PASSWORD DISCLOSURE AND DIGITAL DEVICE EXAMINATION UNDER INDIAN CYBER LAW: AN ANALYSIS OF SECTION 69 OF IT ACT AND THE BNSS, 2023

Ardra Ann Mathew, Sastra Deemed University

ABSTRACT

The increase in the use of encrypted digital devices during criminal investigations posed certain questions regarding the extent and boundaries of compulsory access followed by forensic analysis. In this connection, the issue that has been considered in the research paper concerns whether section 69 of the IT Act, 2000 can be read to require the accused to disclose the password, PIN number or the key for encryption or to authenticate the digital device using biometrics. The above-stated problem will be reviewed in relation to *Virendra Khanna v. State of Karnataka & CBI v. Mahesh Kumar Sharma & Ors.*

Furthermore, the paper discusses the requirements provided by the BNSS, 2023 (BNSS) in relation to the search, seizure, and forensic examination of the digital device. Although the BNSS includes certain requirements relating to the issues related to the examination of the digital evidence, the key objective of the paper is to evaluate whether the BNSS provides sufficient safeguards for collecting and storing non-crime-related information.

The research will be conducted in accordance with Art 20(3) and 21 of the constitution of India relating to compulsion to self-incriminate, right to privacy, information control, proportionality and a fair investigation process. Additionally, the study propose a five-factor test for assessing compelled digital access: the form of authentication and whether it communicates personal knowledge, the State's prior knowledge, the breadth of information exposed, the particularity of the access sought, and the availability of less intrusive means. The study employs Doctrinal Legal Research which examine the relationship between access to the device and search of its content.

Keywords: Digital forensics, Compelled device access, Section 69, Information Technology Act 2000, BNSS 2023, Password disclosure, Encryption key, Biometric Authentication, Self Incrimination.

I. INTRODUCTION

Recent examples like the case of *T. Prabhakar Rao v. State of Telangana* show that the extent of criminal investigations is increasingly going beyond the mere physical acquisition of digital devices and moving into the realm of access and forensics[1].In that case the Supreme Court, hearing an anticipatory bail petition, recorded the accused's undertaking, given through counsel, to reset his iCloud passwords in the presence of forensic experts. His counsel stated that he was not taking shelter under the right to privacy, and the Court did not decide any question under Article 20(3). In the case of a single smartphone, one can store messages, money, cloud credentials, and data from other people. Encryption and biometric authentication may limit access to the data despite the seizure of the device. This leads to an important question: at what point does the state's right to digital evidence end and personal privacy start?

There are different phases involved in digital investigation including seizure, access, extraction, examination, retention, and evidentiary use, and all of them are associated with different constitutional and procedural issues. It does not mean that the right to seize a device automatically gives the right for further access and examination.

The first problem is related to compulsory access in itself. The IT Act 2000 provides for interception , monitoring or decryption of information under Sec 69 of the Act while Section 69(3) provides for assistance by certain individuals for technical reasons[2], but it is quite different from compulsory access of accused for disclosing his password or biometric access[3]. Courts in India have handled this in an inconsistent manner in the cases of *Virendra Khanna,* where compulsory access for password and biometric access was allowed but not in case of *CBI v. Mahesh kumar sharma*[4]. Section 69(3) gets its backing from Section 69(4), which provides that the non-provision of the needed help would be punishable by a jail term not exceeding seven years, along with a monetary fine. This penalty makes the issue all the more crucial, because the real question is no longer whether investigators can demand access to the device, but whether the statutory provisions allow compulsory compliance from the accused at

[1] *T. Prabhakar Rao v. State of Telangana*, S.L.P. (Crl.) No. 7354 of 2025, order (India Oct. 14, 2025).
[2] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India), § 69(3) [hereinafter IT Act].
[3] *Virendra Khanna v. State of Karnataka*, W.P. No. 11759 of 2020, 2021 SCC OnLine Kar 5032, ¶¶ 14.7–14.8 (Kar. HC Mar. 12, 2021) (holding that furnishing a password or biometric key is akin to furnishing fingerprints or a specimen signature and does not attract Article 20(3)).
[4] *CBI v. Mahesh Kumar Sharma*, CBI No. 31/2021, 2022 SCC OnLine Dis Crt (Del) 48 (Dist. Ct. Del.) (relying on *Selvi v. State of Karnataka* in holding that an accused cannot be compelled to disclose the password of a seized computer system, as doing so would violate Article 20(3) of the Constitution and § 161(2) of the Code of Criminal Procedure, 1973).

all. That depends on whether the accused, as a person in charge of the device, can be treated as falling within Section 69(3), and on how such compulsion would interact with Article 20(3).

The second problem comes into light once the access is gained. There might be years of informations contained in the device that have nothing to do with the crime under investigation, and having lawful access doesn't necessarily make it right for the investigator to speculate about all the contents of the device, to recover any deleted information, to investigate any other files, or to take any third party informations. The BNSS, 2023 covers some parts of this process through Sections 94 (production of device), 105 (audio vedio recording of search and seizure), 176(3) (forensic expert's role), and 193(3)(i) (chain of custody report).[5].

Accordingly, this paper seeks an evaluation of whether Indian Law sufficiently regulates both the forced unlocking of the encrypted devices as well as forensic analysis of the content contained therein, without compromising the accused individuals right and of any third party. It examines the ambit of Section 69 of passwords, PIN's and biometrics, issues of self-incrimination from the point of view of judiciary, adequacy of legal provisions regulating the BNSS process of extraction, analysis, storage and use of evidence.

Based on the doctrinal approach, this paper will show how the law of India needs to clearly differentiate between the power of taking control of the device, the power of accessing the device and the power of examining, retaining and using the content within the device. All of which require a different justification both legally and constitutionally. The paper will introduce the application of a five factor test for the purpose of determining compelled digital access; all of which take into account various factors including the type of authentication mechanism used.

