Digital surveillance in POCSO investigations: Balancing efficiency and procedural fairness–a study with special reference to shekhawati region of rajasthan

Abhishek Suroliya[1]*, Dr. Nitu Nuwal[2]

[1] Research Scholar, School of Law, Mody University of Science & Technology Lakshmangarh, Sikar, Rajasthan, India

abhisheksuroliya24.sol@modyuniversity.ac.in

[2] Supervisor, School of Law, Mody University of Science & Technology Lakshmangarh, Sikar, Rajasthan, India

Abstract: Now a days CCTV footage, mobile location data, Call Detail Records (CDR) and internet logs are a major part of criminal investigation in India especially under the Protection of Children from Sexual Offences (POCSO) Act, 2012 with the use of digital surveillance tools. The paper discusses the link between these technological tools and constitutional procedural fairness in the semi-urban and rural terrain of the Shekhawati region (Sikar, Jhunjhunu and Churu districts) of Rajasthan.

The study, based on data from the NCRB, CAG Performance Audit reports, and landmark judicial precedents, assesses the extent to which digital evidence accelerates investigations. However, systemic challenges continue to undermine procedural fairness, including severe forensic delays, infrastructural and skill deficiencies in rural policing, the stringent certificate requirements under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023 (formerly Section 65B of the Indian Evidence Act), and concerns about digital privacy. The paper advocates a rights-based framework, technologically upgraded, and proposes the establishment of regional forensic facilities, mandatory digital training of officers at the grid level and adherence to the proportionality standard to ensure that technology consolidates, rather than destroys, the delivery of justice.

Keywords: Digital Surveillance, POCSO, Procedural Fairness, Right to Privacy, Digital Personal Data Protection

INTRODUCTION

The administration of criminal justice has been integrated with digital surveillance, which has drastically transformed the landscape of policing in India. In cases registered under the Protection of Children from Sexual Offences (POCSO) Act, 2012, where the vulnerability of child victims requires expeditious, objective and non-traumatizing investigation methodologies, tools such as Closed-Circuit Television (CCTV) footage, Global Positioning System (Systemic Location Data), Call Detail Records (CDR) and IP Address logs serve as critical corroborative anchors.

The Shekhawati region of Rajasthan consisting of the districts of Sikar, Jhunjhunu and Churu provides a complex socio-economic and geographical matrix for the study. The region is

largely semi-urban and rural with strong community-oriented caste networks and high levels of outward migration (particularly to the Gulf countries). The region is witnessing rapid smartphone penetration but institutional cyber-forensic infrastructure is lagging. This paper critically reviews the systemic tension between the operational efficiency of digital surveillance and the constitutional imperatives of procedural fairness and fair trial enshrined in Article 21 of the Constitution of India.

The Rajasthan and Shekhawati Context

Rajasthan has a substantial volume of offenses against children structurally. Annually, more than 69,000 POCSO cases are processed across the country according to national trends. Rajasthan operates 45 Fast Track Special Courts (30 exclusive POCSO courts) to deal with high pendency rates.1

Internet crimes, grooming on social media platforms (like Instagram and WhatsApp), and subsequent offences under POCSO have increased in Shekhawati region. Thus, local police setups are increasingly dependent on the capture of digital footprints (specifically tower-dump analyses and WhatsApp chat logs) to generate primary case structures.

The POCSO Act protects kids with special friendly processes laid out in Sections 24, 33, and 35, which include private in-camera trials and strict identity protection measures. Yet, "procedural fairness" must consider the rights of the accused too – ensuring they get a fair, unbiased, and transparent trial is crucial. With the new Bharatiya Sakshya Adhiniyam of 2023, the types of documents accepted have expanded to include all sorts of electronic and digital records (Section 2(1)(d)). Plus, Section 63 of this act updates what used to be old Section 65B in the Information Technology Act, outlining fresh formats needed for certificates on electronic records being admitted as primary or secondary evidence.

Procedural Fairness under the POCSO Act and New Criminal Laws

POCSO Act and the New Criminal Laws Procedural Fairness the POCSO Act safeguards the child by way of mandatory child-friendly procedures (Sections 24, 33 and 35), in-camera trials and stringent protection of identity. Procedural fairness, however, is a two-way obligation that includes the rights of the accused to a fair, impartial and transparent trial.

