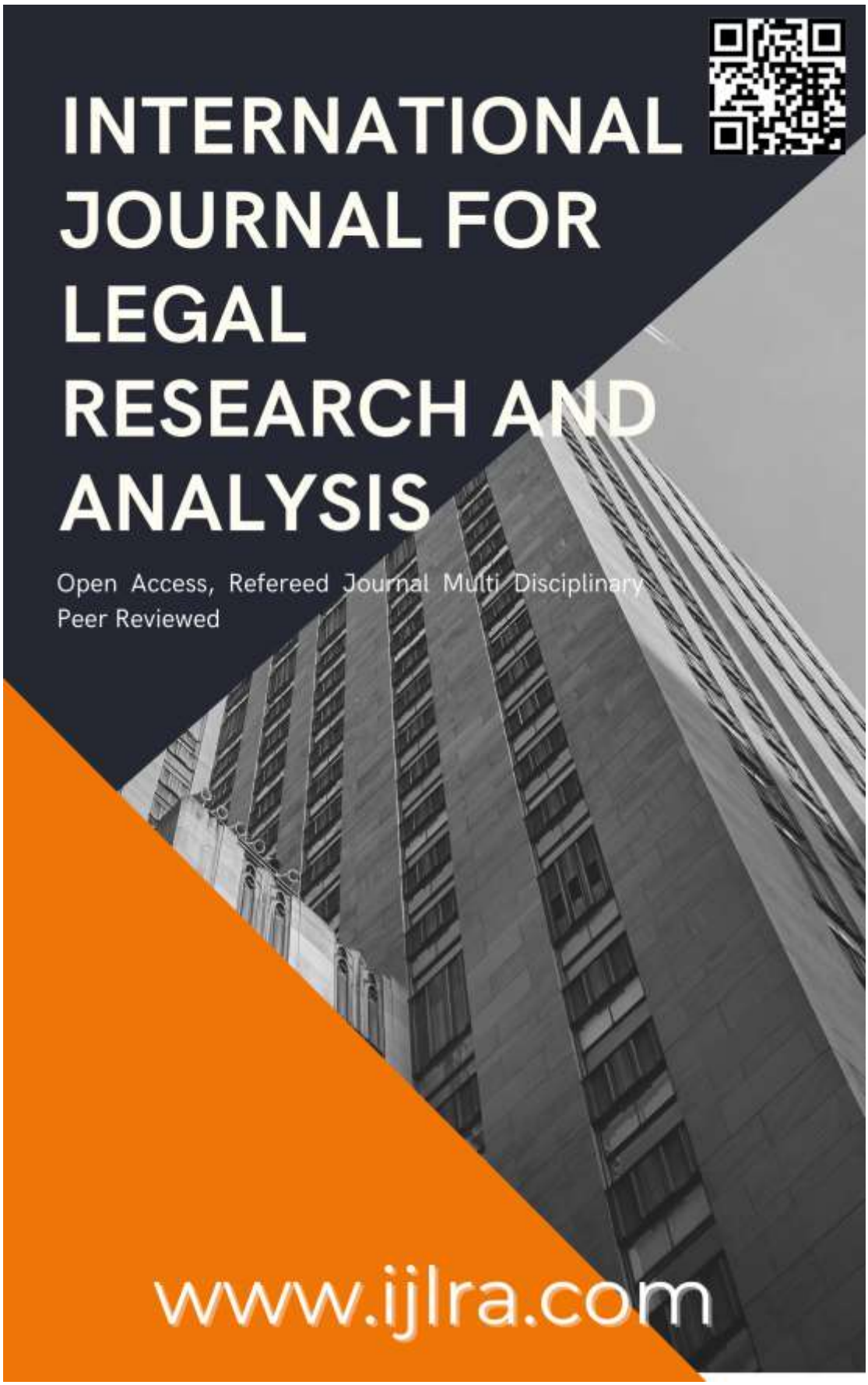

VOLUME 3 • ISSUE 8 • NOVEMBER 2026

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the International Journal for Legal Research & Analysis (IJLRA).

