
SILENCE AFTER THE SANHITA: PRIMARY EVIDENCE, ENCRYPTED DATA, AND ARTICLE 20(3) UNDER THE BHARATIYA SAKSHYA ADHINIYAM, 2023

Sunkireddy Suryaprakash Reddy, Research Scholar, School of Law, Mahindra University, Hyderabad

Dr Mandeep Kaur, Associate Professor of Law, School of Law, Mahindra University, Hyderabad

ABSTRACT

The Bharatiya Sakshya Adhiniyam, 2023 recasts the law of evidence in India while preserving the conceptual scaffolding of its colonial predecessor. By assimilating electronic and digital records into the category of documents and treating them, when produced for inspection, as primary evidence, the new statute generates an unexamined tension with the constitutional privilege against self-incrimination under Article 20(3). This article isolates a precise problem: where an accused holds the decryption key to a device whose contents constitute primary evidence, does the State's demand for that key compel the accused to be a witness against himself? Drawing on the testimonial-physical distinction articulated in *Kathi Kalu Oghad* and refined in *Selvi v. State of Karnataka*, and engaging the comparative act-of-production jurisprudence of the United States, the article argues that compelled decryption occupies a doctrinal space the Sakshya Adhiniyam leaves silent. It proposes a calibrated, proportionality-anchored reading that distinguishes the compelled surrender of a memorized passcode from the seizure of a stored biometric, and locates the constitutional limit in the testimonial content of the act rather than in the data sought.

Keywords: Bharatiya Sakshya Adhiniyam; primary evidence; encryption; Article 20(3); self-incrimination; digital evidence.

I. Introduction

On 1 July 2024, “the Bharatiya Sakshya Adhiniyam, 2023” replaced “the Indian Evidence Act, 1872”, completing a triad of statutes that reorganized India’s criminal-procedure architecture.¹ The reform was presented as a decolonizing exercise, yet “the Sakshya Adhiniyam” retains the structural logic of the 1872 Act, including its taxonomy of primary and secondary evidence.² Section 57 preserves the long-standing rule that primary evidence is the document itself produced for the inspection of the court.³ What the new statute adds, and what its drafters appear not to have fully reckoned with, is the seamless folding of encrypted electronic records into that category.

This article identifies a constitutional fault line running beneath that assimilation. “Article 20(3) of the Constitution” guarantees that no person accused of an offence shall be compelled to be a witness against himself.⁴ For more than six decades, the contours of that privilege have been fixed by the distinction between testimonial compulsion and the furnishing of physical or material evidence, a distinction first drawn in *State of Bombay v. Kathi Kalu Oghad*.⁵ *Selvi v. State of Karnataka* later refined the test by locating its core in the conscious, volitional content of the mind.⁶ The Sakshya Adhiniyam, by contrast, speaks only the language of admissibility. It tells courts when an electronic record may be received, but it is silent on whether the act of unlocking that record may be compelled. A single High Court decision, *Virendra Khanna v. State of Karnataka*⁷, has touched the question and treated a password as analogous to a physical key, but the analysis remains thin and untested before the Supreme Court.

The argument proceeds in five movements. Part II surveys the existing scholarship on compelled decryption and isolates the gap this article addresses. Part III maps how the Sakshya Adhiniyam classifies electronic records and why encrypted data sits uneasily within the primary-evidence rubric. Part IV reconstructs the “Article 20(3)” doctrine, separates three distinct forms of compelled access, and tests each against the privilege. Part V draws on the comparative experience of the United States, the United Kingdom, Australia, and Europe. Part

¹ Bharatiya Sakshya Adhiniyam, No. 47 of 2023, INDIA CODE (2023) [hereinafter BSA].

² Indian Evidence Act, No. 1 of 1872, INDIA CODE (1872) [hereinafter IEA].

³ BSA, *supra* note 1, § 57 (defining primary evidence); see also IEA, *supra* note 2, § 62 (predecessor provision).