1.1. Background of study

As the use of technological devices becomes more common in criminal investigations, there have been shifts in the manner that evidence is accessed, collected, analyzed, and secured. A smartphone, computer, and other digital devices can have plenty of information stored in it, which can include personal messages, financial information, photos, professional email, geolocation information, and information regarding third parties. Passwords, PINs, encryption

[5]Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46, Acts of Parliament, 2023 (India), §§ 94, 105, 176(3), 193(3)(i) [hereinafter BNSS].

keys, and biometric information can limit the access of this kind of information even after seizing the device itself. The issue becomes a legal one since it deals with the ability of the investigators to use this kind of information to compel the accused to disclose digital evidence.

Section 69 of the IT Act, 2000 has laid down statutory provisions for interception, surveillance, and decryption of information using computer resources. But the issue whether the accused can be compelled under the law to reveal his password, PIN number, encryption keys, or biometric details cannot be solved from Section 69 of the IT Act. There have been many judicial decisions such as *Virendra Khanna* and *Mahesh Kumar Sharma* which have provided varied answers to the same issue.

It is important to realize that the legal problem does not end after accessing the device. While the BNSS, 2023 provides for the provisions on the production, searches, seizures, forensic examination, and retention of the electronic device, it does not adequately provide the scope of such extraction, examination, and retention post-seizure. It is, therefore, essential that this paper analyzes compulsory access and forensic examination as two independent yet related processes in view of Articles 20(3) and 21.

1.2. RESEARCH QUESTION

The fundamental research question that this paper attempts to address is whether the existing laws in India are adequate in regulating compelled access to an encrypted digital device and forensic examination thereof, while respecting the rights of the accused individual in accordance with the Constitution and the privacy of other parties.

The paper seeks to address four subordinate queries:

1. Does Sec 69 of ITAct, 2000 authorize or allow the authorization of the accused person to reveal his password/PIN, encryption key or biometric identity in order to have access to the electronic equipment?

2. Is the manner used in cases of Virendra Khanna v State of Karnataka and CBI v Mahesh Kumar Sharma proper balance between compelled digital access and right to refuse self-incrimination under Article 20(3)?

3. What framework should there be under BNSS,2023 regarding the process and legality

of post-seizure, extraction, examination, retention, and admissibility of evidence collected from the digital device.

4. What legislative measures are needed to protect any unrelated, privileged, and third party information that is obtained from the digital forensics analysis?

1.3. RESEARCH OBJECTIVES

- To examine whether Section 69 of the IT Act, 2000 authorises directing an accused to personally disclose a password, PIN or encryption key, or to authenticate a device biometrically.
- To analyse the judicial approaches in *Virendra Khanna* and *Mahesh Kumar Sharma* in light of Articles 20(3) and 21, and to assess how the personal-knowledge test applies to passwords and biometrics.
- To evaluate whether the BNSS, 2023 regulates the scope of extraction, examination and retention of data after a digital device is seized.
- To identify the gaps in protecting unrelated, privileged and third-party information during forensic examination.
- To suggest reforms that balance effective criminal investigation with the rights of the accused and the privacy of third parties.

RESEARCH METHADOLOGY

This paper follows a doctrinal research methodology. It is based on the study and interpretation of existing legal sources: statutory provisions, constitutional provisions and judicial decisions relating to the subject. The primary sources examined are Section 69 of the Information Technology Act, 2000, the relevant provisions of the Bharatiya Nagarik Suraksha Sanhita, 2023 and the Bharatiya Sakshya Adhiniyam, 2023, Articles 20(3) and 21 of the Constitution, and the case law on compelled access to digital devices. Secondary sources, such as scholarly articles and commentary, are used to support and contextualise the doctrinal analysis.

The constitutional principles are considered only to the extent necessary to assess the validity and adequacy of the statutory and procedural scheme for compelled access to, and forensic

examination of, digital devices. Constitutional jurisprudence is therefore used to identify the relevant standards on self-incrimination, privacy, informational autonomy and proportionality.

This paper is primarily concerned with the position under Indian law. Comparative material is used only to a limited extent, to identify procedural safeguards for the protection of privileged, unrelated and third-party information[6].

SCOPE AND LIMITATIONS

This paper discusses two distinct yet related processes of investigation using the digital means of accessing a digital device that is password protected or encrypted using passwords, PIN, encryption key or biometric authentication and subsequently the extraction, forensic analysis, storage and presentation as evidence of digital information contained in the digital device.

Constitutional analysis would be conducted within the scope of Art 20(3) and 21 only insofar as they provide guidelines for the examination of the issues of compelled access and digital examination of the information obtained after seizure. This paper does not conduct a general study of the interpretation of Indian Constitution in regard to privacy, self-incrimination or proportionality.

The paper does not look into intermediary liability under Sec 69A and 79 of the IT Act, 2000[7], Corporate compliance with cybersecurity and civil discovery, or with regard to any technical methods of decryption. Technical extraction and forensics is done only with the aim of demonstrating its significance legally.

The paper is organised in seven parts. Part I sets out the research problem, questions, methodology and scope. Part II reviews the literature and identifies the research gap. Part III examines compelled access under Sec 69 of the IT Act, the Art 20(3) analysis and the five-factor framework, post-seizure examination under the BNSS, and safeguards for unrelated, privileged and third-party data. Part IV sets out the findings. Parts V to VII conclude, make

[6]*See, e.g.*, Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 Tex. L. Rev. 767 (2019); 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); Regulation of Investigatory Powers Act 2000, c. 23, pt. III (UK). These sources are used only to identify safeguard-relevant considerations, not as an independent comparative-law study.

[7]IT Act, *supra* note 2, §§ 69A, 79.

suggestions.

