ANALYSIS OF NUANCES OF ELECTRONIC EVIDENCE: WHETHER THEY LEAD TO A BREACH OF RIGHT TO PRIVACY OR NOT?

Legal Upanishad Journal (LUJournal.com)

Vol 1 Issue 3 | November 2023 | pp. 130-140

Jay Parihar, Law Student, Institute Of Law, Nirma University, Ahmedabad

Riddhi Singh, Law Student, Institute Of Law, Nirma University, Ahmedabad

ABSTRACT:

This paper talks about the significance of 'Electronic Evidence', which is in general parlance also referred to as 'Digital Evidence', and the provisions regarding electronic evidence. The paper has also discussed the fundamental right to privacy. Further in the paper, after highlighting the provisions with respect to electronic evidence and the right to privacy, a critical and comparative analysis is drawn to understand whether the collection, seizure, and search of electronic evidence lead to a violation of the right to privacy of the person involved in a case. Later in the paper, an attempt was made to understand the importance of electronic evidence with the help of case laws involving the question of breach of privacy and what role the electronic evidence plays in deciding the cases.

Keywords: *Digital Evidence, Breach of Privacy, Electronic Evidence, Electronic Messages, Right to Privacy.*

LUJ | Legal Upanishad Journal
www.lujournal.com
info@lujournal.com

1. INTRODUCTION

Modernization, with its advent, brought ease to human beings by making available everything at their fingertips. From fulfilling their requirements to storing important data and information, most of it is done electronically with the help of electronic gadgets and devices. The digitalization has compelled many fields to incorporate it and indulge according to it in the modern era. Thus, in the field of law as well, these data, information, and activities of individuals made available on the internet have become a great source of high importance in conducting trials, proceedings, and rendering judgements by acting as electronic evidence.

Electronic evidences are those evidences or forming part of other evidence that is generated by using certain mechanical processes or electronic methods in order to store, create, or communicate any information, data, files, audio, video, images, and other such sorts of uses in a legal course. Under the IEA, 1872, the provision of Section 65B provides for the admissibility of electronic evidence and records generated by electronic means for the original contents whose direct evidence is admissible[1].

When such information's are collected for the legal requirements and to meet ends of justice, it somehow reveals the information pertaining to the personal domain of the individuals, which they might not feel revealing as it may hamper their lives in various aspects of social and personal level, and sometimes this collection and seizure of electronic evidence is done even without the knowledge of the person whose information is being gathered. Thus, such intrusion of law violates and affects the rights of individuals', namely, the right to privacy, which forms an essential part of the right to life that person enshrines to him by the Supreme Law, i.e., the Constitution of the country.

Therefore, this paper tries to incorporate the issue of a violation of the right to privacy of an individual in the process of the collection and seizure of electronic evidence, as this problem is pertinent in today's world due to all the data and information available in the form of electronic records, which could be easily misused and thus result in a violation of the fundamental rights of a citizen given by the constitution. Overall, the paper tries to find the solution as to how and to what extent fundamental rights are being violated by looking at

[1] Indian Evidence Act, 1872 (Act 18 of 1872), s. 65B

different interpretations of our judiciary system and how it has evaluated and dealt with the provisions regarding the issue at hand.

2. LITERATURE REVIEW:

- Kadimisetty S. Sreenadh & CVN Sai Chand, *Digital Evidence and Victim's Right to Privacy in India* (2020)[2]. This paper talks about the significance of digital evidence and the crucial role it plays in the task of deciding a case. The author tried to demonstrate the methods and procedures as to how the digital evidence could be collected, and later it discussed the repercussions of this collection and seizure on the victims right to privacy in light of the sayings of the Supreme Court in its judgments. The latter half of the paper, which discusses the issue of breach of the right to privacy due to the collection and seizure of digital evidence, gave us a brief understanding of the topic, which was very useful for our research. The paper has discussed the issue considering the provisions of the Indian Constitution and the Code of Criminal Procedure, but a reader of this paper will not find the reference to the Indian Evidence Act, 1872, where the concept lies and which it forms the basis of. Thus, the paper is an easy and quick read targeting a specific group seeking data about the collection and seizure and the preservation of digital evidence.

- Agnidipto Tarafder, *Surveillance, Privacy and Technology: A Comparative Critique of the Laws of USA and India* (2015)[3]. The author of this paper has done a comparative study of the breaches of the right to privacy of citizens in two major democratic nations: the United States of America and India. The paper has analysed the provisions and protections granted to the right to privacy. In our research, this paper has helped us understand the development of the concept of privacy in India. The author of this paper is very focused on the laws and provisions relating to the right to privacy both in India and in the USA, which give immense details about the

[2] Kadimisetty S. Sreenadh & CVN Sai Chand, Digital Evidence and Victim's Right to Privacy in India, CORPUS JURIS THE L. J. (2020)
[3] Agnidipto Tarafder, Surveillance, Privacy and Technology: A Comparative Critique of the Laws of USA and India, 57 J. INDIAN L. INSTITUTE (2015)

development of the provisions in this context in both nations. Lastly, the reader could find that the author has done extensive research for the paper.

