



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

DIGITAL EVIDENCE AND PRIVACY: A LEGAL DILEMMA

~ *Ujjayani Debnath*

I. INTRODUCTION

Modern life leaves a digital trail. Messages, location histories, cloud backups, browsing records and biometric logs together form a detailed portrait of a person, and investigators and litigants increasingly rely on this material to prove facts in court. Digital evidence has therefore become indispensable to adjudication. Yet the same data that proves a fact also exposes the intimate life of the person who generated it. This is the dilemma at the centre of this article: the State's legitimate interest in accurate fact-finding pulls against the individual's claim to informational privacy.

In India the tension has sharpened in recent years. The Supreme Court recognised privacy as a fundamental right in 2017.¹ Parliament replaced the Indian Evidence Act, 1872 with the Bharatiya Sakshya Adhiniyam, 2023 ("BSA"),² substituted the Code of Criminal Procedure with the Bharatiya Nagarik Suraksha Sanhita, 2023 ("BNSS"),³ and enacted the Digital Personal Data Protection Act, 2023 ("DPDP Act").⁴ These instruments were drafted with different priorities and do not speak to each other cleanly. This article examines how they interact, argues that the law of admissibility remains tilted towards reliability rather than rights, and suggests reforms that could reconcile the two interests.

II. THE EVIDENTIARY FRAMEWORK FOR ELECTRONIC RECORDS

Under the BSA, "evidence" expressly includes electronic and digital records, and "document" is defined to include electronic records.⁵ The legislature thus removed any doubt that a

¹*Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).

²Bharatiya Sakshya Adhiniyam, 2023, No. 47, Acts of Parliament, 2023 (India).

³Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46, Acts of Parliament, 2023 (India).

⁴Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

⁵Bharatiya Sakshya Adhiniyam, 2023, §§ 2(1)(c), 2(1)(e).

WhatsApp chat, an email or a CCTV recording can be tendered as proof. The real difficulty lies in authentication, because digital material can be altered and duplicated without visible trace.

Section 63 of the BSA, the successor to section 65B of the Indian Evidence Act, governs the admissibility of electronic records.⁶ It makes such records admissible as documents without production of the original, provided the statutory conditions are met and a certificate accompanies the record. Unlike its predecessor, the new certificate must follow the prescribed schedule, must be signed by both the person in charge of the device or system and an expert, and must state the hash value of the record.⁷ The hash requirement is a welcome integrity safeguard, since a change of even one bit alters the hash.

The jurisprudence leading to this point was unsettled. In *Anvar P.V. v. P.K. Basheer*, the Supreme Court held that secondary electronic evidence is inadmissible without a section 65B certificate.⁸ *Shafhi Mohammad v. State of Himachal Pradesh* relaxed the rule where a party could not procure the certificate,⁹ but *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* overruled *Shafhi* and restored *Anvar*, treating the certificate as mandatory while allowing courts to direct its production at a suitable stage.¹⁰ The BSA effectively codifies the *Khotkar* position and strengthens it. Notably, none of these rules asks how the record was obtained. They test authenticity, not the intrusiveness of the method of acquisition. That silence is where privacy concerns enter.

III. PRIVACY AS A FUNDAMENTAL RIGHT

In *Puttaswamy*, a nine-judge bench unanimously held that the right to privacy is protected under Article 21 as an intrinsic part of life and personal liberty, and the plurality recognised informational privacy as one of its facets.¹¹ The Court also indicated the standard for State interference: the restriction must be backed by law, pursue a legitimate aim, and be proportionate to the object sought.¹² The proportionality standard was later applied in the *Aadhaar* judgment¹³ and in *Anuradha Bhasin v. Union of India*, which required that restrictions on communications be temporary, limited in scope and subject to review.¹⁴

⁶*Id.* § 63; cf. Indian Evidence Act, 1872, No. 1, Acts of the Imperial Legislative Council, 1872, § 65B (India) (repealed).

⁷Bharatiya Sakshya Adhiniyam, 2023, § 63(4) & sched.

⁸*Anvar P.V. v. P.K. Basheer*, (2014) 10 S.C.C. 473 (India).

