*Corresponding Author's Email: animesh.pareek.24@kgpian.iitkgp.ac.in
Proceedings of The World Conference on Social Sciences
Vol. 5 Issue. 1, 2026, pp. 01- 19
DOI: https://doi.org/10.33422/worldcss.v5i1.2182
Copyright © 2026 Author(s)
ISSN: 2783-7785 online

Diamond Scientific Publishing

Legitimate Policing in the Digital Age: Balancing Crime Control and Due Process in Criminal Investigations in India

Animesh Pareek[1*], and Prakash Sharma[2]

[1]Research Fellow & PhD Scholar, Indian Institute of Technology Kharagpur, West Bengal, India

[2] Assistant Professor (Grade-I), Indian Institute of Technology Kharagpur, West Bengal, India

Abstract

Digital forensics has become central to criminal investigation, not because investigators prefer it, but because criminals increasingly operate in digital environments, and the evidence they leave behind is often more precise and more recoverable than anything physical. However, the Indian legal framework has not kept pace. Investigators routinely examine entire devices during searches, pulling in personal data that bears no relation to the alleged offence, and the constitutional protections against self-incrimination and privacy under Articles 20(3) and 21 sit uneasily alongside this practice. The Supreme Court has addressed the admissibility of fingerprints, DNA, and psycho-scientific methods like Narco Analysis and BEAP under specific conditions. However, the question of digital forensic evidence remains unsettled, with the stakes higher given the sheer volume of personal data a phone or laptop contains. This paper argues that digital investigative practices can be constitutionally grounded, but only if they operate within a framework that takes due process seriously. Drawing on Herbert Packer's crime control and due process model, the analysis identifies where Indian law currently falls short and where it might draw from the regulatory approaches taken in the United States, the United Kingdom, and Germany — jurisdictions that have managed, with varying degrees of success, to keep investigative power functional without treating constitutional rights as an inconvenience. The methodology is doctrinal: constitutional provisions, legislation, judicial precedent, and policy guidelines are examined critically rather than simply catalogued.

Keywords: digital policing, privacy, self-incrimination, human rights, criminal investigation

1. Introduction: The Legislative Vacuum in Digital Policing

Criminal procedure in modern states is shaped by two parallel modes of governance: 'law' and 'police' (John, 2025, p. 189), with the law providing the framework for legitimising or constraining police action (Dubber, 2013, p. 61). This governance was further improved with the introduction of new criminal codes in India in 2024. Interestingly, the increased use of digital devices has drawn the attention of the police. However, India's Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), the procedural code, does not codify procedures for conducting such seizures and searches (Bharatiya Nagarik Suraksha Sanhita, 2023, ss. 94, 96),

and the duty to fill these gaps is left with the judiciary. This evidence is relevant under the Bharatiya Sakshya Adhiniyam, 2023 (BSA), which makes it legally admissible in court.

In India, the proliferation of digital devices has significantly influenced criminal activity and investigative practice: law enforcement agencies increasingly rely on digital evidence (Majdoub & Atmani, 2025, p. 152), often causing legal challenges concerning the fundamental right against self-incrimination (Constitution of India, 1950, art. 20(3)) and privacy (Constitution of India, 1950, art. 21). In the Indian criminal justice system, the constitutional validity of physical search and forensic evidence was settled decades ago (Kathi Kalu Oghad v. State of Bombay, 1961); (Selvi v. State of Karnataka, 2010),[1] but the equivalent questions for digital evidence remain open precisely because no comparable procedure exists. The consequence is evident in the recent case of *Ram Ramaswamy v Union of India (pending)* (hereinafter Ramaswamy), and *Foundation for Media Professionals v Union of India (pending)* (hereinafter Foundation for Media Professionals), where the litigants sought a procedural framework for seizure and search of digital devices, because none exists in statute. As an interim order, the apex courts directed the state to frame guidelines and, until then, allowed the agencies to follow the CBI (Central Bureau of Investigation) Manual of 2018, which is not exhaustive in this context.

This paper argues that current policing practices demand a procedural framework that balances the rights of the person with the state's duty to investigate. Further, though judicial activism is permitted in India, it cannot substitute for a statutory framework that must be filled by legislation, empowering and limiting the policing.

1.1. Objective & Methodology

The objective of the paper is to highlight how current policing practices of searching and seizing digital devices violate fundamental rights, and to determine how a balance can be made between the rights of the person and those of the state. Addressing this gap calls for legislation, not further litigation. The work is a doctrinal legal study, focusing on legislation, including the Indian Constitution, BNSS, and BSA, and on reported judicial decisions in which legitimate policing is evaluated in relation to fundamental rights. The analytical framework is based on Herbert Packer's models of 'due process' and 'crime control' to evaluate current practices and propose amendments. Further, a comparative study has been conducted to examine gaps in India relative to the frameworks of the United States of America, the United Kingdom, and Germany, giving a combination of civil and common law. This comparison is functional as each state tries to balance between the state right to have access of digital evidence while protecting the privacy of individuals. The paper therefore uses these systems as benchmarks and source of design options, not as a template which can be pasted as it is in India.

2. Theoretical Foundations of Legitimate Policing in The Digital Age

The police are entrusted with safeguarding law and order, an essential duty for the state. However, their methods must conform to standards of legitimacy, especially when fundamental rights are at stake.

[1] The question related to the constitutional validity of physical evidence was well decided in the case of *Kalu Kathi Oghad v State of Bombay* AIR 1961 SC 1808., while the question related to the scientific techniques used during the investigation was dealt with in *Selvi. v State of Karnataka* (2010) 8 SCC 96. While recently in *Ritesh Sinha v State of U.P* (2019) SCC OnLine SC 956, the collection of voice samples was allowed and was held to be non-testimonial in nature.

2.1. Legitimacy in Policing

Herbert Packer's crime control and due process model remains the most widely used starting point for this inquiry, under which the crime control model prefers a justice system as an assembly line focused on efficient conviction. In contrast, the due process model emphasises individual rights and safeguards against wrongful conviction (Packer, 1968, p.173). Criticising Packer, Roach argues that it ignores the plight of the victims and the complexities of unreported crime (Roach, 1999, p. 672),[2] and expands on his framework by introducing punitive and non-punitive victims' rights models, highlighting the need to account for victims and community interests (Roach, 1999, p. 673). These additions are significant in the present scenario, as they demonstrate a deeper, more complex understanding of the current dynamics and address them.

For the maintenance of law and order, police agencies are given broad investigative powers, including the power to search houses, documents, and devices (Bharatiya Nagarik Suraksha Sanhita, 2023, ss. 94, 96), and even to arrest people for questioning, which is often the quickest means to establish whether the suspect is factually guilty (Packer, 1968, p. 171). However, it also increases the likelihood of an innocent man's conviction (Roach, 1999, p. 678). Though empowered by legislation, the actions become illegitimate due to the lack of a procedural framework, which not only violates fundamental rights but also makes policing prone to being challenged as extra-procedural investigations. Moreover, a legitimate framework is necessary, as it ensures that police actions are respected and shapes people's law-following behaviour through their beliefs in the legitimacy of the law, legal authorities, and their actions (Tyler, 2025, p. 167). Therefore, legitimacy-based policing not only supports procedural fairness but also fosters public cooperation (Tyler, 2025, p. 165).