LITERATURE REVIEW

Literature associated with the subject of compulsory unlocking of the encrypted digital device for forensic analysis can be categorized as:

Research on the problems of Decryption under compulsion and against testimonial self incrimination; Research regarding digital search, forensic examination, and electronic evidence in India; Comparative literature which analyzes different legal responses to the issue of encrypted data. These literatures provide a very strong basis for the current research, but they deal with the separate issues of digital investigation. It is important that we investigate the difference between accessing a device that is encrypted and conducting forensic examination on the accessed data.

2.1. Compelled Access and the Protection against Self Incrimination

Scholarly discourse on Indian jurisprudence of forced access to a digital device has primarily grown out of the landmark case of Virendra Khanna. In their paper titled *'Self-Incrimination and Digital Evidence: Proposing a Framework* Post Viredra Khanna', Vadita Agarwal and Tanishq Kabra have analyzed the constitutional dimensions of compelled decryption in light of Art 20(3) and 21 of the Indian constitution. The authors have criticized the Karnataka High Court's conclusion regarding the non-violation of the rights of self-incrimination and privacy of the accused through forced decryption[8]. Samarth Udasin similarly examines whether compelling an accused to unlock or decrypt a device, by password or biometric identifier, violates Article 20(3), drawing on Kathi Kalu Oghad, Selvi and Puttaswamy, and argues for a statutory framework with judicial oversight, proportionality and safeguards for digital privacy[9]

In the case of the conflict between *Virendra Khanna and Mahesh kumar sharma*, it is evident that there still remains an element of ambiguity in the use of Article 20(3) in connection to compelled digital access. In spite of rejecting the reasoning in *Virendra Khanna case* using

[8] Vadita Agarwal & Tanishq Kabra, *Self-Incrimination and Digital Evidence: Proposing a Framework Post Virendra Khanna*, NUJS L. Rev. Blog (Nov. 29, 2024), https://nujslawreview.org/2024/11/29/232104/ (arguing that *Virendra Khanna* is doctrinally difficult to reconcile with established Article 20(3) principles and has since been treated as *per incuriam* in *CBI v. Mahesh Kumar Sharma*).

[9] *See also* Samarth Udasin, Passwords, Privacy, and Self-Incrimination: Compelled Decryption Under Article 20(3) of the Constitution, 4(1) NFSU J. Forensic Just. (Jan. 2025), https://jfj.nfsu.ac.in/articles?id=99.

Selvi, the latter case did not deal with compelled passwords or biometrics.[10].

The Comparative analysis clearly shows that there is no one answer for the doctrine of foregone conclusion. According to Orin S. Kerr, entering a password is testimonial because it shows knowledge of the password, but compulsion may still be allowed where the government already knows this (foregone conclusion)[11]. Laurent Sacharoff takes a more narrow approach, contending that the compelled decryption must be linked to information that the government can prove the individual is in possession of.[12]. Bryan H Choi raises another question about viewing phones just as "locked boxes of evidence," noting that the compelled disclosure could potentially result in exposure to an exceedingly large amount of information.[13].

Aloni Cohen and Sunoo Park introduce a new technology perspective to the discussion as they analyze the connection between compelled decryption and the features of an encryption system. Their research shows that the constitutional consequences may be determined based on the specific means of gaining access and the message transmitted by the compulsory act.[14]. This is relevant to the Indian scenario due to the fact that the use of passwords and encryption keys entails the communication of knowledge while biometric authentication might entail a completely different aspect of compelled participation.

Accordingly, there is a considerable doctrinal debate in the literature on the question of whether digital access entails any testimonial aspect as well as the extent of prior knowledge possessed by the government as well as the link between opening a phone and the information contained therein. Most importantly, the question raised by Choi regarding the information accessible from a smartphone raises questions on whether the legal issues will end with the opening of the phone.

2.2. Digital Search, Forensic Examination and Electronic Evidence in India

An independent literature corpus from India deals with the problem of regulation of searches,

[10] *Selvi v. State of Karnataka*, (2010) 7 SCC 263 (India) (holding that involuntary administration of narcoanalysis, polygraph, and brain electrical activation profile tests amounts to testimonial compulsion under Article 20(3), but not addressing password or biometric device authentication).
[11] Kerr, *supra* note 6.
[12] Laurent Sacharoff, Unlocking the Fifth Amendment: Passwords and Encrypted Devices, 87 Fordham L. Rev. 203 (2018).
[13]Bryan H. Choi, *The Privilege Against Cellphone Incrimination*, 97 Tex. L. Rev. Online 73 (2019).
[14] Aloni Cohen & Sunoo Park, *Compelled Decryption and the Fifth Amendment: Exploring the Technical Boundaries*, 32 Harv. J.L. & Tech. 169 (2018).

seizures, forensics and electronic evidences. In their paper titled *'Bytes and Rights: Unpacking Search and Seizure of the Electronic Evidence Under India's Legal Framework'*, Devansh Malhotra and Rohit Kumar Shrivastava examine the nexus between the IT Act 2000, BNSS,2023 and BSA 2023. The subject includes searches and seizures, right to privacy, right to fair trial, forensics, chain of custody, encryption and cloud-based information and other procedural matters in the context of digital forensics[15]. However, the research has shown that the issue with the digital evidence is not connected with seizing the digital evidence, but with collecting and investigating it.

Vaibhav Chadha & Janani Sivaraman address the admissibility of electronic evidence in India.The study investigates the transition from Sec 65B of Indian Evidence Act, 1872 to Sec 63 of BSA, 2023[16]. These literature sources are highly pertinent due to the fact that any information gathered through the process of forensics should meet the evidentiary requirements to be used in court.