⁴ INDIA CONST. art. 20, cl. 3 (“No person accused of any offence shall be compelled to be a witness against himself.”).

⁵ *State of Bombay v. Kathi Kalu Oghad*, AIR 1961 SC 1808.

⁶ *Selvi v. State of Karnataka*, (2010) 7 SCC 263.

⁷ *Virendra Khanna v. State of Karnataka*, 2021 SCC OnLine Kar 5032.

VI offers a proportionality-anchored synthesis and concludes that the statute's silence is not neutral; it shifts a constitutional question onto courts without giving them the tools to answer it.

II. Existing Scholarship on Compelled Decryption and Self-Incrimination

The compelled-decryption problem has generated a substantial literature, almost all of it situated within the United States Fifth Amendment tradition. The foundational mapping is Orin Kerr and Bruce Schneier's account of encryption workarounds, which catalogues the technical and legal means by which the State may obtain access to encrypted data and separates them into distinct categories that carry different constitutional weight.⁸ That typology has proved durable because it disaggregates a question that courts had tended to treat monolithically: it distinguishes compelling a suspect to disclose a key, compelling a suspect to enter a passcode, and the State's independent exploitation of a security flaw, each of which engages the privilege differently.⁹

The sharpest doctrinal disagreement is between Orin Kerr and Laurent Sacharoff. Kerr argues that the act of entering a password is testimonial, but that the only fact it implies is that the suspect knows the password; where the State can independently establish that knowledge, the testimonial component is a foregone conclusion and the privilege poses no bar.¹⁰ Sacharoff rejects that minimalist reading. In his account, the act of unlocking a device communicates considerably more than knowledge of the code: it asserts the suspect's control over the device and his possession of the files within it, each of which may itself be incriminating.¹¹ The disagreement is not merely technical; it reflects competing intuitions about what an act of production really says, and it has divided the American courts.

A second strand of scholarship reframes the question through privacy rather than testimony. Paul Ohm has argued that the sheer quantity and sensitivity of data on a modern device collapses older assumptions about the scope of constitutional protection, so that access

⁸Orin S. Kerr & Bruce Schneier, Encryption Workarounds, 106 GEO. L.J. 989 (2018).

⁹Id. at 998–1004 (offering a six-part typology of encryption workarounds).

¹⁰Orin S. Kerr, "Compelled Decryption and the Privilege Against Self-Incrimination, 97 TEX. L. REV. 767, 768 (2019)".

¹¹Laurent Sacharoff, "Unlocking the Fifth Amendment: Passwords and Encrypted Devices, 87 FORDHAM L. REV. 203 (2018)"; "Laurent Sacharoff, What Am I Really Saying When I Open My Smartphone? A Response to Orin S. Kerr", 97 TEX. L. REV. ONLINE 63, 68 (2019).

to a device is qualitatively unlike access to any pre-digital container.¹² Andrew Guthrie Ferguson has extended this reasoning to networked and embedded devices, contending that the constitutional category of effects must be rethought for a world in which intimate data is distributed across objects.¹³ The Supreme Court of the United States gave this intuition constitutional form in *Riley v. California* and *Carpenter v. United States*, recognising that digital data warrants distinct treatment precisely because of its volume and revelatory power.¹⁴

What unites this scholarship is its constitutional setting? It is overwhelmingly concerned with compelled decryption under the Fifth Amendment and its act-of-production doctrine, and to a lesser extent with the Fourth Amendment privacy interest. Comparatively little attention has been paid to how a common-law-rooted constitutional order such as India's would address the same problem, and almost none to the specific mechanism through which the *Bharatiya Sakshya Adhiniyam* reframes the inquiry.¹⁵ By classifying encrypted electronic records as primary evidence, the *Sakshya Adhiniyam* shifts the constitutional question away from the act of production and onto the antecedent act of decryption that renders the primary record intelligible. That shift, and the silence of the statute upon it, is the gap this article addresses.