Various theorists proposed different ways to legitimise policing: Beetham identified three essentials: legality, the existence of established laws; justifiability, rules grounded in shared beliefs of the police and the public; and consent, expressed through public cooperation (Beetham, 1991). Tyler revolutionised policing theory by demonstrating that the process and the way the police treat people are more significant than the outcome of policing (Tyler, 1990). Loader and Walker improvised it from a sociological perspective, their framework called policing as not just a way of controlling crime but a symbol of community itself, giving a message to the citizens of being a valued member of the shared community (Jackson & Bradford, 2011, p. 3); (Tyler, 2025, p. 166); (Bradford & Jackson, 2024, p. 4). Collectively, these theories confirm that policing legitimacy not only demands legislation but rests on the equitable, respectful exercise of lawful authority, which cultivates voluntary compliance and trust (Campbell, 2025, p. 73). No model is sufficient on its own, and a democratic system such as India requires a nuanced balance.

2.2. Technology and Policing

Policing has undergone a major shift in the digital era, with investigations moving from physical to digital searches. These are more efficient and offer a better chance of obtaining evidence that is significant in any trial or proceeding. Policing in the digital era, or digital policing, serves a dual function: it helps police departments deploy limited resources more efficiently (Utset, 2016, p. 1456) while also giving citizens a sense of security through digital surveillance. Although being effective, any expansion of surveillance through technology must

[2] Interestingly, people who are accused of any crime or are investigated by police initially fall under the protection of "due process model", but as soon as their fundamental rights are violated, they become victims, falling under the punitive and non-punitive right model of Kent Roach. In these cases, the state can either penalise the police officer if the actions fall outside the permitted legislative framework or compensate the victims to respect their rights.

be balanced against the risk of social control and eroded privacy (Lyon, 2024). The present actions of confiscation and blanket searches of devices increase the likelihood of violations of protections against self-incrimination and privacy, as they compel individuals to provide access to their digital devices containing private data, leaving users more exposed than necessary. Such actions demand a bifurcated standard that requires stronger justification for intrusion into inherently private information, which would better calibrate the state's power to specify the rationale, scope, and method of its data requests (Lund-Tønnesen & Fossheim, 2025), and must also protect data once obtained. This legitimacy and control can be attained through a legislative framework, which must be demonstrated in text as well as in practice: legislation must be just, fair, and non-arbitrary, state intrusion must be balanced against legitimate interests, and compelled evidence must be replaced by reliable and voluntary (Selvi v. State of Karnataka, 2010). For reducing privacy infringement, the concept of privacy can be shifted from individual fault to a societal duty, in which all data holders, whether government or private, have a duty to protect subjects from harm (Solove, 2021).[3]

This explains how technological advancement has the potential to limitlessly decrease the realm of guaranteed privacy and protection against self-incrimination. Multiple cases are pending before the Supreme Court of India challenging procedure-less digital searches, yet such violations continue. Therefore, India needs a comprehensive law regulating digital policing and, by extension, investigation, that respects both the rights of individuals and the state's protection, as well as the maintenance of law and order. This balance becomes essential in a democratic setup, helping earn the people's faith and enabling the effective implementation of laws.

3. Digital Policing and Judicial Decisions in India: Protection Against Self-Incrimination and Privacy

Digital devices now hold an extraordinary volume of information about their users, not merely what is stored deliberately but a continuous record of transactions and websites visited, leaving electronic traces of a person's activities and interests (Puttaswamy, 2017, para 170). Recognising the evidentiary value of this data, the BNSS empowers the police to compel production of electronic devices during investigation (Bharatiya Nagarik Suraksha Sanhita, 2024, ss 94 & 96), yet leaves the procedure for handling such devices largely undefined. Since these devices often hold the key to solving criminal cases, investigating agencies routinely confiscate them, but the absence of a settled procedure exposes such seizures to constitutional challenge, given that deprivation of life and liberty requires a procedure established by law (Maneka Gandhi v Union of India, 1973). Studies indicate that investigators rarely confine themselves to evidence relevant to the case at hand, resulting in the intrusion into unrelated personal data and exposing individuals to the misuse of information that has no bearing on the investigation (Verma et al., 2016, p. 31).

This evidence usually becomes relevant under section 39 of the BSA, which permits expert opinion to be admitted in court during trial. The reports are submitted by the experts of their examination of the crime scene and the other evidences, which the judicial officers then examine. Section 63 of the BSA remains the only provision that scrutinise digital evidence before it is admitted in a criminal trial. The provision sets out the admissibility criteria by examining whether the evidence produced is genuine and not tampered, and makes dual

[3] Prof. Solove argues that, when seen as individual harm, the duty remains of the person whose privacy is violated. This takes away the protection from data available in public, while equating privacy with secrecy. This limited definition of privacy denies protection in cases of misuse of this publicly available data, which was not meant to be used in that manner. Therefore, the author demands to shift this burden on society, so that even the data available online is protected from any misuse, as it becomes the duty of society.

certification from the user and expert, mandatory. However, it does not examine "how the data was collected" and focuses instead on authenticity and integrity rather than the lawfulness of its acquisition. The absence of an exclusionary 'fruit of the poisonous tree' doctrine for illegally obtained evidence, and "leaving them admissible if they are otherwise relevant and do not infringe a specific constitutional safeguard" (Pooran Mal v. Directorate of Prosecution, 1973), becomes a point of concern while dealing with digital evidence because of the quantity and quality of data they store. Thus, at present the courts are concerned more with the truthfulness and evidentiary value of the material than with the method of its acquisition.

Such conduct risks violating two fundamental rights central to the Indian Constitution, the right to privacy and the protection against self-incrimination, both innate to human personality and therefore inalienable.

3.1. Protection Against Self-Incrimination

Article 20(3) prohibits the state from compelling an accused to give evidence against himself, shielding individuals from forced confessions and coercive investigation. Placing the burden of proof on the prosecution pushes investigators toward digital devices as alternative sources of evidence, which can be unlocked by passwords or biometric means such as fingerprints, retinal scans, or facial recognition (Bhatia, 2022). Barring voluntary disclosure, access is obtained through compulsion, which raises the question of whether the state may compel an individual to unlock a device without falling foul of this constitutional guarantee.

In 2022, the Kerala High Court in *P. Gopalakrishnan alias Dileep v State of Kerala* (hereinafter P. Gopalakrishnan) upheld a bail condition requiring the accused to grant complete access to his mobile phone, relying on the earlier ruling in *Virendra Khanna v State of Karnataka (2021)* (hereinafter Virendra Khanna), which had permitted compelling an accused to unlock his phone during investigation. In contrast, a Special CBI Court in Delhi, in *CBI v Mahesh Kumar Sharma (2022)*, declined to pass a similar order and held both prior rulings to be per incuriam. Notably, all three decisions relied on the same precedents, *State of Bombay v Kathi Kalu Oghad* (hereinafter Kathi Kalu Oghad) and *Selvi v State of Karnataka* (hereinafter Selvi), yet arrived at opposite conclusions.

