# SELF-INCRIMINATION IN THE DIGITAL AGE: CONSTITUTIONAL LIMITS ON PASSWORDS, BIOMETRICS, AND DIGITAL EVIDENCE WITHIN THE AMBIT OF ARTICLE 20(3) OF THE INDIAN CONSTITUTION

Madhurika De[1] & Dr. Kabita Chakraborty[2]

## ABSTRACT

The rapid expansion of digital technologies has significantly transformed the nature of criminal investigations, particularly through the use of digital forensics. This evolution, however, has raised critical constitutional concerns regarding the protection against self-incrimination under Article 20(3) of the Constitution of India. Traditionally, the principle of self-incrimination has been interpreted to protect individuals from being compelled to provide testimonial evidence against themselves. In the digital era, this protection is increasingly challenged by investigative practices involving compelled access to personal devices, including smartphones, computers, and encrypted data systems. While passwords are generally considered knowledge-based and thus protected under Article 20(3), biometric data is often treated as physical evidence, creating a complex constitutional dilemma when such access leads to the exposure of personal digital information. The study further evaluates key judicial interpretations, including Selvi v. State of Karnataka and Justice K.S. Puttaswamy v. Union of India, to assess the evolving scope of privacy and self-incrimination in India. The paper identifies significant legal gaps in the existing framework, particularly under statutes such as the Information Technology Act 2000, which do not adequately address the constitutional implications of digital evidence collection. The study concludes by advocating for a balanced legal framework that harmonizes the needs of effective digital investigation with the constitutional mandate to protect individual liberties, emphasizing the necessity for judicial clarity and legislative reform in the digital age.

**Keywords:** Article 20(3), self-incrimination, digital evidence, passwords, biometrics, constitutional law, privacy, compelled decryption.

[1] Research Scholar, Faculty of Law, The ICFAI University, Tripura
[2] Professor, Faculty of Law, The ICFAI University, Tripura

## 1. INTRODUCTION

"***Privacy is the constitutional core of human dignity.***"
***- Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1***

The digital revolution has fundamentally altered the nature of human interaction, communication, and storage of information. Smartphones today contain vast amounts of personal information, including financial data, photographs, confidential communications, browsing histories, and biometric identifiers. Governments and investigative agencies increasingly rely upon digital evidence in criminal investigations, cybercrime prosecutions, terrorism cases, and financial fraud inquiries. Consequently, constitutional protections that were originally framed in a pre-digital era must now be interpreted in the context of rapidly evolving technologies[3].

Article 20(3) of the Constitution of India provides that "No person accused of any offence shall be compelled to be a witness against himself."[4] This constitutional protection is a fundamental part of criminal law and embodies the wider principle that the State must establish guilt without forcing the accused to contribute to their own conviction. Historically, courts distinguished between testimonial evidence, which is protected, and physical evidence, which may be compelled. However, digital technologies challenge this distinction[5].

A password is often a product of human memory and cognition. Compelling an accused person to disclose a password may therefore amount to forcing the person to reveal the contents of the mind. By contrast, biometric authentication mechanisms such as fingerprints, facial recognition, and iris scans are physical attributes. Whether compelling an accused to unlock a device through biometrics violates Article 20(3) remains a contentious constitutional issue.

The issue gains further complexity following the Supreme Court's acknowledgment of privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India[6]. Digital devices are not merely containers of information; they represent comprehensive archives of personal identity, autonomy, and thought. Therefore, compelled access to digital devices implicates both the

[3] State of Bombay v. Kathi Kalu Oghad, A.I.R. 1961 S.C. 1808 (India).
[4] The Constitution of India art. 20(3).
[5] Supra 3
[6] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).

privilege against self-incrimination and the right to privacy.

The paper analyses the constitutional consequences of compelled password disclosure, biometric unlocking, and the use of digital evidence under Article 20(3). It explores the evolution of self-incrimination jurisprudence in India, evaluates comparative legal approaches, and proposes reforms for safeguarding constitutional liberties in the digital age.

