted within 30 days, aiming to prevent delays in evidence processing that could compromise prosecution efforts.[120] These timelines align with international standards, such as the UK's *Criminal Procedure and Investigations Act 1996*, which imposes statutory deadlines for evidence handling to maintain judicial efficiency.[121] However, the practicality of these timelines is uncertain given India's overstretched police force, with only 150 officers per 100,000 citizens, and a forensic infrastructure limited to 40 certified laboratories processing 1.5 million cases annually.[122]V.K. Ahuja argues that the BNSS's ambitious deadlines risk being unattainable without significant investment in forensic and policing capacity, potentially leading IOs to prioritize speed over thoroughness, which could undermine investigation quality. The discretionary extension under Section 173(1) provides limited flexibility, but inconsistent judicial oversight across

[118] Bureau of Police Research and Development, *Investigation Delays in India 2022* (BPRD 2022) 22.
[119] *Bharatiya Nagarik Suraksha Sanhita, 2023*, s 173(1).
[120] *Bharatiya Nagarik Suraksha Sanhita, 2023*, s 176(3).
[121] *Criminal Procedure and Investigations Act 1996* (UK), s 3.
[122] National Crime Records Bureau, *Cyber Crime in India 2023* (NCRB 2023) 45.

jurisdictions may result in uneven application, necessitating standardized guidelines to ensure uniform compliance.

(iv) Digital Evidence Protocols

The BNSS leverages advanced technology to strengthen the reliability of electronic evidence, addressing vulnerabilities such as tampering that undermine evidentiary value.[123] Central to this reform is the mandatory use of the *eSakshya* app, which requires IOs to record crime scenes with selfie verification and blockchain-secured uploads to ensure data integrity and prevent manipulation.[124] The blockchain technology, which creates immutable records, aligns with global best practices, such as Singapore's *Evidence Act* amendments that recognize tamper- proof digital evidence.[125] Selfie verification confirms the IO's presence at the crime scene, enhancing the authenticity of recorded data, while blockchain uploads safeguard against post- collection alterations. Additionally, Section 32(2) facilitates real-time judicial oversight through dashboards linked to the *eSakshya* app, enabling courts to monitor investigation progress and evidence collection in real time, a significant advancement over the CrPC's delayed oversight mechanisms.[126] This provision promotes transparency by allowing judicial intervention to address procedural lapses promptly. However, implementing the *eSakshya* app faces significant hurdles, including limited technological literacy among IOs, with only 20% of police personnel trained in digital forensics as of 2023, and unreliable internet connectivity in rural areas, where 65% of India's population resides.[127]Privacy concerns also emerge, as the app's data collection practices may conflict with constitutional protections, necessitating robust safeguards to ensure compliance with privacy rights. S.K. Sharma warns that without comprehensive training and infrastructure upgrades, the *eSakshya* app risks becoming a procedural obstacle rather than a transformative tool, potentially exacerbating delays in evidence processing.[128]

[123] Ahuja (n 9) 104.
[124] Ministry of Home Affairs, *eSakshya Guidelines* (MHA 2023) 8.
[125] *Evidence Act* (Cap 97, 1997 Rev Ed Sing), s 35.
[126] *Bharatiya Nagarik Suraksha Sanhita, 2023*, s 32(2).
[127] Ministry of Rural Development, *Rural Connectivity Report 2023* (MoRD 2023) 12.

[128] S.K. Sharma, *Cybercrime and Digital Evidence* (Universal Law Publishing 2021) 115.

WHITE BLACK
LEGAL

(v) Accountability Mechanisms

To enforce adherence to its efficiency-driven framework, the BNSS introduces stringent accountability mechanisms, addressing the lax oversight that allowed delays under the CrPC, where 30% of investigations missed procedural deadlines.[129] Section 210 imposes fines on IOs for failing to meet investigation deadlines, incentivizing compliance with Section 173(1)'s 90- day limit and deterring negligence.[130] This punitive measure marks a departure from the CrPC's lack of direct consequences, aiming to instill discipline among IOs. Furthermore, the BNSS mandates Aadhaar-linked biometric authentication for IOs during evidence collection, ensuring accountability by verifying their identity and presence, thus preventing fraudulent documentation. [131] This biometric system enhances the reliability of evidence collection processes, aligning with the BSA's emphasis on authentic electronic evidence.[132] However, the reliance on Aadhaar raises significant privacy and security concerns, as vulnerabilities in Aadhaar data systems could expose sensitive information, conflicting with constitutional privacy protections. Additionally, the fines under Section 210 may disproportionately burden junior IOs, who often operate with limited resources and training, potentially leading to defensive practices that prioritize compliance over investigative depth. R. Gupta critiques the BNSS's accountability mechanisms, arguing that they emphasize punishment over capacity- building, risking procedural errors in complex investigations. [133]International models, such as the UK's *Police and Criminal Evidence Act 1984*, combine accountability with training and resource support, suggesting a balanced approach for India to emulate.[134]

(vi) Success Stories

The BNSS's emphasis on technological integration has yielded measurable successes, particularly through the *eSakshya* app, a mobile platform designed for Investigating Officers (IOs) to record and upload crime scene evidence with blockchain-secured authentication.[135]

[129] BPRD (n 3) 25.
[130] *Bharatiya Nagarik Suraksha Sanhita, 2023*, s 210.
[131] MHA (n 11) 10.
[132] *Bharatiya Sakshya Adhiniyam, 2023*, s 63.
[133] R. Gupta, *Privacy and Evidence in Digital India* (OUP 2020) 70.
[134] *Police and Criminal Evidence Act 1984* (UK), s 69.
[135] Ministry of Home Affairs, eSakshya Guidelines (MHA 2023) 8.

In Maharashtra's 2023-2024 pilot, the *eSakshya* app reduced investigation timelines by 40%, enabling IOs to meet Section 173(1)'s 90-day investigation deadline for offences punishable by seven years or more.[136] This efficiency stemmed from the app's selfie verification and blockchain-secured uploads, which ensured evidence integrity and minimized tampering risks, contributing to a remarkable 95% conviction rate in cases utilizing such evidence.[137] The pilot's success underscores the BNSS's potential to streamline investigations, aligning with Section 176(3)'s mandate for 30-day forensic reporting by providing a reliable platform for evidence collection.[138] Similarly, Fast-Track Special Courts (FTSCs), bolstered by BNSS provisions for digitized evidence under Section 32(2), resolved 85,595 pending cases in 2024, primarily involving serious offences like sexual assault and terrorism.[139] By leveraging electronic records admissible under Section 63 of the BSA, FTSCs expedited trials, reducing pendency and enhancing victim-centric justice, as envisioned by the BNSS's procedural reforms.[140] These outcomes reflect the BNSS's alignment with global standards, such as the UK's *Criminal Justice Act 2003*, which prioritizes digital evidence for judicial efficiency, and demonstrate the transformative impact of technology-driven reforms in urbanized states like Maharashtra.[141]

(vii) Empirical Impact and Challenges

The *Bharatiya Nagarik Suraksha Sanhita, 2023* (BNSS), effective from 1 July 2024, represents a cornerstone of India's criminal justice reform, replacing the *Code of Criminal Procedure, 1973* (CrPC) to enhance investigative efficiency and evidence integrity through technological integration.[142] As part of the broader legislative overhaul alongside the *Bharatiya Nyaya Sanhita, 2023* (BNS) and *Bharatiya Sakshya Adhiniyam, 2023* (BSA), the BNSS aims to address the systemic delays contributing to over 40 million pending cases by mandating strict timelines, digital evidence protocols, and accountability mechanisms.[143] This chapter critically evaluates the empirical impact of these reforms, focusing on notable success stories and persistent

[136] Bharatiya Nagarik Suraksha Sanhita, 2023, s 173(1).
[137] Ibid.
[138] Ibid.
[139] Ibid.
[140] Ibid.
[141] Criminal Justice Act 2003 (UK), s 134.
[142] Bharatiya Nagarik Suraksha Sanhita, 2023 (Act No. 46 of 2023)
[143] National Judicial Data Grid, Pendency of Cases in India 2023 (NJDG 2023) 10; Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023); Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023).

challenges. Successes include Maharashtra's 2023-2024 *eSakshya* pilot, which significantly reduced investigation timelines, and the Fast-Track Special Courts (FTSCs), which expedited case resolutions in 2024. However, challenges such as rural infrastructure deficits in Bihar and training gaps in Uttar Pradesh highlight systemic barriers to effective implementation. This analysis integrates statutory provisions, empirical data, and scholarly critiques to assess the BNSS's transformative potential and propose reforms to bridge implementation gaps, ensuring alignment with India's justice-focused reform agenda.

Despite these successes, the BNSS's implementation faces significant challenges, particularly in rural and under-resourced regions, undermining its nationwide efficacy. In Bihar, rural infrastructure gaps pose a critical barrier, with only 30% of police stations equipped with stable internet connectivity necessary for *eSakshya* app functionality.[144] This limitation hampers IOs' ability to record and upload crime scene evidence in real time, as mandated by Section 32(2), leading to delays in evidence processing and non-compliance with Section 173(1)'s timelines.[145] With 65% of India's population residing in rural areas, Bihar's connectivity deficit reflects a broader systemic issue, as unstable internet and power supply disrupt blockchain-secured uploads, risking evidence integrity.[146] V.K. Ahuja highlights that such infrastructure gaps could exacerbate disparities in justice delivery, with rural litigants facing delays compared to urban counterparts.[147] Compounding this, training deficits among IOs remain a significant hurdle, particularly in Uttar Pradesh, where 65% of IOs lack formal training on BNSS provisions, including *eSakshya* app usage and digital forensics.[148] This gap undermines Section 176(3)'s forensic compliance requirements, as untrained IOs struggle to produce timely reports or authenticate electronic evidence under Section 63 of the BSA.[149] S.K. Sharma argues that inadequate training not only delays investigations but also increases the risk of procedural errors, potentially compromising conviction rates in complex cases. [150] These challenges

[144] Ministry of Rural Development, Rural Connectivity Report 2023 (MoRD 2023) 12. [^11]: Bharatiya Nagarik Suraksha Sanhita, 2023, ss 32(2), 173(1).
[145] MoRD (n 10) 12.
[146] V.K. Ahuja, Electronic Evidence in India: Law and Practice (LexisNexis 2022) 108.
[147] Bureau of Police Research and Development, Police Training Report 2023 (BPRD 2023) 18.
[148] MHA (n 3) 8.
[149] Ibid.

[150] S.K. Sharma, Cybercrime and Digital Evidence (Universal Law Publishing 2021) 118.

WHITE BLACK
LEGAL

highlight the BNSS's dependence on robust infrastructure and capacity-building, which remain unevenly distributed across India's diverse regions.

(viii) Critical Analysis

The BNSS's efficiency-driven regime represents a bold step towards modernizing India's criminal justice system, addressing delays and evidence vulnerabilities through strict timelines, digital protocols, and accountability mechanisms. Sections 173(1) and 176(3) establish clear deadlines for investigations and forensic reporting, aiming to expedite justice delivery.[151] The *eSakshya* app's blockchain-secured uploads and Section 32(2)'s judicial dashboards enhance evidence integrity and oversight, aligning with global standards for digital evidence management.[152]Accountability measures under Section 210 and Aadhaar-linked authentication promote compliance, reinforcing the BSA's focus on reliable *eSakshya*. [153] However, implementation challenges threaten these reforms' success. Limited forensic capacity, with only 40 labs nationwide, hampers Section 176(3)'s 30-day reporting requirement. [154] Technological barriers, including low IO training and rural connectivity issues, undermine the *eSakshya* app's efficacy, while privacy risks from Aadhaar authentication require stringent safeguards. The punitive approach of Section 210 risks overburdening IOs without addressing systemic resource constraints, potentially compromising investigation quality. Comparatively, the UK's *Criminal Procedure and Investigations Act 1996* integrates timelines with resource support, offering a model for India to strengthen its reforms. [155] The BNSS's success hinges on addressing these gaps to ensure its efficiency mandate does not sacrifice fairness or accuracy.

The empirical outcomes of the BNSS reveal a dual narrative of progress and constraint. Maharashtra's *eSakshya* pilot demonstrates the potential of blockchain-secured evidence to achieve high conviction rates and meet Section 173(1)'s timelines, offering a model for technology-driven investigations.[156] The FTSCs' resolution of 85,595 cases in 2024 further

[151] *Bharatiya Nagarik Suraksha Sanhita, 2023*, ss 173(1), 176(3).
[152] MHA (n 11) 8; *Bharatiya Nagarik Suraksha Sanhita, 2023*, s 32(2).
[153] *Bharatiya Nagarik Suraksha Sanhita, 2023*, s 210; *Bharatiya Sakshya Adhiniyam, 2023*, s 63.
[154] NCRB (n 8) 45.
[155] *Criminal Procedure and Investigations Act 1996* (UK), s 5.
[156] MHA (n 3) 8.

underscores the efficacy of digitized evidence in reducing pendency, aligning with the BNSS's objective of expedited justice. However, Bihar's rural internet deficits and Uttar Pradesh's training gaps expose systemic barriers that threaten the BNSS's uniform implementation. The 30% internet coverage in Bihar's police stations jeopardizes the *eSakshya* app's functionality, risking non-compliance with Section 32(2)'s oversight mechanisms. [157] Similarly, the 65% training deficit in Uttar Pradesh hampers IOs' ability to navigate BNSS provisions, undermining the procedural rigour mandated by Sections 173(1) and 176(3). [158] These disparities reflect a broader urban-rural divide, with states like Maharashtra benefiting from better infrastructure, while Bihar and Uttar Pradesh lag due to resource constraints. R. Gupta critiques the BNSS's ambitious reforms, noting that without equitable investment in connectivity and training, the legislation risks creating a two-tiered justice system. [159] International models, such as Singapore's *Evidence Act* amendments, which pair digital evidence protocols with nationwide training, offer a blueprint for addressing these gaps.[160] The BNSS's reliance on technology, while progressive, demands systemic support to ensure its benefits extend beyond pilot projects to all regions.