The issue pointed out by the literature on the compelled smartphone access is especially important when discussing the second stage. After unlocking of the protected phone, it can hold any communications, photos, financial data, work emails, and the cloud-synchronized data about individuals who are not suspected of any crime. Thus, it becomes clear that the issue of compelled access cannot be evaluated just on the basis of whether the phone was properly unlocked.

Admissibility of evidence and its legality of acquisition are thus separate considerations. Even adherence to the criteria relating to authentication or chain of custody does not in itself settle the question of legality and propriety of the examination that preceded the acquisition. Forensic examination can be conducted to generate reliable evidence while at the same time divulging private information, confidential communications or information belonging to other individuals. Likewise, statutory right to conduct searches or seizure of a digital device does not automatically define the permissible scope of examination of all categories of information contained within.

[15] Devansh Malhotra & Rohit Kumar Shrivastava, *Bytes and Rights: Unpacking Search and Seizure of the Electronic Evidence Under India's Legal Framework*, 4 NFSU J. Forensic Just. 32 (2025).
[16]Vaibhav Chadha & Janani Sivaraman, *Critical Analysis of the Law on Admissibility of Electronic Evidence in India*, 15 Jindal Glob. L. Rev. 119 (2024); *see also* Bharatiya Sakshya Adhiniyam, 2023, No. 47, Acts of Parliament, 2023 (India), §§ 61–63 [hereinafter BSA].

Existing literature on digital evidence in India can be considered useful in studying BNSS and BSA regime, but the problem of access in regard to the forensic process was not considered properly. The purpose of this study is to make a contribution to the above mentioned literature through looking at access, examination, retention and evidentiary use as separate legal processes in digital investigation.

2.3. Comparative Approach to Encrypted Information

Comparative literature is used in this paper primarily to identify measures and methods that are pertinent to the compelled access. For example, in the U.S., the primary issue is the foregone-conclusion doctrine within the Fifth Amendment act-of-production doctrine. Kerr asks whether the government already knows the person knows the password. Sacharoff instead looks at what the government already knows about the data unlocking would produce[17]. Cohen and Park further show that the technological difference could affect the assumption underlying such techniques. These perspectives highlight prior knowledge, particularity and the nature of the compelled act.

Another statutory example can be found in the United Kingdom Part III of the Regulation of Investigatory Powers Act 2000 (sections 49 to 56) provides a scheme for requiring the disclosure of protected information in a comprehensible format, or the disclosure of the means by which it can be accessed[18]. Victoria Williams' analysis of this regime deals with encryption disclosure in the context of surveillance and intelligence law[19]. The UK approach to compelled decryption is relevant to the current research study due to the way in which it highlights the possibility of compelled decryption being governed by particular statutory and procedural mechanisms and not just investigatory power.

The above-mentioned comparative materials are not considered as separate comparative law topics but are significant insofar as they offer safeguards and analysis questions relating to prior knowledge, particularly the nature of the compelled act and disclosure limitations that might aid in assessing the Indian framework.

[17] Kerr, *supra* note 6; Sacharoff, *Unlocking the Fifth Amendment*, *supra* note 12**.**
[18] Regulation of Investigatory Powers Act 2000, *supra* note 6, §§ 49–56.
[19] Victoria Williams, *Surveillance and Intelligence Law Handbook* 195–216 (Oxford Univ. Press 2006).

2.4. Research Gap

The literature reviewed reveals a specific gap at the point where compelled access ends and forensic examination begins. Indian scholarship on *Virendra Khanna and Mahesh kumar sharma,* focuses principally on whether an accused may be compelled to provide accesss to a protected device and how such compulsion interacts with the right against self-incrimination. Scholarship on digital evidence in contrast, addresses search and seizure forensic handling, authentication, admissibility and chain of custody. Comparative scholarship provides additional models for analysing compelled decryption but does not determine the position under the Indian law.

The current research paper seeks to address this problem by considering both compelled access and forensic examination after seizure as two separate yet inter-related processes. This research paper will discuss the legal basis of accessing the device on the grounds provided by sec 69 of IT Act 2000 and further analyze the BNSS framework regarding the extraction, analysis, retention, and presentation of the information retrieved from the digital device. Emphasis will be laid on unrelated, privileged, and third party information. The research paper thereafter intends to find out if Indian law draws a proper distinction between the process of unlocking the device and the subsequent examination of the information obtained thereby.

3. COMPELLED DIGITAL ACCESS AND POST SEIZURE EXAMINATION UNDER INDIAN LAW

3.1. Compelled Access to Encrypted Digital Device under Sec 69 of the IT Act, 2000

The first stage of a digital investigation concerns the State's ability to obtain access to a password protected or encrypted device. This issue is distinct from the subsequent examination of the information contained in the device. Under Sec 69(1) of the IT Act, 2000, the Government, through an authorised officer and for reasons recorded in writing, may direct an agency to intercept, monitor or decrypt information in any computer resource, where necessary for sovereignty, security, public order or the investigation of any offence[20]. Section 69(3) further requires the intermediary, subscriber, or person in charge of the computer resource to extent the necessary assistance for giving effect to such directions[21]. The statutory language

[20]IT Act, *supra* note 2, § 69(1).
[21]IT Act, *supra* note 2, § 69(3); *see also* Information Technology (Procedure and Safeguards for Interception,

therefore establishes a framework for giving effect to interception, monitoring, or decryption directions, including through the assistance contemplated by section 69(3).

Section 69(3) should not be treated as general statutory power to compel an accused to disclose authentication credentials. Its obligation to provide facilities and technical assistance operates in connection with a direction issued under section 69. A direction to an accused personally to type a password, disclose an encryption key or provide biometric authentication presents a different legal questions concerning the compelled act of the accused.

