DIGITAL EVIDENCE AND THE LAW: A STUDY ON SEARCH AND SEIZURE POWERS IN INDIA

Manali Palit, School of Legal Studies, Seacom Skills University, Santiniketan, Bolpur, Birbhum, West Bengal, India

ABSTRACT

India's fast digitisation, driven by widespread smartphone use and internet penetration, has brought about revolutionary changes in a number of industries. But there are also serious issues brought about by this digital revolution, especially with regard to cybercrime and privacy protection. This article highlights any shortcomings and suggests possible fixes in India's legal framework pertaining to the search and seizure of digital evidence.

The study assesses how the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), formerly known as the Criminal Procedure Code, and the Information Technology Act, 2000 (IT Act) regulate digital investigations. In view of the historic ruling that established the right to privacy as a fundamental Indian constitutional right, it also examines court rulings pertaining to privacy. This report also compares international best practices from nations such as the US, EU, UK, and Canada. In the Indian context, this comparative lens draws attention to enduring problems such as jurisdictional disputes, encryption obstacles, evidentiary chain-of-custody complications, and procedural shortcomings in digital forensic procedures.

The paper's main recommendations are based on these observations and include strengthening Mutual Legal Assistance Treaties (MLATs) to improve cross-border cooperation, enacting a comprehensive data protection law immediately, and improving the technical skills and digital forensic training of law enforcement organisations. India can develop a fair, rights-based strategy for combating cybercrime by implementing internationally standardised, privacy-conscious investigative practices and legal protections. In a society that is becoming more digitally connected, such reforms are necessary to protect constitutional liberties and guarantee efficient law enforcement.

Keywords: Digital Evidence, Privacy protection, Search and Seizure, Cybercrime.

INTRODUCTION:

Government initiatives have contributed to India's rapid digitisation. The extensive use of computers, smartphones, and internet technologies has fuelled India's rapid digital transformation, which has transformed governance, business operations, and daily life [1]. The rapid advancement of computer technology has made it imperative for nations to update and modernise their administrative and legal capabilities. The internet and other advancements in information and communication technology contribute to this worldwide connectedness. Because the modern world is borderless, it has created a digital environment where people and organisations can reach a wider audience and open up new development opportunities. A more interconnected global society has been shaped by this evolution, which has also improved opportunities and redefined lifestyles and ways of living [2].

Even though technological advancements have greatly benefited people and society at large, there are also serious drawbacks, particularly in regards to cybercrime and privacy violations [3]. The increasing use of digital devices in investigations has made search and seizure procedures more effective; however, there are still concerns about misuse, unauthorised access, and the erosion of personal privacy. Digital forensic investigation is constantly challenged by the speed at which technology is developing, the increasing variety and quantity of digital devices, and the massive amounts of data that these devices may contain. The landscape of evidence in proceedings has undergone significant change since the advent of the digital age [4].

This essay aims to evaluate how successfully India's legal structure strikes a compromise between the right to privacy and the capacity to conduct investigations by analysing the laws governing the search and seizure of digital evidence. It looks for legal shortcomings and difficulties, such as those related to jurisdictional issues, encryption, and procedural safeguards. By contrasting India's strategy with global best practices, the study seeks to pinpoint areas

[1] Manali Palit, *Protecting Online Consumers: A Deep Dive Into Dark Pattern Regulations in India*, 12 International Journal of Creative Research Thoughts (IJCRT) c238 (2024).
[2] *Explosive growth of technologies & potential for conflict*, (July 1, 2021), https://www.visionofhumanity.org/explosive-growth-of-digital-technologies-creating-new-potential-for-conflict/.
[3] Manali Palit, *A Discussion of a New-Age Cybercrime Involving Pig Butchering Scams in India and Legal Implications*, 11 International Journal of Research and Analytical Reviews (IJRAR) 396 (2024).
[4] Moses Ashawa et al., *Digital Forensics Challenges in Cyberspace: Overcoming Legitimacy and Privacy Issues Through Modularisation*, 5 Cloud Computing and Data Science 140-156 (2024).

where it could be improved. The report concludes with policy recommendations to enhance legal clarity, privacy protection, and the efficiency of investigations in the digital era.