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

Copyright © International Journal for Legal Research & Analysis. All rights reserved.

ABOUT US

The International Journal for Legal Research & Analysis (IJLRA) (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the International Journal for Legal Research & Analysis aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The International Journal for Legal Research and Analysis (IJLRA) is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice.

Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats.

The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published.

By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights.

The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

RESEARCH ARTICLE

GETTING ELECTRONIC EVIDENCE FROM OTHER COUNTRIES IN CYBERCRIME INVESTIGATIONS: LEGAL AND PRACTICAL CHALLENGES. CAN THE POLICE FORCE AN ACCUSED PERSON TO REVEAL AN ENCRYPTION KEY?

Authored by - Adv. Kavita N. Solunke

BA, BSL, LLM, MBA, GDC&A, PG (ADR), Star CCIO; Additional Government Pleader, Arbitrator, Mediator, Bombay High Court; Notary, Government of India, Author of Health to Happiness Book.

Abstract

The increasing use of digital platforms, encrypted communication and cloud-based storage has created new challenges for criminal investigations. Electronic evidence relating to cybercrime is frequently stored on servers located outside the country where the offence is investigated. This makes it harder for law enforcement agencies to gather the necessary information, especially when it requires access to foreign data providers or organisations. Meanwhile, encryption technology has become more complex, making it more difficult for investigators to gain access to evidence on seized devices and raising questions about whether an accused person can be compelled to provide an encryption key or password.

This paper examines these two interrelated issues from the perspective of Indian law. It examines the legal means of access to electronic evidence in foreign jurisdictions, practical restrictions on mutual legal assistance and the evidentiary requirements for electronic evidence in court. It also explores whether compelling the accused to disclose his/her encryption key would amount to violation of protection against self-incrimination enshrined in Article 20(3) of the Constitution of India and right to privacy under Article 21. By comparing judicial decisions, statutory provisions and legal approaches in other jurisdictions, the paper proposes that investigative powers must be balanced with constitutional guarantees. It calls for a more precise definition of the parties' obligations regarding electronic evidence and clearer limits on requiring someone to disclose a password when the disclosure may reveal the person's identity or knowledge and provide information that can be used directly in the prosecution.

Keywords: Cybercrime, Electronic Evidence, Cross-Border Data Access, Encryption, Self-Incrimination, Right to Privacy, Digital Investigation.

Introduction

Information technology has had a profound impact on the nature of offences and investigation processes. Traditional physical crimes are facilitated digitally via computer networks, online communication services and are increasingly committed through these networks and services. Cybercrime could be; financial fraud, identity theft, unauthorised access to computer systems, online harassment and data theft. In numerous such investigations, electronic evidence is increasingly important in helping to identify the accused, establish how an offence has been committed and link individuals to the alleged criminal acts. But it isn't often easy to get this evidence. Unlike traditional physical evidence, electronic records can be stored, transferred and accessed within seconds anywhere at any time. A person using an online service in India may use a service provided by a foreign entity, and the records of the communication or information on an account can be maintained on servers in other countries. Thus, when an Indian investigating agency seeks information held outside its

jurisdiction, the agency may be required to obtain it through international cooperation mechanisms.[1] That means the information may not be directly accessible to an Indian investigating agency, raising legal issues when the agency seeks to obtain it for an investigation. This raises issues about jurisdiction, cooperation among nations, data protection and the legality of a country seeking data in another country.[2]

The issue is complicated even more when electronic evidence is secured with an encryption system. Encryption is a security feature that converts readable data into an unreadable format that can only be accessed with the correct cryptographic key. It helps safeguard personal communications, financial information and confidential data against unauthorised access. This technology is useful for privacy and information security reasons but raises challenges for crime investigation. Where an agency lawfully seizes an electronic device (such as a cell phone, computer or other electronic device), it might not be able to access its contents without having the proper password or encryption key.[3]