This distinction is significant because a direction to an intermediary or service provider to facilitate decryption is conceptually different from compelling the accused to communicate information known exclusively to the accused. A password or encryption key may embody knowledge held in the accused's mind, whereas a fingerprint or facial scan involves a physical characteristic. Treating these forms of authentication as legally identical may therefore obscure the constitutional character of the compelled act.

The Karnataka High Court considers these questions in *Virendra Khanna,* where the accused challenged directions requiring cooperation in unlocking a mobile phone and email account through passwords, passcodes, or biometrics[22]. The Court examined whether such directions violate the protection against self incrimination and the right to privacy and under Art 20(3). The decisions recognized the investigative importance of accessing digital device while examining whether the compelled act constituted testimonial compulsion[23].

The decision in *Mahesh Kumar Sharma* subsequently adopted a different approach, declining to follow *Virendra Khanna* by relying on principles drawn from *Selvi v. State of Karnataka*.[24]. As a first instance decision of a subordinate court, *Mahesh kumar sharma* has no precedential authority to overrule or displace the decision of the Karnataka High Court in *Virendra Khanna.* Its significance lies instead in demonstrating a divergent judicial approach to the constitutional character of the compelled digital authentication. The divergence between the decision therefore demonstrates that the principal difficulty is not simply whether investigators require

Monitoring and Decryption of Information) Rules, 2009, G.S.R. 780(E), rr. 3, 7, 8, 22 (Oct. 27, 2009) (India).

[22] *Virendra Khanna*, *supra* note 3.

[23] *Virendra Khanna*, *supra* note 3, ¶¶ 14.7–14.9 (holding that providing a password or biometric key is analogous to furnishing fingerprints or specimen handwriting, and that such compulsion does not, without more, amount to testimonial compulsion under Article 20(3)).

[24] *Mahesh Kumar Sharma*, *supra* note 4 (declining to follow *Khanna* in reliance on *Selvi*, *supra* note 10).

access to digital evidence, but the legal character of the means by which that access is obtain.

The distinction between passwords and biometrics is particularly relevant. Disclosure of a password communicates knowledge possessed by the accused, while biometric authentication does not necessarily communicate the contents of the accused's mind in the same manner. Nevertheless, both forms of authentication may provide investigators with access to the same extensive body of the digital information. Consequently, the constitutional analysis should consider not only the form of the authentication but also the nature and consequences of the compelled act.

The principal statutory difficulty therefore remains unresolved: Section 69 provides a mechanism concerning interception, monitoring and decryption but the existence of that power does not necessarily answer whether an accused may be compelled to personally communicate the means of accessing a device. A clear distinction must consequently be maintained between the authority to obtain digital information and authority to compel an accused to provide the means of obtaining it.

3.2. Article 20(3), Testimonial Compulsion and the Nature of Authentication

3.2.1. The Personal-Knowledge Test

Article 20(3) safeguards an accused person against being forced to provide evidence that may incriminate them. *State of Bombay v. Kathi Kalu Oghad* , distinguished compelled communication of personal knowledge from the furnishing of identifying or physical characteristic[25]s. *Nandini Satpathy v. P.L. Dani* held that protection operates during police investigation, and *Selvi v. State of Karnataka* reaffirmed the inquiry turns on whether the compelled act communicates personal knowledge[26]. For digital authentication, a password, PIN or encryption key may disclose knowledge held by the individual, whereas a fingerprint or facial characteristic ordinarily operates as physical identification. The classification depends on what the act communicates, not on the technology used.

[25] *State of Bombay v. Kathi Kalu Oghad*, AIR 1961 SC 1808,(India).
[26] *Nandini Satpathy v. P.L. Dani*, (1978) 2 SCC 424, 440–41 (India); *Selvi*, *supra* note 10, ¶¶ 180, 184. *See also* BNSS, *supra* note 5, § 180(2) (corresponding to Code of Criminal Procedure, 1973, § 161(2), and protecting a person examined by police from answers tending to expose that person to a criminal charge, penalty or forfeiture).

In a case concerning crime-scene re-enactment, *State of Tamil Nadu v. Ponnusamy* observed that questions about compelled fingerprints, voice samples and mobile passwords "have arisen in the past and have been judicially settled"[27]. It then stated the operative test: an act that merely requires the accused to act without giving personal testimony is valid, but one that compels disclosure of incriminating information from personal knowledge is impermissible. *Ponnusamy* therefore restates a general test applicable to digital authentication, but establishes no password-specific rule under Sec 69 of the IT Act, 2000.

3.2.2. Divergent Judicial Approaches

A significant difference in judicial approach emerges from the judicial decisions in *Virendra Khanna* and *Mahesh Kumar Sharma*. *Khanna* treated furnishing a password, passcode, PIN or biometrics as analogous to physical evidence rather than testimonial compulsion, but treated examination of the smartphone and email account as a search requiring proper procedure. It therefore set aside the trial court's order of 14 September 2020 directing the accused to furnish those credentials, with liberty to the prosecution to proceed in accordance with law[28]. In Delhi, the Special Court called *Khanna*'s observations *per incuriam* for overlooking the personal-knowledge element in *Selvi*, held that recalling a password uses memory and is therefore a testimonial fact, and dismissed the CBI's application while permitting access to the seized data through a specialised agency or person[29]. *Khanna* is only persuasive in Delhi, since only Supreme Court decisions bind courts across India under Article 141, and *Mahesh Kumar Sharma* neither did nor could formally overrule it[30].

3.2.3. Article 21 and Proportionality

Under *Puttaswamy*, an intrusion into privacy must satisfy legality, a legitimate State aim and proportionality[31]. A device may expose communications, financial records, location data, professional material and third-party information. Even where authentication is non-testimonial, the subsequent search and examination of the device therefore remain subject to these requirements.