In the real world, smartphones and computers are like wallets; in the virtual world, they are like homes; and in a similar way, they are like enormous warehouses. Imagine being a police detective and learning that the person under investigation used his personal computer to help him commit his crimes. An investigation is underway into the murder of the target, who may have left evidence on his computer that he had planned a fake kidnapping to kill his wife. Suppose the investigation in about tax fraud and the target uses a laptop to store her financial documents. Or the investigation is about a drug-smuggling group, and one of the gang members has an Excel worksheet on his computer that lists all the people in the gang who owe him money. In each of these situations, the target's computer contains the crucial evidence you need to support your position in court. You must confiscate the computer and take out the evidence on it in order to identify and bring charges against the culprit [5].

Now picture yourself as someone who has been falsely accused of a terrible crime. When a police detective suspects that your home computer has proof of the crime, they confiscate the computer in order to obtain the evidence. You realize that you have been unfairly targeted as the police take your computer away and that the computer contains a vast amount of extremely personal and possibly embarrassing data stored. By taking possession of that computer, the investigator has gained access to your virtual world including your diary, thousands of private emails, a cache of pornography, drafts of your tax returns, and many more. A lot more information that you were unaware of is also stored on the computer, like web browsing logs that show all of the websites you have visited and search engine queries you have typed in during the past 12 months. Your computer contains all of that data; it is currently being held by the police and is currently under look up [6].

This study looks at how the Indian court system handles the search and seizure of digital evidence and if it complies with international best practices. It examines important laws including the Information Technology (IT) Act and the Code of Criminal Procedure (CrPC), as well as relevant legal decisions. The research paper also cites administrative barriers that delay investigations, including jurisdictional problems and encryption. It evaluates India's

[5] Mark Hamm, *Crimes Committed by Terrorist Groups: Theory, Research and Prevention*, (Sept. 9, 2005), https://www.ojp.gov/pdffiles1/nij/grants/211203.pdf.
[6] *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, (July 28, 2009), https://www.justice.gov/d9/criminal-ccips/legacy/2015/01/14/ssmanual2009_002.pdf.

standing in relation to international norms, including those in the US and the EU, using a comparative perspective and makes policy recommendations to strike A coexistence between individual rights and efficient law enforcement.

STRUCTURE AND SYMMETRY:

This essay is set up to offer a thorough examination of digital evidence search and seizure practices in India. An introduction describing the study's background, scope, and goal comes first. The part on the legal framework looks at important statutes including the Indian Evidence Act (Now the Bharatiya Sakshya Adhiniyam, 2023); the IT Act, and the CrPC (now Bharatiya Nagarik Suraksha Sanhita, 2023). Judicial interpretations that strike a balance between privacy and investigative authority are next examined. The part on procedural issues addresses issues including encryption, chain of custody, and overseas data access. Areas for improvement are highlighted by a comparative analysis of foreign practices. Policy recommendations for legal reforms and capacity building are included at the end of the study, along with a summary of the results and suggestions for further research. Lastly, the references section contains a list of all the sources.

SEARCH AND SEIZURE OF DIGITAL EVIDENCE: PROCESS, CHALLENGES, AND LEGAL FRAMEWORK:

Digital evidence has become an essential part of contemporary investigations due to the increase in the use of computers in criminal activity. In the course of criminal investigations, law enforcement officials now frequently confiscate and search computers, and the evidence they find often serves a crucial part in obtaining convictions. The sheer volume and complexity of data held on digital devices, as well as the technological skills needed to access it, make computer searches intrinsically more difficult than traditional searches for evidence that is physical. Police typically confiscate a suspect's computer and bring it to a lab for thorough examination by forensic experts. Days, months, or even years may pass during these forensic investigations [7].