This raises an important question: Do public safety officials possess the authority to compel someone accused of committing a crime to reveal an encryption key or password? It's not a matter of investigating for convenience. Disclosure may involve a person providing the prosecution with information personally known to him or her and which could help establish the alleged offence. Hence, any such requirement has to be analysed in light of the protection against self-incrimination in the Constitution of India, which states 'No person shall be compelled to be a witness against himself'.[4]

The meaning and ambit of this protection has been explained by the Supreme Court in State of Bombay v. Kathi Kalu Oghad, (1962) 3 SCR 10, especially in terms of the distinction between testimonial evidence and physical evidence.[5] In like manner, in *Selvi v. State of Karnataka*, (2010) 7 SCC 263, the Court acknowledged that the accused has protection under Article 20(3) against being compelled to provide testimonial responses that may have an incriminating effect. These decisions also provide relevant precedents for considering the compelled disclosure of digital credentials. The application of these principles to encryption keys, however, is a relatively new legal issue.[6] A password is not just a physical thing, e.g., fingerprint. It is not clear whether disclosing a password amount to testimonial compulsion. The Indian law also has some statutory provisions relevant to these problems. The Information Technology Act, 2000 contains provisions relating to the interception, monitoring or decryption of information under specific conditions, subject to the safeguards in Section 69. This provision also imposes a duty to assist the authorised agency. But that does not resolve whether the Constitution would allow an accused to be compelled to reveal an encryption key that he or she knows.

Likewise, the Bharatiya Nagarik Suraksha Sanhita, 2023, provides a mechanism for obtaining evidence from foreign jurisdictions. Section 112 allows criminal court to send a letter of request to a competent foreign court or foreign authority for examination of persons and production of relevant documents and things.[7] Additionally, Sections 61 and 63 of the Bharatiya Sakshya Adhiniyam, 2023, specifically address electronic

[1] Ministry of Home Affairs, Government of India, *Mutual Legal Assistance in Criminal Matters*, available at: https://www.mha.gov.in (last accessed 16 November 2026).
[2] United Nations General Assembly, *United Nations Convention against Cybercrime: Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes*, UNGA Res 79/243, 24 December 2024, arts 40 and 44.
[3] National Institute of Standards and Technology (NIST), *Encryption*, Computer Security Resource Center Glossary, available at: https://csrc.nist.gov/glossary/term/encryption (last accessed 16 November 2026).
[4] Constitution of India, art 20(3).
[5] *State of Bombay v Kathi Kalu Oghad*, AIR 1961 SC 1808; (1962) 3 SCR 10.
[6] *Selvi v State of Karnataka*, (2010) 7 SCC 263, particularly paras 100–102 and 136.
[7] Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023), s 112.

records and electronic evidence and prescribe conditions for their admissibility.[8] These provisions show that obtaining and producing electronic evidence, and proving its evidentiary value, are distinct but related legal processes.

One of the central issues is not just whether law enforcement agencies are allowed to use electronic evidence. It is whether the current legal tools are sufficient to access evidence gathered in other countries and information protected by encryption without infringing the Constitution. A legal system that prioritises investigative effectiveness without adequate safeguards can undermine an individual's privacy and right against self-incrimination. An interpretation that is too narrow, however, could restrict legitimate investigative efforts to access electronic evidence. This paper brings to the fore, inter alia, the need for a more balanced and clear legal regime of cross-border electronic evidence and compelled decryption in India. A system of this kind should enable international cooperation, preserve the evidentiary validity of electronic records and set limits on investigating authorities' power to require suspects to disclose encryption keys.[9] The objective should be to ensure that technological developments do not create an exception to established constitutional protections.