III. The *Sakshya Adhiniyam* and the Architecture of Electronic Evidence

A. Documents, Records, and the Collapse of a Distinction

The *Sakshya Adhiniyam* expands the definition of a document to include electronic and digital records, and it treats information given electronically as evidence in its own right.¹⁶ Section 2(1)(e) folds electronically transmitted information into the meaning of evidence,¹⁷ while Section 61 declares that electronic and digital records carry the same legal effect, validity, and enforceability as their paper counterparts.¹⁸ This drafting choice imports, almost wholesale, the definitional apparatus of the "Information Technology Act, 2000", which had

¹²Paul Ohm, "The Fourth Amendment in a World Without Privacy, 81 *MISS. L.J.* 1309 (2012); see also Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 *UCLA L. REV.* 1701 (2010).

¹³Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 *CALIF. L. REV.* 805 (2016).

¹⁴*Riley v. California*, 573 U.S. 373, 393–97 (2014); *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018).

¹⁵Indian scholarly treatment of the question remains limited; the issue has surfaced principally in litigation rather than in the academic literature. See Virendra Khanna, 2021 SCC OnLine Kar 5032.

¹⁶BSA, *supra* note 1, § 2(1)(d) (defining "document" to include electronic and digital records).

¹⁷*Id.* § 2(1)(e) (defining "evidence" to include information given electronically).

¹⁸*Id.* § 61 (electronic and digital records to have the same legal effect as paper records).

already defined an electronic record in capacious terms.¹⁹ The effect is to dissolve the once-clear boundary between a tangible document and an intangible data stream.

The legislative history confirms that this assimilation was deliberate but undertheorized. The Statement of Objects and Reasons accompanying the Bharatiya Sakshya Bill framed the reform as an effort to render the law of evidence fit for the technological age, principally by giving electronic and digital records full evidentiary recognition.²⁰ The Parliamentary Standing Committee on Home Affairs, which examined the three criminal-law Bills, likewise concentrated on the admissibility and reliability of electronic records and did not address the distinct constitutional question of compelled access to encrypted data.²¹ There is no indication in the legislative materials that Parliament turned its mind to how such records are to be rendered intelligible when they are encrypted, still less to whether an accused may be compelled to perform the act of decryption. The integration of electronic records was, in other words, an answer to a problem of proof, not a considered settlement of a problem of constitutional compulsion.

That omission matters because the primary-secondary distinction was built for a world of physical originals. A primary document was the paper one could hold, inspect, and authenticate by its own features. When the original is a sequence of encrypted bits resident on a seized device, the metaphor strains. The explanation to Section 57 attempts to bridge the gap by deeming an electronic record produced for inspection to be primary evidence,²² but it does not address the antecedent question of how the record is to be rendered intelligible when it is encrypted. Encryption introduces a third state of existence that the binary of primary and secondary evidence cannot capture: the ciphertext is fully within the State's physical custody once the device is seized, yet it is evidentially inert until decrypted, and the plaintext the State actually seeks exists nowhere until the act of decryption brings it into being.

¹⁹ Information Technology Act, No. 21 of 2000, § 2(1)(t), INDIA CODE (2000) [hereinafter IT Act] (defining "electronic record").

²⁰ "Statement of Objects and Reasons", Bharatiya Sakshya Bill, 2023 (seeking to make the law of evidence applicable to contemporary technological realities by recognising electronic and digital records).

²¹ "Department-Related Parliamentary Standing Committee on Home Affairs, 248th Report on the Bharatiya Sakshya Bill, 2023" (Rajya Sabha Secretariat, Nov. 2023) (recommending safeguards for the integrity of electronic records without addressing compelled decryption).

²² BSA, *supra* note 1, § 57 expl. (treating an electronic record produced for inspection as primary evidence).