Suppose Ravi Thakur chooses to rob a bank. He stops outside a nearby branch after driving there and goes inside. He slides over a letter at Sashi's counter that is: "This is a stick up.” Give me all of your money, and nobody will be harmed," he said, revealing a pistol's barrel from his

[7]Bartholomew, Paige, *Seize First, Search Later: The Hunt for Digital Evidence*, 30 TOURO L. REV. 825 (2014), available at https://digitalcommons.tourolaw.edu/lawreview/vol30/iss4/10.

jacket. Ravi takes a bag of cash from the frightened teller and runs to his escape vehicle. Now how the investigations work? Through obtaining firsthand accounts from the Sashi and anybody else who may have witnessed Ravi or his escape vehicle. After that, the investigator gathers tangible evidence, such as the note Ravi left behind, which can be examined for handwriting or fingerprints. A fallen object or other hints could potentially help connect Ravi to the crime. If more proof is needed, the investigator may speak with additional witnesses or look for Ravi's vehicle. If suspicions grow, the police may also check Ravi's house for items that fit the robber's description or marked money. After satisfactory proof has been obtained, Ravi is charged and put on trial. The prosecution will use physical evidence, eyewitness accounts, and search results, and each witness will provide their views to prove Ravi's guilt beyond a reasonable doubt.

But if this crime happens online these physical documents and evidence do not have much to prove the crime. In this matter, the search and seizure of digital evidence is needed. Ravi Thakur chooses to take money by breaking into a bank's system rather than visiting there in person in this digital heist. He uses his Internet Service Provider (ISP) to access the internet from his house, deceiving himself by bouncing his signal off servers in other places, such as a library and a university. He makes a fictitious account with a balance of Rupees 5 lakhs and moves the funds to an untraceable offshore account after figuring out the bank's master password. When a bank employee notices the odd account activity the following day, they call the police. Since there are no eyewitnesses or tangible evidence, the investigator looking into the case understands that this digital crime scene is very unusual. Rather, the investigator has to follow digital evidence, beginning with the IP address logs from the bank's system and following them back to Ravi's ISP to the university, library, and so on. He may install monitoring tools to catch Ravi if he attempts again and none of these steps yield data. After obtaining a warrant to inspect Ravi's computer, a forensic specialist examines it to look for data that could implicate him, including passwords or bank transaction records. Ravi is charged and put on trial after his computer shows digital proof of the theft. Government agents, system administrators from the servers Ravi used, bank staff, and his ISP all testify on behalf of the prosecution. In order to establish Ravi's guilt beyond a reasonable doubt, each witness recounts how they helped link the crime to his computer[8].

[8] Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 *Colum. L. Rev.* 279 (2005), https://ssrn.com/abstract=594101.

THE LEGAL FRAMEWORK:

In India, there is no dedicated law for the search and seizure of digital evidences but this are governed by the existing laws. In the event, if there are reasonable grounds exist, the Code of Criminal Procedure,1973, and now the Bharatiya Nagarik Suraksha Sanhita, 2023, grant police officers the authority to search an accused person's electronic devices while conducting an inquiry [9, 10]. Nevertheless, before conducting any search, the police must first secure a search warrant. However, the legislation permits a police officer conducting an inquiry to conduct a search if he has reasonable suspicion that evidence cannot be collected without excessive delay, as long as he documents his reasons in writing after the search. Any police officer may confiscate goods that may be suspected of being stolen or discovered in a way that raises suspicions of criminal activity [11, 12].

The court or officer may issue a summons, or the officer may issue a written order, to the person who is thought to have the document or item, requiring him to appear and produce it, or to produce it, at the time and location specified in the summons or order [13, 14].

A magistrate has the authority to issue a search warrant for any location where they believe something related to an investigation, including digital evidence, may be found [15, 16].