(ix) Proposed Reforms

There are some reforms proposed to address the identified challenges and maximize the BNSS'S impact by enhancing the rural connectivity by investing in broadband infrastructure to ensure 80% of bihar's police stations have stable internet by 2027, enabling eSakshya app functionality as well as the compliance with Section 32(2).[161] Mandatory implementation of BNSS training for 75% of Uttar Pradesh's Ios by 2026, focusing on eSakshya app usage and digital forensics, to meet Section 176 (3)'s forensic requirements.[162]

[157] MoRD (n 10) 12.
[158] BPRD (n 14) 18.
[159] R. Gupta, Privacy and Evidence in Digital India (OUP 2020) 72.
[160] Evidence Act (Cap 97, 1997 Rev Ed Sing), s 35.
[161] MoRD (n 10) 15.
[162] BPRD (n 14) 20.

It is also proposed to expand forensic infrastructure by establishing 50 additional cyber forensic labs by 2030, prioritizing rural states like bihar, to support Section 176(3)'s thirty day reporting mandate and reduce evidence processing delays.[163]

The privacy protocols must be strengthen by developing the guidelines for eSakshya data handling to safeguard privacy, aligning with the EU's General Data Protection Regulation and ensuring compliance with constitutional protections.[164]

(x) Conclusion

The BNSS, 2023, redefines the IO's role through a progressive framework that prioritizes efficiency via strict timelines, digital evidence protocols, and accountability mechanisms. Sections 173(1) and 176(3) mandate 90-day investigations and 30-day forensic reporting, addressing chronic delays.[165] The *eSakshya* app, with selfie verification and blockchain uploads, and Section 32(2)'s judicial dashboards enhance evidence reliability and oversight, supporting the BSA's focus on electronic evidence.[166] Accountability measures under Section 210 and Aadhaar-linked authentication ensure compliance, reinforcing procedural rigour.[167] However, challenges such as limited forensic capacity, technological barriers, and privacy concerns threaten implementation, requiring investment in infrastructure, training, and safeguards. By addressing these gaps, the BNSS can achieve its efficiency mandate, balancing speed, fairness, and reliability to strengthen India's criminal justice system and set a global standard for technology-driven reforms.

The BNSS, 2023, has demonstrated significant empirical impact through Maharashtra's *eSakshya* pilot, which reduced investigation timelines by 40% and achieved a 95% conviction rate, and the FTSCs' resolution of 85,595 cases in 2024, leveraging digitized evidence. [168] [169]These successes highlight the transformative potential of Sections 173(1), 176(3), and 32(2)

[163] National Crime Records Bureau, Cyber Crime in India 2023 (NCRB 2023) 52.
[164] General Data Protection Regulation (EU) 2016/679, art 32.
[165] Ibid.
[166] *Criminal Procedure and Investigations Act 1996* (UK), s 5.
[167] Ibid.
[168] MHA (n 3) 8.
[169] MoRD (n 10) 12.

in enhancing efficiency and evidence integrity. However, persistent challenges, including Bihar's 30% internet coverage in police stations and Uttar Pradesh's 65% IO training deficit, underscore systemic barriers to nationwide implementation.[170] Rural infrastructure gaps and training deficits threaten compliance with BNSS mandates, risking disparities in justice delivery. By investing in connectivity, training, and forensic infrastructure, India can bridge these gaps, ensuring the BNSS's efficiency-driven reforms benefit all regions. The proposed reforms, drawing on international models, aim to strengthen the BNSS's implementation, aligning with its goal of a modern, victim-centric criminal justice system.

4.4 Key Causes of Delay in Criminal Justice

There are plenty of reasons for delay in criminal justice such as Judicial Vacancies and Infrastructure Gaps, Procedural Inefficiencies, Investigation and Prosecution inefficiency and poor Witness Protection.

As of early 2024, over 30% of trial court posts remain vacant, and many courts lack basic digital infrastructure needed to implement BNSS mandates effectively.[171]

Despite reforms, adjournments, non-appearance of witnesses, and delays in filing forensic reports continue to slow the process. The lack of standard operating protocols for complex evidence (e.g., E-Sakshya) further compounds delays.

Law enforcement lacks adequate training and digital tools. Many cases face poor evidence chain maintenance and inefficient case filing, undermining prosecutorial efficiency.

Delayed trials lead to witness fatigue, intimidation, or hostile turnarounds, especially in vulnerable cases. The absence of a national witness protection mechanism delays justice delivery and discourages testimony.[172]

The impact of delayed justice on the accused is that due to prolonged detention, there is denial of their liberty also they face psychological trauma and erosion of the presumption of

[170] BPRD (n 14) 18.
[171] India Justice Report 2023, Tata Trusts, DAKSH.

[172] Centre for Policy Research, "Witness Protection and Justice Delay", 2022.

WHITE BLACK
LEGAL

innocence. Massive backlogs (over 4.5 crore cases as of April 2024) erode public trust and raise systemic cost burdens[173].

4.5 Way Forward

The BNSS, 2023 provides a new legislative opportunity to institutionalize time-bound justice. However, its success depends on efficient enforcement, training, and resource augmentation. Future reforms must include:

I. Monitoring of time compliance metrics.

II. Expansion of fast-track courts.

III. Digitized scheduling systems and AI-based cause list management.

IV. Ensuring inter-agency coordination between police, courts, and forensic units.

WHITE BLACK LEGAL

[173] National Judicial Data Grid, https://njdg.ecourts.gov.in (Accessed 1st April 2025).

CHAPTER 5: THE ROLE OF TECHNOLOGY IN CRIMINAL JUSTICE

5.1 Introduction

The intersection of technology and criminal justice has become a focal point of discussion in recent years, driven by rapid advancements in digital tools and the increasing demand for more efficient, transparent, and accessible legal systems. As societies evolve, so too do the complexities of crime and the mechanisms required to address it. Traditional methods of law enforcement and judicial processes are often ill-equipped to handle the challenges posed by modern criminal activities, particularly those that exploit digital platforms. Consequently, the integration of technology into the criminal justice system is not merely an enhancement; it is a necessity for ensuring justice in the 21st century.

The advent of digital technologies has transformed various sectors, and the criminal justice system is no exception. Innovations such as e-courts, virtual hearings, artificial intelligence (AI), blockchain, and cyber forensics are reshaping how justice is administered. E-courts facilitate the electronic filing of documents and allow for remote participation in hearings, thereby reducing the logistical barriers that often hinder access to justice. Virtual hearings, which gained prominence during the COVID-19 pandemic, have demonstrated the potential for technology to maintain judicial functions even in times of crisis, ensuring that legal proceedings can continue without interruption.

Moreover, the use of AI in criminal justice is revolutionizing how data is analyzed and utilized. AI algorithms can process vast amounts of information to identify patterns, predict outcomes, and assist law enforcement in making informed decisions. This capability is particularly valuable in areas such as predictive policing, where data-driven insights can help allocate resources more effectively and potentially prevent crime before it occurs. However, the reliance on AI also raises ethical concerns regarding bias and accountability, necessitating careful consideration of how these technologies are implemented.

Blockchain technology offers another layer of innovation, providing secure and transparent methods for recording evidence and maintaining the integrity of legal documents. By creating immutable records, blockchain can enhance trust in the judicial process, ensuring that evidence is tamper-proof and verifiable. This is particularly crucial in an era where digital evidence plays an increasingly significant

role in criminal cases.

Despite the promising advancements, the integration of technology into criminal justice is not without its challenges. Issues such as inadequate infrastructure, digital literacy gaps, and privacy concerns must be addressed to ensure that the benefits of technology are equitably distributed. In many developing countries, including India, the judicial system still grapples with outdated practices and limited access to digital resources. The successful implementation of technology in these contexts requires not only investment in infrastructure but also comprehensive training for judicial personnel and robust legal frameworks to protect citizens' rights.

Furthermore, the global landscape of criminal justice technology is diverse, with different jurisdictions adopting varying approaches to digital transformation. Countries like the USA, UK, and Singapore have made significant strides in leveraging technology to enhance their legal systems, providing valuable lessons for others to follow. By examining these global practices, we can gain insights into the potential benefits and pitfalls of technology in criminal justice.

In this chapter, we will explore the multifaceted role of technology in criminal justice, delving into the digital transformation of courts, the application of advanced technological tools, and the insights gained from global practices. We will also address the implementation challenges faced by various jurisdictions, particularly in developing countries, and consider the future of technology in the pursuit of justice. Ultimately, this exploration aims to highlight the critical importance of embracing technological advancements while navigating the ethical and practical challenges they present, ensuring that the criminal justice system remains effective, equitable, and just in an increasingly digital world.

5.2 Digital Transformation: Overview of E-Courts, Virtual Hearings, and Case Management Systems

Digital transformation represents one of the most significant shifts in the criminal justice system, fundamentally altering how courts operate, how cases are managed, and how participants engage with judicial processes. In response to increasing caseloads, demand for greater transparency, and the need for efficiency, many jurisdictions have embraced technologies such as e-courts, virtual hearings, and case management systems. These innovations collectively contribute to enhanced access to justice, reduce delays, and improve the overall functioning of the judicial system.

(i) E-Courts: Digitizing Judicial Processes

The advent of e-courts is central to the digital modernization of criminal justice systems. An e-court is an electronic platform that enables the digitization of traditional court functions, including filing, documentation, scheduling, and communication among stakeholders.

E-filing allows litigants and lawyers to submit court documents electronically, significantly reducing the need for physical submissions and thereby expediting court procedures. This system not only saves time but also ensures accurate and secure record-keeping. Countries like India, through the e-Courts Project, have successfully integrated e-filing systems across several tiers of courts to increase accessibility and reduce inefficiencies.[174]

Modern e-courts employ automated workflows to manage case progress, notifications, and deadlines. This reduces administrative errors associated with manual tracking and enhances transparency by allowing parties real-time access to case statuses.

-courts also facilitate seamless data exchange with law enforcement, prosecutors, and correctional institutions, allowing for synchronous updates and improved coordination among diverse criminal justice stakeholder.[175] To address access issues, particularly in remote or underserved areas, several jurisdictions are developing mobile-enabled e-court platforms. Smartphone applications enable case filing, hearing notifications, and document access. This innovation is critical in increasing legal accessibility in regions with high mobile penetration but limited computer access.[176]

(ii) Virtual Hearings: Revolutionizing Courtroom Participation

Virtual hearings represent a paradigm shift, especially highlighted by disruptions such as the COVID-19 pandemic. Utilizing videoconferencing technology, courts allow parties-including judges, prosecutors, defense attorneys, witnesses, and defendants-to participate remotely.

---

[174] Supreme Court of India e-Courts Project, 'National Judicial Data Grid' https://njdg.ecourts.gov.in/njdgnew/index.php accessed 20 June 2024.

[175] United Nations Office on Drugs and Crime (UNODC), *E-Justice: Using Information and Communication Technologies (ICT) in the Criminal Justice* (2015) 23 https://www.unodc.org/documents/justice-and-prison-reform/14_E-Justice-booklet-LR.pdf accessed 20 June 2024.

[176] World Bank, 'Mobile Access to Justice: Using Technology to Enhance Legal Empowerment' (2018) https://documents.worldbank.org/en/publication/documents-reports/documentdetail/914031524239852378/mobile-access-to-justice-using-technology-to-enhance-legal-empowerment accessed 20 June 2024.

Virtual hearings minimize geographical, physical, and logistical barriers for defendants and witnesses. This is especially impactful for marginalized groups, rural populations, and those with disabilities.[177]

By reducing the need for physical appearances, virtual hearings lower costs for the judiciary, litigants, and public resources. Courts can accommodate more cases simultaneously, thereby addressing backlog pressures.[178]

Ensuring secure, confidential, and reliable communication requires robust technical infrastructure and cybersecurity protocols. Issues such as digital divide, technical glitches, and ensuring fairness in remote testimony present ongoing challenges that courts are addressing through technology upgrades and procedural safeguards.[179] Looking forward, hybrid models that allow parties to choose between in-person and virtual participation are gaining traction. Furthermore, exploratory uses of virtual reality (VR) technology have the potential to recreate courtroom environments virtually, enhancing the experience and understanding of courtroom proceedings for participants and juries alike.[180]

(iii) Case Management Systems (CMS): Automating Judicial Workflow

Case Management Systems are digital platforms designed to handle the administration, tracking, and organization of court cases throughout their lifecycle.

CMS automate routine processes such as docket scheduling, document management, and alerts for critical deadlines. This allows judicial staff and legal practitioners to focus on substantive legal work rather than administrative tasks.

WHITE BLACK LEGAL

[177] National Center for State Courts, 'Virtual Courts: Capstone Report' (2021) 15 https://www.ncsc.org/__data/assets/pdf_file/0024/55317/VC-Capstone-Report.pdf accessed 20 June 2024.
[178] OECD, 'Virtual Courts and Access to Justice: The Impact of COVID-19' (2020) https://www.oecd.org/coronavirus/policy-responses/virtual-courts-and-access-to-justice-the-impact-of-covid-19-b9efec6d/ accessed 20 June 2024.
[179] International Journal for Court Administration, 'Challenges in Implementing Virtual Hearings' (2021) 12(2) 10 https://journals.sfu.ca/ijca/index.php/ijca/article/view/418 accessed 20 June 2024.
[180] The Law Society Gazette, 'Virtual Reality Courtrooms: The Future of Justice?' (2023) https://www.lawgazette.co.uk/clinical/virtual-reality-courtrooms-the-future-of-justice/5113555.article accessed 20 June 2024.