## 2. CONCEPTUAL FOUNDATIONS OF SELF-INCRIMINATION

The privilege against self-incrimination is firmly rooted in common law traditions. Historically, English courts opposed coercive interrogation methods linked to ecclesiastical tribunals and the Star Chamber. Over time, this principle developed into the Fifth Amendment of the United States Constitution, which provides that no individual "shall be compelled in any criminal case to be a witness against himself[7].

The Indian Constitution adopted a similar protection under Article 20(3)[8]. The framers of the Constitution recognized that protection against self-incrimination is essential to preserving human dignity, fairness, and the presumption of innocence. The guarantee seeks to prevent coercive police practices and ensure that criminal convictions are based upon independent evidence rather than forced confessions[9].

Three essential ingredients must exist for Article 20(3) to apply:

a. The individual must be formally accused of an offence.

b. There must be compulsion.

c. The compulsion must result in the person becoming a witness against himself.

The phrase "to be a witness" has been central to constitutional interpretation. Courts have traditionally interpreted it to refer primarily to testimonial or communicative evidence. Accordingly, the distinction between testimonial and physical evidence became crucial.

Testimonial evidence includes oral statements, confessions, and communications that disclose

[7] U.S. Const. amend. V.
[8] Supra 4
[9] Nandini Satpathy v. P.L. Dani, (1978) 2 S.C.C. 424 (India).

personal knowledge. In contrast, physical evidence consists of fingerprints, handwriting samples, blood specimens, DNA samples, and other bodily characteristics. Indian courts have generally maintained that compelling the production of physical evidence does not violate Article 20(3), since such evidence is not regarded as personal testimony.

However, digital evidence complicates this distinction. A password is intangible yet cognitive. It exists within the memory of an individual and often cannot be obtained without mental disclosure. Therefore, the constitutional characterization of passwords differs significantly from conventional physical evidence.

## 3. JUDICIAL INTERPRETATION OF ARTICLE 20(3) IN INDIA

Article 20(3) of the Constitution of India guarantees that "*No person accused of any offence shall be compelled to be a witness against himself*." This provision embodies the constitutional protection against self-incrimination and serves as a fundamental safeguard within India's criminal justice system. The principle is embedded in the broader notions of human dignity, fair trial, and the presumption of innocence, ensuring that the State cannot secure convictions through coercion or forced confessions.

The judicial interpretation of Article 20(3) has evolved significantly through a series of landmark decisions delivered by the Supreme Court of India. Earlier, courts adopted a relatively limited interpretation of the provision by distinguishing between "testimonial" evidence and "physical" evidence. Over time, however, judicial reasoning expanded the scope of protection to include procedural fairness, mental privacy, and the right to silence.

Indian courts have played a significant role in defining the essential elements of Article 20(3), namely: the meaning of an "accused person," the concept of "compulsion," and the phrase "to be a witness against himself." Through various judgments, the judiciary has clarified that while physical evidence such as handwriting, fingerprints samples may be compulsorily obtained, testimonial communications involving personal knowledge and mental processes enjoy constitutional protection.

In the contemporary digital era, these judicial interpretations have acquired renewed significance. Questions concerning compelled disclosure of passwords, biometric unlocking of smartphones, encrypted data, and digital surveillance require courts to reassess traditional

doctrines in light of technological advancements.

One of the earliest constitutional decisions concerning self-incrimination was M.P. Sharma v. Satish Chandra[10]. The Supreme Court considered whether search and seizure violated Article 20(3). The Court held that compulsory production of documents may amount to testimonial compulsion, but searches conducted by authorities did not necessarily violate constitutional protections because the accused was not personally compelled to testify. Although decided before the development of modern privacy jurisprudence, M.P. Sharma laid the groundwork for understanding the relationship between compulsion and evidence gathering.

The landmark decision in State of Bombay v. Kathi Kalu Oghad[11] significantly shaped Indian self-incrimination jurisprudence. The Court drew a distinction between testimonial communication and physical evidence. and physical evidence. It held that obtaining fingerprints, handwriting samples, and specimen signatures did not amount to compelling a person "to be a witness" because such evidence was physical rather than communicative. The Court emphasized that Article 20(3) protects against conveying personal knowledge based on mental faculties. This distinction remains central to contemporary debates concerning passwords and biometrics.