An investigating officer has the power to carry out a search in an emergency without obtaining permission beforehand, as long as a report is subsequently turned in to the magistrate [17, 18].

Allows the power to track, observe, or decode data that is created, transferred, received, or stored in any computer resource when approved by the federal government or state governments. Keeping the peace, preventing incitement to crime, and preserving national security are among the justifications [19].

In order to support investigations, it requires intermediaries to maintain and store information for a predetermined amount of time, as directed by the government [20]. mandates that

[9] Code of Criminal Procedure, 1973, § 165.
[10]Bharatiya Nagarik Suraksha Sanhita, 2023, § 185.
[11] Code of Criminal Procedure, 1973, § 102.
[12]Bharatiya Nagarik Suraksha Sanhita, 2023, § 106.
[13] Code of Criminal Procedure, 1973, § 91.
[14]Bharatiya Nagarik Suraksha Sanhita, 2023, § 94.
[15] Code of Criminal Procedure, 1973, § 93.
[16]Bharatiya Nagarik Suraksha Sanhita, 2023, § 96.
[17] Code of Criminal Procedure, 1973, § 165.
[18]Bharatiya Nagarik Suraksha Sanhita, 2023, § 185.
[19] Information Technology Act, 2000, § 69.
[20] Information Technology Act, 2000, § 67C.

intermediaries, including internet service providers, assist law enforcement agencies in obtaining information for investigative purposes in compliance with government directives [21].

Electronic documents are accepted as admissible proof. As explained in this section, When technological proof is permitted into court, a certificate is necessary to guarantee its legitimacy [22-23]. In the 2020 case of Arjun Pandit Rao Khotkar v. Kailash Kushanrao Gorantyal, the Supreme Court of India made it clear that this certificate is required [24].

JUDICIAL INTERPRETATIONS:

Courts in the Indian judicial system have addressed the important equilibrium between investigative powers and privacy rights, particularly concerning the utilisation of online evidence. The legal landscape surrounding data protection and monitoring was significantly impacted by the historic Justice K.S. Puttaswamy v. Union of India decision from 2017, the Indian Supreme Court acknowledged the right to privacy as a fundamental right under Article 21. Since then, concerns about privacy of data and technological surveillance have been impacted by this ruling, calling for stronger controls on how authorities can access personal data and safeguards to protect people's privacy [25].

According to the Supreme Court's 2014 decision in Anvar P.V. v. P.K. Basheer, strict guidelines must be adhered to in order for electronic evidence to be accepted, highlighting the chain of custody. According to the court, According to Section 65B of the Indian Evidence Act, digital evidence must be accompanied by a certificate to guarantee its validity and dependability. This decision emphasises how important it is to maintain the chain of custody since any alteration could jeopardise the validity of the evidence presented in court [26].

Another important case that examined the limits of governmental power over online platforms was Shreya Singhal v. Union of India (2015). The court ruled that Section 66A of the Information Technology Act was illegal because it restricted free speech online. This decision set a precedent for protecting individual rights online and cautioning against government overreach in obtaining access to or controlling online communications, even though its main

[21] Information Technology Act, 2000, § 79.
[22] The BharatiyaSakshya Adiniyam,2023, § 61.
[23] The Evidence Act, 1872, § 65B.
[24] *The decision in Arjun Panditrao: Admissibility of electronic evidence in India continues to face hurdles*, (June 7, 2021), https://www.scconline.com/blog/post/2021/06/07/electronic-evidence-2/.
[25] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).
[26] *Anvar P.V. v. P.K. Basheer*, (2014) 10 S.C.C. 473 (India).

focus was liberty of expression [27].

The Indian judiciary has typically maintained that a balanced stance is necessary when it comes to encryption. Although no specific case has called for decryption, courts have ruled that any requests for decryption must adhere to constitutional protections. The ongoing debate about whether messaging companies should permit message tracking is exemplified by the WhatsApp traceability case. In this case, courts have emphasised the need to balance user privacy and national security [28].

