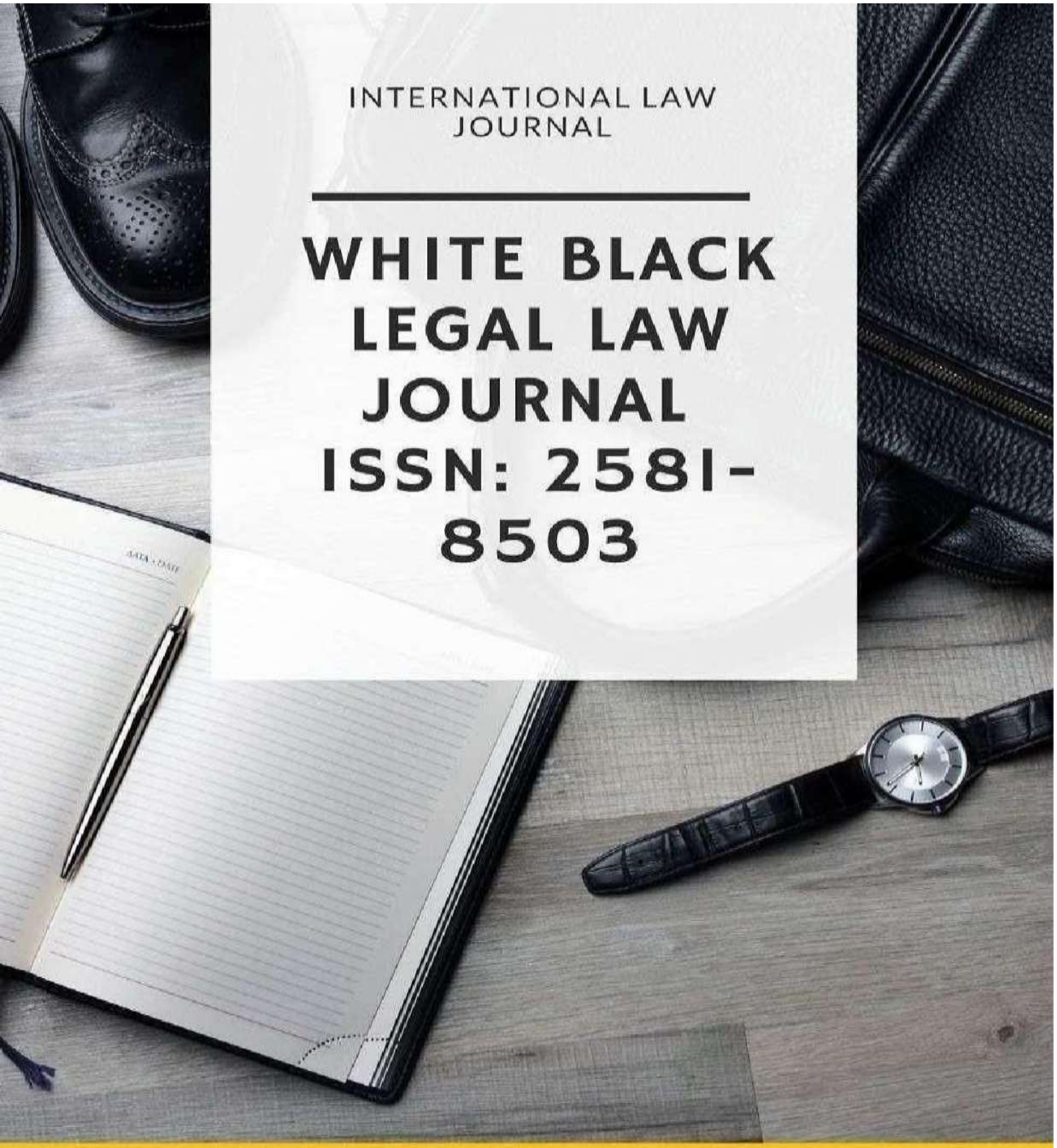

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

SELF-INCRIMINATION IN THE DIGITAL AGE: A STUDY OF PASSWORDS, BIOMETRICS AND ARTICLE 20(3)

AUTHORED BY - ARPITA SINGH & ASTHA SRIVASTAVA

Abstract

The rapid digitization of personal and professional life has fundamentally transformed the nature of evidence in criminal investigations. Traditional doctrines of self-incrimination, rooted in physical and testimonial evidence, are increasingly challenged by digital realities such as encrypted devices, passwords, and biometric authentication systems. This paper examines the scope and applicability of Article 20{3) of the Constitution of India in the context of digital evidence, specifically focusing on whether compelling an accused to disclose passwords or provide biometric access violates the right against self-incrimination. Through an analysis of constitutional provisions, judicial precedents, comparative jurisprudence, and evolving technological frameworks, the paper argues that while biometric data may fall outside the protective ambit of Article 20{3), compelled disclosure of passwords raises serious constitutional concerns. The paper concludes by recommending a nuanced legal framework balancing individual rights with legitimate investigative needs.