In Nandini Satpathy v. P.L. Dani[12], the Supreme Court expanded the scope of protection under Article 20(3). The Court held that the right against self-incrimination extends beyond courtroom testimony and applies during police interrogation. The judgment recognized the right to silence and emphasized that compulsion includes psychological pressure and coercive questioning. This decision strengthened procedural safeguards for accused persons and underscored the constitutional commitment to fair criminal investigations.

The Supreme Court's judgment in Selvi v. State of Karnataka[13] represents one of the most important decisions concerning mental privacy and self-incrimination. The Court considered the constitutionality of narco-analysis, polygraph examinations, and Brain Electrical Activation Profile (BEAP) tests. The Court held that the involuntary use of such techniques violates Article 20(3) as they compel the extraction of personal knowledge without the individual's consent. The judgment emphasized that testimonial compulsion includes forced

[10] M.P. Sharma v. Satish Chandra, A.I.R. 1954 S.C. 300 (India).
[11] Supra 3
[12] Supra 9
[13] Selvi v. State of Karnataka, (2010) 7 S.C.C. 263 (India).

revelation of mental processes. Importantly, the Court recognized a broader concept of mental privacy and cognitive autonomy. Selvi is particularly relevant in the digital context because passwords involve cognitive processes similar to testimonial communication. Compelling disclosure of passwords may therefore violate the constitutional principles articulated in Selvi.

The acknowledgment of privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India[14] brought about a major shift in Indian constitutional jurisprudence.The Supreme Court held that privacy is intrinsic to dignity, liberty, and autonomy under Article 21. The judgment recognized informational privacy and acknowledged that digital technologies create unprecedented threats to individual autonomy. This development has significant implications for digital evidence and compelled access to electronic devices. When the State compels disclosure of passwords or unrestricted access to smartphones, it potentially intrudes into both privacy rights and the privilege against self-incrimination. Therefore, Article 20(3) must now be interpreted alongside the constitutional right to privacy.

## 4. DIGITAL EVIDENCE AND CONSTITUTIONAL CHALLENGES

With the rapid advancement of digital technology, courts have increasingly been confronted with novel forms of evidence such as call data records, GPS location tracking, electronic communications, cloud-stored information, and encrypted digital devices. Judicial interpretation in India has generally treated the collection of such digital evidence as comparable to the collection of physical evidence, particularly where the information is obtained from third-party service providers rather than directly from the accused. In cases involving electronic records and telecommunications data, courts have often emphasized that such information exists independently of the volition or mental processes of the accused person. This approach reflects the traditional judicial distinction between testimonial communication and material or physical evidence under Article 20(3) of the Constitution.

However, the constitutional position becomes significantly more complex in situations involving compelled disclosure of passwords, encryption keys, or access credentials to digital devices. Unlike ordinary physical evidence, passwords are products of human memory and cognition. Requiring an accused person to disclose such information may compel the individual to reveal the contents of his or her mind, thereby amounting to testimonial compulsion

[14] Supra 6

prohibited under Article 20(3). Similarly, compelled decryption of encrypted devices raises concerns regarding cognitive privacy, informational autonomy, and the broader constitutional protection against self-incrimination.

The increasing reliance on smartphones and digital devices in everyday life further intensifies these concerns. Modern electronic devices contain extensive personal information, including financial records, private communications, browsing history, biometric identifiers, and sensitive personal data. As a result, compelled access to such devices not only implicates the protection against self-incrimination but also intersects with the constitutional right to privacy affirmed in Justice K.S. Puttaswamy v. Union of India. Therefore, Indian courts are now required to reinterpret traditional constitutional doctrines in light of emerging technological realities and evolving standards of digital liberty.

## 5. PASSWORDS, BIOMETRICS, AND COMPELLED DECRYPTION

The increasing use of smartphones, encrypted communication platforms, and biometric authentication technologies has created significant constitutional challenges in the context of criminal investigations. Modern digital devices contain extensive personal and sensitive information, including financial records, private communications, photographs, browsing histories, medical information, and confidential documents. Consequently, compelled access to such devices raises serious concerns under Article 20(3) of the Constitution of India, which safeguards individuals from being forced to testify against themselves[15].