[27] *State of Tamil Nadu v. Ponnusamy*, 2026 INSC 507, ¶¶ 85–86, 88, 90 (India May 19, 2026).
[28] *Virendra Khanna*, *supra* note 3, ¶¶ 14.7–14.8, 18.1–18.2, 21.1–21.3.
[29] *Mahesh Kumar Sharma*, *supra* note 4, ¶¶ 35–38, 47, 57.
[30] India Const. art. 141; *Mahesh Kumar Sharma*, *supra* note 4, ¶ 35.
[31] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, ¶¶ 310, 325 (India).

3.2.4. The Five-Factor Framework

These authorities support five factors, to be weighed together and not applied as a checklist:

1. Form of authentication and personal knowledge. Whether a memorised secret (password, PIN, key) or a physical characteristic is compelled. The line is functional, not categorical. Treating biometrics as physical evidence is consistent with *Kathi Kalu Oghad*, but *Ponnusamy* did not decide biometric unlocking.

2. Prior knowledge of the State**.** Whether the State already knows what the act would reveal. The U.S. "foregone conclusion" doctrine is a comparison only, not an exception to Article 20(3)[32].

3. Breadth of information exposed**.** The volume and sensitivity of the data, including privileged and third-party material.

4. Particularity. Whether access is confined to an identified device, account, category or purpose, rather than a general direction to "cooperate". The procedural concern in *Khanna* applies even where authentication is non-testimonial.

5. Less intrusive means. Whether the evidence can be obtained through forensic or specialised means without compelling the accused, as *Mahesh Kumar Sharma* recognised[33].

3.2.5. Where the Law Stands

As of 3 October 2026, *Ponnusamy* is a recent Supreme Court restatement of the distinction between physical assistance and compelled disclosure of personal knowledge, but it does not resolve password disclosure under Section 69. A 2026 Delhi High Court decision, *CBI v. I.M. Quddusi*, held that Section 91 CrPC (now substantially Section 94 BNSS) cannot compel an accused to furnish information based on personal knowledge. It binds Delhi courts but does not address passwords or Section 69[34]. The unresolved issue is how the *Ponnusamy* test should

[32] *Fisher v. United States*, 425 U.S. 391, 410–11 (1976).
[33] *Mahesh Kumar Sharma*, *supra* note 4, ¶¶ 47, 57.
[34] *CBI v. I.M. Quddusi*, 2026:DHC:226 (Del. HC Jan. 12, 2026).

operate when Section 69 is invoked to access an encrypted device and that access exposes information beyond what the investigation demonstrably requires.

3.3. Post Seizure Forensic Examination under the BNSS,2023

Obtaining access to a digital device is only the first stage of the investigation. Once a device is unlocked or otherwise made accessible, investigators may extract, copy, search, analyse, and preserve substantial quantities of information. The legal authorities governing this second stage must therefore be examined separately.

Section 94 of Bharathiya Nagarik Suraksha Sanhitha,2023 provides the procedural framework for requiring the document production and other things including electronic communications and communication devices likely to contain digital evidence[35]. The provision is important because it recognizes the evidentiary significance of electronic material within the ordinary criminal procedure. However a power to require production of a device does not necessarily mean that every item of information stored on or accessible through that device may be examined without limitations. The distinction between possession of the device and the scope of the examination of the contents becomes particularly important where the device contains information unrelated to the offence under investigation.

Section 105 BNSS states that the act of search and seizure is required to be documented through audio-video electronic recording, preferably using a mobile phone.[36]. This is because recording the process of the search and seizure helps ensure transparency as a record is kept of how the search and seizure is done. This may help the courts determine whether all procedures have been complied with and also may resolve any confusion about the way the digital evidence was obtained. Recording the process of search, however, is not enough to determine the scope of the subsequent forensic examination of data.

Another section in BNSS, which illustrates the trend towards forensics, is Section 176(3). With respect to any information relating to an offence that attracts a maximum sentence of seven years imprisonment or higher, the statute mandates the officer in charge, as per the statutory implementation machinery, to engage a forensic expert to examine the crime scene to collect

[35] BNSS, *supra* note 5, § 94 (corresponding to § 91 of the Code of Criminal Procedure, 1973).
[36] BNSS, *supra* note 5, § 105 (a newly introduced provision, with no direct CrPC equivalent, mandating audio-video recording of search and seizure proceedings).

forensic evidence and videography of the process[37]. This section acknowledges the fact that modern criminal investigation relies increasingly on scientific and electronic evidences. On the other hand, greater reliance on forensics makes procedural protections in respect of collection, filtering, access and storage of information much more relevant.

Particular clause 193(3)(i) BNSS, pertaining to the details of the police report upon completion of investigation, falls within this wider scope of evidence[38]. Any digital evidence collected through investigation might finally become part of the evidentiary process, in accordance with the provisions of the BSA, 2023[39]. It is important, nonetheless, to note that the admissibility of any digital evidence does not equate to the legitimacy of its collection process.

This is especially relevant when it comes to investigating crimes that involve digital tools. Authentication, preservation, and chain of custody determine whether the digital record can be admissible in evidence. However, they cannot, in and of themselves, provide answers to the questions about whether the investigators were authorized by law to examine the device and whether the examination was within the scope of investigation. Hence, reliable evidence might still bring up questions about its legitimacy.

Hence, while the BNSS provides a number of significant procedures for conducting investigations, it does not create any statute framework for regulating the extent of the investigation of personal digital devices after seizure. This problem becomes even more acute in cases where the digital device holds information far exceeding the content of the investigation[40].