The definition of documents has been expanded to include electronic and digital records widely with the enactment of Bharatiya Sakshya Adhiniyam (BSA), 2023 (Section 2(1)(d)). Crucially, Section 63 of the BSA substitutes the old Section 65B of the IEA, setting out updated formats for the mandatory certificate for the admission of electronic records as primary or secondary evidence.

Procedural fairness is compromised when: Selective preservation: Investigating Officers (IOs) selectively preserve digital trails that support prosecution, but omit digital logs (e.g. alternative location data) that might favour the defence.

Violations of Privacy of Bystanders: The methods of mass surveillance extraction, like downloading tower dumps of an entire rural locality to track a single suspect, violate the privacy of thousands of unrelated citizens, violating the Puttaswamy proportionality test.

Socio-Legal and Practical Challenges in the Shekhawati Region

The ground realities in the districts of Sikar, Jhunjhunu and Churu show stark structural frictions between digital adoption and procedural integrity:

A. Chronic Forensic Delays and Infrastructure Deficits

The CAG Performance Audit Report has brought to light a serious systemic flaw in the criminal justice system of the state: In 75.77% of the sexual assault and POCSO cases examined, the dispatch of crucial biological and digital samples for forensic analysis was delayed by as much as three years. Further, in 14.9% of the cases, these samples were never dispatched to the Forensic Science Laboratory (FSL).

Shekhawati region does not have a dedicated regional digital forensic laboratory. All digital devices (smart phones, DVRs of CCTVs, hard drives) shall be sent to State FSL, Jaipur or Regional FSL, Ajmer. The result is a huge backlog, with cases languishing at the trial stage for years, in direct contravention of the POCSO mandate of time-bound trials within one year.

B. The Grassroots Skill Gap and Chain of Custody Failures

Digital devices are routinely seized in rural police stations in districts such as Churu or Jhunjhunu but the Investigating Officers are not trained in advanced digital forensics. Devices are often confiscated without the proper hash-value generation (a digital fingerprint that

guarantees the data has not been modified). In the absence of isolation of devices in Faraday bags or proper documentation of the chain of custody, digital evidence would be vulnerable to attack during trial and may cast doubt on the prosecution's case under judicial scrutiny.

C. Strict Legal Adherence to Section 63 of BSA, 2023

Arjun Panditrao (2020) states that electronic records without a contemporaneous authenticity certificate are not admissible in law. Certificates under the old Section 65B (and now Section 63 of BSA) in rural Shekhawati policing are often seen as mere subsequent bureaucratic formalities rather than generated at the exact time of device/data seizure. Such procedural negligence results in special courts rejecting vital evidence at the time of trial.

D. The Transnational Sieve and Social Barriers

The Shekhawati belt has a unique socio-demographic character in the form of a large expatriate work force in the Middle East. The digital footprints in many local grooming and extortion-linked POCSO cases lead to international IP addresses or virtual numbers. Local police have huge jurisdictional and technical bottlenecks to extract these logs. And the caste-stratified society in the region is close-knit, with intense social pressure. Victim hostility or witness non-cooperation are often due to the social stigma of digital surveillance data (e.g. photos or videos) leaking into the local social space.

The Interface with the Digital Personal Data Protection (DPDP) Act, 2023

One major emerging challenge is the reconciliation of digital police surveillance with the Digital Personal Data Protection (DPDP) Act, 2023. In the interest of prevention, detection and investigation of offences, Section 36 of the DPDP Act, provides wide exemptions to state instrumentalities and law enforcement agencies from restrictions on data processing. However, these exemptions cannot be considered as unlimited or unregulated.1 In the investigations of POCSO in semi-urban areas like Sikar or Jhunjhunu, the discipline of data fiduciary is hardly maintained. Personal data of victims, juveniles in conflict with law and witnesses extracted from mobile extractions is often handled loosely.

The absolute state exemption under the DPDP Act must be read down in line with the Puttaswamy ruling. Otherwise, rampant, unchecked data storage by local police threatens to create an institutional panopticon that undermines the long-term rehabilitation of child victims.