- Tejas D. Karia, *Digital Evidence: An Indian Perspective* (2008)[4]. This paper encompasses the legal provisions and the nuances of the admissibility of the evidence generated and stored electronically, with a focus on the conditions and standard parameters on the basis of which the said electronic evidence can be made admissible in the court of law in India. Overall, the paper helped us in our research in understanding the India perspective in regards to the implications of legal provisions and the admissibility of the evidence in India. Thus, this paper is the result of a comprehensive study made by the author, which comprises various legal provisions that highlight and give a deep understanding of digital evidence in the context of the Indian legal framework.

3. PROVISIONS AS PER INDIAN EVIDENCE ACT, 1872

The IT Act's Second Schedule introduced new Evidence Act clauses 65A and 65B. Section 5 of the Evidence Act[5] states that evidence can only be offered about facts that are in question or relevant and not other facts, and Section 136 enables a judge to decide whether the evidence is admissible[6]. Section 65A of the Evidence Act[7] adds a new provision allowing the contents of electronic documents to be proved in accordance with Section 65B. Section 65B states that, notwithstanding anything in the Evidence Act, any information included in a digital record, whether it is the contents of a document or communication printed on paper or stored, recorded, or copied in optical or magnetic media produced by a computer (also referred to as computer output in the Act), is considered a document and is admissible as

[4] Tejas D. Karia, Digital Evidence: An Indian Perspective, 5 DIGITAL EVIDENCE & ELEC. SIGNATURE L. REV. (2008)
[5] Indian Evidence Act, 1872 (Act 18 of 1872), s. 5
[6] Indian Evidence Act, 1872 (Act 18 of 1872), s. 136
[7] Indian Evidence Act, 1872 (Act 18 of 1872), s. 65A

LUJ | Legal Upanishad Journal
www.lujournal.com
info@lujournal.com

evidence without additional evidence of the original's production, provided the conditions stated u/s 65(2) are satisfied[8].

The following are the main components of electronic evidence, according to the Indian Evidence Act:

1. The person who has legal authority over the electronic equipment must produce such information in electronic records.
2. The information must be stored as part of the person's routine everyday activities.
3. This information was saved while the user was conducting typical daily activities on the electronic device.
4. When storing or replicating the material information, the electronic equipment must be in a functional state to avoid any potential harm to its operation or distorting the accuracy and authenticity of its material contents.
5. Any type of information storage, copying, or counterpart creation required for production as electronic evidence in a court of law must be free of distortion, manual editing, or manipulation, and it must be true and reliable information that can be admitted as evidence in a court of law.

4. ELECTRONIC MESSAGE

As indicated by the arrangements of Section 88A[9], there is an assumption that an electronic message that the sender passed to the recipient to whom the message is expected to be received through an electronic mail server coordinates with the message that it is the same message that is put into the computer of the sender and is not interpreted in the transmission. No one's identity as the sender of the message, however, is presumed. This section just accepts the authenticity of the sender, not the actual message itself. The definition of electronic records, along with the wide range of documents and systems used for the production of information under the Information Technology Act of 2008, includes, for example, DVDs, CDs, pen drives, telegraphs, audio, video contents, and others that are legally admissible in court.

[8] Indian Evidence Act, 1872 (Act 18 of 1872), s. 65(2)
[9] Indian Evidence Act, 1872 (Act 18 of 1872), s. 88A

5. RIGHT TO PRIVACY: FUNDAMENTAL RIGHT

Across the world, the right to privacy is acknowledged as a fundamental human right and the most crucial aspect of human dignity, forming part of the right to life, and many consider it one of the pillars of democracy. Most governments currently guarantee, to varying degrees, that this right available to all their citizens. As a result, privacy is effectively a limited, but fundamental, right that is universally granted. Privacy is a multifaceted right. It is believed to be of crucial importance, especially in the modern world, because it is essentially a privilege allowed to individuals to safeguard their activities, choices, and private ideas conveyed in the sphere from being revealed or scrutinized by the world at large. Privacy is recognised as a fundamental human right in many international accords. It is a two-fold right that secures the rights of one's own and those of the other individual as well. Privacy is not only restricted to the body of an individual, but it also covers the individual's choice to be free, not intruded upon by others, to have personal freedom and autonomy relating to one's audio, video, data, and other personal information that he or she does not want to make public, thus not violating the personal space of an individual by unwanted interference.