⁹*Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 5 S.C.C. 311 (India).

¹⁰*Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 S.C.C. 1 (India).

¹¹*Puttaswamy*, (2017) 10 S.C.C. 1 (plurality opinion).

¹²*Id.*

¹³*Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2019) 1 S.C.C. 1 (India).

¹⁴*Anuradha Bhasin v. Union of India*, (2020) 3 S.C.C. 637 (India).

Even before *Puttaswamy*, the Court had accepted that surveillance requires procedural safeguards. In *PUCCL v. Union of India*, it read privacy into telephone conversations and prescribed guidelines for interception under the Telegraph Act.¹⁵ Those safeguards survive in statutory form in section 69 of the Information Technology Act, 2000 and the 2009 Interception Rules, which permit interception, monitoring and decryption only on the orders of a competent authority, for specified grounds and subject to review.¹⁶ The critical point is that the executive controls both the order and the review. There is no prior judicial authorisation, which distinguishes the Indian model from those of many other constitutional democracies.

IV. WHERE THE TWO COLLIDE: SEARCH, SEIZURE AND COMPELLED DISCLOSURE

The clash is most visible when an investigating agency seizes a smartphone or laptop. A single device can hold a person's correspondence, finances, health records, photographs and location history. Ordinary search-and-seizure provisions were drafted for physical premises and do not account for this volume and sensitivity. The BNSS allows summons for documents and things, including electronic communication, and empowers search and seizure.¹⁷ It also requires audio-video recording of search and seizure¹⁸ and mandates forensic examination in serious offences.¹⁹ These are real improvements. However, the statute is silent on the permissible scope of a device search, on data minimisation (extracting only what is relevant), on the retention and destruction of cloned images, and on the protection of privileged material such as lawyer-client communications.

Compelled decryption raises a related problem. Article 20(3) protects an accused against being compelled to be a witness against himself. In *State of Bombay v. Kathi Kalu Oghad*, the Court distinguished testimonial compulsion from the giving of physical specimens such as fingerprints and handwriting.²⁰ In *Selvi v. State of Karnataka*, it held that involuntary narco-analysis, polygraph and brain-mapping tests violate Articles 20(3) and 21, reasoning in part from mental privacy.²¹ Whether a passcode is testimonial (knowledge held in the mind) or non-testimonial (like a fingerprint) remains unsettled at the Supreme Court level. By contrast, in

¹⁵*People's Union for Civil Liberties v. Union of India*, (1997) 1 S.C.C. 301 (India).

¹⁶Information Technology Act, 2000, No. 21, Acts of Parliament, 2000, § 69 (India); Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, G.S.R. 780(E) (India).

¹⁷Bharatiya Nagarik Suraksha Sanhita, 2023, §§ 94, 106, 185.

¹⁸*Id.* § 105.

¹⁹*Id.* § 176(3).

²⁰*State of Bombay v. Kathi Kalu Oghad*, A.I.R. 1961 S.C. 1808 (India).

²¹*Selvi v. State of Karnataka*, (2010) 7 S.C.C. 263 (India).

Ritesh Sinha v. State of Uttar Pradesh, the Court held that a Magistrate may order an accused to give voice samples, since the power serves the investigation and is not barred by Article 20(3).²² The line between compelled samples and compelled disclosure therefore needs clearer articulation, especially for devices that unlock through biometrics.

Data held by third parties compounds the difficulty. Cloud providers, telecom operators and messaging intermediaries hold vast personal data, and agencies may reach it without the user's knowledge. The DPDP Act offers limited protection here, because it exempts processing for the prevention, detection, investigation or prosecution of offences and allows the Central Government to exempt State instrumentalities altogether.²³ A statute meant to protect personal data thus largely steps aside precisely where the risk to privacy is greatest.