Self-incrimination is violated only when three conditions coincide: the person is accused of an offence, required to give evidence against himself, and compelled to produce it. *Virendra Khanna* and *P. Gopalakrishnan* treated device unlocking as physical rather than testimonial evidence, misreading *Kathi Kalu Oghad*, which held that any positive, volitional act producing evidence amounts to testimony, and failing to appreciate that Article 20(3) protects against the act of compulsive extraction of evidence, as distinct from mere passive submission (Sekhri, 2019, p. 180). Physical evidence, such as blood or hair, is used only for comparison and is not inherently incriminating. In contrast, testimonial evidence is incriminating in itself because it conveys the direct product of the accused's own mind. Supplying a password is not, by itself, incriminating, but it becomes so once it establishes that the accused owned the device and controlled its incriminating contents.

The courts further reasoned that granting access does not amount to bearing witness, since the officer must still prove the contents under the law of evidence (Virendra Khanna v. State of Karnataka, 2021). This reasoning also does not withstand scrutiny, since Article 20(3) concerns the investigative process itself rather than how evidence is later proved in court. Taken to its logical end, it would place even direct oral confessions outside constitutional protection, since these, too, must be proved under the Evidence Act, 1872 (Bhatia, 2022) (now the Bharatiya Sakshya Adhiniyam, 2023).

3.2. Right to Privacy

Privacy is most usefully understood as the right to be left alone (Brandeis & Warren, 1890), or the right to control who knows what about one's communications and activities (Callaghan & Shiner, 2026, p.93), and is recognised internationally under Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR). In India, a nine-judge bench in *Justice K.S. Puttaswamy v Union of India (2017)* (hereinafter Puttaswamy) recognised privacy as a fundamental right within Article 21, extending personal liberty beyond physical restraint to freedom from informational encroachment. The tension between privacy and search first surfaced in *M.P. Sharma v Satish Chandra (1954)*, and later in *Kharak Singh v State of U.P (1964)*, where Justice Subba Rao's dissent first located privacy outside the Constitution's express text. Subsequent decisions, including *Gobind v State of Madhya Pradesh (1975)*, *R. Rajagopal v State of Tamil Nadu (1994)*, *PUCL v Union of India (1997)*, *Mr X v Hospital Z (1998)*, and *Ram Jethmalani v Union of India (2011)*, progressively broadened privacy to cover autonomy, dignity, informational control, and confidentiality.

Digital investigation magnifies this concern, since access to a device for even a narrow purpose often opens a person's entire digital life, including images, messages, browsing history, and passwords unconnected to the investigation. This intrusion extends beyond the device owner to everyone digitally connected to it, none of whom have consented to disclosure (Shah et al., 2024, p. 298). The increased use of digital policing, therefore, demands proportionality: any power of interception must be confined to defined circumstances, such as a public emergency or public safety, and weighed against privacy as an irreducible guarantee (Ramachandran, 2014, p. 5). Privacy operates as a double-edged sword, restraining state intrusion while obliging the state to safeguard it actively, and yields to reasonable restrictions such as national security or crime prevention only where legality, a legitimate aim, and proportionality are satisfied together (Puttaswamy, 2017, para T5). These principles remain underdefined in practice, making guidelines comparable to those in *PUCL* for telephonic surveillance necessary for digital evidence as well.

Virendra Khanna and *P. Gopalakrishnan* dismissed privacy objections as falling within *Puttaswamy's* exceptions. However, the Supreme Court took a different view in an interim order in *S. Martin v Directorate of Enforcement (2024)*, restraining the Enforcement Directorate from accessing or copying personal data from seized devices. The high courts erred in equating digital seizure with the seizure of physical documents, overlooking that physical seizure is confined to specified documents. In contrast, a digital seizure exposes the contents of an entire device. Concerns over the arbitrary seizure of devices, especially those belonging to media professionals, have since reached the Supreme Court, which has asked the centre to formulate guidelines on the search and seizure of electronic evidence (Foundation for Media Professionals v Union of India, 2022).

3.3. Digital Personal Data Protection Act, 2023

The specific legislation made for the protection of personal data is the Digital Personal Data Protection Act, 2023 (DPDP). It determines the rights and duties of a fiduciary, such as a telecom company, cloud service provider, or device manufacturer, in relation to the data principal whose data they hold. Generally, the legislation requires providing notice under section 5, obtaining consent under section 6, and implementing reasonable safeguards and retention limits under section 8. However, when the state demands such information under section 17, then most of the requirements are diluted. This freedom leaves fiduciaries with no way to deny such a demand or determine the relevance of the request and removes the fiduciary's ability to raise any restrictions based on sections 5, 6, or 8. Moreover, it is up to the

requesting authority to determine the volume and nature of the information requested, with the fiduciary being entirely dependent on that authority. Rules should therefore allow fiduciaries to seek clarification of, or challenge, facially disproportionate demands, and to publish aggregate transparency reports.

Section 17(1)(c) and 17(2)(a) stand out among other sections, as 17(1)(c) explicitly excludes processing "in the interest of prevention, detection, investigation or prosecution of any offence" from the scope of application of the DPDP, while section 17(2)(a) exempt a "instrumentality of the State" as the Central Government may notify from the entire Act through a notification issued in the official Gazette on the grounds of "public order." The scope of application of these two sections is even broader than it appears at first glance, since the definition of personal data in section 2(t) explicitly includes information collected offline and subsequently digitised. According to section 3, it also covers processing performed for purposes not explicitly related to personal data protection, such as investigation and prosecution. Therefore, special provision in DPDP does not require investigating authorities to follow any restrictions when collecting evidence from a fiduciary, which is protected by the UK's Data Protection Act 2018 (DPA). Interestingly, part III of DPA confines its law-enforcement exemption to a "competent authority" defined under schedule VII, acting for a defined criminal-justice purpose, retaining at least a nominal proportionality check. While, section 17 of DPDP, imposes no equivalent limitation on which agency may invoke the exemption or how far its request may reach. Moreover, the DPA also mandates that a regulatory body must adopt appropriate administrative and technical measures to ensure that processing is limited to the specific purpose and that any personal data processed is deleted as soon as possible after the purpose is achieved, which remains absent in DPDP. This is done despite the fact that no prior authorisation is required for such processing, except for the requirement to notify the regulatory authority.

Compared with DPA, the DPDP fails to provide the same degree of protection and to satisfy four criteria. First, there is no identification of the competent authorities with the right to use this exemption. Second, the absence of an explicit provision for processing in order to achieve law enforcement objectives. Third, it nowhere mandates the creation of a paper trail regarding the use of this exemption by competent authorities, which can subsequently be subjected to scrutiny by a regulatory authority. Fourth, no compulsion to delete the personal data obtained by investigating agencies, which is there for the fiduciaries when their purpose of collection has expired (DPDP Rules, 2025; Rule 8). The absence of these protections leaves agencies completely free to obtain, use, and retain the data without any scrutiny. These gaps can be addressed through rulemaking, without amending section 17, by reading the exemption through the proportionality test in *Puttaswamy* (2017), which requires legality, a legitimate aim, necessity and procedural safeguards. The protection demands multiple checks, beginning with, *ex ante* review before the access of content or sensitive data which should require prior written authorisation from a magistrate or an independent reviewing officer, recording necessity and scope, with emergency access ratified within a fixed period. Moreover, *ex post* review becomes necessary, where the data principals should be notified once disclosure no longer jeopardises the investigation, and affected persons and fiduciaries should be able to challenge it before the High Court under Article 226 of the Indian Constitution. The audit trails should be kept, wherein every demand should be logged with the requesting authority, statutory basis, data categories and date, and these logs should be open to audit by the oversight authority proposed in this paper. And lastly, data should be deleted or anonymised on closure of the investigation, acquittal or discharge, with certification of deletion. Therefore, data principals remain vulnerable, even with constitutional protections and specific legislation protecting digital data.