One of the most debated issues in contemporary constitutional law is whether passwords and biometric authentication methods should receive protection under the privilege against self-incrimination. The distinction becomes important because Indian jurisprudence traditionally differentiates between testimonial evidence and physical evidence. Testimonial evidence involves communication based on personal knowledge or mental processes, whereas physical evidence consists of bodily characteristics or material evidence that exists independently of the will of the accused.

Passwords are generally regarded as testimonial in nature because they originate from the cognitive processes and memory of an individual. A password is not merely a physical object;

[15] Shanmuga Sundaram & P.R.L. Rajavenkatesan, Protection against Self-Incrimination – Principles and Practice: A Comparative Analysis, Indian J. L. & Just. (Univ. of N. Bengal, 2022), available at https://ir.nbu.ac.in

rather, it is knowledge possessed exclusively by the user. Compelling an accused person to disclose a password may therefore amount to forcing that person to reveal the contents of his or her mind. Such disclosure directly involves mental faculties and communicative testimony, thereby attracting constitutional protection under Article 20(3). The reasoning adopted by the Supreme Court in Selvi v. State of Karnataka supports this interpretation by recognizing that involuntary extraction of personal knowledge violates the constitutional guarantee against self-incrimination.

In contrast, biometric identifiers such as fingerprints, facial recognition, retina scans, and voice samples are generally treated as physical evidence. Indian courts have historically permitted the compulsory collection of physical evidence on the ground that such evidence does not involve testimonial communication. In State of Bombay v. Kathi Kalu Oghad, the Supreme Court held that fingerprints, handwriting samples, and specimen signatures constitute physical characteristics and are therefore not protected under Article 20(3). Applying this reasoning, investigative agencies may argue that compelling biometric unlocking of devices does not amount to testimonial compulsion.

However, the issue is not entirely settled in the digital context. Although biometric identifiers are physical in nature, their use to unlock smartphones or encrypted devices grants investigators access to extensive digital information, much of which may be deeply personal and unrelated to the alleged offence. Therefore, biometric unlocking differs substantially from ordinary fingerprint collection because it acts as a gateway to an individual's private digital ecosystem. This raises broader concerns relating to informational privacy and personal autonomy.

Compelled decryption presents an even more difficult constitutional problem. Decryption orders may require an accused person to unlock encrypted devices, reveal access credentials, or assist investigative agencies in accessing protected digital data. Such actions may effectively compel the accused to participate in the process of evidence creation against oneself. The constitutional challenge lies in balancing the legitimate interests of law enforcement agencies in investigating serious crimes against the fundamental rights of individuals to privacy, dignity, and protection from self-incrimination[16].

[16] Abhinav Sekhri, The Right Against Self-Incrimination in India: A Critical Analysis, 5 Nat'l L. Sch. India Rev. 1 (2016); Selvi v. State of Karnataka, (2010) 7 S.C.C. 263 (India).

The recognition of privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India has further reinforced the case for stronger constitutional protections in digital investigations. Digital devices today serve as repositories of personal identity and autonomy.. Consequently, unrestricted State access to encrypted devices may lead to disproportionate intrusions into private life.[17]

In the absence of clear legislative guidelines in India regarding compelled decryption, courts are likely to play a central role in defining the constitutional limits of digital investigations. A balanced constitutional approach would require courts to distinguish between physical evidence and cognitive disclosure while ensuring that investigative powers remain subject to principles of proportionality, necessity, and judicial oversight.

## 6. COMPARATIVE CONSTITUTIONAL PERSPECTIVES WITH USA, UK, EUROPEAN UNION

The constitutional challenges arising from compelled disclosure of passwords, biometric authentication, and digital evidence are not unique to India. Courts and legislatures in various jurisdictions have faced challenges in striking a balance between the need for effective criminal investigations and the protection of privacy, liberty, and the right against self-incrimination. Comparative constitutional analysis provides valuable insights into how different legal systems approach compelled decryption and digital surveillance. The experiences of the United States, the United Kingdom, and the European Union are particularly significant because they reflect differing constitutional traditions and legal philosophies regarding individual rights and State power.