1. Introduction

The doctrine against self-incrimination is a cornerstone of criminal jurisprudence, designed to protect individuals from coercive state practices. In India, this principle is enshrined under Article 20(3) of the Constitution, which states: "No person accused of any offence shall be compelled to be a witness against himself."

Historically, this protection was understood in the context of oral testimony and physical evidence. However, the emergence of digital technologies-particularly smartphones, encrypted communication, and biometric authentication-has created new complexities. Today, crucial evidence often resides in password-protected devices or encrypted digital platforms, raising an important question: Can the state compel an accused to unlock digital devices without violating constitutional protections?

This paper seeks to explore this question by examining:

- The scope of Article 20(3)
- The distinction between testimonial and physical evidence
- Judicial interpretations in India and abroad
- The legal status of passwords versus biometrics

2. Constitutional Framework: Article 20(3)

Article 20(3) provides protection against self-incrimination and applies when three conditions are satisfied:

1. The person is accused of an offence
2. There is compulsion
3. The compulsion results in self-incriminating testimony

The landmark judgment in M.P. Sharma v. Satish Chandra (1954) initially adopted a broad interpretation, equating self-incrimination with protection against search and seizure.
However, this view was later refined.

In State of Bombay v. Kathi Kalu Oghad (1961), the Supreme Court clarified that

- The protection applies only to testimonial compulsion
- It does not extend to physical evidence, such as fingerprints or handwriting samples

This distinction between testimonial and physical evidence forms the backbone of the modern understanding of Article 20(3).

3. Understanding "Testimonial Compulsion"

The concept of testimonial compulsion is central to determining whether a particular act violates Article 20(3).

3.1 Testimonial Evidence

Testimonial evidence involves:

- Personal knowledge
- Mental processes
- Communication of facts

Examples:

- Oral statements
- Written confessions
- Disclosure of passwords

3.2 Physical Evidence

Physical evidence refers to:

- Bodily characteristics
- Non-communicative acts

Examples:

- Fingerprints
- DNA samples
- Voice samples

The Supreme Court has consistently held that compelling physical evidence does not violate Article 20(3) because it does not involve the "mental faculties" of the accused.

4. Digital Evidence and the Challenge to Traditional Doctrine

Digital evidence blurs the line between testimonial and physical evidence. Unlike traditional objects, digital devices:

- Store vast amounts of personal data
- Are often encrypted

- Require active cooperation to access

This raises a fundamental issue:
Is unlocking a device a physical act or a testimonial one?

5. Passwords vs Biometrics: A Legal Distinction

5.1 Passwords: Testimonial in Nature

Passwords are:

- Stored in the mind of the user
- Products of cognition and memory

Compelling a person to reveal a password requires:

- Disclosure of knowledge
- Use of mental faculties

Therefore, it is widely argued that : Forcing disclosure of passwords amounts to testimonial compulsion
This aligns with the reasoning in:

Selvi v. State of Karnataka (2010), where the Court held that involuntary techniques like narco-analysis violate Article 20(3) because they extract personal knowledge.

5.2 Biometrics: Physical Evidence

Biometric data includes:

- Fingerprints
- Facial recognition
- Iris scans

These are:

- Physical attributes

- Not dependent on mental processes
- Courts have generally treated biometrics as analogous to fingerprints.

Compelling biometric access is often considered constitutionally permissible

6. Judicial Developments in India

6.1 Selvi v. State of Karnataka {2010)

This case is pivotal in understanding self-incrimination in modern contexts. The Supreme Court held that:

- Techniques like narco-analysis, polygraph tests, and brain mapping violate Article 20(3)
- They involve involuntary extraction of personal knowledge

The Court emphasized:

- The importance of mental privacy
- The distinction between physical and testimonial evidence

6.2 Application to Digital Context

Although Indian courts have not yet definitively ruled on passwords vs biometrics, principles from existing cases suggest:

Passwords Protected (testimonial) Biometrics Not protected (physical)

7. Comparative Jurisprudence

7.1 United States

The Fifth Amendment provides protection against self-incrimination.

Passwords

US courts have generally held that:

- Compelling disclosure of passwords violates the Fifth Amendment

Example:

United States v. Doe (2012): Passwords are testimonial

Biometrics

Courts are divided:

Some allow compelled fingerprint unlocking Others recognize privacy concerns

7.2 United Kingdom

Under the Regulation of Investigatory Powers Act (RIPA): Authorities can compel disclosure of encryption keys Refusal can lead to criminal penalties

This reflects a more state-centric approach.