3.4. Other Statutory Routes to Digital Materials

Other than BNSS, there exists two regimes that operate alongside, having weaker safeguards for the individuals. First, the Information Technology Act, 2000 (IT Act). Section 69(1) lets the Central or State Government direct any agency to intercept, monitor or decrypt information in a computer resource, including "for the investigation of any offence". This ground is wider than the "public emergency or public safety" threshold on which the Telegraph Act regime reviewed in *PUCL* (1997) rested. Under section 69(3), subscribers, intermediaries and persons in charge of the computer resource must extend technical assistance, and section 69(4) punishes default with imprisonment for upto 7 years. Orders are issued by the Union or State Home Secretary under the Interception Rules, 2009 and are reviewed only by a committee of senior executive officials. Section 69B is governed by separate Traffic Data Rules, 2009. The telecom regime has meanwhile moved from the Indian Telegraph Act, 1885 to the Telecommunications Act, 2023, whose section 20 authorises interception. The Interception Rules, 2024 supersede Rules 419 and 419A of the Telegraph Rules which keep the earlier model, making the orders lasting for 60 days and extendable upto 180 days. The records are destroyed every six months, and review is by executive committees alone, with no judicial or parliamentary oversight. The effective system causes issues, first, section 69(3) allows decryption to be compelled by executive order, without the separate judicial order that the framework in Part 5 requires under Article 20(3), and potentially against the suspect himself. Second, intercepted material reaches criminal trials without any BNSS safeguard. *Shreya Singhal* (2015) upheld the blocking power in section 69A partly because of reasoned orders and a writ remedy; the same reasoning supports requiring judicial authorisation for decryption and content interception. Other than this, more power is provided through Prevention of Money Laundering Act, 2002 allows the Enforcement Directorate to search and seize under sections 17 and 18 on recorded "reasons to believe", the validity of which was upheld in the case of *Vijay Madanlal Choudhary v. Union of India* (2022).

Since these routes (including section 20 of the Telecommunications Act, 2023) sit outside the BNSS, safeguards confined to it can be bypassed. The framework proposed in this paper should therefore bind every agency seeking digital material, and the oversight authority's audits should cover these powers as well.

3.5. Third Party Doctrine

The third-party doctrine, originating in *Smith v. Maryland* (1979) in the United States, holds that a person who voluntarily shares information with a third party accepts the risk of its disclosure, since no expectation of privacy attaches to information already surrendered (Agarwal & Kabra, 2024, p. 345). It argues that accessing user data held by providers such as WhatsApp or Facebook does not violate privacy, as they hold only the data shared by the user. In India, the doctrine surfaced in *District Registrar and Collector, Hyderabad v Canara Bank (2005)* (hereinafter Canara Bank), where the Supreme Court held that privacy attaches to persons rather than places, thereby extending the protections available in a home to intangible spaces such as the internet and mobile phones. The protection was expanded in *Puttaswamy*; the consequences of breach are taken up in Part 3.6.

Moreover, the Indian courts remain divided on the protection of these rights: while Virendra Khanna and P. Gopalakrishnan treat device unlocking as an indispensable investigative tool, *Selvi, Puttaswamy*, and *Canara Bank* firmly protect against self-incrimination and uphold privacy against state encroachment. This divergence, together with the limited application of the third-party doctrine to digital contexts and the absence of statutory safeguards comparable to PUCL, points to the need for comprehensive legislation. Such a law cannot make privacy absolute, since investigation will always require some intrusion. However, it can make the

terms of that intrusion explicit through a statute built on *Puttaswamy's* threefold test, supported by judicial pre-authorisation, data minimisation, time bound warrants, and exclusionary rules for violations, so that fundamental rights remain genuine constraints rather than formalities in a data driven era (Chandrachud, 2025).

3.6. Admissibility of Unlawfully Obtained Digital Evidence

The statutory routes above matter because Indian law attaches few consequences to breaching them. In *Pooran Mal v. Director of Inspection (Investigation)* (1974), a Constitution Bench held that evidence obtained through an illegal search is not shut out for that reason alone: relevance is the test, unless the Constitution or another law expressly or by necessary implication prohibits its use. The Court declined to import the Fourth Amendment exclusionary rule, relying partly on *M.P. Sharma* (1954), which had denied a constitutional right to privacy. The rule was applied earlier in *R.M. Malkani* (1973) and has been repeatedly reaffirmed. Its exception has force only where a statute supplies the prohibition: in *State of Punjab v. Baldev Singh* (1999), a Constitution Bench treated the safeguard in section 50 of the NDPS Act as such a prohibition. Without one, tainted material continues to be admitted. In *Dr Naresh Kumar Garg v. State of Haryana* (2026), the Court accepted that the search was illegal yet held that the material gathered could still be relied upon, subject to relevancy and admissibility.

Puttaswamy unsettles this functioning by overruling *M.P. Sharma* on privacy, it makes an unlawful search not merely irregular but an infringement of Article 21, which must satisfy legality, legitimate aim and proportionality. No bench has yet held that this alters *Pooran Mal*, and a two-judge bench cannot do so, but the question is ripe for a reference. For digital evidence the stakes are higher. Section 63 of the BSA tests integrity and authenticity, not lawfulness of acquisition, so a forensically authenticated image of an entire device may be admitted though obtained without valid authority.

The reform proposed here need not wait for that reference. *Pooran Mal*'s own exception, an express or necessarily implied prohibition in law, allows Parliament to legislate exclusion. Drawing on the United States (*Mapp v. Ohio*; the good-faith exception in *United States v. Leon*), the United Kingdom (section 78 of PACE) and Canada (*R v. Grant*), the statute should adopt a tiered rule: (i) mandatory exclusion for core breaches, namely a search without judicial authorisation, a search beyond the warrant's scope, and decryption compelled without the separate order; (ii) discretionary exclusion for technical breaches, weighing seriousness, prejudice and bad faith; (iii) exclusion of derivative evidence unless an independent source or inevitable discovery is shown; and (iv) written reasons whenever tainted evidence is admitted. Exclusion may cost convictions, and victims bear that cost (Roach, 1999). Compensation and departmental action should therefore supplement the rule, not replace it.

4. Comparative Legislative Models: Statutory Approaches to Digital Search and Seizure

4.1. The United States of America

The Constitution of the United States contains no explicit provision protecting the right to privacy or against self-incrimination; both are instead derived from the Fourth and Fifth Amendments, respectively.