### 6.1 UNITED STATES

#### 6.1.1 Fifth Amendment Jurisprudence

The Fifth Amendment to the United States Constitution provides that no person "shall be compelled in any criminal case to be a witness against himself." American courts have interpreted this provision to protect individuals against testimonial compulsion, particularly where the compelled act reveals the contents of a person's mind. The constitutional protection

[17] Suyash Sarvankar, Key Disclosure Laws and the Right Against Self-Incrimination in India, SSRN (2017), https://ssrn.com/abstract=3063854

closely resembles Article 20(3) of the Indian Constitution and has heavily influenced global jurisprudence on self-incrimination[18].

In the context of digital evidence, United States courts have increasingly examined whether compelled disclosure of passwords or decryption keys amounts to testimonial communication. Courts generally distinguish between physical evidence and cognitive disclosure. If disclosure requires an individual to use memory, thought processes, or mental knowledge, it may attract constitutional protection under the Fifth Amendment[19].

### 6.1.2. Foregone Conclusion Doctrine

American courts have developed the "foregone conclusion doctrine" to determine whether compelled disclosure violates the privilege against self-incrimination. Under this doctrine, disclosure may be constitutionally permissible if the government can independently establish with reasonable certainty that it already knows about the existence, location, and authenticity of the evidence sought[20]. In such circumstances, the compelled act is considered to add little or no testimonial value.

However, the doctrine remains controversial in the digital context. Critics argue that encrypted smartphones and computers contain vast quantities of private information, and compelled decryption effectively forces individuals to assist investigators in accessing incriminating evidence. Consequently, many scholars contend that the doctrine inadequately protects digital privacy and cognitive liberty.

### 6.1.3. Password vs Biometric Distinction

United States courts often distinguish between passwords and biometric authentication methods. Passwords are generally considered testimonial because they involve memorized knowledge and cognitive processes. Compelling a person to disclose a password may therefore violate the Fifth Amendment[21].

[18] Doe v. United States, 487 U.S. 201 (1988) (distinguishing testimonial communication from physical evidence); Fisher v. United States, 425 U.S. 391 (1976).
[19] United States v. Hubbell, 530 U.S. 27 (2000) (holding that compelled production requiring use of mind violates the Fifth Amendment where it is testimonial in nature).

Biometric identifiers such as fingerprints and facial recognition are usually treated as physical evidence rather than testimonial communication. Courts have often compared biometric unlocking to fingerprint collection or DNA sampling, which traditionally fall outside constitutional protection. Nevertheless, this distinction has been increasingly questioned because biometric unlocking provides access to highly sensitive digital information stored on electronic devices.

The American experience demonstrates the growing tension between traditional constitutional doctrines and modern technological realities.

### 6.2 United Kingdom

#### 6.2.1 Regulation of Investigatory Powers Act (RIPA)

The United Kingdom has adopted a comparatively broader approach toward State investigative powers in digital matters. The Regulation of Investigatory Powers Act (RIPA), enacted in 2000, grants authorities the power to compel individuals to disclose encryption keys or decrypted information where necessary for national security, crime prevention, or public safety purposes[22].

Under RIPA, law enforcement agencies may issue notices requiring individuals to provide access to encrypted data. Failure to comply with such notices may itself constitute a criminal offence punishable by imprisonment.

#### 6.2.2 Mandatory Disclosure Provisions

Unlike the constitutional approach adopted in the United States, the United Kingdom does not recognize an absolute privilege against self-incrimination in the same manner. British law places greater emphasis on investigative necessity and national security concerns. Consequently, mandatory disclosure provisions under RIPA permit compelled decryption under certain statutory safeguards.

However, these provisions have attracted criticism from civil liberties groups and privacy advocates. Critics argue that mandatory disclosure undermines personal autonomy, weakens

[22] Regulation of Investigatory Powers Act 2000, c. 23 (UK),section 49–53.

encryption protections, and creates excessive surveillance powers. Concerns have also been raised regarding proportionality, judicial oversight, and potential misuse of State authority.