The parties and judges can access real-time updates on case status, pending actions, and outcomes, promoting transparency and accountability. Many CMS now incorporate analytic dashboards that provide insights into court efficiency metrics, case disposition times, and backlog management, assisting policymakers and administrators in optimizing resources and improving judicial outcomes.[181] Advanced CMS in some jurisdictions integrate AI to predict case durations, estimate backlog risks, and recommend optimized hearing scheduling. Machine learning algorithms analyze historical case data to support proactive management, leading to more efficient justice delivery systems.[182]The cloud technology enables scalable, accessible CMS implementations with lower infrastructural investments. Additionally, blockchain-based decentralized CMS concepts are being explored to improve data integrity, reduce fraud, and provide auditable evidence trails across justice sector entities.[183]

5.3 Technological Integration in India's Criminal Justice System

The Interoperable Criminal Justice System (ICJS), conceptualized and implemented by the Ministry of Home Affairs (MHA), represents a groundbreaking effort to harmonize India's fragmented criminal justice institutions into a cohesive digital network. By linking the police (via the Crime and Criminal Tracking Network & Systems, or CCTNS), courts (through the e-Courts project), prisons (e-Prisons), prosecution agencies, and forensic laboratories, the ICJS eliminates redundancies and accelerates procedural timelines.[184] Central to this initiative is the National Digital Evidence Platform (NDEP), which enables real-time sharing of critical documents such as FIRs, charge sheets, forensic reports, and court orders across states and agencies.[185] For example, in the 2023 Mumbai-Delhi interstate warrant case, biometric records and digital case files were transmitted instantaneously, reducing the traditional 30-day inter- state warrant execution process to mere hours.[186] This system also empowers victims through integrated dashboards, allowing them to track case progress via SMS alerts—a feature

[181] International Justice Monitor, 'Using Data Analytics for Judicial Efficiency' (2022) https://www.ijmonitor.org/2022/05/using-data-analytics-to-boost-judicial-efficiency/ accessed 20 June 2024.
[182] Deloitte, 'AI in Case Management: Predictive Analytics for Courts' (2020) https://www2.deloitte.com/us/en/pages/public-sector/articles/ai-in-case-management.html accessed 20 June 2024.
[183] IBM Blockchain, 'Blockchain in Justice: Enhancing Case Management' (2021) https://www.ibm.com/blog/blockchain-in-justice-systems/ accessed 20 June 2024.
[184] Ministry of Home Affairs, *ICJS Implementation Report* (New Delhi: MHA, 2023) 12.
[185] National Crime Records Bureau, *CCTNS Integration Manual* (2022) 9.

[186] *State v. Rajesh Kumar* [2023] DLHC 4567.

WHITE BLACK
LEGAL

particularly impactful for survivors of sexual violence in states like Uttar Pradesh, where over 1,200 rape cases were monitored in real time in 2023. [187] Despite these advancements, infrastructural disparities persist: only 60% of police stations are fully integrated with CCTNS, and rural districts such as Bastar (Chhattisgarh) face bandwidth limitations, delaying NDEP adoption and perpetuating procedural inefficiencies.[188]

5.4 Virtual Courts and Video Conferencing: Revolutionizing Judicial Access

The Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, under Section 339, formally institutionalizes virtual court proceedings, marking a paradigm shift in India's judicial process.[189] Courts now routinely conduct bail hearings, witness examinations, and custody extensions via video conferencing, significantly reducing delays and enhancing access for vulnerable populations. For instance, in Gujarat, child abuse survivors testify remotely through secure video links, sparing them the trauma of confronting accused individuals in physical courtrooms.[190] Between 2020 and 2023, states like Delhi, Maharashtra, and Gujarat conducted over 1.5 crore virtual hearings, demonstrating the scalability of digital proceedings even during the COVID-19 pandemic.[191] The Supreme Court's landmark judgment in *Swapnil Tripathi v. Supreme Court of India (2018)* further reinforced this shift by mandating the live-streaming of constitutional matters, thereby upholding the principles of transparency and open justice under Article 19(1)(a) of the Constitution.[192] However, challenges remain entrenched in rural India: courts in Jharkhand and Odisha report that 40% of video hearings are disrupted due to unstable internet connectivity, undermining the promise of equitable justice.[193]

5.5 Artificial Intelligence (AI): Transforming Judicial Efficiency and Evidence Analysis

AI tools like SUPACE (Supreme Court Portal for Assistance in Courts Efficiency) are redefining judicial workflows by automating labor-intensive tasks. Launched in 2021, SUPACE scans voluminous case files, extracts relevant legal precedents, and generates draft

[187] Uttar Pradesh Police, *Victim Services Portal Annual Report* (Lucknow: UPP, 2023) 5.
[188] NITI Aayog, *Digital Divide in Criminal Justice* (New Delhi: Government of India, 2023) 22.
[189] Bharatiya Nagarik Suraksha Sanhita 2023 (India), s 339.
[190] Gujarat High Court, *Child Witness Protection Guidelines* (2022) 14.
[191] Supreme Court of India, *Virtual Courts Annual Report* (2023) 9.
[192] *Swapnil Tripathi v. Supreme Court of India* (2018) 10 SCC 628.
[193] NITI Aayog (n 5) 45.

orders, reducing judges' research time by 30%.[194] In Punjab and Telangana, Smart Case Listing Algorithms prioritize cases based on urgency, such as bail applications involving marginalized groups or elderly litigants. This innovation has reduced pendency rates by 22% in Punjab's trial courts, as highlighted in the state's 2023 judicial report.[195]

AI's role in validating digital evidence is expanding rapidly. Delhi's Cyber Crime Unit employs metadata analysis tools to audit the chain of custody for digital evidence, flagging discrepancies in timestamps or file hashes that may indicate tampering.[196] Similarly, Mumbai Police's CCTV-Geolocation Cross-Referencing System integrates AI to match surveillance footage with mobile GPS data, resolving 85% of hit-and-run cases within six months—a stark improvement from the previous average of 18 months.[197]

5.6 Blockchain: Securing the Integrity of Digital Evidence

Blockchain technology, with its immutable and decentralized architecture, is being piloted under the E-Sakshya initiative to safeguard digital evidence from tampering. In Karnataka, the High Court uses blockchain to maintain decentralized audit trails for high-profile narcotics cases, ensuring that forensic reports, seizure memos, and witness statements remain unaltered across agencies.[198] Delhi's pilot program embeds judicial seals on digital orders, enabling real- time verification of authenticity through cryptographic hashes. [199] However, blockchain's immutability poses a conflict with the Right to Erasure under the pending Digital Personal Data Protection Act (DPDPA), as courts cannot alter or delete erroneous entries without consensus across nodes—a legal and technical quandary yet to be resolved.[200]

5.7 Global Benchmarks: Lessons from the USA, UK, and Singapore

(i) United States: Rigorous E-Discovery and Metadata Standards

The U.S. enforces stringent e-discovery protocols under Federal Rules of Evidence (Rule 902), mandating the pre-trial exchange of structured digital evidence, including emails, server logs,

[194] Supreme Court of India, *SUPACE Evaluation Report* (2022) 14.
[195] Punjab Judicial Academy, *AI in Case Management* (Chandigarh: PJA, 2023) 18.
[196] Delhi Police, *Cyber Crime Unit Manual* (2023) 33.
[197] Mumbai Police, *Annual Crime Report* (2023) 27.
[198] Karnataka High Court, *Blockchain Pilot Report* (Bengaluru: KHC, 2023) 11.
[199] Ministry of Electronics and IT, *E-Sakshya Framework* (New Delhi: MeitY, 2023) 8.

[200] Digital Personal Data Protection Bill 2023 (India), cl 9(2).

WHITE BLACK
LEGAL

and financial records, in machine-readable formats. [201] Courts routinely validate evidence authenticity through AI-driven tools, as seen in *United States v. Microsoft Corp. (2018),* where metadata analysis played a pivotal role in confirming the integrity of cloud-stored documents.[202]

(ii) United Kingdom: Unified Case Management and Virtual Juries

The UK's Common Platform integrates police, prosecutors, and courts into a single digital workspace, allowing victims to receive SMS updates on trial progress.[203] During the COVID- 19 pandemic, the UK piloted virtual jury trials, though these faced criticism for excluding jurors lacking digital access, highlighting the tension between innovation and inclusivity.[204]

(iii) Singapore: Intelligent Courtrooms and Blockchain Audits

Singapore's Intelligent Courtroom Ecosystem employs AI for case scheduling and blockchain for evidence audits, as exemplified in *Public Prosecutor v. Tan Hou Wang (2023),* where blockchain-verified transaction records were pivotal to securing a conviction in a cross-border fraud case.[205] The system's efficiency is reflected in Singapore's 98% case clearance rate for commercial disputes, setting a global benchmark for tech-driven justice.[206]

5.8 Challenges: Bridging the Gap Between Vision and Reality

In India, still there is a infrastructural inequality as only 35% of rural courts have reliable internet access, compared to 85% in urban areas as per the NITI Aayog's 2023 report. On the other hand, outdated hardare and erratic power supply creates an obstacle for digital adoption in districts like Barpeta (Assam).[207] It is particularly important to highlight that according to 2024 ICJS survey revealed that 65% of trial judges lack training in AI tools forcing them to rely on clerical staff for technical tasks. [208] The absence of laws governing algorithmic accountability has led to concerns about bias in predictive policing tools, such as facial

[201] Federal Rules of Evidence (USA), r 902(14).
[202] *United States v. Microsoft Corp.*, 584 U.S. 2018.
[203] UK Ministry of Justice, *Common Platform Handbook* (London: MoJ, 2022) 6.
[204] R Smith, 'Virtual Juries in the UK' (2021) 44(3) JLS 230.
[205] *Public Prosecutor v. Tan Hou Wang* [2023] SGHC 140.
[206] Singapore Judiciary, *Annual Report 2023* (Singapore: SJ, 2023) 15.
[207] NITI Aayog (n 5) 50.
[208] Integrated Criminal Justice System, *Judicial Training Survey* (2024) 12.

recognition systems in Hyderabad that misidentified marginalised communities in 12% of cases.[209]

The proliferation of AI-driven surveillance tools, such as Delhi's facial recognition systems, raises constitutional concerns under *Justice K.S. Puttaswamy v. Union of India (2017)*, which affirmed privacy as a fundamental right.[210]

5.9 Recommendations: Paving the Way for Equitable Tech-Driven Justice

The Legislative Reforms required to enact a Unified Digital Evidence Protocol under the BSA to standardize AI and blockchain use, drawing inspiration from Singapore's Electronic Transactions Act (ETA).[211] Also launch a Digital Bench Training Program in National Judicial Academies, focusing on AI literacy, cybersecurity, and blockchain management.[212] The need for Infrastructure Expansion by establishing blockchain-secured evidence hubs in all High Courts and mandate video testimony for vulnerable witnesses, particularly in sexual violence and child abuse cases.[213]To expedite the enactment of the Digital Personal Data Protection Act (DPDPA) to address surveillance risks and reconcile blockchain's immutability with the Right to Erasure.[214] To collaborate with tech firms to develop open-source AI tools, ensuring transparency and accountability through judicial oversight, as demonstrated in Karnataka's blockchain pilots.[215]

WHITE BLACK LEGAL

[209] Law Commission of India, *AI and Legal Accountability* (2023) 19.
[210] *Justice K.S. Puttaswamy v. Union of India* (2017) 10 SCC 1.
[211] Bharatiya Sakshya Adhiniyam 2023 (India), ss 63–65.
[212] National Judicial Academy, *Training Module Proposal* (Bhopal: NJA, 2024) 5.
[213] Ministry of Law and Justice, *Blockchain Expansion Plan* (2024) 7.
[214] Digital Personal Data Protection Bill 2023 (India), cl 9(2).
[215] NITI Aayog, *Public-Private Partnerships in Justice* (2024) 10.

CHAPTER 6: SUGGESTIONS FOR REFORMS

The preceding chapters have underscored the transformative potential of India's criminal justice reforms, particularly through the *Bharatiya Nagarik Suraksha Sanhita (BNSS)* and *Bharatiya Sakshya Adhiniyam (BSA),* 2023, while also exposing systemic inefficiencies that hinder their implementation. Despite progressive statutory timelines, digitization mandates, and judicial safeguards, gaps in infrastructure, institutional preparedness, and stakeholder accountability persist, perpetuating delays and eroding public trust. The chronic backlog of over 5 crore pending cases, coupled with a judge-population ratio of 1:73,000 and uneven adoption of digital tools, reveals a pressing need for holistic reforms. This chapter proposes actionable solutions to bridge the chasm between legislative intent and ground-level realities, drawing on empirical insights, comparative jurisprudence, and technological innovations. By reimagining investigative practices, judicial processes, and institutional frameworks, these suggestions aim to fortify the pillars of time-bound justice, ensuring that constitutional guarantees under Article 21 translate into equitable and expeditious outcomes for all citizens. The reforms outlined here span four dimensions: legal-procedural, technological, institutional, and capacity-building, offering a roadmap to transform India's criminal justice system into a responsive, transparent, and future-ready institution.

6.1 E-Sakshya Reforms: Simplifying Certification, Enhancing Forensic Capabilities, and Training Programs

Introduction

The E-Sakshya/ E-evidence reform initiative is important step toward the modernized digilisation of India's judicial framework. Rooted in the broader digital India campaign, E- Sakshya aims to streamline judicial processes through e-governance, improve forensic science infrastructure, and imbue legal professionals with the technical expertise necessary for the digital era. These reforms are critical to reducing judicial delays, improving the accuracy of case adjudication, and ensuring accessibility for litigants.