Legal Framework and Challenges in Obtaining Cross-Border Electronic Evidence

Cybercrime does not respect borders, and accessing electronic evidence from overseas is now a significant difficulty faced by investigating agencies. The records of a foreign company may be part of an offence in India. Foreign territory is generally outside the jurisdiction of Indian police. Investigators will need to take into account, however, the laws of the country in which the information is stored and controlled, the procedures and requirements for international cooperation and disclosure.[10]

For evidence outside India there is a formal mechanism as provided in Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS). An investigating officer, or an officer of a higher rank, may apply for a letter of request to a competent court or authority in another country.[11] The request may ask for an examination of a person who knows the facts, the taking of the statement of the person and the production of documents or things relevant to the request. The evidence gathered by this method is conveyed to the Indian court, and subsection (3) treats the evidence received as evidence gathered during the investigation.[12] The letter of request should be sent in the manner directed by the Central Government. This does not permit Indian officers to use coercive force abroad.

The other important avenue is mutual legal assistance. Mutual legal assistance involves a formal request by one country to another for assistance in a criminal investigation or proceeding. This may involve collecting documents, examining witnesses and obtaining statements from persons who may have relevant information; carrying out searches or obtaining documents etc., depending on the requirements of the requested country and the available arrangements. The Ministry of Home Affairs is the central body in India for seeking and giving mutual legal assistance for criminal matters.[13] Also, the Ministry of External Affairs may be engaged in the matter where requests are forwarded through diplomatic channels. If a provider requires a request recognised by its jurisdiction, this route is important.

[8] Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), ss 61 and 63.
[9] Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023), s 112(1).
[10] Ibid, s 112(1)–(2).
[11] Ibid, s 112(3).
[12] Ministry of External Affairs, Government of India, *Mutual Legal Assistance in Criminal Matters*, available at: https://www.mea.gov.in/mutual-legal-assistance-in-criminal-matters.htm (last accessed 16 November 2026).
[13] Ministry of Home Affairs, Government of India, *Guidelines on Mutual Legal Assistance in Criminal Matters*, Internal Security-II Division (2019).

These procedures may be lengthy. A request may require specific details of the alleged offence, the relevance of the information, the persons or accounts involved, and the assistance being sought. Additional documents or a specific type of legal authorisation may be required in the requested country. Requests missing information, or requests that are generally too broad and contradictory to local law may be delayed, returned or rejected.[14] There are also differences in criminal procedure and the law of privacy that impact disclosure. An offence investigated in India might be defined differently in the requested country, and any requirements for dual offences, proportionality or protection of personal information may apply.

One of the important factors in digital investigations is time. Data can be retained, modified by users or lost if a service ceases to exist. Investigators should therefore differentiate between preservation and production. In a preservation request, a provider is asked to preserve identified data for a specified period pending the legal process, without necessarily requiring the provider to disclose the contents of the data. A later production request or order may be required. The evidence may be lost before the formal mutual legal assistance process can be completed. Narrowing down the account, period and data desired can minimize delay.[15]

The domestic power to intercept, monitor or decrypt information in computer resources is provided under section 69 of the Information Technology Act 2000.[16] It enables the Central Government or a State Government (or a person designated by the Central Government) to instruct an appropriate agency to carry out the activity provided that certain requirements are met and in the interests of the sovereignty and integrity of India, the defence of India, the security of the State, friendly relations with foreign States, public order, or preventing incitement to the commission of a cognizable offence relating to these matters, or for the investigation of an offence. A subscriber, intermediary or person in charge of the computer resource shall provide the required facilities and technical assistance upon a request by an authorised agency under this section. Failure to provide assistance may attract the punishment specified in this section. The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 provide the procedures and safeguards on these powers.[17]

This should not, however, be interpreted as an unlimited power to gain access to data from any foreign system, or to force foreign companies to share data. It operates subject to statutory conditions, restrictions and jurisdictional limits. Investigators may still need foreign state cooperation under its law and procedures, where the relevant provider or information is located outside India. If a domestic legal requirement conflicts with the legal requirements of another country, the latter may apply to the provider.[18]

Obtaining the information is not the only evidentiary issue. Investigators also have to determine its origins, its integrity and relevance. Records should be captured and moved via documented processes that preserve metadata and minimise the possibility of changes to the record. The Bharatiya Sakshya Adhiniyam, 2023 (BSA), recognises electronic and digital records as evidence. Section 61 does not permit their rejection solely because they are electronic. Their admissibility is subject to the requirements of Section 63.[19] Section 63