The Fourth Amendment protects the right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, requiring a sworn application before a neutral magistrate, supported by specific facts establishing probable cause (Losavio & Keeling, 2014, p. 198). Its application to digital searches is comparatively recent. In *Riley v California (2014)*, the Supreme Court unanimously held that police must obtain a warrant

before searching a smartphone seized during an arrest, recognising that the sheer quantity and sensitivity of information at stake heightened the chances of violation of privacy (Ferguson, 2022, p. 833). In *Jones v United States (2012)*, prolonged warrantless GPS tracking was held to be violative of the reasonable expectation of privacy, and in the pivotal case of *Carpenter v United States (2018)*, the Court held by a 5-4 majority that acquiring 127 days of cell site location data without a warrant violated the Fourth Amendment, with Chief Justice Roberts describing such data as profoundly illuminating. Together, these decisions establish that digital searches are qualitatively distinct from physical ones, that older precedents cannot resolve novel surveillance questions, and that the doctrine must continue to evolve alongside technology (Ferguson, 2022, p. 836).

The Fifth Amendment protects individuals from being compelled to testify against themselves when the state seeks to compel the unlocking of a device. The judicial decisions remain divided on the unlocking of digital devices: the Ninth Circuit in *United States v Payne (2024)* held that biometric unlocking is a non-testimonial physical act requiring no cognitive exertion, while the D.C. Circuit in *United States v Brown (2025)* reached the opposite conclusion, holding that it communicates the suspect's knowledge that a particular finger or code grants access to incriminating material. In the absence of Supreme Court guidance, most circuit courts have nonetheless treated compelled disclosure as testimonial, as in *In re Grand Jury Subpoena (2021)* and *United States v Blake (2017), which* held that compelling the disclosure of a password contravenes the Fifth Amendment. Moreover, a Florida court in *G.A.Q.L. (2018) held that disclosing a passcode forces a suspect to reveal the contents of his mind, thereby making it* testimonial. Even so, the foregone conclusion doctrine, established in *Fisher v United States (1976)* and later extended to digital searches, permits compelled unlocking. It permits the authorities, where the government already knows the specific evidence sought, provided the password is shown to exist, to be possessed by the suspect, and to be genuine, offering a measured mechanism for balancing the rights of the accused against investigative needs (Agarwal & Kabra, 2024, p. 341).

4.2. United Kingdom

The United Kingdom (UK) has no written constitution but protects these rights through the European Convention on Human Rights (ECHR) through the domestic Human Rights Act 1998 (HRA) (University of Oxford, 2025). Article 6 of HRA protects against self-incrimination through the right to silence, while Article 8 of HRA protects privacy (Luk, 2001, p. 223). Unlike the American approach, UK law imposes a statutory duty to disclose access codes and device data, overriding both in defined circumstances. The Police and Criminal Evidence Act, 1984, authorises investigators to examine data on a device, treating existing material as pre-existing evidence rather than compelled testimony, while section 49 of the Regulation of Investigatory Powers Act, 2000, empowers authorities to compel decryption, with non-compliance punishable under section 53 by up to two years' imprisonment, rising to five for offences involving national security or child indecency. Section 41 of the Police, Crime, Sentencing and Courts Act 2022 further governs data from devices voluntarily submitted.

In *R v S and A (2008)*, the Court of Appeal held that a suspect cannot invoke the right to silence to withhold encryption keys, treating such material as independent evidence akin to a document. It upheld the proportionality of this approach under Article 6. In the case of *Tajan Spaulding* (Cartledge, 2016), a suspect who refused to disclose his phone password was sentenced to eight months' imprisonment. The English conception of privacy traces back to Semayne's Case of 1604, where Sir Edward Coke declared a person's home to be his castle, and today privacy is protected under Article 8 of the HRA, permitting interference only where it is legal, necessary, proportionate, and reasonably foreseeable. Search and seizure orders

remain subject to judicial review on grounds of legality, rationality, procedural propriety, and proportionality (Andreja, 2025, p. 8), while the General Data Protection Regulation imposes further oversight on authorities handling data for criminal investigation.

4.3. Germany

Germany, bound by the ECHR, is required under Article 25 of the Grundgesetz (Constitution of Germany) to interpret domestic law consistently with international law. Search and seizure of digital evidence is governed principally by the Code of Criminal Procedure. At the same time, the Grundgesetz provides the constitutional foundation from which courts have derived rights such as informational self-determination and the confidentiality of IT systems. Article 1(1) guarantees the inviolability of human dignity, underpinning protection against self-incrimination, while Article 2(1) protects the free development of personality, including freedom from compelled testimony. Article 10 protects the confidentiality of correspondence and telecommunications, subject only to law and strictly necessary for serious offences (OHCHR, 2013). The Federal Constitutional Court has read these articles together to prohibit disproportionate remote searches in the absence of protective principles. The principle of nemo tenetur protects testimonial disclosures, such as passwords, while permitting the compelled production of physical evidence, such as fingerprints.

The question of whether compelling a suspect to unlock a phone violates this protection was addressed in Jalloh v Germany (2006), which set out a three-factor test examining the nature and degree of coercion, procedural safeguards, and the use of the resulting evidence. In 2025, the Federal Court of Justice, in *case 2 StR 232/24* (Toor & Pesselse, 2025, p. 285), held that agencies may compel a suspect to use a fingerprint to unlock a phone provided prior judicial authorisation exists and proportionality is established through clear evidence that the suspect deliberately used the device to commit the offence under investigation.

Some of these safeguards can be brought into India's system without difficulty. Magistrates already issue warrants under the BNSS, so requiring prior judicial authorisation for digital searches builds on something that exists. Audit trails and deletion rules can be introduced through rules and procedure, and an independent oversight body could follow the UK's Investigatory Powers Commissioner. Though, there exists limits, as the UK and Germany work follows ECHR, and courts enforces these rights proactively, which remains absent in India. Moreover, India also handles a far larger volume of cases with weaker forensic capacity, so any rollout has to be gradual. Further, in India policing is a State subject, therefore none of this works without State cooperation. Hence, these models can be adapted after making changes as per the India's conditions, and cannot be copied.

5. Legislating Digital Search and Seizure: A Statutory Framework for India

A legislative reform is accurate solution for these gaps, rather than continued reliance on judicial improvisation, as courts can only resolve the conflicts, and can't specify the scope of lawful device search in all aspects, moreover the absence of guidelines not only weakens the investigating agencies' own cases but also increases the risk that suspects' fundamental rights are violated (Katkuri, 2024, p. 23). Additionally, India has historically preferred the 'Crime Control Model' over the 'Due Process Model' in practice (Sarmah, 2016, p. 28), and without codified guidelines, this preference persists by default rather than by considered legislative choice. The proposals below set out the elements such a statute should contain.

Moreover, the changes to domestic law can also be aligned with international guidance, such as the digital investigation guidelines of the UNODC (United Nations Office on Drugs and Crime), which cover the identification, collection, acquisition, and preservation of digital

evidence, and the Budapest Convention (Convention on Cybercrime, 2001). This not only harmonises national laws but also facilitates cross-border cooperation against cybercrime.