(i) Simplifying Certification Processes

The certification of legal documents, a vital procedural step in judicial administration, currently suffers from procedural complexity and geographic inconsistencies. Empirical data from the National Judicial Data Grid (NJDG) reveal a disparity in the time taken for certifications across different states, with delays ranging typically from two weeks to over two months depending on the jurisdiction and the nature of the document.[216]Such delays often cascade into longer case backlogs and impede swift justice delivery.

These delays arise not only from outdated manual certification methods but also from the lack of a standardized procedure, leading to different processes being employed across courts.[217] For instance, some states require in-person verification, while others use postal services, significantly extending processing times.

To overcome these barriers, the Ministry of Law and Justice has proposed the adoption of digital certification mechanisms, which include e-signatures and blockchain-based authenticity verification systems, to simplify and expedite the certification process.[218] An emphasis on interoperability is crucial so that certified documents can be universally recognized across jurisdictions.

In addition to digitization, the government envisages a standardization protocol for certification processes across states, which would reduce redundancy and bring uniformity. This is expected to facilitate smoother inter-state judicial cooperation and reduce clerical errors.

According to the Ministry of Law and Justice's 2022 Annual Report on Judicial Reforms, states that piloted digital certification protocols experienced a 30% reduction in the average time required to certify legal documents.[219] For example, Rajasthan's e-Court project integrated digital certification with the e-filing system, cutting certification times down from an average of 21 days to 14 days.[220]

[216] National Judicial Data Grid (NJDG). *Judicial Metrics and Case Management Report*. 2023. http://njdg.ecourts.gov.in
[217] Ministry of Law and Justice. *Report on Certification Procedures in Indian Courts*. 2021. http://lawmin.gov.in
[218] Ministry of Law and Justice. *Digitization of Certification Processes*. 2022. http://law.gov.in
[219] Ministry of Law and Justice. *Annual Report on Judicial Reforms*. 2022. http://lawmin.gov.in
[220] Rajasthan e-Court Project. *Impact Assessment*. 2022. http://ecourts.gov.in/rajasthan

The report further noted an increase in the acceptance rate of electronically certified documents by courts, indicating judicial readiness to handle digital workflows.

(ii) Enhancing Forensic Capabilities

Forensic science stands as a cornerstone in evidence-based adjudication; however, the current infrastructure in India remains inadequate with respect to resources, personnel training, and technological advancement. The 2021 study by the *Journal of Forensic Sciences* highlighted that over 50% of forensic laboratories in India operate with suboptimal equipment, are poorly staffed, and face delayed processing times.[221]

The situation is dire, considering the rising caseload in criminal justice and the concomitant need for reliable forensic evidence to secure convictions. Delays in forensic reports have contributed to prolonged judicial processes, with some cases delaying due to pending forensic analyses for over six months.[222]

Recognizing these deficiencies, the government plans to allocate significant financial and technical resources toward upgrading forensic laboratories nationwide under the National Forensic Science Authority (NFSA). The goal is to equip these labs with advanced techniques such as enhanced DNA sequencing tools, digital forensics labs for cybercrime, and automated toxicology analyzers.[223]

Furthermore, collaboration with reputed academic and scientific institutions is proposed to improve the quality of forensic education and research. Establishing accredited forensic training academies aimed at upskilling forensic officers and technicians forms a critical element of this reform.[224]

The state of Maharashtra serves as a benchmark in this area. After receiving targeted funds to upgrade forensic laboratories and implement digital evidence management systems, the conviction rate in criminal cases relying on forensic evidence increased by 40% between 2018

[221] Singh, R., & Kumar, P. "Challenges in Forensic Science Infrastructure in India", *Journal of Forensic Sciences*, Vol. 66, Issue 3, 2021, pp. 989-998.
[222] National Crime Records Bureau. *Crime and Judicial Statistics Report*. 2022. https://ncrb.gov.in
[223] National Forensic Science Authority (NFSA). *Strategic Plan for Forensic Upgradation*. 2023. http://nfsa.gov.in
[224] Indian Institute of Forensic Sciences. *Annual Training Report*. 2022. http://forensics.in

and 2022.[225] The state's forensic modernization project also reduced the turnaround time of forensic reports from an average of 90 days to 45 days, drastically improving trial timelines.

(iii) Training Programs for Legal Professionals

Legal professionals, including judges, lawyers, and court staff, face significant challenges adapting to the digital transformation of judicial processes. A comprehensive survey by the Bar Council of India (BCI) in 2022 revealed that 62% of responding legal practitioners felt underprepared to utilize digital filing systems, e-hearings, and electronic evidence management.[226]

This digital divide hampers the effective implementation of reforms such as e-filing, virtual hearings, and the use of forensic reports, which increasingly rely on digital platforms. The lack of formal, ongoing digital literacy training further exacerbates this challenge.

To combat this knowledge gap, the judiciary proposes instituting mandatory training and continuing legal education modules focusing on digital tools, cyber law, and forensic science. Workshops and seminars, both virtual and in-person, will be conducted regularly to keep legal professionals abreast of evolving technologies and protocols.[227]

Additionally, online platforms offering modular courses on e-governance, artificial intelligence applications in law, and blockchain-enabled secure record-keeping are proposed to democratize access to training resources. The creation of an integrated Learning Management System (LMS) for the judiciary is envisioned to monitor skill development systematically.

A pilot digital training initiative led by the Karnataka High Court in 2023 reported a 25% increase in the competence level of lawyers handling digital case management tools and virtually conducted hearings, as assessed through pre- and post-training evaluations. It also resulted in higher user satisfaction rates with digital judicial services.[228]

[225] Maharashtra Crime and Forensics Department. *Forensic Modernization Project Report*. 2022. http://maharashtra.gov.in/crimeforensics

[226] Bar Council of India. *Survey on Digital Competency of Legal Professionals*. 2022. http://barcouncilofindia.org

[227] Supreme Court of India. *Initiatives for Judicial Capacity Building*. 2023. http://supremecourtofindia.nic.in

[228] Karnataka High Court. *Report on Pilot Digital Training Initiative*. 2023. http://karnatakajudiciary.kar.nic.in

Conclusion

The reforms outlined under the E-Sakshya initiative represent a comprehensive approach towards judicial modernization. Simplifying certification processes through digitization promises to accelerate procedural timelines, while enhancing forensic capabilities ensures the robustness and scientific accuracy of evidence presented in courts. Furthermore, systematic training programs aim to empower legal professionals to navigate a rapidly evolving digital judicial landscape effectively.

Together, these reforms bring the promise of a more accessible, efficient, and credible judiciary, ultimately advancing the rule of law and public trust in the legal system.

6.2 Time-Bound Justice Reforms: Expanding Fast-Track Courts, Setting Trial Deadlines, and Streamlining Procedures

Introduction

Efficient and timely delivery of justice is a foundational pillar for the rule of law and public trust in the judiciary. However, chronic delays have long undermined the effectiveness of India's judicial system, with millions of cases pending for years or even decades.[229] The consequences of such delays are far-reaching-compromising the rights of litigants, allowing crimes to remain unpunished, and eroding faith in the justice delivery framework. This sub- chapter explores comprehensive, time-bound justice reforms focusing on the expansion of fast-track courts, introduction of enforceable trial deadlines, procedural streamlining, and innovative methods to radically transform the judicial process, including ideas uncommonly discussed in mainstream reforms.

(i) Expanding and Reimagining Fast-Track Courts

The inception of fast-track courts in India was a landmark effort to resolve cases of grave public importance such as sexual violence and corruption with greater expedition. Despite these efforts, current judicial statistics reveal a stark mismatch between the number of fast- track courts and case pendency in related categories. The Supreme Court's 2022 Annual Report states that roughly 1,800 fast-track courts operate nationwide, yet an estimated backlog

[229] Law Commission of India, *Procedural Reforms in the Justice Delivery System* (Report No 276, 2017).

exceeds 4.5 million cases requiring urgent attention.[230] This reveals that the issue is not merely number but also the operational effectiveness and strategic deployment of these courts. It is imperative to not only increase fast-track courts but also reimagine their function. Specialized fast-track courts tailored to emerging types of crime should be instituted, including courts dedicated exclusively to cybercrimes, financial fraud, environmental law violations, and even domestic violence cases. Judges in these courts should receive specialized training in the technical aspects and nuances pertinent to their docket, fostering informed and quicker adjudications.

Moreover, fast-track courts should be digitally empowered with case management systems incorporating AI-based docket prioritization to intelligently schedule hearings, reduce adjournments, and flag procedural anomalies for prompt correction.[231] Leveraging technology to augment human decision-making within these courts is an area ripe for reform that remains largely untapped.

(ii) Enforceable Trial Deadlines with Accountability Mechanisms

One of the most profound systemic weaknesses ingrained in the Indian judiciary is the absence of enforceable and meaningful timelines for the completion of trials. In an environment lacking clear accountability, prolonged litigations not only offend justice but also incentivize deliberate procedural delays.

The Law Commission of India's 2022 report confirms that over 60% of lower court cases remain unresolved beyond three years, [232] underscoring the urgent need to institute definitive timelines. Merely prescribing deadlines, however, is insufficient; an ecosystem that enforces these deadlines through mechanisms like publicly accessible performance dashboards for individual courts and judges can foster transparency and pressure for timely adjudication.

To counter fears of compromised judicial quality amid accelerated timelines, phased judicial audits should be institutionalized. These audits would evaluate the quality and fairness of fast- tracked judgments, balancing speed with justice integrity.

[230] Supreme Court of India, *Annual Report 2022* https://supremecourtofindia.nic.in accessed 1 July 2024.
[231] National Judicial Data Grid, *Case Disposition Statistics 2023* http://njdg.ecourts.gov.in accessed 1 July 2024
[232] Law Commission of India, *Report on Judicial Delays and Reforms* (2022) http://lawcommissionofindia.nic.in accessed 1 July 2024.

(iii) Time-Stamped Digital Case Diaries

An innovative reform involves the deployment of a blockchain-backed digital case diary system mandating time-stamped records for every hearing, filing, and judicial order. This immutable ledger can serve as incontrovertible proof of trial progress or delay, enforce deadlines, and enable litigants and supervisors to track case development in real-time. If delays exceed statutory limits, automatic notification protocols could trigger administrative review actions.

(iv) Streamlining Judicial Procedures: Reducing Complexity and Encouraging Innovation

Procedural complexity is another significant bottleneck in time-bound justice delivery. The current procedural framework is characterized by excessive documentation, frequent adjournments, and redundant filings that lengthen case timelines unnecessarily.

To address this, the judicial procedural code must be comprehensively revisited with the objective of simplifying and digitizing court processes. The digitization of filings and evidence submissions on interoperable platforms accessible nationwide can harmonize procedural standards and minimize delays caused by physical document handling.

In tandem, expanding Alternative Dispute Resolution (ADR) pathways such as mediation, arbitration, and negotiation can substantially lessen the burden on courts.[233] However, beyond conventional ADR, integrating hybrid dispute resolution mechanisms-combining digital negotiation platforms with human mediation-can offer litigants a faster, more transparent hearing environment.

(v) AI-Powered Preliminary Case Assessment

Introducing AI-driven triaging tools at the point of case filing can revolutionize judicial case handling. By preliminarily assessing cases for complexity, urgency, and required resources, courts can dynamically assign cases to appropriate adjudicatory forums-fast-track courts, ADR

[233] Law Commission of India (n 4)

platforms, or regular benches-thereby optimizing judicial resource allocation and preventing unnecessary slowdowns.[234]

Additionally, AI can identify procedural anomalies or predict potential delays based on historical data, enabling preemptive intervention to keep cases on schedule.

Conclusion

Time-bound justice reforms require a multi-dimensional approach combining expansion and specialization of fast-track courts, enforceable deadlines with accountability, procedural simplification, and ambitious innovations like blockchain case diaries and AI-assisted case management.[235] Embracing novel ideas such as judicial time banking, community judicial facilitators, and immersive VR-assisted trials can place Indian judiciary at the forefront of global reform efforts. These reforms, grounded in judicial statistics, legal commission recommendations, and international experiences, promise to restore faith in timely and fair justice delivery.

6.3 Technology Integration: Leveraging AI, Blockchain, and Training for Transformation of Judicial Processes

Introduction

The integration of advanced technologies such as artificial intelligence (AI) and blockchain into judicial systems is no longer a futuristic concept but an essential reform imperative to meet the demands of modern justice delivery. India's judiciary, confronted with growing case backlogs and procedural complexity, stands to gain significantly from technology-driven efficiency, transparency, and accuracy. This sub-chapter offers a detailed exploration of AI- driven case management, blockchain-based secure record-keeping, and comprehensive capacity-building programs for legal professionals, underpinning these with innovative ideas and practical considerations that go beyond mainstream discourse.

[234] J Tan and S Lee, 'Impact of Trial Deadlines on Judicial Efficiency' (2021) 12(1) *International Journal of Court Administration* 45.
[235] Maharashtra State Legal Services Authority, *Pilot Program Impact Report* (2023) https://maharashtralaw.nic.in accessed 1 July 2024.

(i) Artificial Intelligence: Revolutionizing Judicial Case Management and Legal Research

AI can exponentially increase judicial system productivity by automating routine tasks, enhancing decision-making, and optimizing resource deployment.

Current case management often suffers from manual scheduling conflicts, adjournment- driven delays, and uneven workload distribution. AI-powered platforms can analyze past case data and judge availability to generate optimal court calendars, dynamically adjust docket priorities based on case urgency or complexity, and generate early warnings for procedural delays using predictive analytics. This allows courts to intervene proactively.

Beyond scheduling, AI-powered judicial assistants can support judges by summarizing case histories, highlighting relevant prior rulings, and even suggesting areas requiring judicial scrutiny. Machine learning algorithms can identify patterns in litigation behavior, spotting cases prone to delay or frivolous filings, thus supporting judicial discretion.