B. Admissibility and the Certificate Regime

“Section 63 of the Sakshya Adhiniyam governs the admissibility of electronic records and substantially reproduces the regime formerly housed in Section 65B of the 1872 Act.”²³ “The jurisprudence under the predecessor provision is therefore directly relevant. In *Anvar P.V. v. P.K. Basheer*²⁴, the Supreme Court held that a certificate authenticating electronic evidence was a condition precedent to admissibility. *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*²⁵, later clarified the mandatory character of that requirement while recognising narrow exceptions where the device is not within the producing party’s control. The Sakshya Adhiniyam codifies the certificate in Section 63(4) and prescribes its form in the Schedule”.²⁶

The certificate regime, however, addresses authenticity and integrity. It assumes the data is already legible. It says nothing about the prior step of decryption, where the very intelligibility of the record depends on an act that may originate in the mind of the accused. Where a device is encrypted with a passcode known only to the accused, no certifying official can lawfully produce intelligible output without the accused’s mental contribution. The certificate regime therefore silently presupposes either that the data is unencrypted, that the State possesses the key by lawful technical means, or that the accused has supplied it. The third possibility is the one the statute never confronts, and it is the one that raises the constitutional question this article addresses.

IV. Article 20(3) and the Forms of Compelled Access

A. The Foundational Distinction

“The privilege against self-incrimination entered Indian constitutional law through *M.P. Sharma v. Satish Chandra*, which read Article 20(3) broadly to cover the compelled production of documents.”²⁷ “An eleven-judge bench in *Kathi Kalu Oghad*” then narrowed the privilege by distinguishing testimonial compulsion from the furnishing of physical evidence such as “fingerprints”, “handwriting specimens”, and “bodily samples”.²⁸ The line the Court drew was

²³BSA, supra note 1, § 63 (admissibility of electronic records); cf. IEA, supra note 2, § 65B (predecessor regime).

²⁴*Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473, ¶ 22.

²⁵*Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1, ¶ 73.

²⁶BSA, supra note 1, § 63(4) (certificate requirement); id. sch. (form of certificate).

²⁷*M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300.

²⁸*Kathi Kalu Oghad*, AIR 1961 SC 1808 (distinguishing testimonial compulsion from the furnishing of physical evidence).

between communicating knowledge held in the mind and supplying material that exists independently of the will.

“Selvi v. State of Karnataka is the modern fulcrum. The Court held that narco-analysis, polygraph examination, and brain electrical activation profiling violate “Article 20(3)” because they extract the conscious content of the mind without consent.”²⁹ Crucially, Selvi located the privilege within the substantive guarantee of personal liberty and made voluntariness the touchstone of constitutional validity.³⁰ Nandini Satpathy v. P.L. Dani had earlier extended the privilege to the investigative stage, confirming that compulsion need not occur in the courtroom to engage the constitutional bar.³¹ Two features of Selvi bear on the present problem: the Court protected the conscious content of the mind as a constitutionally insulated interior space,³² and it made consent the organising principle, so that evidence extracted under compulsion does not survive the privilege.³³

B. Three Forms of Compelled Access

The decisive analytic move, drawn from the Kerr-Schneier typology but adapted to Indian doctrine, is to recognise that compelled access is not a single act but at least three distinct ones, each with a different constitutional character.³⁴ Conflating them, as the Sakshya Adhiniyam’s uniform treatment of electronic records invites courts to do, produces error. The three forms are the “compelled disclosure of a password”, the “compelled entry of a password” without its disclosure, and biometric unlocking.

First, “compelled disclosure of a password”. Here the accused is required to articulate and communicate a memorized alphanumeric code. This is the clearest case for the privilege. The passcode exists only as a fact within the mind, and compelling its articulation compels the accused to communicate the conscious content of his memory, which falls squarely within the testimonial core that Selvi protects.³⁵ On the analysis advanced here, compelled disclosure is

²⁹Selvi, (2010) 7 SCC 263, ¶223 (holding narco-analysis, polygraph, and BEAP tests violative of Article 20(3)).

³⁰Id. ¶ 191 (locating the privilege within the substantive guarantee of personal liberty).