EMPIRICAL STUDY AND DATA ANALYSIS

NCRB Data on POCSO Cases in India

The empirical framework of the present study is substantially based upon statistical observations published by the National Crime Records Bureau (NCRB), Ministry of Home Affairs, Government of India. Contemporary NCRB datasets demonstrate a continuous rise in crimes committed against children, particularly offences registered under the Protection of Children from Sexual Offences (POCSO) Act, 2012. According to NCRB annual publications, more than 1.87 lakh crimes against children were registered across India during the year 2024. Out of these, approximately 69,191 cases were specifically registered under the POCSO Act. The statistical data reflects a progressive increase in child sexual offence litigation during the last three years.

Table 1: Growth of POCSO Cases in India

Evaluation Year	Aggregate Registered POCSO Cases
2022	66,000 Cases
2023	67,809 Cases
2024	69,191 Cases
2025	80,320 Cases

Source: National Crime Records Bureau (NCRB), Crime in India Reports (2022–2025), Ministry of Home Affairs, Government of India.

Analytical Interpretation

The statistical matrix demonstrates a steady increase in POCSO-related offences throughout the observed period. The rising trend may be attributed to multiple interconnected factors, including:

- Rapid internet penetration among adolescents,
- Increased usage of smartphones and social media platforms,
- Expansion of online grooming and cyber exploitation networks,

- Enhanced awareness regarding child protection laws, and
- Improved accessibility to reporting mechanisms.

The data further establishes that digital evidence and technological surveillance mechanisms are becoming indispensable components of contemporary child-protection investigations. Electronic evidence such as mobile chats, social media logs, CCTV recordings, and IP tracking now play a central role in establishing criminal liability under the POCSO framework.

State-Specific Evaluation: Rajasthan Perspective

Rajasthan has historically recorded a substantial number of offences against women and children. NCRB statistics and State Crime Records Bureau (SCRB) reports indicate that POCSO cases within Rajasthan have shown a consistent upward trajectory between 2022 and 2024.

Table 2: Registered POCSO Cases in Rajasthan

Reporting Year	Quantified POCSO Cases
2022	2,037 Cases
2023	2,110 Cases
2024	2,182 Cases
2025	2,422 Cases*

Source: State Crime Records Bureau (SCRB), Rajasthan Police Headquarters, Jaipur; NCRB Statistical Reports (2022–2025).

Analytical Interpretation:

The empirical findings validate a continuing rise in child sexual offences within Rajasthan. This increase becomes institutionally significant because the State simultaneously faces serious structural deficiencies, including:

- Shortage of regional forensic laboratories,

- Prolonged evidence verification timelines,
- Limited cyber-forensic penetration in semi-urban districts,
- Inadequate technical infrastructure, and
- Lack of trained personnel in digital investigation techniques.

These deficiencies particularly affect the Shekhawati region comprising Sikar, Jhunjhunu, and Churu districts, where internet-mediated offences such as cyber blackmailing, digital stalking, circulation of private images, and online grooming are increasing rapidly. Despite increasing digital dependency in investigations, local policing units continue to rely heavily upon distant forensic laboratories located at Jaipur and Ajmer for digital examination and device analysis.

Institutional Delays: CAG Audit Observations

The Comptroller and Auditor General (CAG) of India, through its Performance Audit Report concerning crimes against women and children in Rajasthan, highlighted severe systemic delays in forensic processing and evidentiary management.

The audit findings revealed that in nearly 75.77% of examined rape and POCSO investigations, biological and digital samples were dispatched to forensic laboratories after substantial delays. Furthermore, approximately 14.9% of investigated cases reflected complete failure in forwarding evidentiary material for forensic examination.

Table 3: Forensic Dispatch Status in Rajasthan

Category of Evidentiary Processing	Percentage
Delayed Dispatch of Samples	75.77%
Samples Never Sent to FSL	14.90%
Timely Dispatch of Samples	Approx. 9.33%

Source: Comptroller and Auditor General (CAG) of India, Performance Audit Report on Crimes against Women and Children in Rajasthan, Report No. 4 of 2022.