A pilot project in the Delhi district courts integrating AI for scheduling and case prediction reported a 40% reduction in administrative delays and a 25% improvement in case clearance rates within its first year.[236]

Manual legal research burdens lawyers and judges with enormous volumes of case law and statutory materials. AI natural language processing (NLP) tools, such as semantic search engines, can swiftly identify the most pertinent precedents and statutes, substantially reducing research time and enhancing judgment quality.

To foster trust in AI recommendations, integrating explainable AI (XAI) methodologies in research platforms will allow users to understand the reasoning paths AI used to surface particular precedents, creating transparency and aiding judicial acceptance.

(ii) Securing Transparency and Immutable Records

Ensuring the sanctity and accessibility of judicial records is critical. Blockchain's distributed ledger technology (DLT) provides an immutable, auditable, and secure framework for judicial

[236] National Judicial Data Grid, *Report on AI Pilot in Delhi District Courts*, 2023, http://njdg.ecourts.gov.in

data management. By recording every action-filings, orders, evidence submissions-as cryptographically secured, time-stamped blocks, blockchain guarantees that records cannot be altered retroactively. This secures evidence against tampering and increases litigant confidence that judicial processes remain fair and transparent. Implementing blockchain-based decentralized evidence repositories can enable litigants, lawyers, and forensic labs to submit and access evidence securely without intermediary interference, reducing delays and data loss risks. Smart contracts could automate integrity checks and control access permissions dynamically. The blockchain-ledgered action logs provide real-time, verifiable audit trails accessible to authorized stakeholders, thereby reducing corruption opportunities and streamlining complaint redressal. Estonia's e-Justice platform exemplifies effective blockchain use by securing court decisions and filings, markedly improving adjudication speed and public transparency.[237]

(iii) Training Judges and Lawyers for a Digital Judiciary

Technological advancements necessitate a paradigm shift in legal education and continual professional development. By regularly conducting workshops and accredited online courses focusing on AI literacy, digital data handling, blockchain applications, and cyber law should become mandatory for judges and practicing lawyers. Employing a blended learning approach combining self-paced and instructor-led modules can maximize accessibility. Creating a formal "Judicial Technology Certification" that judges and lawyers must renew every few years would institutionalize tech competence and incentivize continuous learning. By establishing court- located help desks staffed with technical experts can offer immediate support, troubleshoot disruptions, and build user confidence. Peer mentoring networks comprising tech-savvy judges and lawyers can facilitate experience sharing.

A 2023 Bar Council of India survey showed that after digital literacy initiatives, 70% of participants increased efficiency and confidence using e-legal tools, confirming the importance of sustained capacity building.[238]

(iv) Proposals

[237] Estonian Ministry of Justice, *e-Justice and Blockchain Overview*, 2021, https://justice.ee
[238] Bar Council of India, *Survey on Digital Literacy and Technology Adoption among Legal Professionals*, 2023, http://barcouncilofindia.org

The AI-Enabled Sentencing and Judgment Drafting such as pilot AI tools could assist in drafting impartial and data-driven sentencing recommendations based on statutory guidelines and precedent patterns. While final decisions remain with judges, AI support can reduce cognitive overload and promote consistency. By integrating blockchain with virtual court platforms could ensure secured, tamper-proof recording of virtual hearings, maintaining evidentiary integrity and auditability even in remote proceedings. In the future, IoT devices paired with data analytics could automate real-time evidence collection and verification (e.g., from surveillance or mobile data) fed directly into court systems, streamlining factual verification.

Conclusion

The path to judicial modernization in India passes inevitably through the effective integration of AI and blockchain, underpinned by robust training frameworks. Embracing innovative applications such as explainable AI, decentralized evidence repositories, and judicial technology certification schemes will push the Indian legal system towards unprecedented efficiency, transparency, and credibility. Pragmatic policy support, infrastructure investment, and cultural adaptation alongside technology adoption are critical to realizing this vision.

6.4 Policy Recommendations: A Comprehensive Framework for Judicial Reform Introduction

The Indian judiciary is at a pivotal moment, necessitating robust policy reforms to address existing gaps and adapt to the rapid evolution of technology. This sub-chapter outlines key policy recommendations focused on legislative updates, increased judicial resources, and collaborative strategies involving government, legal professionals, and technology experts. By fostering a holistic approach to reform, these recommendations aim to create a more efficient, transparent, and accessible judicial system.

(i) Legislative Updates

The current legal framework often lags behind technological advancements, creating inefficiencies and ambiguities. Legislative updates are essential to ensure that laws reflect contemporary realities, particularly in areas such as digital evidence, cybercrime, and data privacy. Amendments to the Indian Evidence Act and the Information Technology Act should

explicitly address the admissibility of digital evidence, including electronic contracts, emails, and blockchain records. This will provide clarity and enhance the integrity of digital transactions in legal proceedings. [239] The introduction of comprehensive data protection legislation, such as the Personal Data Protection Bill, is crucial to safeguard individuals' rights in the digital age. This legislation should outline clear guidelines for data handling, consent, and accountability, particularly for legal practitioners handling sensitive information. [240] By Establishing technology-driven legislative review committees composed of legal experts, technologists, and policymakers can facilitate ongoing assessments of existing laws. These committees would be tasked with identifying outdated provisions and recommending timely amendments to ensure legal frameworks remain relevant and effective.[241]

(ii) Increased Judicial Resources

There is a need to enhance the Funding for Courts by addressing the chronic backlog of cases and improve judicial efficiency, increased funding for courts is imperative. This funding should be allocated for upgrading court facilities with modern technology, including digital filing systems, video conferencing capabilities, and secure evidence management systems, will streamline operations and enhance accessibility. [242] To Hire additional judges, clerks, and administrative staff is essential to reduce case pendency. A well-resourced judiciary can handle caseloads more effectively, ensuring timely justice delivery.[243] Investing in training programs for judicial personnel is vital to equip them with the skills necessary to navigate technological advancements and modern legal challenges. Mandatory training sessions on emerging technologies, digital evidence handling, and cyber law should be instituted for judges and court staff. This will ensure that personnel remain updated on best practices and legal standards.[244] By doing a collaboration with educational institutions i.e. law schools and technology institutes to develop specialized training modules can enhance the skill sets of legal professionals. These programs should focus on practical applications of technology in legal contexts.[245]A report by

[239] Indian Evidence Act, 1872 (Amended 2000).
[240] Personal Data Protection Bill, 2023
[241] Ministry of Law and Justice, *Report on Legislative Review Committees*, 2022.
[242] National Judicial Academy, *Report on Judicial Infrastructure Development*, 2023.
[243] Supreme Court of India, *Annual Report on Judicial Resources*, 2022.
[244] Bar Council of India, *Training Programs for Legal Professionals*, 2023.

[245] Indian Institute of Legal Technology, *Collaboration Reports*, 2022.

WHITE BLACK
LEGAL

the National Judicial Academy indicated that jurisdictions with well-funded training programs for judges saw a 30% increase in case resolution rates within two years.[246]

(iii) Collaborative Strategies:

For effective judicial reform, it requires collaboration among various stakeholders, including government bodies, legal professionals, and technology experts. This collaborative approach can lead to the development of comprehensive reform strategies that address the multifaceted challenges facing the judiciary.

By Engaging technology firms in partnerships to develop judicial software solutions can enhance efficiency. For example, creating a centralized digital platform for case management and legal research can streamline processes and reduce redundancy.[247] Regular consultations with legal associations, such as the Bar Council of India, can provide valuable insights into the practical challenges faced by legal practitioners. These consultations should inform legislative proposals and reform initiatives.[248]

To Establish judicial reform task forces comprising representatives from the government, legal community, and technology sector can facilitate ongoing dialogue and collaboration. These task forces would be responsible for identifying priority areas for reform, developing actionable strategies, and monitoring implementation progress.[249]

WHITE BLACK LEGAL

[246] National Judicial Academy, *Effectiveness of Training Programs*, 2021.
[247] Ministry of Electronics and Information Technology, *Public-Private Partnerships in E-Governance*, 2023.
[248] Bar Council of India, *Consultative Reports on Judicial Reform*, 2022..
[249] Judicial Reform Task Force, *Progress Reports*, 2023.

CHAPTER 7: COMPARATIVE ANALYSIS - INDIA AND OTHER JURISDICTIONS

7.1. E-Sakshya Comparison: Contrasting India's framework with the USA, UK, and Singapore.

Introduction

The rapid digitization of legal processes and increasing reliance on electronic records in judicial proceedings necessitate robust and clear legal frameworks governing the admissibility, authentication, and evidentiary value of electronic evidence. The jurisdictions of India, the United States (USA), the United Kingdom (UK), and Singapore represent diverse approaches shaped by their respective legal traditions, technological ecosystems, and policy priorities. This sub-chapter undertakes a detailed comparative analysis of the electronic evidence regimes in these jurisdictions, with particular reference to the evolving Indian "E-Sakshya" framework and its counterparts abroad. The analysis emphasizes statutory provisions, procedural rules, judicial interpretations, and ongoing reforms as of 2025, aiming to elucidate strengths, limitations, and emerging trends.

(i) India: E-Sakshya and the Bharatiya Sakshya Bill

India's electronic evidence regime is undergoing significant transformation with the proposed Bharatiya Sakshya Bill, 2023 which is now Bhartiya Sakshya Adhiniyam, which aims to replace the Indian Evidence Act, 1872, particularly its provisions on electronic records under Section 65B. The current legal framework, originally designed in an era prior to digital proliferation, has faced criticism for its rigid authentication requirements, notably the mandatory production of a certificate (Section 65B certificate) to prove the genuineness of electronic evidence, which has led to judicial inconsistencies and delays.[250]

The BSA seeks to modernize the approach by allowing more flexible and alternative modes of authentication of electronic evidence, aligning more closely with global best practices observed in common law jurisdictions.[251] Furthermore, the BSA aims to facilitate the use of electronic

[250] Asian Journal of Law and Society, "Paper in the Age of the Digital: The Curious Case of 65-B Certificates in India," Cambridge University Press, 2025

[251]CyberPeace.org, "Indian Criminal Law Reform: Bharatiya Sakshya Bill and Digital Evidence," February 2025.

WHITE BLACK
LEGAL

records in court proceedings, including provisions for virtual evidence presentation, reflecting the broader push for digitalization in India's judiciary under initiatives like E-Sakshya.[252]

E-Sakshya, as part of India's digital court ecosystem, focuses on enabling the electronic filing, management, and presentation of evidence, integrating technological tools for secure storage and retrieval. This infrastructure complements the legal reforms by providing practical mechanisms to operationalize electronic evidence handling in courts.[253]

After the BSA replaces IEA 1872,

I. Recognition of electronic records as equivalent to paper documents.

II. Relaxed authentication requirements, allowing multiple routes for proving electronic evidence integrity.

III. Provisions for virtual testimony and electronic submission of evidence.

IV. Integration with digital court infrastructure (e.g., E-Sakshya platform).

Despite these advances, challenges remain, including uneven technological adoption across jurisdictions and concerns about cybersecurity and data privacy.[254]

(ii) United States: Federal Rules of Evidence and Electronic Records

The United States has a mature and comparatively advanced legal framework for electronic evidence, primarily governed by the Federal Rules of Evidence (FRE), which underwent significant amendments in 2017 to address the challenges posed by electronic and digital evidence.[255]

Under FRE, particularly Rules 901 and 902, electronic records are admissible provided their authenticity is established. Rule 902 includes a list of self-authenticating documents that require no extrinsic evidence of authenticity, which includes certified electronic records, digital signatures, and data from reliable sources such as business records or public authorities.[256]

[252] CyberPeace.org, "Way ahead for digitalisation in Indian courts," 2025.
[253] Global Arbitration Review, "Commercial Arbitration: India," April 2025.
[254] ICNL, "India Civic Freedom Monitor: Data Protection and Digital Privacy," 2023-2025.
[255] Federal Rules of Evidence Amendments, "Electronic Evidence," 2017, U.S. Government Publishing Office.
[256] Ibid.

The amendments introduced a more relaxed and flexible regime that permits parties to authenticate electronic evidence through a variety of means, including metadata analysis, hash values, and expert testimony. This flexibility reduces procedural hurdles and facilitates the use of electronic evidence in federal courts.[257]

Moreover, the USA benefits from well-established electronic discovery (e-discovery) protocols that govern the collection, preservation, and presentation of digital evidence, supported by technological tools and procedural safeguards.[258]

Key Features:

a. Multiple authentication routes under FRE 901 and 902.
b. Self-authenticating electronic evidence categories.
c. Comprehensive e-discovery framework.
d. Judicial guidance on handling metadata and digital forensics.
e. Broad acceptance of electronic evidence subject to relevance and reliability.

The U.S. framework balances evidentiary rigor with pragmatic considerations of digital realities, though challenges related to privacy and cross-border data flows persist.[259]

(iii) United Kingdom: Electronic Evidence and the Civil Procedure Rules

The UK legal system has evolved its electronic evidence rules through both statutory provisions and procedural reforms, especially in civil litigation.[260] The Civil Procedure Rules (CPR), supported by the Practice Direction on Electronic Documents, provide detailed guidance on the disclosure, inspection, and use of electronic evidence in courts.[261]

The UK approach emphasizes proportionality and cooperation between parties, encouraging early exchange and identification of electronic evidence to reduce litigation costs and delays.

[257] Sethia, "Admissibility of Electronic Records: A US Perspective," Journal of Evidence, 2019.
[258] The Sedona Conference, "Principles and Best Practices for Electronic Document Production," 2023.
[259] CyberPeace.org, "Meta GDPR Violation and Data Privacy Concerns," 2025.
[260] UK Ministry of Justice, "Civil Procedure Rules & Practice Directions on Electronic Evidence," 2024.

[261] Ibid.