3.4. Unrelated, Privileged and Third Party Data , The Need for Procedural Safeguard

The vastness of information available on modern-day devices presents a challenge that cannot be addressed solely by answering the question whether access to the device was lawful. A

[37] BNSS, *supra* note 5, § 176(3) (permitting State Governments up to five years from commencement to notify the date from which the forensic-visit mandate takes effect).
[38] BNSS, *supra* note 5, § 193(3)(i) (corresponding to § 173(2)(i) of the Code of Criminal Procedure, 1973, but adding a new requirement to state the chain of custody for electronic devices in the police report).
[39] BSA, *supra* note 16, § 63 (replacing § 65B of the Indian Evidence Act, 1872, as the admissibility provision for electronic records); *see Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1 (India) (on the certification requirement).
[40] *See also Foundation for Media Professionals v. Union of India*, W.P. (Crl.) No. 395/2022 (India Nov. 7, 2023) (order) (recording submissions that investigating agencies had seized journalists' devices without adequate guidelines and directing that proposed guidelines for search and seizure of digital devices be circulated to the Union and State Governments).

smartphone can have personal communication, photographs, bank records, business communication, cloud-based information and information belonging to relatives, co-workers or other third-parties. Therefore, when the device becomes unlocked, the question shifts from whether the investigators can look into the device to what extent can they look into the information that becomes available.

The first protection that needs to be implemented is the requirement of particularity. The forensic examination must be related to the crime and types of information which serve as a good foundation for investigation. The unrestricted examination of every application, message, photograph or document may reveal information that is irrelevant to the crime in question. Compelled decryption literature illustrates the significance of particularity and prior knowledge of government[41].

The second measure suggested by this paper is data minimization. It means that, wherever possible, the investigator should collect and preserve only the information which is directly connected to the purpose of the investigation. It is particularly important in the context of the forensic imaging process since in this case the investigator gets a complete copy of the digital device instead of just some specific file or communication. Thus, data minimization is suggested in this paper as a proposed procedural safeguard and not an explicit general rule under the BNSS.

Finally, there is an issue of the privileged information. The digital devices can contain certain communications which are covered by the legal professional privilege[42]. If no limits are set on the forensics examination process, the investigator might get access to this information. Therefore, a mechanism to detect, separate and protect such information must be in place.

In addition to these issues, third-party information constitutes an issue of privacy in its own right. That the information is stored in the device of the accused is not proof that all of it belongs to the accused or pertains only to the accused. There may be messages, photos, contact details and correspondences which pertain to third parties who are not suspects in the offence under investigation.

[41] Sacharoff, *Unlocking the Fifth Amendment*, *supra* note 12; Kerr, *supra* note 6.
[42] BSA, *supra* note 16, § 132 (professional communications), corresponding to §§ 126–127 of the Indian Evidence Act, 1872; *cf. In re Search Warrant for Law Offices Executed on March 19, 1992*, 153 F.R.D. 55 (S.D.N.Y. 1994) (used here only as an illustrative comparative model for a filter mechanism).

Also worthy of note in this regard, from a legal perspective, is the DPDP Act, 2023. This Act serves as an important and albeit limited, point of reference in relation to the handling of personal data. However, despite its relevance to the protection of personal data, its applicability to criminal investigations should take into account its statutory limitations and exclusions[43]. Hence, it should not be used as an all-encompassing guide as far as the forensic examination of devices in criminal investigations is concerned. Nonetheless, the statutory provisions on digital personal data emphasize the importance of access control and protection against disclosure where the devices store information pertaining to persons other than the accused.

The foregoing discussion highlights that the mere ability to lawfully access a digital device does not necessarily mean that one has full authority to examine all of its contents. The creation of a viable framework necessitates a differentiation between access, extraction, examination, retention and the use of evidence. Specifically, the forensic examination must be justified and protected through particularity, proposed data minimization measures, protections for communications that could potentially be covered by the legal professional privilege and protections for third party information. The crucial point, therefore, is not only whether investigators can legally access the device but also whether the examination of its contents is sufficiently related to the purpose of such access.

4. FINDINGS AND DISCUSSION

This paper reaches four findings, one for each subordinate research question. Together they test the central hypothesis: that Indian law does not adequately distinguish between the power to access a digital device and the power to examine, retain and use its contents.

The first finding concerns Section 69 of the IT Act, 2000 and compelled disclosure. Section 69 provides a mechanism for the interception, monitoring and decryption of information through a computer resource. Section 69(3) requires subscribers, intermediaries and persons in charge of a computer resource to extend the facilities and technical assistance needed to give effect to such a direction, and Section 69(4) penalises non-compliance. The provision therefore clearly contemplates assistance in obtaining access to a computer resource and the information in it. It does not expressly state that an accused may be required to personally disclose a password,

[43] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India), § 17(1)(c), (2) [hereinafter DPDP Act] (exempting processing for the prevention, detection, investigation, or prosecution of offenses from several of the Act's obligations, subject to conditions prescribed by the Central Government).

PIN or encryption key, or to unlock a device biometrically. Assistance by an intermediary or service provider is conceptually different from compelling an accused to communicate information held in their own mind. The finding is therefore one of statutory ambiguity rather than statutory prohibition. Section 69 supplies a statutory route to decryption, but it cannot by itself answer whether an accused can be compelled to authenticate, which is a question under Article 20(3).

That question leads to the second finding, on the judicial approaches to compelled access. *Virendra Khanna v. State of Karnataka* and *CBI v. Mahesh Kumar Sharma* take opposing positions on whether compelled authentication attracts Article 20(3). The Karnataka High Court in *Khanna* treated furnishing a password, passcode or biometric as analogous to providing physical or identifying evidence, while treating examination of the device as a search requiring procedural safeguards. The Special Court in *Mahesh Kumar Sharma* declined to follow *Khanna*, holding that recalling a password involves mental effort and personal knowledge and is therefore testimonial. It nevertheless allowed the investigating officer to access the data through a specialised agency. The two decisions do not carry equal weight. *Khanna* is a High Court decision, while *Mahesh Kumar Sharma* is a trial-court decision that cannot overrule or displace it. Its value lies in showing a divergent reasoning, not in settling the law. *Selvi* and *Kathi Kalu Oghad* supply the foundational distinction between personal knowledge and physical evidence, but neither concerned passwords or biometric authentication. *Ponnusamy* (2026) restates that distinction as a general constitutional test, and *Quddusi* applies it to Section 91 CrPC (now Section 94 BNSS), but neither decides password disclosure under Section 69. The finding is that Indian law has no settled doctrine on compelled digital authentication. The United States "foregone conclusion" doctrine and Part III of the UK Regulation of Investigatory Powers Act 2000 are useful comparators, but neither is part of Indian law.