5.1. Proposed Statutory Elements & Operational Changes

A framework for digital search and seizure must be organised around three analytically distinct stages: prior to the search, during its execution, and following its conclusion. Each stage implicates different risks to the individual, and the safeguards attaching to each must be calibrated accordingly.

5.1.1. Prior to the Search

Judicial authorisation is the threshold requirement before any search and seizure, demanding probable cause rather than generalised suspicion. It is at this stage that the legality-necessity-proportionality standard articulated in *Puttaswamy* acquires operative content, rather than functioning merely as doctrinal ornamentation. A warrant must be approved by the magistrate and specify the scope of the search, the file types, date ranges, and folders to be examined. A warrant devoid of such particulars is, in substance, an authorisation for unrestricted access to the entirety of an individual's digital life. It should also be time-bound, with thirty days as a defensible outer limit, so that investigative authority does not persist indefinitely, while extensions require re-approval by the court.

5.1.2. During the Search

Privacy is mostly violated during the procedure; most attention is required at this stage. The vulnerability requires that forensic extraction proceed via encoding, de-coding or hash verification (Law et al., 2011), and that a documented chain of custody be maintained throughout to preserve its integrity. Forensic acquisition should be limited to logical extraction, including copying only file types, date ranges or keywords specified in the warrant. It should use bit stream imaging of the storage media (copying deleted and unallocated data) when technologically feasible. Hash techniques (MD5/SHA-256) should be used on the target device, and the image must be calculated and compared, with a discrepancy indicating tampering. Decryption of the devices would require a separate judicial order, distinct from the search warrant, due to its direct relevance to Article 20(3) of the Indian Constitution (Protection against self-incrimination). This requirement should also bind decryption directions under section 69(3) of the IT Act, which currently issue on executive order alone. In other cases, when evidence is stored on cloud servers, the warrants must specify the targeted accounts or servers, since the physical seizure of a device is different from granting access to data held by third-party vendors. Moreover, to receive assistance from other jurisdictions globally, a bilateral agreement must be entered into to facilitate information exchange between law enforcement agencies. The bulk copying of an entire device's contents by investigating agencies should be prohibited (Majdoub & Atmani, 2025, p.153). Where investigators encounter material falling outside the warrant's scope, the supplementary judicial authorisation must be obtained before proceeding further. Importantly, the formative period of this procedure and the vulnerability of the stored data should not permit the collection of data that would otherwise be permissible under the plain view doctrine. This doctrine allows an investigating officer to collect evidence even without a warrant when he is legally present, has legal access to the evidence, and has probable cause to believe that the evidence is part of a crime (Harris v. United States, 1968). Moreover, the devices containing privileged material require an unbiased examination; they must be reviewed under the supervision of an independent party. This safeguard proceeds not from any presumption of bad faith on the part of investigators, but from the recognition that privilege, once breached, cannot meaningfully be restored.

5.1.3. Following the search

Material falling outside the scope of the warrant should be purged within a fixed period, ninety days being a workable benchmark, extendable only upon further judicial order supported by continuing cause. The individual concerned should be notified that a search occurred within a reasonable time, and afforded a genuine opportunity to contest its scope and manner before a court, as a matter of right rather than as an incident of subsequent criminal proceedings. Non-compliance should attract the tiered exclusionary rule set out in Part 3.6. A good-faith exception should be confined to reasonable reliance on a facially valid warrant later found defective. The rule should be enacted in the BSA or BNSS so that it operates as the "express prohibition in law" that *Pooran Mal* recognises.

5.2. Infrastructure and Training

The statute should also establish an independent oversight authority to oversee the activities of forensic digital investigators (Campbell, 2025, p. 70), including the functioning and auditing of forensic labs, the training of personnel in data handling and forensic tools, and reporting to Parliament. Officers should be trained specifically on privacy safeguards and advanced forensic techniques (Goswami & Goswami, 2023, p. 22); (Goswami & Goswami, 2024, p. 80), as Dworkin observed, a government that does not take rights seriously does not take law seriously either (Goswami & Goswami, 2019, p. 462). AI tools already used in the Indian judiciary, such as SUVAS (Supreme Court Vidhik Anuvaad Software) and SUPACE (Supreme Court Portal for Assistance in Court's Efficiency), could similarly assist in searching and extracting data while preserving privacy safeguards (Solanki & Pareek, 2026, pp. 7-8), but only within the statutory limits proposed above, not as a substitute for them.

5.3. Feasibility and Compliance Metrics

The reforms proposed are not self-executing and require hand-holding. It takes years and funding to train and supervise. It can be achieved through dedicated work, initial one year to constitute the authority, draft model protocols and train a core cadre of trainers; then, the training of investigating officers, prosecutors and magistrates will demand another two to three years; and about five years for national coverage and a first full audit cycle. Costs fall mainly under staffing, forensic imaging and secure storage, and recurring training, and should be settled in a fiscal note before enactment. Policing is a state subject, while BNSS is a central law; therefore, there must be cooperation between the state and the centre. This can be secured through model rules issued by the Centre, central funds released against State compliance milestones, and a standing Centre-State coordination forum. The oversight authority need not be created from scratch, but must be structurally independent of the police and prosecuting agencies to remove bias, and report directly to Parliament, along the lines of existing independent regulators. Independence requires a selection committee that includes a judicial member and the Leader of the Opposition, fixed tenure with removal only for proved misbehaviour, and a budget protected from executive reduction. Its powers should include auditing search and retention records, compelling documents, accrediting forensic procedures, and inquiring into complaints. It should not direct individual investigations or displace judicial review, and its orders should be appealable to the High Court. The diluted implementation of Police Complaints Authorities after *Prakash Singh* (2006) shows that independence must be statutory, not discretionary. For training purposes, the technical staff from CERT-In (Indian Computer Emergency Response Team) and forensic labs on deputation, and turn to the Bureau of Police Research and Development and judicial academies, without any loss of independence, since they are resources, not administrative powers. The operation of the system must be measured regularly and must show what percentage of searches have a proper record of scope compliance, the average retention period of forensic images against the 90-day benchmark,

judicial reviews initiated and their outcomes, and complaints by people who were never charged. The authority, not the police, should verify these figures through random sampling, and publish them quarterly in machine-readable form, with consequences such as enhanced audit for persistent non-compliance. This would make the activities auditable and, hence, their credibility measurable, rather than merely subject to assertion. Moreover, these accreditation and inspection results should not be restricted to the prosecution and should be available to the defence in accordance with the fair trial principles.

6. Conclusion: Legitimacy as the Future of Digital Policing

The integration of technology into policing has transformed investigative processes, blurring the line between prevention and prosecution while raising significant concerns about individual rights. In India, the increasing reliance by law enforcement on digital evidence has highlighted the tension between effective crime control and the protection of constitutional guarantees, particularly the rights to privacy and protection against self-incrimination (Bhandari & Lahiri, 2020). Courts have grown more willing to admit digital evidence, but the current gaps in legislative and procedural frameworks leave both law enforcement and citizens vulnerable as agencies lack clear guidance, and individuals risk arbitrary intrusion. Judicial activism has partially filled this void (Chandrachud, 2025; Goswami, 2015-2023), but court-made safeguards alone are insufficient as a substitute for comprehensive legal reform. This calls for a legitimate and effective digital policing framework grounded in the principles of legality, necessity, proportionality, and judicial oversight.