³¹Nandini Satpathy v. P.L. Dani, (1978) 2 SCC 424.

³²Selvi, (2010) 7 SCC 263, ¶ 222 (distinguishing the content of the mind from the physical attributes of the accused).

³³Id. ¶ 225 (voluntariness as the touchstone of constitutional validity).

³⁴Kerr & Schneier, *supra* note 8, at 1001–04 (separating compelled disclosure of a password from compelled entry of a password).

³⁵Selvi, (2010) 7 SCC 263, ¶ 222 (protecting the conscious content of the mind).

testimonial and barred.

Second, compelled entry of a password without disclosure. Here the accused is directed to enter the code himself so that the State never learns it. This is the form over which American scholarship divides. On Kerr's minimalist view, "the act communicates only that the accused knows the password, a fact that may be a foregone conclusion".³⁶ On Sacharoff's view, the act communicates additionally that the accused controls the device and possesses its files, each potentially incriminating.³⁷ Indian doctrine, lacking a foregone-conclusion exception and protecting the content of the mind categorically, has no principled basis for treating compelled entry as less testimonial than compelled disclosure: in both, the accused must draw upon and act on the contents of his memory, and in both the act authenticates his relationship to the device. The Virendra Khanna analogy of a password to a physical key fails precisely here, because a physical key exists in the world whereas a memorized code exists only as a mental fact.³⁸ Compelled entry should therefore also be treated as testimonial.

Third, biometric unlocking. Here the State applies the accused's fingerprint, face, or iris to the sensor. This furnishes a physical attribute of the body, akin to the fingerprint in *Kathi Kalu Oghad* and the voice sample held non-testimonial in *Ritesh Sinha*.³⁹ "It does not require the accused to communicate the content of his mind, and so it falls outside the testimonial core of Article 20(3)". It does not follow that biometric compulsion is unconstrained; as Part VI explains, it remains subject to the privacy and proportionality filters of *Puttaswamy*. The constitutional point is narrower: only the first two forms engage the self-incrimination privilege, and the bar against involuntary self-incriminating communication cannot be evaded by re-labelling the compelled act as the production of a primary record.⁴⁰

V. Comparative Approaches to Compelled Decryption

A. The United States: Act of Production and the Foregone Conclusion

"United States doctrine refines the privilege through the act-of-production doctrine, under

³⁶Kerr, *supra* note 10, at 779 (the implied testimony of compelled entry is limited to knowledge of the password).

³⁷Sacharoff, A Response to Orin S. Kerr, *supra* note 11, at 68 (compelled unlocking implicitly asserts knowledge, control, and possession).

³⁸Virendra Khanna, 2021 SCC OnLine Kar 5032, ¶ 17 (treating a compelled password as analogous to a physical key).

³⁹*Ritesh Sinha v. State of Uttar Pradesh*, (2019) 8 SCC 1 (India) (compelled voice samples not testimonial).

⁴⁰BSA, *supra* note 1, § 23 (rendering involuntary confessions to police inadmissible).

which the compelled production of documents may itself be testimonial because it concedes the existence, possession, and authenticity of the material; the foregone-conclusion exception removes the privilege where the State already knows what it will find.”⁴¹ Applied to encryption, the American courts have split. “In *Commonwealth v. Gelfgatt*, the Massachusetts Supreme Judicial Court compelled decryption where the defendant’s capacity to decrypt was a foregone conclusion, while the Indiana Supreme Court in *Seo v. State* reached the opposite result, holding that compelled decryption communicated the existence and accessibility of files and was therefore testimonial”.⁴² The split tracks the Kerr-Sacharoff disagreement and remains unresolved at the level of the Supreme Court.