The United Kingdom model reflects a more security-oriented framework in which investigative efficiency often receives greater priority than individual privacy rights.

## 6.3 EUROPEAN UNION

### 6.3.1. Privacy and Proportionality Standards

The European Union adopts a rights-based approach grounded in privacy, dignity, and proportionality principles. European constitutional jurisprudence is largely shaped by the European Convention on Human Rights (ECHR) and the Charter of Fundamental Rights of the European Union[23]. Article 8 of the European Convention on Human Rights (ECHR) safeguards the right to respect for private and family life, while Article 6 ensures the right to a fair trial. European courts typically hold that any State interference with privacy must meet the requirements of legality, necessity, and proportionality.

In digital investigations, European legal systems often emphasize that surveillance measures and compelled disclosure powers must be narrowly tailored and subject to independent judicial supervision.

### 6.3.2. Human Rights Approach

The European Court of Human Rights has consistently recognized that technological surveillance poses serious risks to democratic freedoms and individual autonomy. Consequently, European jurisprudence seeks to maintain a careful balance between public security and civil liberties.

Unlike purely security-oriented models, the European approach focuses on protecting human dignity and informational self-determination. Data protection regulations such as the General Data Protection Regulation (GDPR) further strengthen privacy rights by imposing strict obligations concerning data collection, processing, and retention.

[23] Saunders v. United Kingdom, 1996-VI Eur. Ct. H.R. 2044 (holding that privilege against self-incrimination is not absolute under ECHR framework).

The European framework demonstrates the importance of integrating human rights principles into digital investigation laws and constitutional interpretation.

### 6.4. A COMPARATIVE ANALYSIS

Comparative constitutional analysis reveals that no uniform global approach exists regarding compelled decryption and digital self-incrimination. Different jurisdictions prioritize different constitutional values depending upon their legal traditions and political frameworks. Nevertheless, several important lessons emerge for India.

First, the distinction between passwords and biometric identifiers requires careful constitutional scrutiny. Passwords involve cognitive disclosure and are more closely associated with testimonial communication, whereas biometrics are generally treated as physical evidence. However, the digital consequences of biometric unlocking cannot be ignored because such access may expose vast amounts of private information.

Second, any framework governing compelled decryption must incorporate safeguards relating to proportionality, necessity, and judicial oversight. Broad and unrestricted investigative powers may undermine constitutional liberties and privacy rights.

Third, India must acknowledge the increasing significance of informational privacy in the digital era. The recognition of privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India offers a strong constitutional foundation for establishing comprehensive digital rights protections.

Finally, Indian constitutional jurisprudence should evolve toward a technology-sensitive interpretation of Article 20(3) that balances effective law enforcement with the preservation of dignity, autonomy, and cognitive liberty. Comparative experiences demonstrate that constitutional democracies must continuously adapt legal principles to address emerging technological challenges while safeguarding fundamental rights.

## 7. EMERGING TECHNOLOGIES AND FUTURE CHALLENGES

Rapid technological advancements are continuously reshaping the relationship between constitutional rights and State investigative powers. Technologies such as artificial intelligence, facial recognition systems, cloud computing, mass surveillance mechanisms, and

advanced encryption tools have significantly expanded the capacity of governments to collect, analyze, and monitor digital information. Although these technologies may strengthen law enforcement efficiency and national security, they also give rise to serious concerns regarding privacy, individual autonomy, and the constitutional protection against self-incrimination under Article 20(3) of the Constitution of India.

The digital age therefore requires courts and legislatures to reassess traditional constitutional doctrines in light of emerging technological realities.

### 7.1 Artificial Intelligence and Predictive Policing

AI is increasingly used in criminal investigations for predictive policing, data analysis, and profiling, improving efficiency but raising concerns about privacy, discrimination, and procedural fairness. Continuous surveillance and algorithmic profiling may indirectly infringe protections under the Indian Constitution, including Article 20(3), while the absence of clear legal safeguards risks threats to individual liberty and due process.