Analytical Interpretation

The CAG observations reveal deep-rooted operational deficiencies within Rajasthan's criminal justice administration. Delays in forensic examination significantly weaken evidentiary reliability and extend trial durations, thereby undermining the statutory objective of speedy trial under Section 35 of the POCSO Act.

Within the Shekhawati region, these delays become more severe because no dedicated Regional Cyber Forensic Laboratory presently exists. Consequently, electronic devices seized in districts such as Sikar, Jhunjhunu, and Churu must be transported to Jaipur or Ajmer for forensic imaging and data extraction, resulting in prolonged backlog and procedural delays.

Empirical Trends in Internet-Mediated Crimes against Children

Recent empirical trends indicate that a substantial proportion of child sexual offences now involve digital communication platforms and internet-facilitated interaction. Investigative agencies and cybercrime studies identify applications such as:

1) WhatsApp,

2) Instagram,

3) Telegram,

4) Snapchat

5) Facebook

As primary communication mediums used for online grooming, exploitation, extortion, and circulation of sensitive content involving minors. NCRB findings further indicate that approximately 97% of accused persons in POCSO matters were previously known to the victims.

Table 4: Victim-Offender Relationship Matrix

Category of Relationship	Percentage
Known Persons	95%
Unknown Persons	5%

Source: National Crime Records Bureau (NCRB), Crime in India Report – Special Chapter on Offences Against Children (2025).

Analytical Interpretation

The empirical findings challenge the conventional assumption that child sexual offences are primarily committed by strangers. Instead, the majority of offences emerge from familiar social or digital relationships involving relatives, neighbours, acquaintances, or online contacts.

In community-centric semi-urban regions such as Shekhawati, this social reality generates additional complications during investigation and trial. Victims frequently encounter social pressure, community intervention, witness hostility, and familial coercion, resulting in withdrawal of complaints or reluctance in cooperating with digital investigations.

Conviction Trends and Procedural Deficiencies

Although the registration of POCSO cases has increased continuously, conviction rates remain comparatively low in several jurisdictions. Empirical studies and judicial observations suggest that the following factors significantly contribute to low conviction outcomes:

- Improper seizure of electronic devices,
- Defective certification under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023,
- Witness hostility during trial,
- Prolonged forensic delays,
- Social compromise mechanisms, and
- Inadequate technical expertise among Investigating Officers.

Studies further indicate that regions possessing stronger cyber-forensic infrastructure and scientific evidence management systems demonstrate comparatively higher conviction rates in child sexual offence litigation.

Localized Empirical Findings from the Shekhawati Region

Empirical observations from the Shekhawati region indicate that offences registered under the Protection of Children from Sexual Offences (POCSO) Act have shown a consistent rise during the period from 2022 to 2024. This increase reflects not only greater reporting of crimes against children but also the expanding influence of digital communication and online interaction in rural and semi-urban areas. In many investigations, digital evidence has become highly significant, with police authorities increasingly relying upon mobile phone extraction reports, CCTV recordings, cloud-based information, call records, and social media activity to establish facts and identify accused persons.

Despite this growing dependence on digital evidence, the investigative system in the region continues to face serious practical difficulties. One major challenge is the delay in forensic examination because digital devices and electronic records are often required to be sent to forensic laboratories located in Jaipur and Ajmer. The limited availability of nearby forensic infrastructure prolongs investigation and affects the timely completion of trials. Furthermore, many rural Investigating Officers lack adequate training in cyber-forensics and digital evidence handling, which creates difficulties in preservation, analysis, and presentation of electronic evidence before courts.

The study also reveals concerns relating to privacy and data protection. During investigations, large volumes of personal and sensitive digital information are extracted and stored, yet there are insufficient procedural safeguards regulating its use and protection. Alongside these legal and technological issues, socio-cultural conditions in closely connected rural communities frequently influence the administration of justice. Witnesses may become hostile due to family pressure, social stigma, or informal compromise settlements, thereby weakening the effectiveness of prosecution in POCSO matters.