The third finding moves from access to what happens after the device is unlocked, and concerns the adequacy of the BNSS framework. The BNSS contains relevant procedural provisions: Section 94 (production), Section 105 (audio-video recording of search and seizure), Section 176(3) (forensic expert in offences punishable with seven years or more) and Section 193(3)(i) (chain of custody in the police report). These improve transparency and documentation. They do not regulate the substantive scope of what may be extracted, examined and retained after seizure, and they do not separate material connected to the offence from unrelated, privileged

or third-party material. A search may be properly recorded and the resulting evidence technically authentic, while the examination itself is excessive or disproportionate. Legality of acquisition and reliability of evidence are separate questions. Compliance with authentication and chain-of-custody requirements under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023 does not establish that the examination was lawfully limited.

The fourth finding follows from this gap and concerns safeguards for unrelated, privileged and third-party information. None of the provisions examined, whether in the IT Act, the BNSS or the Bharatiya Sakshya Adhiniyam, 2023, provides specific safeguards for identifying and segregating privileged communications, minimising retention of unrelated data, or protecting third-party information found on a seized device. The DPDP Act, 2023 is a limited reference point because Section 17 exempts processing for the investigation of offences from several of its obligations. These interests therefore depend largely on judicial discretion, which is an uncertain safeguard given the volume of private information on a modern device.

Taken together, the findings confirm the hypothesis. The existing framework does not separate the authority to take a device, the authority to access it, and the authority to extract, examine, retain and use its contents. Each raises a distinct constitutional and procedural question. The five-factor framework proposed in this paper gives courts a structured way to assess compelled access: the form of authentication and whether it communicates personal knowledge; the State's prior knowledge; the breadth of information exposed; the particularity of the request; and the availability of less intrusive means. The factors are to be weighed together, not applied as a checklist or statutory conditions. The first two address the Article 20(3) question. The last three address the Article 21 requirements of legality, necessity and proportionality that follow from *Puttaswamy*. The framework does not treat the "foregone conclusion" doctrine as an exception to Article 20(3). It uses prior knowledge only as a factor relevant to what the compelled act actually reveals.

5. CONCLUSION

The analysis focused on whether the existing Indian legal framework provides sufficient safeguards when authorities compel access to encrypted digital devices and later examine the data obtained from them. It finds that the present framework leaves significant gaps in protecting the rights of accused persons and the privacy of unrelated third parties during both processes.

On access, Section 69 of the IT Act provides a mechanism for decryption but does not clearly authorise compelling an accused to disclose a password, PIN or encryption key. The question therefore remains statutorily ambiguous and constitutionally unresolved. The judicial divergence between *Khanna* and *Mahesh Kumar Sharma* does not reflect a conflict between authorities of equal weight. It reflects a High Court decision and a differing trial-court decision, with no authoritative ruling from the Supreme Court on password or biometric authentication, even though *Ponnusamy* has restated the general test.

On examination, the BNSS regulates production, recording, forensic involvement and chain of custody, but it does not define the limits of extraction, examination and retention after a device is unlocked. Neither the BNSS, the IT Act, the BSA, 2023 nor the DPDP Act provides adequate protection for unrelated, privileged and third-party information.

The paper therefore proposes that three authorities be treated separately in law: the authority to take a device, the authority to access it, and the authority to extract, examine, retain and use its contents. The five-factor framework offers courts a way to apply Articles 20(3) and 21 to this process without importing another jurisdiction's legal regime wholesale. Measures to give it effect are set out in the Suggestions that follow.

Ultimately, the lawful seizure or unlocking of a device should not entitle investigators to an unrestricted examination of a person's digital life. Indian cyber and criminal procedure law should move from a device-centred approach to an information-centred one, in which every stage of digital investigation is justified, limited, documented and subject to effective oversight.

6. SUGGESTIONS

The above findings lead to the following recommendations to be undertaken, mainly by legislators:

1. **Clarification of Section 69's scope**. The clarification by the legislature (or, alternatively, the rulemaking body empowered by the IT Act) regarding the circumstances in which the accused should be directed to personally reveal or authenticate their data could be useful in differentiating the obligation to do so from the existing one in Section 69(3).

2.Requirements for the particularity of post-seizure digital forensic examinations. The BNSS, or its implementing rules, could require directions or warrants issued for the purpose of

examining the seized digital data to specify the categories of the information sought to be examined, the period during which the information was created, or the investigative purposes pursued by the examination.

3. **Privilege segregation protocol**. A standing review or filtering process for identifying and segregating privileged communications, perhaps drawing on processes used in other jurisdictions in relation to document seizure, might be considered for application to digital forensics, ensuring that privileged communications can be segregated prior to their availability to the investigating team.

4. **Data minimization and retention restrictions**. In terms of proposed minimization protection, a requirement in forensic protocols could be that, if a forensic copy of the relevant device is created, only information related to the specific investigation would be retained after the review period with justification for any additional retention.

5. **Third party notice or review mechanisms**. It may be worth considering a review process either through judicial review or forensic review process, regarding information contained in a seized device, which concerns primarily third parties who have no connection to the investigation.