The Evidence Guides published by the judiciary provide practical frameworks for presenting electronic records, including considerations for authenticity, integrity, and admissibility.[262]

The UK has also adopted the Electronic Communications Act 2000 and the Civil Evidence Act 1995, which facilitate the recognition of electronic communications and evidence. Furthermore, the UK's Data Protection Act 2018 and alignment with the GDPR impact evidential considerations concerning privacy and data protection.[263]

Key Features:

a. Procedural emphasis on early disclosure and cooperation.

b. Practice Directions providing detailed electronic evidence protocols.

c. Legal recognition of electronic communications and signatures.

d. Integration of data protection laws with evidentiary rules.

e. Judicial guides promoting technological competence among practitioners.

The UK framework is noted for its procedural sophistication and alignment with technological advancements, though it faces challenges in criminal proceedings where electronic evidence admissibility is more stringently scrutinized.[264]

(iv) Singapore: Electronic Transactions Act and Evidence Act Reforms

Singapore offers a robust statutory framework for electronic evidence, primarily governed by the Electronic Transactions Act (ETA) and the Evidence Act.[265] The ETA, first enacted in 1998 and updated subsequently, provides legal recognition for electronic records and signatures, ensuring their validity and enforceability equivalent to paper-based documents.[266]

Singapore's Evidence Act includes specific provisions for the admissibility and authentication of electronic records, allowing evidence to be admitted if its integrity is established through

[262] Judiciary of England and Wales, "Guide to Electronic Evidence," 2023.
[263] UK Data Protection Act 2018 and GDPR, 2018.
[264] Law Commission of England and Wales, "Electronic Evidence in Criminal Proceedings," 2022.

[265] Singapore Statutes Online, "Electronic Transactions Act," Revised 2023.
[266] Ibid.

appropriate means, including certification by a person occupying a responsible position in relation to the operation of the relevant device or system.[267]

Singaporean courts have demonstrated technological adaptability by issuing practice directions encouraging the use of electronic evidence and facilitating remote hearings and digital submissions.[268] The city's strategic position as a global legal and technological hub has fostered innovative applications of electronic evidence in commercial arbitration and litigation.[269]

Key Features:

a. Statutory recognition of electronic signatures and records under ETA.
b. Flexible authentication standards under the Evidence Act.
c. Judicial encouragement of digital evidence practices.
d. Integration with Singapore's arbitration-friendly legal environment.
e. Emphasis on technological neutrality and innovation-friendly policies.

Singapore's legal framework is recognized for its clarity and proactivity in embracing digital evidence, with ongoing reforms to further streamline evidentiary standards and support the digital economy.[270] Singapore's legal framework is characterized by clear statutory provisions that recognize electronic transactions and evidence. The judiciary's proactive stance on digital evidence and remote proceedings, combined with a business-friendly environment, makes it a leading jurisdiction in embracing electronic evidence.

(v) Cross-Disciplinary Insights

The evolution of electronic evidence frameworks intersects with technological innovation, data privacy, and international arbitration regimes. For instance, India's efforts to enhance electronic evidence admissibility support not only domestic litigation efficiency but also its growing role in international commercial arbitration, where digital evidence is increasingly pivotal.[271] Similarly, the USA's sophisticated e-discovery protocols inform global best practices

[267] Evidence Act (Chapter 97), Singapore, 2023.
[268] Supreme Court of Singapore, "Practice Direction on Electronic Evidence," 2024.
[269] Singapore International Arbitration Centre (SIAC), "Use of Electronic Evidence in Arbitration," 2023.

[270] CyberPeace.org, "Singapore's Digital Evidence Legal Framework," 2025.
[271] Global Arbitration Review, "India's Arbitration Law and Electronic Evidence," 2025.

for handling complex cross-border digital evidence challenges, critical in transnational litigation and cybersecurity incidents.[272]

Data privacy laws such as the EU's GDPR and India's Digital Personal Data Protection Act shape the boundaries of evidence admissibility, requiring courts and litigants to balance evidentiary needs with individual rights and compliance obligations. [273] The integration of procedural reforms with technological infrastructure, as seen in India's E-Sakshya and Singapore's digital court initiatives, exemplifies the importance of judicial digital literacy and system interoperability for effective electronic evidence management.[274]

(vi) Technical Deep Dive: Authentication Mechanisms in Electronic Evidence

Authentication of electronic evidence remains a cornerstone of admissibility. The Indian framework's reliance on Section 65B certificates has been criticized for its formalism, requiring a detailed certificate from a person in charge of the device or system that produced the electronic record. This has led to inconsistent judicial interpretations and evidentiary hurdles.[275]

In contrast, the U.S. FRE allows authentication through testimony of a witness with knowledge ,comparison by an expert or trier of fact, distinctive characteristics and the circumstances, certified records under Rule 902(11).

The UK's approach emphasizes procedural cooperation and judicial discretion, supplemented by technological protocols for verifying metadata and digital signatures. [276] Singapore's certification approach under its Evidence Act requires a responsible person to attest to the integrity of the electronic record but allows flexibility depending on case circumstances.[277]

Advances in blockchain technology, cryptographic hashing, and digital timestamping present new frontiers for authentication, offering immutable audit trails and enhanced evidentiary

[272] The Sedona Conference, "Cross-Border Electronic Evidence," 2024.
[273] LW.com, "India's Digital Personal Data Protection Act 2023 vs. GDPR," 2023.
[274] CyberPeace.org, "Digitalisation of Indian Courts: Challenges and Opportunities," 2025.
[275] Asian Journal of Law and Society, supra n 1.

[276] UK Judiciary, supra n 13.
[277] Singapore Evidence Act, supra n 18.

reliability. Future reforms in all jurisdictions may increasingly incorporate these technologies to augment traditional authentication methods.[278]

(vii) CASE STUDY

(A) Google Android Ecosystem Penalty and Digital Evidence in India

In 2022, India's Competition Commission (CCI) imposed a historic penalty of ₹1,337 crore (approximately $161 million) on Google for abusing its dominance in the Android ecosystem, marking a watershed moment in India's antitrust enforcement. The case (*In Re: Alphabet Inc. & Ors.*, Case No. 39 of 2018)[279] centered on allegations that Google used restrictive contracts to stifle competition, forcing smartphone manufacturers to pre-install apps like Google Search and Chrome to access the Play Store. To prove this, the CCI relied on a vast array of digital evidence, including forensic analysis of Android's source code, which revealed how Google locked competitors out of critical Application Programming Interfaces (APIs). Internal emails and transaction logs further exposed coercive revenue-sharing agreements with manufacturers like Samsung and Xiaomi, demonstrating how Google's practices skewed the market to control 98% of India's mobile ecosystem.[280]

Google fiercely contested the admissibility of metadata and chat logs, arguing they violated Section 65B of the Indian Evidence Act, 1872 [281] which mandates strict certification for electronic records. The CCI countered by assembling a Technical Advisory Committee (TAC) under Section 36 of the Competition Act, 2002,[282] comprising digital forensics experts, economists, and data scientists. The TAC decoded Google's proprietary algorithms and demonstrated how its practices harmed competition, particularly through Mobile Application Distribution Agreements (MADAs) that forced manufacturers to bundle 11 Google apps.[283]

The case became a catalyst for legal reform. In 2023, India introduced the Bharatiya Sakshya Bill,[284] which simplifies the authentication of government-seized digital evidence by adopting

[278] Dalton, TR, "Defining Private Property Rights on Celestial Bodies," Cornell Law Scholarship, 2010.
[279] *In Re: Alphabet Inc. & Ors.*, Competition Commission of India Case No. 39 of 2018, Order (20 October 2022).
[280] Ibid, paras 89, 112 (API restrictions and revenue-sharing agreements).
[281] Indian Evidence Act 1872, s 65B; *Shafhi Mohammed v. State of Himachal Pradesh* (2018) 2 SCC 801.
[282] Competition Act 2002 (India), s 36; Competition Commission of India, *Technical Advisory Committee Report* (2022).
[283] *In Re: Alphabet Inc. & Ors.* (n 1) para 112.

[284] Bharatiya Sakshya Bill 2023 (India), cls 61(2)–61(3).

a presumption of integrity for data collected via state-approved forensic tools. Additionally, the E-Sakshya Initiative[285] mandates blockchain-based storage for antitrust evidence, ensuring tamper-proof logs through platforms like IndiaChain. These reforms reflect India's push to modernize its legal framework amid rising tech disputes, balancing corporate accountability with the practical challenges of handling digital evidence.

(B) USA Federal Court's Handling of Electronic Evidence in Cybercrime Prosecution Background

In *United States v. Mikhailov* (Case No. 3:23-cr-00456, Northern District of California, 2024),[286] the U.S. Department of Justice (DOJ) prosecuted members of an international ransomware syndicate responsible for crippling critical healthcare infrastructure across multiple states. The defendants, operating under the alias "BlackHydra," targeted hospital networks, encrypting patient databases and demanding Bitcoin ransoms exceeding $50 million. The attacks disrupted emergency services, delayed life-saving surgeries, and compromised sensitive medical records, prompting a multi-agency investigation involving the FBI, Cybersecurity and Infrastructure Security Agency (CISA), and Europol.

Central to the prosecution were two categories of digital evidence:

- **Encrypted Chat Logs**: Extracted from Telegram channels used by the group to coordinate attacks. These logs, obtained through Mutual Legal Assistance Treaties (MLATs) with Estonia, revealed detailed plans to exploit vulnerabilities in hospital firewalls and evade detection.

- **Blockchain Transaction Records**: Traced through a labyrinth of Bitcoin wallets on the dark web, linking ransom payments to accounts controlled by the defendants. The FBI utilized Chainalysis Reactor, a blockchain analysis tool, to map transactions across mixers and tumblers, ultimately identifying wallets linked to the defendants' aliases.

[285] Ministry of Electronics and Information Technology, 'E-Sakshya Framework' (Press Release, 1 April 2023).

[286] *United States v. Mikhailov*, ND Cal Case No. 3:23-cr-00456, Docket Entry 142 (2024).

The case underscored the growing sophistication of cybercriminal networks and the judiciary's reliance on advanced digital forensics to secure convictions in an era of increasingly complex cybercrimes.

Admissibility Under FRE 902(11)

The prosecution faced significant challenges in authenticating the Telegram chat logs and blockchain records, as defense attorneys argued the evidence was tampered with during extraction. The DOJ leveraged Federal Rule of Evidence 902(11),[287] which permits self- authentication of electronic records through a certification of integrity from a qualified custodian.

The FBI's Cyber Division submitted a Chain of Custody Report affirming that the Telegram data was extracted using Cellebrite UFED, a forensic tool that preserves metadata (e.g., timestamps, user IDs) without altering original files. The report included cryptographic hash values (SHA-256) to verify the logs' authenticity. The court cited *United States v. Gasperini* (948 F.3d 72, 2d Cir. 2020),[288] where the Second Circuit upheld that hash-value verification satisfies FRE 901's authenticity requirements. Judge William Alsup emphasized, *"The use of cryptographic hashing is now a gold standard in digital forensics, ensuring evidence remains unaltered from seizure to trial."*

Expert Testimony:

Digital Forensic Analysts from the FBI demonstrated how Chain analysis Reactor mapped Bitcoin transactions across mixers and tumblers to the defendants' wallets.

Cybersecurity Experts testified that the group's use of Ransomware-as-a-Service (RaaS) tools mirrored tactics in prior attacks on European energy grids, establishing a pattern of criminal behavior.

Legal Precedent and Broader Implications

The *Mikhailov* case catalyzed the DOJ's **2024 Guidelines on Cyber Evidence**, [289] which institutionalize best practices for handling digital evidence:

[287] Federal Rules of Evidence, r 902(11).
[288] *United States v. Gasperini*, 948 F.3d 72 (2d Cir 2020).
[289] US Department of Justice, *2024 Guidelines on Cyber Evidence* (2024) 9–12.

- **ISO/IEC 27037 Compliance**: Mandates adherence to this international standard for data preservation, requiring agencies to document the "who, what, when, and how" of digital evidence collection. This includes using write-blockers to prevent data alteration and maintaining audit trails.

- **MLAT Protocol Updates**: Streamlines cross-border evidence requests, requiring partner nations to certify compliance with ISO/IEC standards. Estonia's cooperation, for instance, set a benchmark for rapid MLAT responses (14 days vs. the prior 6-month average). The defense contested the reliability of blockchain analysis, arguing that pseudonymous wallets could not definitively link payments to the defendants. The court rejected this, emphasizing that circumstantial evidence (e.g., chat logs discussing wallet addresses) sufficed under *United States v. Ulbricht* (858 F.3d 71, 2d Cir. 2017),[290] which upheld Bitcoin transaction tracing in the Silk Road case. Additionally, the defense claimed the Telegram logs were obtained without a search warrant under the Stored Communications Act (SCA). The DOJ countered that the MLAT process with Estonia-a nation with reciprocal data-sharing laws-rendered the SCA inapplicable. Judge Alsup agreed, citing *Microsoft Corp. v. United States* (584 U.S. 2018),[291] which affirmed the primacy of MLATs in cross-border data disputes.

Outcome

The jury convicted all five defendants on charges of computer fraud, extortion, and money laundering, with sentences ranging from 12 to 25 years. The case set critical precedents:

Courts now routinely accept blockchain and encrypted chat evidence, provided ISO/IEC protocols are followed. The DOJ's success spurred similar MLAT-driven prosecutions in the EU and Asia, targeting ransomware groups like Conti and REvil.

Conclusion

The *Mikhailov* case exemplifies the U.S. judiciary's adaptability in confronting cybercrime's technical complexities. By harmonizing international law, forensic innovation, and procedural rigor, it reinforces the viability of digital evidence in safeguarding public infrastructure and upholding justice in the digital age. This precedent underscores the necessity for global legal

[290] *United States v. Ulbricht*, 858 F.3d 71 (2d Cir 2017).
[291] *Microsoft Corp. v. United States*, 584 U.S. 2018.

frameworks to evolve alongside technological advancements, ensuring accountability in an increasingly interconnected world.

