THE RIGHT AGAINST SELF-INCRIMINATION IN THE DIGITAL AGE: A COMPARATIVE LEGAL ANALYSIS OF INDIA AND THE UNITED STATES

Annpurna, Research Scholar, School of Law and Governance, Central University of South Bihar, Gaya [1]

ABSTRACT

One of the strongest safeguards of constitutional liberty is the right against self-incrimination, which protect individuals from being forced to give evidence again themselves. Originating from the rejection of the English Star Chamber's coercive methods in the seventeenth century, it has since been made constitutional in both India and the United States. No one shall "be compelled in any criminal case to be a witness against himself," according to the U.S. Fifth Amendment, while Article 20(3) of the Indian Constitution guarantees that "no person accused of any offence shall be forced to be a witness against himself." The right against self-incrimination in India and the US is compared in this paper, with an emphasis on the difficulties brought about by the digital age. It explores the privilege's constitutional and historical underpinnings, looks at significant court rulings, such as Boyd, Miranda, Hubbell, and Riley in the United States and M.P. Sharma, Kathi Kalu Oghad, Selvi, and Puttaswamy in India, and assesses how legislatures and courts have modified the privilege to fit novel investigative situations. Particular focus is placed on areas where traditional testimonial-physical distinctions have not worked well, such as forced password disclosure, biometric authentication, and decryption of encrypted data.

Keywords: Self-incrimination, Digital age, Article 20(3), Fifth Amendment, Privacy rights

[1] Research Scholar, School of Law and Governance, Central University of South Bihar, Gaya

Introduction

"Technology is a queer thing. It brings you great gifts with one hand, and it stabs you in the back with the other." – C.P. Snow[2]

A fundamental safeguard against arbitrary state power has long been the right against self-incrimination. It upholds human dignity and the presumption of innocence by shielding people from being forced to produce evidence that could be used against them. Its origins can be traced to the English rejection of the Star Chamber's coercive tactics, which included forcing accused individuals to take the ex-officio oath and confess under threat of punishment.[3] When forced confessions were outlawed in the seventeenth century, it was acknowledged that they were incompatible with the rule of law. In the United States, this principle was constitutionalized in the Fifth Amendment of 1791,[4] which provides that no person "shall be compelled in any criminal case to be a witness against himself." Its broad and unqualified phrasing has allowed the Supreme Court to develop expansive doctrines such as Miranda rights, the act of production principle, and the foregone conclusion test, which adapt the privilege to varied contexts ranging from custodial interrogation to compelled production of documents. In India, the principle was incorporated into Article 20(3) of the Constitution of 1950,[5] which states: "No person accused of any offence shall be compelled to be a witness against himself." Although narrower in scope, applying only to individuals formally accused of crimes- Article 20(3) has been interpreted in landmark cases such as M.P. Sharma v. Satish Chandra,[6] State of Bombay v. Kathi Kalu Oghad,[7] Selvi v. State of Karnataka,[8] and Justice K.S. Puttaswamy v. Union of India.[9] These doctrines have become more complex than ever with the advent of the digital age. Large volumes of personal, financial, and professional data are now stored on smart phones, laptops, cloud storage, encrypted communications, and biometric authentication. There are new concerns regarding whether forcing an accused person to divulge a password, grant biometric access, or decrypt encrypted files qualifies as testimonial compulsion. In India, the Criminal Procedure (Identification) Act of 2022 and Section 69 of the Information Technology Act of

[2] C.P. Snow, Technology…is a queer thing. It brings you great gifts with one hand, and it stabs you in the back with the other, N.Y. Times, Mar. 15, 1971.
[3] Mike Redmayne, Rethinking the Privilege Against Self-Incrimination, 27 Oxford J. Legal Stud. 209 (2007).
[4] U.S. Const. amend. V.
[5] Constitution of India, art. 20(3).
[6] M.P. Sharma v. Satish Chandra, AIR 1954 SC 300.
[7] State of Bombay v. Kathi Kalu Oghad, AIR 1961 SC 1808.
[8] Selvi v. State of Karnataka, (2010) 7 SCC 263.
[9] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