[14] Convention on Cybercrime, 23 November 2001, ETS No 185, arts 16, 17 and 29. These provisions address expedited preservation of stored computer data and international cooperation. The Convention is used here as a comparative reference, not as a treaty binding on India.
[15] The Information Technology Act, 2000 (Act 21 of 2000), s 69(1)–(4).
[16] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, rr 3–9.
[17] Ministry of Home Affairs, Government of India, *Guidelines on Mutual Legal Assistance in Criminal Matters*, Internal Security-II Division (2019).
[18] National Institute of Standards and Technology, *Guide to Integrating Forensic Techniques into Incident Response*, NIST Special Publication 800-86 (2006). This provides technical guidance on collecting, preserving and examining digital evidence.
[19] Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), ss 61 and 63.

outlines conditions for the admissibility of electronic records. Even though a record meets these requirements, it does not automatically establish that the record is authentic, complete or correctly attributed to the accused. Further evidence, technical examination and proof of collection may be required. It should include a record of all requests, responses, transfers and forensic steps taken to ensure that the court can determine how the material was retrieved and that its integrity was not compromised during retrieval.

The problem is not that there are no legal mechanisms, but the gap between the speed and complexity of digital investigations and the existing mechanisms. What is missing in the Indian system is the encouragement of early preservation, accurate and properly authorised requests, secure transfer of records and increased cooperation with foreign partners and authorities. Any enhancement must also comply with the regulations of the requested State, as well as the privacy rights of individuals whose data may be collected. Effective cross-border evidence-gathering must be efficient and must not permit excessive or indiscriminate access.[20]

Compelled Disclosure of Encryption Keys, Article 20(3) and the Right to Privacy

The use of encryption in digital devices raises a difficult question for criminal investigations: can an accused person be required to disclose a password or encryption key that allows police to access stored information? The issue involves a conflict between obtaining evidence and protection against compelled self-incrimination. It cannot be answered simply by showing that a device is relevant to an investigation. The legal character of the act demanded from the accused must also be considered.[21]

Article 20(3) of the Constitution of India provides that no person accused of an offence shall be compelled to be a witness against himself. Three requirements must be satisfied: the person must be an accused, the act must involve compulsion, and the compelled act must be testimonial and self-incriminating. The protection is not confined to statements made during trial. In *State of Bombay v. Kathi Kalu Oghad*, the Supreme Court explained that the guarantee extends to compelled testimony obtained during an investigation, but distinguished testimonial communication from physical identifying material. It held that obtaining fingerprints, palm impressions or specimen handwriting does not ordinarily compel an accused to be a witness against himself.[22]

This distinction matters when considering passwords and encryption keys. A fingerprint or DNA sample is generally treated as physical evidence because it does not itself communicate the individual's knowledge or belief. A password, by contrast, is information stored in the person's mind. Requiring an accused to state it may communicate that the person knows the credential and can use it to access specific information. It may also give investigators access to messages, documents or records relevant to the prosecution. These features support the argument that compelled disclosure may be testimonial. However, the Supreme Court has not specifically decided whether an accused can be compelled to reveal an encryption key. The issue must therefore be examined by applying existing constitutional principles.

In *Selvi v. State of Karnataka*, the Supreme Court considered involuntary narco-analysis, polygraph examination and brain electrical activation profile tests.[23] It held that compelling an accused to undergo these techniques violated Article 20(3), because they sought to elicit personal knowledge and responses without voluntary consent. The judgment reaffirmed that testimonial compulsion may occur outside the courtroom and concerns the communicative character of evidence.[24] Its reasoning is relevant because a demand for a memorised password may require the accused to communicate knowledge personally held. However, the