B. The United Kingdom: RIPA Section 49 Notices

“The United Kingdom has legislated where India is silent. Section 49 of the Regulation of Investigatory Powers Act 2000 empowers an authorised officer to serve a notice requiring a person believed to hold a key to protected information to disclose that key or to put the information into intelligible form.⁴³ Failure to comply is a criminal offence under Section 53, punishable by up to two years’ imprisonment, rising to five years in national-security and child-indecency cases.⁴⁴ Critically, the statute does not exempt the disclosure from operating against the suspect, and it builds in a proportionality requirement at the point of issue rather than a self-incrimination exception.”⁴⁵ The British approach thus resolves the tension by legislative fiat, subordinating the privilege to a proportionality-screened disclosure duty, an approach that has drawn sustained criticism precisely because it compels the production of mind-dependent keys under threat of imprisonment.

C. Australia: The Assistance and Access Act

“Australia’s Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018” takes a different route, “directing its compulsion primarily at communications providers rather than at suspects”. “It authorises technical assistance and technical capability notices requiring providers to render assistance that is reasonable,

⁴¹*United States v. Hubbell*, 530 U.S. 27, 43 (2000) (act-of-production doctrine); *Fisher v. United States*, 425 U.S. 391, 410 (1976) (foregone-conclusion exception).

⁴²*Commonwealth v. Gelfgatt*, 11 N.E.3d 605 (Mass. 2014); contra *Seo v. State*, 148 N.E.3d 952 (Ind. 2020).

⁴³Regulation of Investigatory Powers Act 2000, c. 23, § 49 (UK).

⁴⁴*Id.* § 53 (offence of failing to comply; maximum two years’ imprisonment, rising to five years in national-security and child-indecency cases).

⁴⁵*Id.* § 49(2)(c) (disclosure requirement must be proportionate to what is sought).

proportionate, and technically feasible, while expressly prohibiting the building of systemic weaknesses or backdoors”.⁴⁶ The Australian model is instructive for India because it locates the burden of access on the corporate intermediary rather than on the accused, thereby largely sidestepping the self-incrimination problem; the constitutional difficulty that the Sakshya Adhiniyam raises arises only where the State turns its demand on the accused himself.

D. The European Position

The European approach is anchored in privacy and in the procedural fairness guarantee of the European Convention. “In *Saunders v. United Kingdom*, the European Court of Human Rights located the privilege against self-incrimination” within the “fair-trial guarantee of Article 6”, while drawing the now-familiar distinction between compelled testimony and material having an existence independent of the will of the accused, such as breath, blood, and bodily samples.⁴⁷ “That distinction maps closely onto the Indian testimonial-physical divide and supplies comparative support for treating a memorized passcode, which has no existence independent of the will, as protected, while leaving biometric attributes, which do, outside the privilege.”

The comparative lesson is methodological rather than doctrinal. The Indian privilege contains no foregone-conclusion carve-out, and the British solution of a proportionality-screened disclosure duty would, if transplanted, require either constitutional amendment or a substantial judicial reworking of *Selvi*. The value of the comparative material lies in its demonstration that the constitutional answer should follow the nature of the compelled act, the line that *Saunders* and *Kathi Kalu Oghad* share, rather than the value of the data behind the lock or the gravity of the suspected offence.

VI. A Proportionality-Anchored Synthesis

Puttaswamy reoriented Indian rights adjudication around proportionality and recognised informational privacy as intrinsic to Article 21.⁴⁸ Any State demand to decrypt now engages two overlapping guarantees: the privilege under Article 20(3) and the privacy interest under

⁴⁶Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth) sch. 1, § 317ZG (Austl.) (prohibiting the building of systemic weaknesses).

⁴⁷*Saunders v. United Kingdom*, App. No. 19187/91, 23 Eur. H.R. Rep. 313 (1996).

⁴⁸*Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1, ¶ 323. (recognising informational privacy as intrinsic to Article 21).

Article 21. The two operate in sequence rather than in parallel. Article 20(3) is a categorical bar: where compulsion reaches testimonial content, no balancing saves it. Article 21 governs the residue: once a compelled act is found to fall outside the testimonial core, “the privacy interest still subjects the demand to the four-pronged proportionality test of legitimate aim, rational connection, necessity, and balancing”.⁴⁹ The correct sequence is to ask first whether the compelled act is testimonial, and only if it is not to proceed to proportionality; conflating the two risks letting the magnitude of the State’s interest dissolve a protection the Constitution intended to be absolute.