8. Privacy and the Puttaswamy Judgment

In Justice K.S. Puttaswamy v. Union of India (2017), the Supreme Court recognized: Right to privacy as a fundamental right under Article 21

This has significant implications:

- Digital data is deeply personal
- Accessing it involves privacy intrusion

Therefore, any compulsion must satisfy:

- Legality
- Necessity
- Proportionality

9. Interplay Between Article 20(3) and Article 21

The digital age requires a combined reading of:

- Article 20(3): Protection against self-incrimination
- Article 21: Right to privacy

Forcing access to digital devices may:

- Violate mental autonomy
- Expose private life details

Thus, even if biometric compulsion is allowed under Article 20(3), it may still be challenged under Article 21.

10. Emerging Challenges

10.1 Encryption

Strong encryption prevents unauthorized access, making cooperation essential.

10.2 Cloud Storage

Data is no longer confined to devices, complicating jurisdiction and access.

10.3 Artificial Intelligence

Al-based surveillance raises concerns about indirect self-incrimination.

11. Need for Legal Reform

India currently lacks a clear statutory framework addressing:

- Digital self-incrimination
- Password disclosure
- Biometric access
- Suggested Reforms
- Clear legislative guidelines on digital evidence
- Judicial safeguards for compelled access
- Distinction between passwords and biometrics
- Oversight mechanisms to prevent misuse

12. Critical Analysis

The distinction between passwords and biometrics, though widely accepted, is not without criticism.

12.1 Problems with Biometric Exception

- Biometrics are deeply personal
- Cannot be changed like passwords

- Forced use may violate dignity

12.2 Expanding Scope of Testimonial Evidence

Some scholars argue that:

Any act requiring cooperation should be protected Digital access inherently reveals personal knowledge

13. Conclusion

The right against self-incrimination under Article 20(3) of the Constitution of India, historically rooted in the protection of personal liberty and human dignity, faces unprecedented challenges in the digital age. As technology transforms the nature of evidence, the traditional distinction between testimonial and physical evidence-central to constitutional interpretation-becomes increasingly strained. Digital devices today are not mere physical objects; they are repositories of an individual's thoughts, communications, associations, and private life.

This paper has demonstrated that compelled disclosure of passwords fundamentally differs from the extraction of physical evidence. Passwords are products of cognition, memory, and knowledge, and their disclosure necessarily involves the use of mental faculties. Therefore, compelling an accused to reveal a password squarely falls within the ambit of "testimonial compulsion" and must be protected under Article 20(3). Such compulsion not only risks self-incrimination but also undermines the broader principle of mental autonomy that the Constitution seeks to preserve.

In contrast, biometric identifiers such as fingerprints, facial recognition, and iris scans have been traditionally classified as physical evidence, and their compelled use has generally been considered constitutionally permissible. However, this paper argues that even this distinction requires reconsideration. Unlike traditional physical evidence, biometric data serves as a gateway to vast amounts of personal digital information. Compelling biometric access does not merely involve identification-it enables state intrusion into the most intimate spheres of an individual's private life. Consequently, while biometrics may fall outside the strict scope of Article 20(3), their use must be carefully scrutinized under Article 21, particularly in light of the right to privacy affirmed in Justice K.S. Puttaswamy

(Retd.) v. Union of India.

The convergence of Articles 20(3) and 21 necessitates a more holistic constitutional approach. Any state action compelling access to digital devices must satisfy the tests of legality, necessity, and proportionality. Blanket or coercive measures risk eroding fundamental rights and enabling excessive surveillance. At the same time, the legitimate interests of law enforcement in accessing digital evidence cannot be ignored, especially in an era where crimes are increasingly facilitated through encrypted platforms.

Therefore, the need of the hour is a nuanced and forward-looking legal framework. Judicial interpretation must evolve to recognize the qualitative differences between digital and traditional evidence, while the legislature must step in to provide clear guidelines governing compelled decryption and digital access. Safeguards such as prior judicial authorization, limited scope of access, and strict oversight mechanisms are essential to prevent misuse.

Ultimately, the balance between individual liberty and state power must tilt in favor of constitutional morality. The right against self-incrimination is not merely a procedural safeguard-it is a reflection of the fundamental principle that the state must prove its case without forcing individuals to contribute to their own conviction. In the digital age, preserving this principle is not only a constitutional necessity but also a moral imperative.

Bibliography

Cases

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

State of Bombay v. Kathi Kalu Oghad, AIR 1961 SC 1808. Selvi v. State of Karnataka, (201O) 7 sec 263.

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

United States v. Doe, 670 F.3d 1335 {11th Cir. 2012).

Statutes

Constitution of India, arts. 20(3), 21. Information Technology Act, 2000.

Indian Evidence Act, 1872.

U.S. Const. amend. V.

Books & Articles

H.M. Seervai, Constitutional Law of India.

D.D. Basu, Introduction to the Constitution of India.

Orin S. Kerr, "The Fifth Amendment and Unlocking Encrypted Devices," 98 Tex. L. Rev. 767 {2020).

WHITE BLACK
LEGAL