(C) Singapore Commercial Arbitration Incorporating Electronic Evidence

Background

In 2023, a high-stakes commercial arbitration administered by the Singapore International Arbitration Centre (SIAC) resolved a USD 28 million dispute between *M/s Oceanic Shipping Co.* (a Singapore-based freight operator) and *TransGlobal Logistics Pte Ltd* (a Malaysian logistics firm) over alleged breaches of a maritime cargo contract.[292] The dispute centered on the failure to deliver perishable goods worth USD 12 million and subsequent claims for reputational damages. The arbitration gained international attention for its reliance on blockchain-verified transaction records and digitally signed contracts, setting a benchmark for the admissibility of electronic evidence in cross-border disputes under Singapore's Electronic Transactions Act (ETA) 2021 [293] and the UNCITRAL Model Law on Electronic Transferable Records (MLETR).[294]

The claimant, *Oceanic Shipping*, submitted a digital contract executed via Singapore's SignWithSG framework-a government-backed digital identity system-along with blockchain-based bills of lading hosted on TradeLens, a platform co-developed by IBM and Maersk.[295] The respondent, *TransGlobal*, contested the authenticity of these records, arguing that digital signatures and blockchain entries were insufficient to prove contractual obligations under traditional arbitration norms.

Evidentiary Framework and Tribunal Analysis

The tribunal, chaired by former Singapore Supreme Court Justice Steven Chong, admitted the electronic evidence under Singapore's ETA 2021, which aligns with the UNCITRAL MLETR adopted by Singapore in 2022.[296] Key considerations included:

[292] *M/s Oceanic Shipping Co. v. TransGlobal Logistics Pte Ltd*, SIAC Arbitration No. ARB-098/2023, Award (2023).
[293] Electronic Transactions Act 2021 (Singapore).
[294] UNCITRAL Model Law on Electronic Transferable Records (2017).

[295] IBM, 'TradeLens: Revolutionizing Global Trade' (Press Release, 2022).
[296] Ministry of Law Singapore, 'Adoption of UNCITRAL MLETR' (2022).

- **Admissibility of Blockchain Records**: The tribunal accepted TradeLens' blockchain entries as "secure electronic records" under Section 8 of the ETA,[297] which recognizes data integrity if secured through cryptographic methods. The platform's use of SHA-256 hashing and decentralized consensus mechanisms ensured that timestamps, cargo temperatures, and GPS coordinates could not be altered post-upload. Expert testimony from IBM's blockchain architect confirmed that TradeLens met ISO/TC 307 standards for distributed ledger technology.[298]

- **Validity of Digital Signatures**: *Oceanic Shipping*'s contracts were executed via SignWithSG, Singapore's national digital signing framework. Under Section 17 of the ETA,[299] electronic signatures are presumed valid if generated through a secure system approved by the Infocomm Media Development Authority (IMDA).[300] The tribunal dismissed *TransGlobal*'s objections, noting that SignWithSG's two-factor authentication and audit trails satisfied the UNCITRAL Model Law's functional equivalence principle for signature reliability.[301]

- **Cross-Border Recognition**: The tribunal emphasized Singapore's adoption of the MLETR, which harmonizes electronic transferable records (ETRs) across jurisdictions. [302] By referencing the 2022 Singapore Convention on Mediation, [303] the tribunal affirmed that blockchain evidence from TradeLens-a platform used in 60+ countries-met international enforceability standards under Article 12 of the MLETR.[304]

Legal Impact and Jurisdictional Precedent

The case reinforced Singapore's position as a global hub for tech-driven dispute resolution. Notable outcomes include:

The tribunal concluded proceedings in 5 months (vs. the SIAC average of 11 months) by leveraging e-discovery tools and virtual hearings under SIAC Rules 2021.[305] This efficiency was

[297] Electronic Transactions Act 2021 (Singapore), s 8.
[298] ISO/TC 307, *Blockchain and Distributed Ledger Technologies* (2020).
[299] Electronic Transactions Act 2021 (Singapore), s 17.
[300] Infocomm Media Development Authority, *SignWithSG Technical Specifications* (2023).
[301] UNCITRAL Model Law on Electronic Signatures (2001), Art 6.
[302] Ministry of Law Singapore (n 5).

[303] United Nations Convention on International Settlement Agreements Resulting from Mediation (Singapore Convention) 2020.
[304] UNCITRAL Model Law on Electronic Transferable Records (2017), Art 12.
[305] SIAC Rules 2021, r 19.3.

cited in the 2024 Global Arbitration Review as a model for complex tech disputes. [306] Following the award, major Asian shipping consortiums, including the Japan Maritime Exchange, integrated TradeLens into their operations, citing the tribunal's validation of blockchain's legal reliability.[307] The Ministry of Law (MinLaw) issued Guidelines on Digital Evidence in Arbitration (2024), mandating arbitrators to consider blockchain and AI- generated records as prima facie admissible if compliant with ETA standards.[308]

Conclusion

The comparative analysis reveals that while India is actively reforming its electronic evidence laws and digital court infrastructure to achieve parity with advanced jurisdictions, significant room for development remains in judicial training, infrastructure, and harmonization with data privacy regulations. The USA's regime exemplifies comprehensive procedural and substantive standards, balancing evidentiary rigor with pragmatic technological adaptation. The UK's procedural focus and Singapore's statutory clarity offer complementary models emphasizing cooperation and innovation.

As electronic evidence becomes ubiquitous, these jurisdictions' evolving frameworks will continue to influence and inform each other, underscoring the need for international convergence on standards, especially in cross-border litigation and arbitration contexts.

7.2. Time-Bound Justice Comparison: Analyzing global approaches to timely trials.

Overview

This seventh chapter provides a comprehensive comparative analysis of time-bound justice frameworks in India, the United States, the United Kingdom, and Singapore. Given the paramount importance of timely justice for upholding the rule of law, reducing case backlogs, and enhancing public trust, this analysis synthesizes statutory provisions, judicial interpretations, procedural mechanisms, and institutional reforms aimed at expediting judicial processes. Particular emphasis is placed on how legal frameworks and political will shape the operationalization of time-bound justice in each jurisdiction. The report integrates legal

[306] Global Arbitration Review, *Tech-Driven Arbitration Trends* (2024).
[307] Japan Maritime Exchange, *Annual Report 2024* (2024).
[308] Ministry of Law Singapore, *Guidelines on Digital Evidence in Arbitration* (2024).

doctrinal analysis with empirical data on case disposal rates and backlog reduction, highlighting both successes and challenges.

India and Singapore demonstrate formal statutory efforts and constitutional directives emphasizing time-bound justice; however, their operational realities diverge considerably due to systemic factors. The USA and UK rely more heavily on procedural rules and judicial case management, balancing expediency with due process, influenced by their distinct common law traditions and federal structures. This report concludes with cross-disciplinary insights about the political economy of judicial reforms and the implications for legal compliance and governance.

(i) Legal Frameworks Governing Time-Bound Justice

(A) India

India's commitment to time-bound justice is constitutionally anchored in Article 21, which guarantees the right to life and personal liberty, interpreted judicially to encompass the right to a speedy trial.[309]The Supreme Court of India has in numerous judgments emphasized this right as fundamental.[310] The Code of Criminal Procedure (CrPC) and the Civil Procedure Code (CPC) provide statutory time limits for certain stages of trial, but these are often aspirational due to systemic inefficiencies.

The 2015 enactment of the Commercial Courts Act introduced explicit timelines for commercial disputes, mandating disposal within six months to one year, depending on case complexity.[311] Moreover, the National Judicial Data Grid (NJDG) launched in 2015 enhances monitoring of case pendency, aiming to institutionalize accountability for delay.

However, the judiciary faces a colossal backlog exceeding 45 million cases as of 2025, limiting the effectiveness of statutory timelines. [312] The pendency reflects infrastructure deficits, shortage of judges, and procedural complexities.

(B) United States

[309] Supreme Court of India, *Hussainara Khatoon v. State of Bihar*, AIR 1979 SC 1369.
[310] Supreme Court of India, *State of Maharashtra v. M.H. George*, AIR 1965 SC 722.
[311] The Commercial Courts Act, 2015 (India), No. 21 of 2015.
[312] National Judicial Data Grid (NJDG), Ministry of Law and Justice, India, 2025.

The USA does not have a single codified right to speedy trial applicable uniformly across civil and criminal matters; however, the Sixth Amendment guarantees a speedy trial in criminal prosecutions.[313] The Speedy Trial Act of 1974 imposes deadlines for federal criminal trials, generally requiring indictment within 30 days of arrest and trial within 70 days of indictment.[314]State courts have analogous rules, but with significant variance.

Civil litigation timing in the USA is governed by procedural rules (Federal Rules of Civil Procedure) emphasizing case management conferences and discovery schedules to expedite resolution.[315] Courts employ active case management, including sanctions for dilatory tactics.

Despite these mechanisms, delays persist due to complex discovery, plea bargaining, and resource constraints. The federal judiciary reported an average time to disposition of approximately 12 months for civil cases in 2023, with criminal cases resolved faster due to statutory mandates.[316]

(C) United Kingdom

In the UK, the principle of timely justice is embedded within the Human Rights Act 1998 through Article 6 of the European Convention on Human Rights, which guarantees the right to a fair and public hearing within a reasonable time.[317] The Civil Procedure Rules (CPR) 1998 emphasize proportionality and case management to avoid unnecessary delays.[318]

Criminal justice timeliness is supported by statutory provisions such as the Criminal Procedure Rules 2020, mandating case progression timelines and pre-trial reviews.[319] The introduction of the 'Digital Case System' has enhanced efficiency.

Despite reforms, the UK judiciary has encountered delays exacerbated by budget cuts and increasing caseloads, particularly post-Brexit and during the COVID-19 pandemic.[320] As of 2024, average civil case resolution time approximates 9 months in the High Court.[321]

[313] U.S. Constitution, Sixth Amendment.
[314] Speedy Trial Act of 1974, Pub.L. 93-619, 18 U.S.C. SectionSection 3161–3174.
[315] Federal Rules of Civil Procedure, 1938 (amended 2024).
[316] Administrative Office of the U.S. Courts, "Federal Judicial Caseload Statistics," 2023.
[317] Human Rights Act 1998 (UK), Section 6; European Convention on Human Rights, Article 6.

[318] Civil Procedure Rules 1998 (UK), Part 1 and Part 3.
[319] Criminal Procedure Rules 2020 (UK).
[320] UK Ministry of Justice, "Justice Statistics Quarterly," Q1 2024.
[321] UK Ministry of Justice, 2024 Annual Report.

(D) Singapore

Singapore stands out for its structured and effective time-bound justice framework. The Constitution does not explicitly mention speedy trial rights; however, the judiciary interprets Article 9(1) (liberty of the person) to include prompt trials.[322]

Singapore's judiciary employs strict procedural timelines codified in the Supreme Court Rules and subordinate legislation. The State Courts and Supreme Court maintain key performance indicators (KPIs) targeting case disposal timelines, routinely publishing statistics demonstrating average civil case resolution within 6 months and criminal trials within 3-6 months.[323]

The judiciary's strategic use of technology (Integrated Criminal Case Management System) and alternative dispute resolution mechanisms have significantly reduced delays. [324] Singapore's model is often benchmarked internationally for judicial efficiency.

(ii) Institutional Mechanisms and Reforms for Time-Bound Justice

India's National Judicial Data Grid (NJDG) represents a landmark initiative to enhance transparency and accountability in case management by providing real-time data on case pendency and disposal rates.[325] However, the lack of uniform enforcement and infrastructural limitations hamper impact. In contrast, US federal courts employ case management tools such as the Case Management/Electronic Case Files (CM/ECF) system, enabling judges to monitor deadlines actively and impose sanctions for non-compliance.[326] State courts vary widely, with some adopting similar electronic case management systems.

The UK's Civil Justice Council promotes active judicial case management, supported by digital tools like the Digital Case System (DCS), which streamline filing, hearing scheduling, and document management. [327] Singapore's judiciary integrates case management with

[322] Constitution of the Republic of Singapore, Article 9(1).
[323] Singapore Judiciary Annual Report, 2024.
[324] Integrated Criminal Case Management System (ICCMS), Singapore, 2023.

[325] NJDG, Ministry of Law and Justice, India, 2025.
[326] United States Courts, CM/ECF System Overview, 2024.
[327] Civil Justice Council, UK, "Digital Case System Implementation Report," 2023.

performance KPIs, conducting regular audits and reviews to ensure compliance with timelines.[328]

This institutional rigor contributes to its low backlog. India's Commercial Courts Act 2015 introduced mandatory pre-institution mediation and strict timelines for case disposal.[329] The 2019 Code of Civil Procedure amendments introduced provisions for fast-track courts.

The US Speedy Trial Act imposes statutory deadlines with exceptions for complexity and continuity, balancing expedition with fairness.[330] Civil litigation reforms emphasize Alternative Dispute Resolution (ADR) to reduce court burdens.

The UK's Civil Procedure Rules encourage use of ADR and summary judgment procedures to expedite cases without trial. [331] The Criminal Procedure Rules 2020 introduced case progression timetables with judicial oversight.

Singapore's legislative framework mandates pre-trial conferences, mediation, and case management conferences, supported by statutory deadlines.[332] The judiciary also applies cost sanctions for delays.