Cross-border data access issues are currently being brought to light by the 2020 lawsuit Facebook Inc. v. Union of India. The primary issues in this Supreme Court case are jurisdiction over data stored outside of India and the role that mutual legal assistance treaties (MLATs) play in obtaining access to such data. The court has addressed the privacy concerns of Indian users and highlighted the importance of international cooperation, stating that due process must be followed when obtaining data from other countries [29].

These cases demonstrate how Indian courts have progressively created a framework that balances the demands of law enforcement with the need for privacy, especially with regard to digital evidence and cyber investigations. Procedural safeguards and the requirement for constitutionally sound digital data management procedures have been reinforced by each ruling.

COMPARATIVE ANALYSIS:

The legal systems of various nations have evolved to strike a balance between the demands of law enforcement and the right to privacy. The methods described here focus on best practices for ensuring data integrity, establishing a chain of custody, fixing encryption problems, and facilitating cross-border data access—all of which are important considerations when handling evidence stored electronically.

United States:

The United States has enacted several laws to safeguard private rights and address the unique

[27] *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1 (India).
[28] *Del HC| Whatsapp challenges Intermediary Rules, says traceability will break end-to-end encryption, breach privacy; Union of India says no Fundamental Right is absolute*, SCC Times (May 27, 2021), https://www.scconline.com/blog/post/2021/05/27/del-hc-whatsapp-challenges-intermediary-rules-says-traceability-will-break-end-to-end-encryption-breach-privacy-union-of-india-says-no-fundamental-right-is-absolute/.
[29] *Facebook Inc. v. Union of India*, 2020 SCC OnLine SC 508 (India).

challenges posed by the acquisition of digital evidence. The Electronic Communications Privacy Act (ECPA) sets guidelines for data access and electronic communications in order to safeguard users' privacy.

Additionally, the 2018 Clarifying Lawful Overseas Use of Data (CLOUD) Act encourages cross-border data access by allowing law enforcement to access data stored abroad through bilateral agreements with other countries. In addition to guaranteeing that law enforcement can access necessary data without infringing on people's right to privacy, these regulations set strict standards for data retrieval, storage, and use.

When the U.S. Supreme Court decided in Carpenter v. United States that law enforcement needs a warrant to obtain cell-site location data, it notably upheld Fourth Amendment protections for digital privacy in the context of investigations [30].

European Union:

A rights-based approach to safeguarding digital evidence and privacy has been adopted by the European Union. The General Data Protection Regulation (GDPR), which went into effect in 2018, has set forth comprehensive data protection guidelines that affect how digital evidence is handled, particularly in cross-border investigations.

Strict privacy regulations must be followed in data management and transfer under GDPR, and any access to personal data must be justified. To achieve investigative goals, the least amount of data is needed. Additionally, in cases such as Digital Rights Ireland Ltd v. Minister for Communications, the European Court of Justice (ECJ) has reinforced these protections after ruling that data retention regulations lacking adequate privacy safeguards violated fundamental rights [31]. Through GDPR and related case law, the EU prioritises accountability, transparency, and individual privacy when handling digital evidence, offering a model that protects privacy while permitting lawful access for investigations.

United Kingdom:

The Investigatory Powers Act of the United Kingdom, commonly referred to as the "Snooper's Charter," governs the collection of digital evidence. It includes protections such as independent supervision and the "double-lock" process, which requires a court commissioner and a senior

[30] *Carpenter v. United States*, 138 S. Ct. 2206 (2018).
[31] *Digital Rights Ireland Ltd. v. Minister for Communications*, Case C-293/12, ECLI:EU:C:2014:238.

official to approve requests for data access.

The UK also complies with the GDPR's rules for cross-border data transfer, which balance privacy concerns with security requirements. The decision in the Big Brother Watch v. United Kingdom case by the European Court of Human Rights emphasised the necessity of proportionality in monitoring procedures and reaffirmed the necessity of mandatory and targeted digital surveillance [32].