[20] Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023), s 112; Ministry of Home Affairs, Government of India, *Guidelines on Mutual Legal Assistance in Criminal Matters*, Internal Security-II Division (2019).
[21] Constitution of India, art 20(3).
[22] *State of Bombay v Kathi Kalu Oghad*, AIR 1961 SC 1808; (1962) 3 SCR 10.
[23] *Selvi v State of Karnataka*, (2010) 7 SCC 263.
[24] Ibid, paras 100–102.

techniques in *Selvi* are not identical to password disclosure. The judgment is relevant by way of constitutional analogy, not as a direct ruling on decryption. A separate line of authority concerns the provision of physical or identifying samples. In *Ritesh Sinha v. State of Uttar Pradesh*, the Supreme Court recognised a Magistrate's power to direct an accused to provide a voice sample during an investigation. The Court treated a voice sample as physical evidence for comparison, rather than compelled testimony.[25] This reinforces the distinction between providing an identifying characteristic and communicating personal knowledge. It does not establish that an accused can be compelled to disclose a password in the same way. A voice sample is compared with an existing recording; a password may unlock a device and expose information otherwise inaccessible to investigators.

The Information Technology Act, 2000, adds a statutory dimension. Section 69 permits authorised directions for interception, monitoring or decryption on specified grounds, including the investigation of an offence, subject to prescribed procedures and safeguards. Section 69(3) requires a subscriber, intermediary or person in charge of a computer resource to provide facilities and technical assistance when called upon by an authorised agency. Section 69(4) provides punishment for failure to assist. However, the provision does not expressly resolve how this obligation applies when the person asked to disclose a key is an accused under investigation.[26] It also does not state that Article 20(3) is displaced. The assistance requirement must therefore be interpreted consistently with the constitutional guarantees under Article 20(3).[27]

The Bharatiya Nagarik Suraksha Sanhita, 2023, provides a further safeguard. Section 180(2) generally requires a person questioned by police to answer truthfully, but protects that person from questions whose answers would tend to expose them to a criminal charge, penalty or forfeiture. This provision may be relevant when investigators ask an accused to disclose a password during questioning. Its precise application to a demand for a credential, rather than an ordinary question, remains unclear. It nevertheless confirms that police questioning is not an unrestricted power to compel self-incriminating answers.[28]

Article 21 provides an additional constitutional consideration. In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, the Supreme Court recognised privacy as a fundamental right. Access to an encrypted device may reveal private communications, photographs, financial records, location information and third-party data. State interference must satisfy legality, a legitimate state aim and proportionality. A demand for a device's entire password may expose substantially more information than is necessary for a particular investigation. Authorities should consider whether targeted access or forensic extraction of specified data is available.[29]

Investigators may argue that encryption should not create an absolute barrier to investigating particularly serious offences. A device may contain evidence needed to identify offenders, locate victims or prevent further harm. Yet investigative necessity alone cannot determine constitutionality. The nature of the information demanded, the accused's status, the risk of self-incrimination and the scope of access must all be considered. India should clarify these questions through legislation or authoritative judicial interpretation. Until then, compelled disclosure of a memorised encryption key should not automatically be treated in the same way as providing fingerprints or other physical evidence.

Comparative Legal Analysis, Doctrinal Gaps, Recommendations and Conclusion

[25] Ibid, paras 136–137.
[26] *Ritesh Sinha v State of Uttar Pradesh*, (2019) 8 SCC 1.
[27] Information Technology Act, 2000 (Act 21 of 2000), s 69(1), (3) and (4).
[28] Constitution of India, art 20(3); Information Technology Act, 2000, s 69.
[29] *Justice K.S. Puttaswamy (Retd.) v Union of India*, (2017) 10 SCC 1.

The difficulties associated with cross-border electronic evidence and compelled decryption are not limited to India. Different countries have adopted different approaches to balancing investigative requirements with the protection of individual rights. A comparative examination of these approaches helps identify possible solutions for Indian law, particularly because cybercrime investigations frequently involve international service providers and encrypted digital devices.