Three propositions follow. First, the compelled disclosure or entry of a memorized passcode should be treated as presumptively testimonial and therefore barred, because both extract and act upon the conscious content of the mind in the manner *Selvi* condemned.⁵⁰ Second, the compelled use of a biometric attribute may be permissible, consistent with *Kathi Kalu Oghad* and *Ritesh Sinha*, because it furnishes a physical characteristic rather than a communication, though it remains subject to the proportionality and privacy filters of *Puttaswamy*.⁵¹ Third, the existing decryption-assistance obligations under the Information Technology Act, which carry criminal penalties for non-compliance, must be read down so as not to compel testimonial acts; their reach should be confined to physical keys and to situations falling outside the testimonial core.⁵²

This synthesis also reconciles the production power. While the *Bharatiya Nagarik Suraksha Sanhita*, successor to Section 91 of the old Code, permits a court to order production of a document, that power has never extended to compelling testimonial communication, and the *Sakshya Adhiniyam* does not enlarge it.⁵³ Expert testimony on the integrity of recovered data, admissible under Section 39, can authenticate evidence lawfully obtained without resort to compelled mental disclosure,⁵⁴ and the Court’s caution about the susceptibility of electronic records to manipulation reinforces the need for a clean evidentiary chain that does not depend

⁴⁹*Modern Dental College v. State of Madhya Pradesh*, (2016) 7 SCC 353. (four-pronged proportionality test); *Puttaswamy*, (2017) 10 SCC 1, ¶ 638.

⁵⁰*Selvi*, (2010) 7 SCC 263, ¶¶ 222–225.

⁵¹*Ritesh Sinha*, (2019) 8 SCC 1; *Puttaswamy*, (2017) 10 SCC 1, ¶ 638.

⁵²IT Act, *supra* note 7, § 69(3)– (4) (decryption-assistance obligation; imprisonment up to seven years for non-compliance).

⁵³*Bharatiya Nagarik Suraksha Sanhita*, No. 46 of 2023, § 94, INDIA CODE (2023) (production power; successor to Code of Criminal Procedure, 1973, § 91).

⁵⁴*BSA*, *supra* note 1, § 39(2) (admissibility of expert opinion on electronic evidence).

on coerced acts of the accused.⁵⁵

VII. Conclusion

The Sakshya Adhiniyam modernized the vocabulary of evidence without modernizing its constitutional sensibility. By assimilating encrypted records into the primary-evidence category, it created an evidentiary expectation that the data will be legible, while leaving unaddressed the act that makes it so. That act, where it draws on the memorized content of the mind, sits at the heart of the Article 20(3) privilege. The statute's silence is not a gap to be filled by analogy to physical keys; it is a constitutional question that demands a principled answer. Courts should hold that compelled passcode disclosure and compelled passcode entry are testimonial and barred, that biometric compulsion survives only the proportionality filter, and that statutory decryption-assistance duties must be confined to the physical-evidence category. Until the Supreme Court speaks, the silence after the Sanhita will be filled by the uneven reasoning of trial courts, and a six-decade-old distinction will be asked to govern a technology its authors could not have imagined.⁵⁶

The constitutional privilege against self-incrimination was designed to prevent the State from converting an accused into a source of evidence against himself. In the digital age, the question is no longer merely whether an individual may be compelled to speak, but whether he may be compelled to unlock the evidentiary value of knowledge existing only within his mind. The answer to that question will shape the future relationship between constitutional liberty and digital criminal investigation.

⁵⁵Tukaram S. Dighole v. Manikrao Shivaji Kokate, (2010) 4 SCC 329. (caution on the susceptibility of electronic records to manipulation).