2000 both increase state authority in ways that go against Article 20(3). Similar conflicts between constitutional rights and law enforcement requirements are highlighted in the US by the use of laws like the Electronic Communications Privacy Act (ECPA) and the All Writs Act, as well as case law pertaining to forced decryption.[10]

Historical and Constitutional Foundations of the Right against Self-Incrimination

In the wake of coercive judicial practices, the right against self-incrimination was established in seventeenth-century England. People were essentially forced to confess by the Star Chamber and High Commission, which forced them to take oaths and respond to questions under threat of punishment. The idea that no one should be forced to incriminate themselves developed in English common law when these tribunals were abolished in 1641 due to their abuses.[11] This concept was later incorporated into the US Constitution. "No person shall be compelled in any criminal case to be a witness against himself," according to the Fifth Amendment of 1791. Inspired by English history, the framers aimed to prevent the government from going too far. One of the strongest constitutional protections in American law was established when the U.S. Supreme Court gradually expanded the privilege beyond trials to include compelled acts of production, grand jury proceedings, and custodial interrogations.[12] Article 20(3) of the Indian Constitution of 1950, which states that "no person accused of any offence shall be compelled to be a witness against himself," incorporates the privilege. Article 20(3), in contrast to the Fifth Amendment, only applies to those who are formally accused of crimes and only during criminal proceedings. Nonetheless, the framers' concern about police abuses and their desire to offer safeguards in line with democratic principles are reflected in its inclusion. The privilege has many reasons for being, including upholding the presumption of innocence, preserving dignity by avoiding forced confessions, promoting fairness by discouraging coercion, and, more and more in the digital age, protecting privacy.[13]

Judicial Interpretation and Legislative Framework in India

Judicial Precedent

[10] Electronic Communications Privacy Act: Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).
[11] John H. Langbein, The Historical Origins of the Privilege Against Self-Incrimination, 21 J. L. & Crim. 104 (1977).
[12] Malloy v. Hogan, 378 U.S. 1 (1964).
[13] Leonard W. Levy, The Right Against Self-Incrimination: History and Judicial History, 84 Pol. Sci. Q. 1 (1969) (Oxford Univ. Press).

The first significant interpretation occurred in M.P. Sharma v. Satish Chandra,[14] where an eight-judge panel determined that since there was no coerced testimony involved, the search and seizure of documents did not violate Article 20(3). The Court emphasized that testimonial compulsion is the only thing that the privilege guards against.

The Court clarified it in State of Bombay v. Kathi Kalu Oghad[15] that handwriting, fingerprints, and photos are not testimonial because they don't require mental abilities.[i] The Court clarified that in order to testify, one must use their intellect to convey knowledge. The testimonial-physical dichotomy was solidified by this ruling.

However, the Court expanded the application of Article 20(3) in Nandini Satpathy v. P.L. Dani.[16] According to Justice Krishna Iyer, in situations where there is a legitimate fear of self-incrimination, even suspects cannot be forced to answer questions. The Court underlined that the privilege is a protection of human rights and not a technicality.

The court invalidated mandatory polygraph, brain mapping, and narco-analysis tests in Selvi v. State of Karnataka.[17] It reasoned that such methods violated both Article 20(3) and Article 21 because they involuntarily extracted testimonial knowledge. Selvi made a significant connection between mental privacy and self-incrimination.

Last but not least, privacy was acknowledged as a fundamental right in Justice K.S. Puttaswamy v. Union of India,[18] which based it on liberty and dignity. Puttaswamy supports claims that forced digital disclosures implicate both self-incrimination and privacy rights, despite the fact that it is not an Article 20(3)[19] case.

Legislative Framework

The situation made harder by the legal framework of India. In the interest of public order, security, or sovereignty, the government may require the decryption of digital data under Section 69 of the Information Technology Act of 2000.[20] Prison time is the penalty for

[14] Supra 6 at 2.
[15] Supra 7 at 2.
[16] Nandini Satpathy v. P.L. Dani, AIR 1978 SC 1025.
[17] Supra 8 at 2.
[18] Supra 9 at 2.
[19] Supra 5 at 2.
[20] Information Technology Act, No. 21 of 2000.

noncompliance. Critics contend that this clause violates Article 20(3) because passwords and key require mental knowledge.