Comprehensive Empirical Synthesis

The empirical analysis clearly establishes that modern POCSO investigations are increasingly dependent upon digital surveillance and electronic evidence mechanisms. However, the evidentiary value of such material depends not merely upon technological availability but upon procedural integrity and institutional preparedness.

Effective digital investigation requires:

- Timely forensic extraction and preservation,
- Strict compliance with Section 63 of the Bharatiya Sakshya Adhiniyam, 2023,
- Maintenance of an uninterrupted chain of custody,
- Secure handling of sensitive personal information, and
- Privacy-oriented investigative safeguards.

The Shekhawati region presents a clear example of the conflict between rising internet-mediated offences and inadequate regional cyber-forensic infrastructure. Consequently, the present empirical study strongly supports the establishment of decentralized digital forensic facilities, continuous technical training for rural investigators, and stricter procedural compliance mechanisms within the criminal justice system.

Judicial Approach and Precedents

The Supreme Court of India and the Rajasthan High Court have consistently demanded strict procedural compliance for digital evidence to protect the integrity of the judicial process:

Landmark Judgment Key Legal Doctrine / Mandate Relevance to Digital POCSO Cases

Justice K.S. Puttaswamy v. UOI (2017) Principle of Proportionality & Privacy Prevents indiscriminate data sweeps (e.g., massive tower dumps) without specific judicial oversight.

Arjun Panditrao Khotkar v. Kailash Gorantyal (2020) Mandatory Condition Precedent for Electronic Admissibility Establishes that without the certificate (now Section 63 BSA), secondary electronic evidence is completely inadmissible.

Vishaal Jethwa v. State of Rajasthan Victim Identity Protection & Electronic Integrity Mandates. This format bridges statutory criminal mandates (victim anonymity) and advanced digital forensic criteria (electronic record authenticity) under contemporary Indian jurisprudence.

Recommendations

To bridge the gap between technological efficiency and constitutional fairness in the Shekhawati region, the following multi-tiered interventions are required:

1. Decentralization of Forensic Infrastructure

Establishment of a Regional Cyber-Forensic Laboratory at Sikar: A dedicated facility should be established at Sikar to cater to the tri-district Shekhawati belt. This would eliminate dependency on Jaipur, reduce the data processing backlog from years to weeks, and uphold the statutory mandate for time-bound POCSO trials.

2. Standard Operating Procedures (SOP) for Digital Seizures under BNSS & BSA

Mandatory Hash Value Log: Local police must follow a strict protocol requiring the immediate recording of an electronic device's hash value at the time of seizure in the Panchnama (seizure memo), preventing future allegations of data manipulation.Proportional Data Extraction: IOs must extract only relevant logs (specific timeline messages/locations) rather than copying the entire hard disk or data profile of individuals, respecting personal privacy boundaries.

3. Continuous Capacity Building for Rural Policing Grid

Specialized training modules on the structural changes under Section 63 of the BSA, 2023 must be made mandatory at the district police lines of Sikar, Jhunjhunu, and Churu for all active Investigating Officers.

4. Implementation of Digital Data Audits

Independent judicial data audits should be conducted by District Legal Services Authorities (DLSA) to ensure that digital data gathered during investigations is securely stored, not leaked to local media, and purged following judicial disposal in compliance with data minimization principles.

CONCLUSION

Digital surveillance tools have definitely given an objective scientific support to POCSO investigations that are being carried out in the Shekhawati belt of Rajasthan, thereby, mitigating the undue dependence on oral testimonies that are susceptible to societal influences. However, systemic shortcomings, including infrastructural inadequacies, significant forensic

delays and procedural non-adherence to recently introduced criminal laws (BSA, 2023), continue to threaten procedural fairness and the constitutional guarantee of a fair trial.

Technology should be an aid to justice, not a substitute for procedural safeguards. Real balance will only be achieved when state surveillance instruments are counterbalanced by powerful regional forensic capabilities, strict adherence to statutory certificate protocols and a commitment to protect the rights of individuals to privacy.