A legitimate and effective digital policing system requires the formulation of explicit statutory standards for the search and seizure of digital devices, along with court pre-authorisation and data-minimisation measures to safeguard individual rights. The establishment of time-bound warrants and exclusionary provisions for rights violations is crucial for ensuring accountability. It also demands a continuous evaluation of investigatory authorities to adapt to advancing technologies and prevent potential abuses. Ultimately, the protection of fundamental rights should not be perceived as an impediment to successful policing, but rather as the cornerstone of public trust and the legitimacy of law enforcement in a democratic society. Achieving an appropriate balance between governmental authority and personal liberties is crucial for a robust and equitable criminal justice system in India in the digital era.

Acknowledgment

This paper is an output of the doctoral work of the first author, under the supervision of the second author.

References

Agarwal, V. and Kabra, T. (2024). *Self-incrimination and digital evidence: Proposing a framework post-Virendra Khanna*. NUJS Law Review, vol. 17, p. 325.

Bhandari, V. and Lahiri, K. (2020). *The surveillance state, privacy and criminal investigation in India: Possible futures in a post-Puttaswamy world*. University of Oxford Human Rights Hub Journal, vol. 15.

Bharatiya Nagarik Suraksha Sanhita, 2023 (India), §§ 94, 96.

Bharatiya Sakshya Adhiniyam, 2023 (India).

Bhatia, G. (February 7, 2022). *The Kerala High Court rules on mobile phone data and the right against self-incrimination: A critique. Indian Constitutional Law and Philosophy*. [Online]. Available: https://indconlawphil.wordpress.com/2022/02/07/the-kerala-high-court-rules-on-mobile-phone-data-and-the-right-against-self-incrimination-a-critique/

Bradford, B., & Jackson, J. (2024). Legitimacy, relational norms and reciprocity. In *Research handbook on law and psychology* (pp. 343–360). Edward Elgar Publishing. https://doi.org/10.4337/9781800881921.00034

Campbell, E. (2025). *Techno-digital policing and speculative fictions: Towards a criminology of the future.* Crime, Media, Culture, vol. 21(1), pp. 69–95. https://doi.org/10.1177/17416590241253543

Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

Cartledge, J. (April 05, 2016). *Gun crook jailed for refusing to give up phone passcode. Daily Mirror.* [Online]. Available: https://www.mirror.co.uk/news/uk-news/gun-crook-jailed-refusing-give-7690901

CBI v. Mahesh Kumar Sharma, 2022 SCC OnLine Dis Crt (Del) 48.

Chandrachud, D. Y. (2025). *Why the constitution matters: Selected speeches of Justice DY Chandrachud on fundamental rights, landmark judgments and the constitution's role in safeguarding democracy.* Penguin Random House India.

Constitution of India, 1950, arts. 20(3), 21.

Convention on Cybercrime, 2001 (Budapest Convention).

Council of Europe. (1950). Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended). Council of Europe Treaty Series - No. 5. [Online]. Available: https://www.echr.coe.int/documents/d/echr/convention_ENG

Digital Personal Data Protection Act, No. 22 of 2023 (India).

District Registrar and Collector, Hyderabad v. Canara Bank, (2005) 1 SCC 496.

Dr. Naresh Kumar Garg v. State of Haryana & Ors., 2026 INSC 176.

Dubber, M. D. (2013). Preventive justice: The quest for principle. In A. Ashworth, L. Zedner, & P. Tomlin (Eds.), *Prevention and the limits of the criminal law* (pp. 61–92). Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199656769.003.0004

Ferguson, A. G. (2022). *Why digital policing is different*. Ohio State Law Journal, vol. 83(4), p. 817.

Fisher v. United States, 425 US 391 (1976).

Foundation for Media Professionals v. Union of India, Writ Petition (Criminal) No. 395 of 2022.

G.A.Q.L. v. State, 257 So. 3d 1058 (Fla. 4th DCA 2018).

Gobind v. State of Madhya Pradesh, (1975) 2 SCC 148.

Goswami, G. K. (2015–2023). *Forensic law*. Annual Survey of Indian Law (Indian Law Institute).

Goswami, G. K. and Goswami, A. (2019). *Obligated voice sampling: A judicial endorsement in Ritesh Sinha v State of Uttar Pradesh*. Journal of the Indian Law Institute, vol. 61(4), pp. 455–462.

Goswami, G. K. and Goswami, A. (2023). *Spreading wings of forensic science*. Supreme Court Cases (Journal), vol. 9, p. J-18.

Goswami, G. K. and Goswami, A. (2024). *Inclusive innovations in forensic epistemology and pedagogy: A proposed framework*. Asian Journal of Legal Education, vol. 11(1), pp. 74–82. https://doi.org/10.1177/23220058231206946

Harris v. United States, 390 U.S. 234

Human Rights Act, 1998 (UK).

In re Grand Jury Subpoena, 23 F.4th 1088, 1094 (9th Cir. 2021).

India. (1950). The Constitution of India. [Online]. Available: https://www.indiacode.nic.in/handle/123456789/19151?view_type=search&sam_handle=123456789/1362

Indian Stamp Act, 1899, Act No. 2 of 1899.

Indian Telegraph Act, 1885, Act No. 13 of 1885, § 5(2).

Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (India).

Information Technology Act, 2000, ss. 69, 69B (India).

Jackson, J., & Bradford, B. (2011). *Legitimacy and the social field of policing*. British Journal of Sociology, 62(3), 498–520. https://doi.org/10.2139/ssrn.1914458

Jalloh v. Germany, (2006) 44 EHRR 667.

John, R. M. (2025). The Supreme Court, criminal laws and procedure. In S. Muralidhar (Ed.), *InComplete justice?* (p. 189). Juggernaut.

Jones v. United States, 132 S. Ct. 945, 947–52 (2012).

Justice K. S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

Katkuri, S. (2024). *Legal challenges and lacunas in the digital forensics jurisprudence in India.* International Journal of Law, vol. 10(3), pp. 23–29.

Kharak Singh v. State of UP, (1964) 1 SCR 332.

KJF v. Surrey Police, [2022] UKIP Trib 7.

Law, F. Y. et al. (2011). *Protecting digital data privacy in computer forensic examination*. Sixth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering. IEEE, pp. 1–6. https://doi.org/10.1109/SADFE.2011.15

Losavio, M. and Keeling, D. (2014). *Evidentiary power and propriety of digital identifiers and the impact on privacy rights in the United States*. Journal of Digital Forensics, Security and Law, vol. 9(2), p. 16. https://doi.org/10.15394/jdfsl.2014.1181

Luk, J. W. (2001). *Identifying terrorists: Privacy rights in the United States and the United Kingdom.* Hastings International and Comparative Law Review, vol. 25, p. 223.