Canada:

Judicial oversight of law enforcement access and reasonable privacy expectations are central to the Canadian approach to digital evidence. According to the Supreme Court of Canada's ruling in R. v. Spencer, law enforcement normally requires a warrant in order to obtain subscriber data from ISPs because Internet users have a legitimate expectation of privacy with regard to their personal data. In order to handle cross-border data requests, Canada has also set up the Mutual Legal Assistance Treaty (MLAT) system. This procedure entails cooperation and judicial clearance to guarantee privacy and sovereignty while accessing data outside [33]. This methodical, privacy-conscious approach emphasises how important it is for Canada to find a balance between the defence of individual rights and the power of investigation.

Although the Information Technology Act of 2000 in India covers some aspects of cybercrime, it is devoid of specific regulations regarding the collecting of digital evidence, especially with regard to encryption, chain of custody, and cross-border data requests. Although proposed data protection proposals show a shift towards stronger privacy protections, India has not yet enacted legislation that is comparable to the GDPR. The Supreme Court of India has highlighted privacy as a fundamental right in decisions such as Justice K.S. Puttaswamy (Retd.) v. Union of India, highlighting the necessity for India's legal system to change in a way that strikes a balance between privacy and the need for investigations [34]. The necessity for thorough regulations governing digital evidence is further highlighted by the fact that the reliability and In Indian courts, the lack of specific instructions for processing such evidence may affect its legality.

RECOMMENDATIONS:

Accomplish effectively balance the demands of investigations with the right to privacy, India

[32] *Big Brother Watch v. United Kingdom*, Apps. Nos. 58170/13, 62322/14, and 24960/15.
[33] *R. v. Spencer*, [2014] 2 S.C.R. 212 (Can.).
[34] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).

should consider enhancing its digital search and seizure protocols. Given the Puttaswamy ruling's emphasis on privacy, a comprehensive data protection law might outline specifications for digital searches, backed by judicial oversight to ensure that searches are necessary and appropriate.

A systematic chain of custody for digital evidence, akin to Canadian protocols, would prevent tampering and improve the integrity of evidence in court (R. v. Spencer). Efficient data acquisition to combat cross-border cybercrimes would also be made easier by stronger mutual legal assistance treaties (MLATs) and collaborations with countries that have robust data-sharing laws, such as the EU's GDPR framework (Digital Rights Ireland Ltd v. Minister for Communications).

Encryption policies should balance privacy and security by allowing limited, controlled access under court supervision in national security-related situations. Last but not least, specialised training in digital forensics for law enforcement would ensure that digital evidence is handled legally, resolving procedural problems and enhancing investigative abilities.

CONCLUSIONS:

In conclusion, as it continues to embrace rapid technological advancement, India offers both opportunities and challenges in terms of managing digital evidence while upholding individual rights. India's legal system requires particular adjustments to manage the complexities of digital investigations, even though it is changing gradually. This paper highlights the need for India to revise its search and seizure laws, with an emphasis on incorporating privacy rights and developing clear procedural standards. Court decisions like Puttaswamy have laid the groundwork for viewing privacy as a fundamental right, but concrete measures like a specific data protection law, stricter chain-of-custody protocols, enhanced cross-border collaboration, and digital forensics training are required to ensure that digital evidence will be handled equitably as effectively as possible.

Through examining international best practices, India can learn valuable lessons about developing a balanced approach that protects citizens' privacy without compromising the ability of law enforcement to enforce the law. India can use models from countries like the United States, the European Union, the United Kingdom, and Canada to ensure that its framework for digital evidence is robust, transparent, and rights-focused. In conclusion, India's laws and regulations must prioritize both effective crime investigation and civil rights protection if the nation is to suitably meet the demands of the digital age. A judicial system

that is equipped to manage digital evidence in a way that preserves democratic principles and boosts confidence in the legal system and law enforcement would benefit from this alignment.