V. ADMISSIBILITY OF IMPROPERLY OBTAINED DIGITAL EVIDENCE

Indian courts have historically followed the common-law position that relevance, not the manner of acquisition, decides admissibility. In *R.M. Malkani v. State of Maharashtra*, a telephone recording was admitted on the reasoning that a tape-recording is admissible if it is relevant, its authenticity is established and it is not tainted by improper inducement.²⁴ In *Pooran Mal v. Director of Inspection*, the Court declined to import the American exclusionary rule and held that evidence is not excluded merely because the search that yielded it was illegal.²⁵

After *Puttaswamy*, this approach deserves reconsideration. If privacy is a fundamental right, evidence obtained by violating it without satisfying the test of legality, necessity and proportionality cannot be treated as though nothing occurred. The absence of any exclusionary consequence removes the deterrent against unlawful digital surveillance and leaves the right without an effective remedy. Conversely, a rigid exclusionary rule risks letting serious offenders escape on technicalities. A calibrated course, discussed below, would let courts weigh the seriousness of the breach against the gravity of the offence and the probative value of the material.

VI. A COMPARATIVE PERSPECTIVE

Other jurisdictions offer instructive contrasts. In *Riley v. California*, the United States Supreme Court held unanimously that police must generally obtain a warrant before searching a mobile

²²*Ritesh Sinha v. State of Uttar Pradesh*, (2019) 8 S.C.C. 1 (India).

²³Digital Personal Data Protection Act, 2023, § 17(1)(c), (2)(a).

²⁴*R.M. Malkani v. State of Maharashtra*, (1973) 1 S.C.C. 471 (India).

²⁵*Pooran Mal v. Director of Inspection*, (1974) 1 S.C.C. 345 (India).

phone seized incident to arrest, stressing the quantity and quality of information such devices hold.²⁶ In *Carpenter v. United States*, the Court held that acquiring historical cell-site location records is a search requiring a warrant, despite the third-party doctrine.²⁷ The European approach rests on Article 8 of the European Convention on Human Rights and Articles 7 and 8 of the Charter of Fundamental Rights, under which interference must be lawful, necessary and proportionate.²⁸ Applying these standards to bulk interception in *Big Brother Watch v. United Kingdom*, the Grand Chamber demanded independent authorisation and effective end-to-end oversight.²⁹

The common thread is prior independent, usually judicial, authorisation coupled with proportionality review. Neither is a settled feature of the Indian framework, although the principles in *Puttaswamy* supply the constitutional foundation for both.

VII. THE WAY FORWARD

Reconciling evidence and privacy does not require abandoning either. Five reforms merit consideration. First, the BNSS should require prior judicial authorisation for the search of digital devices and for the interception of communications, with the order specifying the data categories, time period and purpose. Secondly, the law should prescribe minimisation and retention rules, including the destruction of cloned data once proceedings end and a mechanism to screen out privileged and irrelevant material. Thirdly, the section 63 certificate regime should be supported by mandatory forensic protocols and documented chain of custody, so that reliability is proved by process and not by a signature alone. Fourthly, the courts or the legislature should adopt a structured discretion to exclude evidence obtained through serious and deliberate privacy violations, weighing the factors identified above. Finally, the blanket exemptions under the DPDP Act should be narrowed through purpose limitation and independent oversight, and the position on compelled passcodes and biometrics should be settled authoritatively, preferably by the Supreme Court in light of Article 20(3).

VIII. CONCLUSION

Digital evidence is now central to the administration of justice, and no serious legal system can afford to ignore it. Equally, no constitutional system that guarantees privacy can allow the State

²⁶*Riley v. California*, 573 U.S. 373 (2014).

²⁷*Carpenter v. United States*, 585 U.S. 296 (2018).

²⁸Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 221; Charter of Fundamental Rights of the European Union arts. 7–8, 2012 O.J. (C 326) 391.

²⁹*Big Brother Watch v. United Kingdom*, App. Nos. 58170/13, 62322/14 & 24960/15 (Grand Chamber May 25, 2021), <https://hudoc.echr.coe.int>.

unfettered access to the digital lives of its citizens in the name of investigation. India's new statutes have strengthened the reliability of electronic evidence but have not yet answered the harder question of how such evidence may lawfully be acquired. Until legislation and judicial doctrine embed judicial authorisation, proportionality and a meaningful remedy for violations, the dilemma will persist. A rights-respecting evidence law is not an obstacle to justice; it is a condition of its legitimacy.