Lund-Tønnesen, J. and Fossheim, K. (2025). *Excessive digital surveillance and data privacy invasion as a creeping crisis.* Risk, Hazards and Crisis in Public Policy, vol. 16(1), p. e70005. https://doi.org/10.1002/rhc3.70005

Lyon, D. (2024). *Surveillance: A very short introduction*. Oxford University Press. https://doi.org/10.1093/actrade/9780198796848.001.0001

M.P. Sharma v. Satish Chandra, 1954 AIR 300.

Majdoub, I., & Atmani, K. (2025). Privacy paradigm shift: Zero knowledge proofs in criminal e-evidence collection. In *Cybercrime unveiled: Technologies for analysing legal complexity* (pp. 151-175). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-80557-8_7

Maneka Gandhi v. Union of India, (1978) 1 SCC 248.

Mapp v. Ohio, 367 U.S. 643 (1961)

Mr X v. Hospital Z, (1998) 8 SCC 296.

O'Callaghan, P., & Shiner, B. (2026). Privacy 6.0: Privacy as mental integrity. In *The law and ethics of freedom of thought, Volume 2: Cognitive liberty, mental privacy, and international law* (pp. 93–115). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-91466-9_4

O'Callaghan, P. (2012). Refining privacy in tort law. Springer Science and Business Media. https://doi.org/10.1007/978-3-642-31884-9

Office of the United Nations High Commissioner for Human Rights. (2013). *Report on the right to privacy in the digital age. United Nations.* https://ohchr.org

P. Gopalakrishnan v. State of Kerala, 2022 SCC OnLine Ker 3490.

Packer, H. (1968). The limits of the criminal sanction. Stanford University Press. https://doi.org/10.1515/9780804780797

People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301.

Police and Criminal Evidence Act 1984 (PACE) (UK).

Police and Criminal Evidence Act 1984, s. 78.

Pooran Mal v. Director of Inspection (Investigation), (1974) 1 SCC 345

Prevention of Money Laundering Act, 2002, ss. 17, 18 (India).

R Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.

R v. Grant, 2009 SCC 32

R v. S and A, [2008] EWCA Crim 2177.

R.M. Malkani v. State of Maharashtra, (1973) 1 SCC 471.

Ram Jethmalani v. Union of India, (2011) 8 SCC 1.

Ram Ramaswamy v. Union of India, Writ Petition (Criminal) No. 138 of 2021.

Ramachandran, C. (2014). *PUCL v Union of India revisited: Why India's surveillance law must be redesigned for the digital age*. NUJS Law Review, vol. 7, p. 105.

Regulation of Investigatory Powers Act 2000 (RIPA), §§ 49, 53 (UK).

Riley v. California, 134 S. Ct. 2473 (2014).

Ritesh Sinha v. State of U.P., (2019) SCC OnLine SC 956.

Roach, K. (1999). *Due process and victims' rights: The new law and politics of criminal justice.* University of Toronto Press. https://doi.org/10.3138/9781442674127

Roach, K. (1999). *Four models of the criminal process*. Journal of Criminal Law and Criminology, vol. 89(2), pp. 671–716. https://doi.org/10.2307/1144140

S. Martin v. Directorate of Enforcement, Writ Petition(s) (Criminal) No(s). 515/2024.

Sarmah, A. (2016). *Privacy and the right against self-incrimination: Theorising a criminal process in the context of personal gadgets*. CALJ, vol. 3, p. 28.

Sekhri, A. (2019). *The right against self-incrimination in India: The compelling case of Kathi Kalu Oghad.* Indian Law Review, vol. 3(2), pp. 180–211. https://doi.org/10.1080/24730580.2019.1646963

Selvi v. State of Karnataka, (2010) 8 SCC 96.

Semayne v Gresham, [1604] 5 Coke 91.

Shah, M. G., Gupta, A. and Bajpai, A. (2024). *Search and seizure of electronic devices in India: Time for a change?* International Journal of Evidence and Proof, vol. 28(4), pp. 298–311. https://doi.org/10.1177/13657127241230694

Shreya Singhal v. Union of India, (2015) 5 SCC 1.

Solanki, T. and Pareek, A. (2026). *AI and technology in the Indian judiciary: A step toward enhancing efficiency and equity.* Legal Reference Services Quarterly, vol. 45(1), pp. 91–92. https://doi.org/10.1080/0270319X.2026.2617784

Solove, D. J. (2021). The myth of the privacy paradox. *George Washington Law Review, 89*(1), 1–52. https://www.gwlr.org/the-myth-of-the-privacy-paradox/ https://doi.org/10.2139/ssrn.3536265

State of Bombay v. Kathi Kalu Oghad, AIR 1961 SC 1808.

State of Punjab v. Baldev Singh, (1999) 6 SCC 172.

Telecommunications Act, 2023 (Act 44 of 2023); Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024.

Tyler, T. R. (2025). *Legitimacy-based policing.* Criminology and Public Policy, vol. 24(2), pp. 165–187. https://doi.org/10.1111/1745-9133.12695

United States v. Blake, 868 F.3d 960 (11th Cir. 2017).

United States v. Brown, 2025 US App LEXIS 129.

United States v. Leon, 468 U.S. 897 (1984)

University of Oxford. (September 4, 2025). *Misrepresentations around human rights and immigration fuelling calls to quit ECHR.* [Online]. Available: https://www.ox.ac.uk/news/2025-09-04-misrepresentations-around-human-rights-and-immigration-fuelling-calls-quit-echr

UNODC. (n.d.). *Standards and best practices for digital forensics*. [Online]. Available: https://www.unodc.org/cld/en/education/tertiary/cybercrime/module-4/key-issues/standards-and-best-practices-for-digital-forensics.html

USA v. Payne, 2024 WL 1647253 (9th Cir. 2024).

Utset, M. A. (2016). *Digital surveillance and preventive policing*. Connecticut Law Review, vol. 49, p. 1453.

van Toor, D. A. G. and Pesselse, G. *2025 Unlocking the meaning of the privilege against self-incrimination for biometrically secured smartphones: A response to Zontek's 'Biometric encryption of smart devices and the prohibition against self-incrimination in criminal procedure. Old guarantees in the new world*.' European Journal of Crime, Criminal Law

and Criminal Justice, vol. 33(3), pp. 285–301. https://doi.org/10.1163/15718174-bja10064

Veas, J. E. (2025). *Smartphone decryption via forced fingerprinting and the right against self-incrimination: The German Federal Court (BGH) addresses the problem*. Computer Law and Security Review, vol. 59, p. 106215. https://doi.org/10.1016/j.clsr.2025.106215

Verma, R., Govindaraj, J. and Gupta, G. (2016*). Data privacy perceptions about digital forensic investigations in India.* IFIP International Conference on Digital Forensics. Springer International Publishing, pp. 25–45. https://doi.org/10.1007/978-3-319-46279-0_2

Vijay Madanlal Choudhary v. Union of India, (2022) 10 SCC 24. https://doi.org/10.18231/j.joapr.2022.10.4.19.24

Virendra Khanna v. State of Karnataka, 2021 SCC OnLine Kar 5032.

Warren, S. D. and Brandeis, L. D. (1890). *The right to privacy.* Harvard Law Review, vol. 4, p. 193. https://doi.org/10.2307/1321160