### 7.2 Facial Recognition Systems

Facial recognition technology enables mass surveillance through biometric data collection, often without consent, raising serious concerns about privacy, anonymity, and personal autonomy. Its use in public spaces and criminal investigations risks constant monitoring of citizens, potentially undermining constitutional protections under Article 21, including dignity and liberty.

### 7.3 Cloud Computing and Cross-Border Data Access

Cloud computing stores data across global servers, making criminal investigations increasingly cross-border and legally complex. Access to such data can conflict with privacy and sovereignty laws, while raising concerns under Article 20(3) due to compelled disclosure of digital information. The lack of clear international standards creates legal uncertainty, forcing a balance between effective investigations and constitutional rights[24].

[24] Christopher Kuner, Transborder Data Flows and Data Privacy Law, 18 Int'l Data Privacy L. 201 (2018).

### 7.4 Digital Surveillance and National Security

National security concerns have expanded State surveillance powers through tools like communication interception, metadata tracking, and spyware for counterterrorism and public order. While justified, excessive surveillance can threaten privacy, free expression, and democratic freedoms, requiring proportionality and oversight[25]. Such practices may also implicate Article 20(3), while the *Justice K.S. Puttaswamy v. Union of India* ruling reinforces privacy as a fundamental right limiting State action.

### 7.5 Quantum Encryption and Future Investigations

Emerging technologies like quantum computing could reshape digital security by strengthening encryption while also enabling powerful decryption capabilities that challenge privacy protections. This shift may intensify tensions between State investigative powers and individual rights, especially regarding access to secure data and AI-generated evidence. As existing doctrines may be insufficient, Indian constitutional law will need to evolve to protect fundamental rights in a rapidly advancing technological landscape.

## 8. CRITICAL ANALYSIS

Indian constitutional law on self-incrimination under Article 20(3), shaped by decisions like *State of Bombay v. Kathi Kalu Oghad*, was developed in a traditional evidentiary framework and does not fully address present-day digital realities such as encrypted devices, biometric unlocking, compelled password disclosure, and extensive electronic data searches. These technological changes have weakened the clear divide between physical and testimonial evidence, making it difficult to define when digital compulsion becomes constitutionally impermissible. In the absence of a detailed statutory framework, investigative practices risk becoming inconsistent, raising concerns about privacy, autonomy, and procedural fairness under Article 21. Although effective digital tools are necessary for tackling cybercrime and safeguarding national security, such powers must remain proportionate, justified, and subject to judicial oversight, consistent with the principles laid down in *Justice K.S. Puttaswamy v. Union of India*. Accordingly, there is a pressing need to modernize legal standards to ensure a

[25] PUCL v. Union of India, (1997) 1 S.C.C. 301 (India) (telephone tapping safeguards); Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).

balanced protection of investigative needs and digital constitutional rights.

## 9. RECOMMENDATIONS

9.1. Indian constitutional law on self-incrimination under Article 20(3), developed in cases like *State of Bombay v. Kathi Kalu Oghad*, is based on traditional notions of physical and testimonial evidence and does not fully address modern digital realities.

9.2. Emerging issues such as encrypted devices, biometric unlocking, compelled password disclosure, and large-scale electronic data extraction have blurred the distinction between physical and testimonial evidence.

9.3. The lack of a clear statutory and constitutional framework creates uncertainty in regulating digital searches and investigative procedures.

9.4. This gap increases the risk of excessive surveillance, arbitrary data access, and potential violations of privacy and autonomy under Article 21.

9.5. Although law enforcement requires effective digital tools to address cybercrime and national security concerns, such powers must remain proportionate, necessary, and subject to judicial oversight.

9.6. The principles laid down in *Justice K.S. Puttaswamy v. Union of India* reinforce the need to protect informational privacy as a fundamental right.

9.7. Therefore, Indian law needs updated standards to balance investigative efficiency with strong safeguards for digital autonomy and constitutional right.

## 10. CONCLUSION

The emergence of digital technologies has fundamentally transformed the constitutional understanding of self-incrimination, privacy, and State investigative powers. Traditional legal distinctions between testimonial and physical evidence are increasingly inadequate in addressing modern digital realities.