⁵⁶Kathi Kalu Oghad, AIR 1961 SC 1808 (foundational distinction reaffirmed across six decades of doctrine).

REFERENCES

1. Andrew Guthrie Ferguson, The Internet of Things and the Fourth Amendment of Effects, 104 CALIF. L. REV. 805 (2016).
2. Department-Related Parliamentary Standing Committee on Home Affairs, 248th Report on the Bharatiya Sakshya Bill, 2023 (Rajya Sabha Secretariat, 2023).
3. Orin S. Kerr, Compelled Decryption and the Privilege Against Self-Incrimination, 97 TEX. L. REV. 767 (2019).
4. Orin S. Kerr & Bruce Schneier, Encryption Workarounds, 106 GEO. L.J. 989 (2018).
5. Laurent Sacharoff, Unlocking the Fifth Amendment: Passwords and Encrypted Devices, 87 FORDHAM L. REV. 203 (2018).
6. Laurent Sacharoff, What Am I Really Saying When I Open My Smartphone? A Response to Orin S. Kerr, 97 TEX. L. REV. ONLINE 63 (2019).
7. Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA L. REV. 1701 (2010).
8. Richard A. Epstein, "Privacy, Property Rights and Misrepresentations", 12 Geo. Mason L. Rev. 455 (2004).
9. Susan W. Brenner & Barbara A. Frederiksen, "Computer Searches and Seizure: Some Unresolved Issues", 8 Mich. Telecomm. & Tech. L. Rev. 39 (2002).
10. Stephen E. Henderson, "Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search", 55 Cath. U. L. Rev. 373 (2006).

Book:

1. Erin Murphy, "The New Forensics: Criminal Justice, False Certainty and the Second Generation of Scientific Evidence" (NYU Press, 2015).

2. Gautam Bhatia, *The Transformative Constitution: A Radical Biography In Nine Acts* (HarperCollins India 2019).
3. M.P. Jain, *Indian Constitutional Law* (LexisNexis, latest ed.).
4. H.M. SEERVAI, *Constitutional Law of India: A Critical Commentary* (Universal Law Publishing, 4th ed.).

Report:

1. Justice B.N. Srikrishna Committee Report on Data Protection (2018)
2. Law Commission of India, 180th Report on Article 20(3) of the Constitution of India and the Right to Silence (2002).

Acts:

1. Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, INDIA CODE (2023).
2. Bharatiya Sakshya Adhiniyam, No. 47 of 2023, INDIA CODE (2023).
3. Indian Evidence Act, No. 1 of 1872, INDIA CODE (1872).
4. Information Technology Act, No. 21 of 2000, INDIA CODE (2000).
5. Regulation of Investigatory Powers Act 2000, c. 23 (UK).
6. Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth) (Austl.).

Case Laws:

1. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
2. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
3. Carpenter v. United States, 138 S. Ct. 2206 (2018).
4. Commonwealth v. Gelfgatt, 11 N.E.3d 605 (Mass. 2014).

5. Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
6. Justice K.S. Puttaswamy (Aadhaar-5J) v. Union of India, (2019) 1 SCC 1
7. Kathi Kalu Oghad, State of Bombay v., AIR 1961 SC 1808.
8. Modern Dental College v. State of Madhya Pradesh, (2016) 7 SCC 353.
9. M.P. Sharma v. Satish Chandra, AIR 1954 SC 300.
10. Nandini Satpathy v. P.L. Dani, (1978) 2 SCC 424.
11. People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.
12. Riley v. California, 573 U.S. 373 (2014).
13. Ritesh Sinha v. State of Uttar Pradesh, (2019) 8 SCC 1.
14. Saunders v. United Kingdom, App. No. 19187/91, 23 Eur. H.R. Rep. 313 (1996).
15. Selvi v. State of Karnataka, (2010) 7 SCC 263.
16. Seo v. State, 148 N.E.3d 952 (Ind. 2020).
17. Virendra Khanna v. State of Karnataka, 2021 SCC OnLine Kar 5032.