The efficacy of time-bound justice is inextricably linked to political will, resource allocation, and systemic governance. India's democratic complexity and federal structure complicate uniform reforms, despite constitutional mandates. Political priorities often skew towards law and order rather than judicial capacity building.[333]

In the USA, decentralization allows state-level innovation but also creates disparities. Political polarization impacts judicial appointments and resource distribution, affecting timeliness.[334] The UK's centralized judiciary benefits from integrated reforms but faces fiscal constraints amplified by post-Brexit policy shifts.[335] Singapore's authoritarian governance model enables

[328] Singapore Judiciary, Performance KPIs, 2024.
[329] Commercial Courts Act, 2015 (India).
[330] Speedy Trial Act of 1974 (USA).
[331] Civil Procedure Rules 1998 (UK).
[332] Supreme Court Rules (Singapore), Order 24.

[333] Bhatia, S., "Political Economy of Judicial Reforms in India," *Indian Journal of Law and Society*, 2023.
[334] Smith, J., "Judicial Efficiency and Federalism in the USA," *American Law Review*, 2024.
[335] Brown, A., "Brexit and the UK Judiciary," *European Legal Studies*, 2024.

swift judicial reforms and resource prioritization, reflecting an alignment between political stability and judicial efficiency.[336]

(iii) Sensitivity Analysis and Future Directions

Improving time-bound justice requires addressing to increase judges per capita significantly reduces backlog and case duration. India's target to double its judicial strength by 2030 could reduce case pendency by 40%.[337] Enhance Technological Integration by adding Digital case management systems improve efficiency; investments in AI-assisted docketing and virtual hearings could cut timelines by 15-20%.[338]

Emphasizing ADR and fast-track courts demonstrably accelerates case resolution. Adoption rates above 50% correlate with 25% lower average case duration.[339] To keep sustained political commitment with adequate budgetary allocations is critical. Countries with stable governance and judicial autonomy (e.g., Singapore) outperform others consistently.

Limitations

Some scholars argue that aggressive timelines risk compromising procedural fairness and quality of adjudication.[340]For example, a strict six-month disposal mandate may limit thorough evidence examination in complex cases.

Moreover, emphasis on numerical efficiency might incentivize case dismissals or settlements unfavorable to substantive justice.[341] These critiques underscore the need to balance speed with quality and equity.

Conclusion

Time-bound justice is a multidimensional challenge influenced by constitutional safeguards, legislative frameworks, institutional capacity, political environment, and technological adoption. India's constitutional right to speedy trial confronts systemic barriers resulting in

[336] Tan, L., "Authoritarian Governance and Judicial Efficiency," *Asian Journal of Comparative Law*, 2023.
[337] National Court Management Plan, India, 2025.

[338] World Justice Project, "Digital Courts and Efficiency," 2024.
[339] OECD, "Alternative Dispute Resolution and Judicial Efficiency," 2023.
[340] Sharma, R., "Speed vs. Fairness in Criminal Trials," *Journal of Criminal Justice Studies*, 2024.
[341] Lee, M., "The Risks of Judicial Expediency," *Law and Society Review*, 2023.

extensive delays, whereas Singapore's integrated approach yields exemplary efficiency. The USA and UK balance statutory mandates with judicial discretion, achieving moderate success.

Sustainable improvements necessitate holistic reforms encompassing judicial strengthening, procedural innovation, technological integration, and political commitment. Comparative lessons underscore the feasibility of accelerated justice without sacrificing fairness, contingent on context-sensitive adaptation.

7.3. Lessons for India: Adapting International Best Practices to the Indian Context

India's criminal justice system faces persistent challenges including case backlogs, protracted trials, infrastructural constraints, and limited access to justice for marginalized communities. The experience of E-Sakshya, combined with lessons drawn from successful international digital justice initiatives, offers valuable insights for reform tailored to India's unique socio- legal milieu.

International jurisdictions such as Singapore, Australia, and Estonia have demonstrated that effective digital integration-through comprehensive case management systems, electronic evidence handling, and remote hearing facilities-can significantly improve judicial efficiency and transparency.[342] These countries emphasize not only technological adoption but also the need for enabling policy frameworks, capacity building, and stakeholder buy-in, which are crucial for sustainable reform.[343]

For India, the adaptation of such best practices requires careful contextualization. The diversity of the legal ecosystem, including multiple languages, varying infrastructural capabilities, and socio-economic disparities, necessitates a decentralized yet interoperable technological architecture. [344] Lessons from Estonia's e-justice model underscore the significance of robust data security and privacy legislation, which India must strengthen consistent with its data protection regime to build public trust.[345] Additionally, Australia's

[342] See Tan S., 'Digital Transformation of Justice Systems: Singapore's Experience' (2020) 34(2) *Asian Journal of Legal*

Technology 92; Smith J., 'E-Justice in Estonia' (2019) 12(1) *European Journal of Law and Technology* 45.
[343] Brown L. and Green P., *Implementing Legal Technology: Lessons from Australia* (Routledge 2021) 67–70.
[344] Kaur R., 'Challenges in Implementing Digital Justice in India' (2022) 21(3) *Indian Journal of Law and Technology* 135.
[345] Lepp K., 'Data Privacy and E-Justice: The Estonian Framework' (2021) 15(4) *International Journal of Law and Information Technology* 110

emphasis on user-centric design and continuous training highlights the imperative of enhancing digital literacy among judicial officers, lawyers, and litigants to overcome resistance and optimize usage.[346]

Moreover, India's legal procedures often involve extensive paperwork and in-person interactions, which requires thoughtful digitization that integrates seamlessly with existing legal traditions and practices rather than imposing wholesale disruption.[347] Pilot projects such as E- Sakshya can serve as incubators for refining interfaces and workflows sensitive to local needs, facilitating incremental but effective transformation.[348]

Importantly, embedding comprehensive monitoring and evaluation frameworks modeled on international standards will allow policymakers to measure impact rigorously and iteratively improve digital justice solutions in India.[349] With tailored policy backing and sustained capacity development, the integration of international best practices through platforms like E-Sakshya can significantly advance India's goal of delivering justice that is timely, accessible, and accountable.

WHITE BLACK LEGAL

[346] Brown and Green (n 2) 98–102.
[347] Sharma A., 'Integrating Digital Systems with Traditional Legal Practice in India' (2020) 16(2) *Journal of Legal Reform* 57.
[348] Patil S. and Desai M., 'E-Sakshya as a Model for Indian Courts' (2023) 28(1) *Journal of Indian Judicial Studies* 23.
[349] United Nations Office on Drugs and Crime, *Guidelines on Monitoring Digital Justice Initiatives* (UNODC 2020) 14–19.

CHAPTER 8- CONCLUSION

8.1. SUMMARY

This dissertation has examined the potential evolution of E- Sakshya made in advancing time- bound justice within India's criminal justice system. The study reveals that E-Sakshya effectively tackles the long-standing issues of delays and inefficiencies in judicial proceedings by harnessing technology to enhance case management efficiency, promote transparency, and foster communication among the various participants. By digitizing important judicial processes, E-Sakshya democratizes access to justice and speeds up case resolution, especially for underserved communities that have historically had difficulty navigating the legal system. As an example of how creative digital solutions can act as catalysts for systemic change, the platform promotes a framework for justice delivery that is more accountable, effective, and equitable. All things considered, E-Sakshya is a big step toward fulfilling the constitutional guarantee of prompt and equitable justice for all citizens.

8.2. KEY INSIGHTS

Several important insights that advance our knowledge of the relationship between technology and criminal justice reform have been gleaned from the research. First, E-Sakshya's implementation emphasizes how crucial it is to use technology strategically to address systemic issues in the legal system. By automating repetitive administrative duties and offering instant access to case data, E-Sakshya lessens the workload for court staff and lowers the possibility of human error, increasing overall effectiveness. Second, by emphasizing accountability and transparency, the platform represents a major step forward in the fight against malpractice and corruption in the legal system. The opacity that frequently permeates court proceedings is reduced by E-Sakshya, which empowers litigants and promotes an accountable culture among judicial actors by enabling all authorized stakeholders to access and update case information in real-time.

Third, by offering digital access to legal resources and case information, E-Sakshya's design fosters

inclusivity and closes the gap for underserved groups who might not have the resources to attend traditional legal proceedings. In accordance with international human rights norms and constitutional mandates, this democratization of access to justice strengthens the idea that everyone should have access to justice, irrespective of socioeconomic background or geographic location. Judicial administrators can also make well-informed decisions about the allocation of resources and the creation of policies thanks to the data-driven insights produced by E-Sakshya. Through case management pattern analysis and bottleneck identification, judicial authorities can carry out focused interventions that boost operational effectiveness and enhance case results overall. By taking an evidence-based approach, E-Sakshya departs significantly from the anecdotal decision-making methods of the past and sets the stage for future judicial reforms.

Lastly, there is a need for Coordination, integration and preservation of issues within specific time period as mentioned under Section 176(3) & Section 173(1) requires forensic reports to be submitted within 30 days and mandates that investigations for offences punishable by seven years or more be completed within 90 days, with a possible 30-day extension upon judicial approval, ensuring expeditious case progression respectively, If the Ios does not reach the crime scene at the specific time frame and does not address at the adequate timing, this can seriously affect the merit of the case.

Now by investing more on connectivity, training of the investigating officers, and forensic infrastructure, India can bridge these gaps, ensuring the BNSS's efficiency-driven reforms benefit all regions.

8.3. FUTURE DIRECTIONS

Moving towards the futuristic perspective, many critical avenues for research and policy development emerge from this study. Firstly realizing the total potential of digitalized justice that demands scalable solutions tailored to diverse jurisdictional contexts, with particular attention to rural and resource constrained regions. The platform must be adapt to local legal frameworks and cultural nuances to ensure its effectiveness across various settings. Secondly, some of the integrating emerging technologies such as blockchain and artificial intelligence offers promising avenues to further automate and protect judicial processes. Blockchain technology could provide immutable records of evidence alongwith case proceedings, hence increasing the integrity of the judicial process, while artificial intelligence could facilitate predictive analytics, enabling judicial

authorities to give importance on the cases based on urgency and complexity. Thirdly, strong ethical and legal frameworks must be developed for privacy, prevent bias and provide transparency in algorithmic decision-making.The establishment of comprehensive regulations that protect individual rights must be prioritized by the policymakers alongwith that promoting innovation in the justice sector.

Furthermore, uninterrupted investment in capacity building will be essential to equip judicial actors with requisite digital competencies and foster cultural acceptance of technology within judicial system. On going professional development programs should be established to improve digital knowledge among the judges, lawyers and law enforcement officials, ensuring that they are well prepared to navigate the evolving landscape of digital justice. Finally, continuous empirical evaluation and user centric design must guide frequentative refinements of E-Sakshya and similar platforms. Engaging with users- judicial actors, litigants and legal practitioners- will provide valuable insights into the practical challenges and opportunities associated with digital justice initiatives. This feedback loop will be crucial to ensure that technological innovations remain aligned with the needs and expectations of all stakeholders involved in the justice process.

To conclude now, this dissertation affirms that E-sakshya helps in reducing the time wastage to achieve justice and create transparency as well as accessible justice. The integrated approach outlined here will be pivotal in shaping a resilient, efficient, and inclusive criminal justice system that is fit for the challenges of the 21st century.

REFERENCES LIST

Primary Sources Legislation

- *Bharatiya Nagarik Suraksha Sanhita* 2023 (India).
- *Bharatiya Nyaya Sanhita* 2023 (India).
- *Bharatiya Sakshya Adhiniyam* 2023 (India).
- *Digital Personal Data Protection Act* 2023 (India).
- *Information Technology Act* 2000 (India).
- *Police and Criminal Evidence Act* 1984 (UK).

- *Criminal Justice Act* 2003 (UK).
- *General Data Protection Regulation* (EU) 2016/679.
- *Evidence Act* (Cap 97, 1997 Rev Ed Sing).

Cases

- *Anvar P.V. v. P.K. Basheer* (2014) 10 SCC 473.
- *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020) 7 SCC 1.
- *K.S. Puttaswamy v. Union of India* (2017) 10 SCC 1.
- *Public Prosecutor v. Tan Hou Wang* [2023] SGHC 140.
- *Selvi v. State of Karnataka* (2010) 7 SCC 263.
- *Shafhi Mohammad v. State of Himachal Pradesh* (2018) 5 SCC 311.
- *State (NCT of Delhi) v. Navjot Sandhu* (2005) 11 SCC 600.
- *State of Punjab v. Deepak Mattu* (2020) SCC Online SC 821.
- *United States v. Microsoft Corp.*, 584 U.S. 201.

Secondary Sources

WHITE BLACK
LEGAL

Books

- Ahuja VK, *Electronic Evidence in India: Law and Practice* (LexisNexis 2022).
- Gupta R, *Privacy and Evidence in Digital India* (OUP 2020).
- Sharma SK, *Cybercrime and Digital Evidence* (Universal Law Publishing 2021).
- Swaminathan P, *Electronic Evidence: Challenges and Solutions* (Eastern Book Company 2019).
- *European Convention on Human Rights* (1953).

Journal Articles

- Bhatia S, 'Political Economy of Judicial Reforms in India' (2023) 21(3) *Indian Journal of Law and Society* 135.
- Smith J, 'E-Justice in Estonia' (2019) 12(1) *European Journal of Law and Technology* 45.
- United Nations Office on Drugs and Crime, *Guidelines on Monitoring Digital Justice Initiatives* (UNODC 2020).

Reports & Policy Documents

- Bureau of Police Research and Development, *Investigation Delays in India* (BPRD 2022).
- Ministry of Home Affairs, *eSakshya Guidelines* (MHA 2023).
- National Crime Records Bureau, *Cyber Crime in India* (NCRB 2023).
- NITI Aayog, *Digital Divide in Criminal Justice* (Government of India 2023).

Websites & Online Sources

- National Judicial Data Grid, *Pendency of Cases in India 2023* (NJDG, 2023) https://njdg.ecourts.gov.in accessed 15 May 2024.
- Singapore Judiciary, *Annual Report 2023* (Singapore: SJ, 2023) https://www.judiciary.gov.sg accessed 20 June 2024.