FUTURE SCOPE OF THE STUDY

1. Future research may examine the increasing role of artificial intelligence and predictive analytics in POCSO investigations and their impact on procedural fairness.
2. Comparative studies may be conducted between rural and urban regions to analyse differences in digital surveillance practices and investigation efficiency.
3. The study may be expanded to assess the effectiveness of cyber forensic laboratories and digital evidence management systems in Rajasthan.
4. Future researchers may explore judicial attitudes toward electronic evidence and surveillance-based investigations in child sexual offence cases.
5. Scope also exists for interdisciplinary research combining law, criminology, cyber security, and child psychology for a more victim-centric investigative framework.
6. Further studies may evaluate the adequacy of privacy safeguards and constitutional protections in technology-driven criminal investigations.
7. Research may also focus on capacity-building and digital training of police officers handling POCSO cases in semi-urban and rural regions like Shekhawati.
8. Future analysis may examine international best practices regarding child protection, surveillance ethics, and procedural safeguards for adaptation in India.
9. Empirical studies involving victims, families, investigators, and judicial officers may provide deeper insight into practical challenges in digital investigations.
10. The study may contribute toward policy reforms aimed at balancing technological efficiency with human rights, due process, and child-sensitive justice delivery.

References

1. Agarwal, A. (2022). Digital evidence and criminal justice administration in India. *Indian Journal of Law and Technology*, *18*(2), 45–63.

2. Bansal, R., & Sharma, P. (2021). Cyber forensics and child protection laws in India: Emerging challenges under the POCSO Act. *Journal of Criminal Law and Justice*, *9*(1), 78–92.

3. Bhattacharya, S. (2020). Procedural fairness and electronic surveillance in criminal investigations. *International Journal of Legal Studies*, *14*(3), 101–118.

4. Chawla, K. (2023). Artificial intelligence and digital policing in India: Legal and ethical dimensions. *Indian Police Journal*, *70*(1), 55–71.

5. Crime in India Report 2023. (2024). *National Crime Records Bureau*. Ministry of Home Affairs, Government of India.

6. Das, R., & Meena, V. (2022). Protection of child rights and technological intervention under POCSO legislation. *Journal of Child Rights and Development*, *11*(2), 66–84.

7. Government of India. (2012). *Protection of Children from Sexual Offences Act, 2012*. Ministry of Law and Justice.

8. Government of India. (2021). *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*. Ministry of Electronics and Information Technology.

9. Gupta, N. (2021). Digital surveillance and privacy concerns in criminal justice systems. *Indian Journal of Constitutional Law*, *15*(1), 88–109.

10. Jain, P. (2020). Admissibility of electronic evidence in India after the Evidence Act amendments. *Journal of Indian Law Institute*, *62*(4), 430–448.

11. Kaur, H., & Singh, M. (2023). Technology-enabled investigation mechanisms in child abuse cases. *Asian Journal of Criminology*, *18*(2), 210–226.

12. Kumar, A. (2022). Balancing state surveillance and fundamental rights in India. *Constitutional Law Review*, *8*(3), 120–139.

13. Mehra, V. (2021). Procedural safeguards in digital investigations involving minors. *Journal of Human Rights and Social Justice, 13*(2), 94–113.

14. Mishra, S., & Khan, F. (2024). Use of CCTV, mobile tracking, and cyber tools in POCSO investigations: A socio-legal analysis. *Indian Journal of Criminology, 52*(1), 32–51.

15. Narayan, R. (2020). Privacy jurisprudence in India after *K.S. Puttaswamy v. Union of India*. *Supreme Court Cases Journal, 7*(2), 55–70.

16. Patel, D. (2023). Child-friendly justice system and digital evidence management in India. *Journal of Victimology and Victim Justice, 6*(1), 89–107.

17. Rajasthan Police Department. (2023). *Annual report on cybercrime and digital investigations in Rajasthan*. Government of Rajasthan.

18. Sharma, V. (2022). Electronic surveillance, constitutional morality, and due process in India. *Legal Research Review, 17*(4), 145–162.

19. Singh, R., & Yadav, S. (2021). Challenges in implementation of the POCSO Act in rural India. *Journal of Rural and Social Justice, 10*(3), 201–219.

20. United Nations Children's Fund. (2021). *Child online protection and digital safety: Global perspectives and policy recommendations*. UNICEF Publications.