This study demonstrates that passwords and encryption keys involve cognitive disclosure and therefore fall within the protective scope of Article 20(3) of the Constitution of India. Biometric

authentication methods, although generally classified as physical evidence, raise significant constitutional concerns because they provide access to extensive private digital information.

The jurisprudence developed in cases such as State of Bombay v. Kathi Kalu Oghad, Selvi v. State of Karnataka, and Justice K.S. Puttaswamy v. Union of India provides an important constitutional foundation for protecting cognitive liberty, mental privacy, and informational autonomy in the digital age.

However, Indian jurisprudence remains underdeveloped in relation to compelled decryption, digital surveillance, and emerging technologies. The absence of comprehensive legislative safeguards creates significant constitutional uncertainty and risks undermining fundamental rights.

A technology-sensitive interpretation of Article 20(3) is therefore essential. Courts and legislatures must develop constitutional standards that balance investigative efficiency and national security with the preservation of privacy, dignity, and individual liberty.

The future trajectory of digital constitutionalism in India will depend upon the ability of constitutional institutions to adapt traditional legal principles to rapidly evolving technological realities. In a democratic society governed by the rule of law, technological advancement must remain subject to constitutional limitations designed to preserve human dignity and fundamental freedoms.

## 11. REFERENCES

### 11.1. Cases


- Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).
- Selvi v. State of Karnataka, (2010) 7 S.C.C. 263 (India).
- Nandini Satpathy v. P.L. Dani, (1978) 2 S.C.C. 424 (India).
- State of Bombay v. Kathi Kalu Oghad, A.I.R. 1961 S.C. 1808 (India).
- M.P. Sharma v. Satish Chandra, A.I.R. 1954 S.C. 300 (India).
- People's Union for Civil Liberties v. Union of India, (1997) 1 S.C.C. 301 (India).
- Fisher v. United States, 425 U.S. 391 (1976).
- Doe v. United States, 487 U.S. 201 (1988).
- United States v. Hubbell, 530 U.S. 27 (2000).
- In re Grand Jury Subpoena Duces Tecum, 670 F.3d 1335 (11th Cir. 2012).
- United States v. Kirschner, 823 F. Supp. 2d 665 (E.D. Mich. 2010).
- United States v. Wade, 388 U.S. 218 (1967).


### 11.2. Statutes & Constitutional Provisions


- Constitution of India, art. 20(3), art. 21.
- U.S. Const. amend. V.
- Regulation of Investigatory Powers Act 2000 (UK).
- European Convention on Human Rights, arts. 6, 8.
- Charter of Fundamental Rights of the European Union, arts. 7, 8.

## 11.3. Journal Articles


- hanmuga Sundaram & P.R.L. Rajavenkatesan, Protection against Self-Incrimination – Principles and Practice: A Comparative Analysis, Indian J. L. & Just. (Univ. of N. Bengal, 2022), available at https://ir.nbu.ac.in.

- Suyash Sarvankar, Key Disclosure Laws and the Right Against Self-Incrimination in India, SSRN (2017), https://ssrn.com/abstract=3063854 (arguing that compelled decryption may violate Art. 20(3)).

- Akarsh Singh, Analysis of Right Against Self-Incrimination Under Article 20(3) of the Constitution, Indian J. L. & Legal Res., Vol. 3, Issue 1 (2021), https://www.ijllr.com (open access journal).

- Abhinav Sekhri, The Right Against Self-Incrimination in India: The Compelling Case of Kathi Kalu Oghad, Indian L. Rev. 3(2) 180–211 (2019), https://doi.org/10.1080/24730580.2019.1646963 (open access via publisher link/archived versions).

- Shrabasti Sarkar, Right to Silence in India – An Analysis of Its Scope, Use and Efficacy, J. Legal Stud. & Res. (2021), https://journal.thelawbrigade.com (open access journal).

- Naman Jain & Mayank Singh, The Evolving Ecosystem of Predatory Journals: A Case Study in Indian Perspective, arXiv (2019), https://arxiv.org/abs/1906.06856