The United States provides an important example of constitutional protection against compelled disclosure. The Fifth Amendment to the United States Constitution protects individuals against being compelled to act as witnesses against themselves. In *Fisher v. United States*, 425 U.S. 391 (1976), the Supreme Court recognised the distinction between the contents of documents and the testimonial aspects of producing them. The Court explained that the act of production may communicate information about the existence, possession or authenticity of documents. This reasoning later became relevant to disputes involving encrypted devices.[30]

In *United States v. Hubbell*, 530 U.S. 27 (2000), the Supreme Court held that compelled production of documents could have testimonial significance where the individual had to use personal knowledge to identify and assemble the requested material.[31] This decision is relevant to encryption because revealing a password may communicate knowledge that cannot be obtained merely by examining the physical device. However, American courts have not adopted a completely uniform approach to compelled decryption. Some decisions have distinguished between circumstances where investigators already know the existence and ownership of the relevant files and situations where disclosure would reveal previously unknown information. The American approach therefore demonstrates that whether an act is testimonial may depend on the circumstances of the particular investigation. The United Kingdom follows a different statutory approach. Section 49 of the Regulation of Investigatory Powers Act 2000 provides a mechanism through which authorities may issue a notice requiring disclosure of protected information or the provision of intelligible information in specified circumstances.[32] Section 53 establishes offences relating to failure to comply with a valid notice without a reasonable excuse. This framework provides statutory authority for compelling disclosure of protected information, subject to specified legal conditions and safeguards.[33] This framework demonstrates that a legislature can establish specific procedures for compelled decryption rather than relying solely on general investigative powers. However, the United Kingdom's approach cannot automatically be adopted in India because the constitutional protection under Article 20(3) requires independent consideration.[34]

Cross-border evidence collection also requires attention to international developments. The Budapest Convention on Cybercrime, 2001, provides mechanisms for international cooperation in cybercrime investigations. It includes provisions dealing with expedited preservation of stored computer data, preservation and partial disclosure of traffic data, and mutual assistance concerning stored computer data. Its purpose is to improve cooperation between countries while maintaining procedural safeguards.[35] India is not a party to the Convention, although its provisions remain relevant as a comparative reference when considering possible improvements to India's international cooperation framework. The comparison suggests that India should avoid granting broad powers to compel decryption without clearly defining their limits. A statutory framework should distinguish between providing a physical sample and communicating a memorised password. It should also distinguish between access to a particular file and access to the entire

[30] *Fisher v United States*, 425 US 391 (1976).
[31] *United States v Hubbell*, 530 US 27, 36–45 (2000).
[32] Regulation of Investigatory Powers Act 2000 (UK), s 49.
[33] Ibid, s 53.
[34] Constitution of India, art 20(3).
[35] Convention on Cybercrime, 23 November 2001, ETS No 185, arts 16, 17, 29 and 31.

contents of a device. These differences affect both the application of testimonial compulsion and the protection of privacy.[36]

First, every decryption request should require written authorisation from a competent authority and identify the investigation, device or account, and information sought. Access should be necessary and proportionate to the seriousness of the offence under investigation. Where possible, investigators should use targeted forensic methods instead of obtaining unrestricted access to the device. Independent review and records identifying the material accessed would help prevent the excessive collection of personal data.

Secondly, legislation should clarify the relationship between Section 69 of the Information Technology Act and Article 20(3).[37] It should specify whether an accused may be required to disclose a memorised credential and under what conditions. Any rule must preserve the distinction between testimonial communication and the production of physical evidence. It should also prevent compelled disclosure from indirectly requiring an accused to provide an incriminating statement. Clear legislation would reduce uncertainty for investigators, accused persons and courts.