The Criminal Procedure (Identification) Act of 2022,[21] permits the taking of physical and biometric measurements from individuals who have been arrested or accused. Although it is justified as helping with identification, using forced fingerprint or iris scans on smart phones raises questions about self-incrimination. Puttaswamy says that privacy-based scrutiny may restrict the law's application, but judicial challenges are still pending.

Judicial Interpretation and Legislative Framework in the United States

Judicial Precedent

In the case of Boyd v. United States,[22] the Court ruled that forced production of private documents was unconstitutional, connecting self-incrimination to privacy. Boyd established the groundwork for acknowledging acts of production as testimonial, even though it was later narrowed.

The Court ruled in Miranda v. Arizona,[23] that police must advise suspects of their rights to remain silent and to have legal representation while being questioned. The Fifth Amendment was practically operationalized by this doctrine.

In the case of Doe v. United States,[24] the act of production doctrine was refined when it was decided that signing a consent directive for bank records was not testimonial. However, forced document production was deemed testimonial in United States v. Hubbell[25] because it relied on the accused's mind to demonstrate the documents' existence and authenticity.

The Eleventh Circuit ruled in In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011,[26] that forced hard drive decryption was unconstitutional because it necessitated the disclosure of mental knowledge. In contrast, the District of Colorado allowed compulsion in United States

[21] Criminal Procedure (Identification) Act, No. 11 of 2022, India.
[22] Boyd v. United States, 116 U.S. 616 (1886).
[23] Miranda v. Arizona, 384 U.S. 436 (1966).
[24]Doe v. United States, 487 U.S. 201 (1988).
[25]United States v. Hubbell, 530 U.S. 27 (2000).
[26] In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335 (11th Cir. 2012).

v. Fricosu[27] on the grounds that the government was already aware of the contents, citing the foregone conclusion doctrine.

Legislative Framework

A colonial-era law known as the All Writs[28] Act has been used to force businesses such as Apple to help law enforcement crack encrypted devices. Opponents contend that applying this 1789 law to contemporary encryption violates constitutional rights.[29]

Government access to digital communications is governed by the Electronic Communications Privacy Act (ECPA), 1986.[30] Although it is mainly about surveillance, when people are forced to grant access, it crosses over into self-incrimination. However, the Fifth Amendment serves as the main defense because the ECPA does not provide specific protections for testimonial compulsion.

Digital Age Challenges

Passwords

Passwords are undoubtedly testimonies. Forcing disclosure would be against Article 20(3) in India. Despite the lack of a Supreme Court precedent, Kathi Kalu Oghad's reasoning points to robust protection.

Courts in the United States support this strategy. The Eleventh Circuit ruled in In re Grand Jury Subpoena Duces Tecum[31] that forced password disclosure was unconstitutional because it made the accused divulge their innermost thoughts.

Biometrics

Biometrics make things more difficult. In India, forced fingerprints are not covered by Article 20(3) since they are typically regarded as tangible evidence. However, this reasoning breaks down when it comes to smart phones because biometric unlocking reveals a ton of data.

[27] United States v. Fricosu, 841 F. Supp. 2d 1232 (D. Colo. 2012).
[28] All Writs Act, 28 U.S.C. 1651.
[29] Supra 4 at 2 .
[30] Electronic Communications Privacy Act of 1986, 18 U.S.C. 510–2523.
[31] Supra 26 at 5.

Puttaswamy supports claims that biometric coercion infringes on privacy.

Courts in the United States typically view biometrics as non-testimonial and physical. However, a district court declined to require biometric unlocking in In re Application for a Search Warrant, acknowledging that this kind of compulsion was functionally testimonial.

Encryption and Decryption

The most significant hurdle is encryption. Even for non-accused individuals, compelled decryption is permitted in India under Section 69 of the IT Act. One could argue that this clause violates both Article 20(3) and Article 21 because decryption necessitates mental knowledge.