REFERENCES:

1. Manali Palit, *Protecting Online Consumers: a Deep Dive into Dark Pattern Regulations in India*, 12 International Journal of Creative Research Thoughts (IJCRT) c238 (2024).
2. *Explosive growth of technologies & potential for conflict*, (July 1, 2021), https://www.visionofhumanity.org/explosive-growth-of-digital-technologies-creating-new-potential-for-conflict/.
3. Manali Palit, *A Discussion of a New-Age Cybercrime Involving Pig Butchering Scams in India and Legal Implications*, 11 International Journal of Research and Analytical Reviews (IJRAR) 396 (2024).
4. Moses Ashawa et al., *Digital Forensics Challenges in Cyberspace: Overcoming Legitimacy and Privacy Issues through Modularisation*, 5 Cloud Computing and Data Science 140-156 (2024).
5. Mark Hamm, *Crimes Committed by Terrorist Groups: Theory, Research and Prevention*, (Sept. 9, 2005), https://www.ojp.gov/pdffiles1/nij/grants/211203.pdf.
6. *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, (July 28, 2009), https://www.justice.gov/d9/criminal-ccips/legacy/2015/01/14/ssmanual2009_002.pdf.
7. Bartholomew, Paige, *Seize First, Search Later: The Hunt for Digital Evidence*, 30 TOURO L. REV. 825 (2014), available at https://digitalcommons.tourolaw.edu/lawreview/vol30/iss4/10.
8. Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 *Colum. L. Rev.* 279 (2005), https://ssrn.com/abstract=594101.
9. Code of Criminal Procedure, 1973, § 165.
10. Bharatiya Nagarik Suraksha Sanhita, 2023, § 185.
11. Code of Criminal Procedure, 1973, § 102.
12. Bharatiya Nagarik Suraksha Sanhita, 2023, § 106.
13. Code of Criminal Procedure, 1973, § 91.
14. Bharatiya Nagarik Suraksha Sanhita, 2023, § 94.
15. Code of Criminal Procedure, 1973, § 93.
16. Bharatiya Nagarik Suraksha Sanhita, 2023, § 96.
17. Code of Criminal Procedure, 1973, § 165.
18. Bharatiya Nagarik Suraksha Sanhita, 2023, § 185.

19. Information Technology Act, 2000, § 69.
20. Information Technology Act, 2000, § 67C.
21. Information Technology Act, 2000, § 79.
22. The BharatiyaSakshya Adiniyam,2023, § 61.
23. The BharatiyaSakshya Adiniyam,2023, § 63.
24. The Evidence Act, 1872, § 65B.
25. *The decision in Arjun Panditrao: Admissibility of electronic evidence in India continues to face hurdles*, (June 7, 2021), https://www.scconline.com/blog/post/2021/06/07/electronic-evidence-2/.
26. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).
27. *Anvar P.V. v. P.K. Basheer*, (2014) 10 S.C.C. 473 (India).
28. *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1 (India).
29. *Del HC| Whatsapp challenges Intermediary Rules, says traceability will break end-to-end encryption, breach privacy; Union of India says no Fundamental Right is absolute*, SCC Times (May 27, 2021), https://www.scconline.com/blog/post/2021/05/27/del-hc-whatsapp-challenges-intermediary-rules-says-traceability-will-break-end-to-end-encryption-breach-privacy-union-of-india-says-no-fundamental-right-is-absolute/.
30. *Facebook Inc. v. Union of India*, 2020 SCC OnLine SC 508 (India).
31. *Carpenter v. United States*, 138 S. Ct. 2206 (2018).
32. *Digital Rights Ireland Ltd. v. Minister for Communications*, Case C-293/12, ECLI:EU:C:2014:238.
33. *Big Brother Watch v. United Kingdom*, Apps. Nos. 58170/13, 62322/14, and 24960/15.
34. *R. v. Spencer*, [2014] 2 S.C.R. 212 (Can.).
35. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).