Thirdly, India should improve the process for obtaining evidence from abroad. Investigators should identify relevant accounts promptly, seek preservation where appropriate and submit focused mutual legal assistance requests with adequate supporting material. Standardised request formats, trained cybercrime officers and secure channels for transmitting electronic records could reduce delays. Cooperation with foreign providers must follow lawful procedures and respect the jurisdiction of the state where disclosure is sought. Maintaining the chain of custody and complying with the Bharatiya Sakshya Adhiniyam, 2023, remain important for the collection and presentation of electronic evidence.[38]

A counter-argument is that restrictions on compelled decryption may allow serious offenders to conceal evidence behind encryption. This concern is genuine, particularly where delays in obtaining evidence may endanger victims or frustrate investigations. However, a general obligation to disclose every password would be excessive. It could expose unrelated personal information, confidential communications and third-party data. A targeted procedure subject to independent review offers a more defensible balance between investigative needs and individual rights.

Conclusion

The use of encryption, cloud storage and digital communication has increased with the changing dynamics of criminal investigations. Electronic evidence can be stored overseas, by foreign service providers, and/or protected using encryption techniques that prevent investigators from obtaining relevant information. When seeking evidence through other countries, cooperation must be obtained and foreign procedures must be followed, and when seeking access to encrypted information, it may be questioned whether a person can be compelled to provide such information without violating the right against self-incrimination. Indian legislation should resolve both concerns while not compromising protection under the Constitution.

The Bharatiya Nagarik Suraksha Sanhita, 2023, empowers authorities to seek assistance and access to evidence from foreign authorities, and Section 69 of the Information Technology Act, 2000 confers powers on the authority to intercept, monitor and decrypt. The Bharatiya Sakshya Adhiniyam, 2023, provides rules for the admissibility and use of electronic records as evidence. In practice however, these provisions do not eliminate the practical difficulties. Mutual legal assistance requests can be lengthy and may have other procedural and legal complications due to the obligations imposed on foreign providers and differences in

[36] *Fisher v United States*, 425 US 391, 410–13 (1976); *United States v Hubbell*, 530 US 27, 36–45 (2000).
[37] Information Technology Act, 2000 (Act 21 of 2000), s 69(1)–(4); Constitution of India, art 20(3).
[38] Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), ss 61 and 63; Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023), s 112.

procedures for collecting and producing electronic evidence. To investigate successfully, investigators must have definite procedures, prompt preservation methods, trained personnel, and reliable chain-of-custody procedures.

Compelled decryption must also be approached with great care. The rights to be free from self-incrimination, as guaranteed under Article 20(3), and the right to privacy and personal liberty, under Article 21, are both protected. Statements or other evidence obtained from an accused may reveal knowledge held by that person, whereas fingerprints and other identification samples are treated as physical evidence. The Supreme Court has not specifically determined whether an accused may be compelled to reveal an encryption key. The relevant principles are given in decisions like Kathi Kalu Oghad, Selvi and Ritesh Sinha but these decisions do not directly resolve the issue. Section 69 of the Information Technology Act should, therefore, be used in conjunction with – and not in contravention of – the constitutional guarantees to ensure that disclosure requirements comply with constitutional guarantees.

A balance should be struck between effective investigation and the prevention of excessive access. Legislation or judicial interpretation must clearly explain whether and when an accused can be compelled to provide a memorised credential and clarify the distinction between such disclosure and the provision of physical evidence. Any decryption request should be made by a competent authority, be limited to information that is relevant and be justified by the principles of necessity and proportionality. Access records, logs of accessed content and safeguards for unrelated personal and third-party data should be integrated into the process. India needs to enhance cooperation with foreign authorities and enter into mutual legal assistance agreements while focusing on strengthening the mutual legal assistance procedures for cross-border investigations and standardising the requests made.

Strong encryption might be said to make it easier for perpetrators to conceal information. However, the convenience of investigation must not be allowed to override constitutional safeguards or individual freedoms. Targeted access measures could help investigators, while limiting unwarranted intrusions on privacy and the right against self-incrimination.

Finally, encryption should never be a complete barrier to criminal investigations, and it should not be used as a pretext to undermine fundamental rights. A clearly defined, proportionate and accountable legal framework can improve access to electronic evidence and strengthen prosecutions and protect the freedoms of individuals. Digital investigations are not only judged by how many pieces of evidence they capture but also by how they are conducted: in legally, ethically and constitutionally appropriate ways.