The foregone conclusion doctrine is applied by courts in the United States. Because the government was already aware of the contents, forced decryption was permitted in In re Boucher. Compulsion was allowed in Fricosu for similar reasons. The Supreme Court emphasized in Doe, nevertheless, that testimonial acts cannot be forced without prior knowledge. Therefore, if the doctrine is applied too widely, it could undermine the Fifth Amendment.

Comparative Analysis

The fundamental idea that physical evidence may be coerced but testimonial coercion is forbidden is acknowledged by both India and the United States. Both categorize biometrics as physical and passwords as testimonial. However, both systems struggle to apply this framework to digital devices, which hold vast amounts of personal information.

The Fifth Amendment has a more expansive reach, encompassing all individuals and being applicable in civil, administrative, and criminal proceedings. In contrast, Article 20(3) is more limited and only applies to those who are accused in criminal cases. While Indian courts continue to adhere to strict classifications from Kathi Kalu Oghad, American courts have created flexible doctrines such as Miranda, act of production, and foregone outcome.

These distinctions are reflected in legislation. A broad state power that may be unconstitutional is represented by Section 69 of the Indian IT Act. Similar conflicts arise in the United States when the All Writs Act and ECPA are used, although they are lessened by more stringent judicial supervision.

However, India's Puttaswamy recognition of privacy offers a revolutionary framework that might be more protective than American functionalism. On the other hand, U.S. jurisprudence recognizes acts of production and decryption as potentially testimonial, providing India with lessons in functional analysis. Every jurisdiction can share knowledge with the others.

Way Forward

The privilege against self-incrimination must evolve to remain meaningful in the digital age. The testimonial/physical dichotomy, while once adequate, is increasingly unworkable. Biometric unlocking of smart phones, though formally "physical," functionally reveals testimonial information by granting access to private data. Courts must move beyond rigid categories to functional analysis.

In India, Section 69 of the IT Act should be amended to comply with Article 20(3) and Article 21. Judicial oversight must be mandatory for decryption orders, with proportionality and necessity tests applied. Courts should reinterpret Kathi Kalu Oghad in light of Selvi and Puttaswamy, recognizing that digital compulsion implicates both self-incrimination and privacy.

In the U.S., the foregone conclusion doctrine must be narrowed. Courts should require that the government's knowledge of evidence be specific and comprehensive before allowing compulsion. The All Writs Act should not be stretched to modern encryption disputes; Congress should enact updated legislation balancing security with constitutional rights.

Globally, both jurisdictions should adopt safeguards such as limits on scope (access only to relevant files), derivative use restrictions, and data minimization. Such reforms would harmonize their laws with international human rights standards under Article 8 of the European Convention on Human Rights.

Ultimately, the privilege is not a relic but a living guarantee. In an era of pervasive surveillance and data-driven policing, it is indispensable. Its continued vitality depends on the willingness of courts and legislatures to reinterpret and reform it in line with technological realities.

Conclusion

Born out of opposition to the Star Chamber's abuses, the right against self-incrimination has

stood as a constitutional protection for centuries. It was enshrined in Article 20(3) of the Indian Constitution and the Fifth Amendment of the United States Constitution, both of which reflected commitments to liberty, justice, and dignity. However, this age-old assurance has been put to the test in the digital age. The traditional testimonial/physical distinction has become more complex due to smart phones, encrypted communications, and biometric authentication, revealing the shortcomings of outdated doctrines. In contrast to India's Article 20(3), which is more restrictive, the United States provides more comprehensive protections that apply to all individuals and in all situations. Indian courts have been more inflexible than U.S. courts, which have developed flexible doctrines like act of production and foregone conclusion. However, the framework that India's Puttaswamy recognition of privacy offers may go beyond US jurisprudence in preserving informational autonomy. The way forward is obvious: both jurisdictions need to change. Courts must use contextual strategies that consider the practical effects of coercion. Legislators must implement measures to prevent the abuse of required digital disclosures. These reforms ought to be guided by international human rights standards. In the end, the right against self-incrimination is a substantive guarantee of liberty rather than a formality. Its survival in the digital age hinges on astute legislative reform and audacious judicial reasoning. It will remain a bulwark of freedom if it is maintained and modified. If ignored, it runs the risk of deteriorating just when people are most at risk from the growing influence of the digital state.