"Right to be left alone; the freedom of a person from any unwarranted publicity; the right to live without any unwarranted intrusion by the public in things with which the public is not necessarily concerned," according to the Black's Law Dictionary. In order to widen its application, the Supreme Court has chosen to read Article 21[10] in combination with the Universal Declaration of Human Rights.

6. EVOLUTION OF DIGITAL EVIDENCE THROUGH LANDMARK JUDGEMENTS

Digital evidence is defined as information or specific data installed for the purpose of investigation that can be saved or transferred by an electronic device. In the celebrated case of Justice K. S. Puttaswamy (Retd.) v. UOI[11], the nine-judge chair of the Apex Court ruled that an individual's "right to privacy" is a part and parcel of Article 21 of the Indian

[10] INDIA CONST. art 21
[11] Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCC 1

Constitution, which provides for the right to life. The court has also made it clear that even though a person is held to be guilty, his or her right to privacy also needs to be protected, and only that part that is essential for the establishment of his crime should be interfered with without hampering his or her dignity.

If we consider the recent Supreme Court decision in the case of P Gopalakrishnan v. State of Kerala[12] and another, which deals with the contents of a memory card or pen drive, it would be considered a document under the Indian Evidence Act. Section 207 of the Criminal Procedure Code requires the magistrate to provide the accused with police reports and documentation for the purpose of a fair trial.

Thus, the question of whether the contents of evidence collected or generated electronically in the form of clips, films, etc. on various devices such as pen drives, software, memory, and other storage cards are deemed documents or not arises in some instances. What if the electronic evidence's contents violate the victim's right to privacy? The issue is whether the victim's right to privacy should take precedence over procedural compliance under Section 207 of the Criminal Procedure Code. What happens between these two is a question before the court. However, the Supreme Court resolved the matter. The Honourable Supreme Court decided this question, declaring that the contents of a pen drive or memory card would be treated as documents, and the accused has the right to get a copy from the magistrate under S. 207 of the Cr.P.C., save in certain instances that violate the victim's privacy[13].

Anvar P.V. v. P.K. Basheer and Others**[14]**: The Supreme Court gave a significant verdict in this case. It had determined and assisted in resolving differences between High Court judgements on the admissibility of electronic (record) evidence.

The sole way to prove electronic evidence as primary or secondary evidence is to produce the original, a copy, or a counterpart attached to a certificate under Section 65B.

The only way any evidence can be admitted in Indian courts is if it is relevant. Any evidence that is acceptable in court must prove an important fact; otherwise, it will be rejected. In many cases, law enforcement officers may collect evidence through illegal tactics in order to

[12] P.Gopalakrishnan Alias Dileep v. State Of Kerala, (2001) 4 SCC. 638
[13] Code of Criminal Procedure, 1973 (Act 2 of 1974), s. 207
[14] Anvar PV v. PK Basheer & Ors, 2014 10 SCC 473

report it to a higher authority. There are various methods of illegally obtaining evidence, such as phone tapping, voice recording, eavesdropping, illegal searches, breaching someone's personal space, and others. Many cases have addressed the question of whether illegally obtained evidence is admissible in a court of law to serve justice.

R.M. Malkani v. State of Maharashtra[15]: The case was about a phone call between a doctor and the corner of Bombay, where the coroner was charged with bribery based on the recording of the phone call. The anti-corruption agency used this recording as evidence, so the question before the court was whether evidence that invaded the officer's privacy and was taken illegally was admissible in court. It was argued that the tape recording did not follow the legal procedure and violated Articles 21 and 20 (3)[16]. The court disagreed, stating that the appellant conducted the conversation voluntarily and without coercion and that the protection under Article 21 was for an innocent person against wrongful interference, not for a guilty citizen against the efforts of the police to uphold the law and prevent corruption of public servants. It was determined that in this case, the method utilised to gather evidence, even though illegal, was not for illicit purposes.

The Puttaswamy decision, as well as the right to privacy as part of Articles 14, 19, and 21[17], have added a new dimension to the admissibility of illegally obtained evidence. The judgement correctly establishes the right to consent in connection with both the physical body and personal data. Thus, in the 2017 case, the Apex Court set the precedent that the right to privacy is also not absolute and can be put to certain limitations by reasonable restrictions. The effects of the decisions might be seen in the following cases:

In 2019, the Supreme Court of India held in Ritesh Sinha v. State of Uttar Pradesh[18] that a judicial order to an accused person to submit a voice sample as evidence intrudes on a person's privacy, and the Hon'ble Justice Deepak Gupta held that the fundamental right to privacy cannot be construed as absolute and must yield to compelling public interest.

[15] R. M. Malkani v. State Of Maharashtra, 1973 SCR (2) 417
[16] INDIA CONST. arts. 21, 20(3).
[17] INDIA CONST. arts. 14, 19, 21.
[18] Ritesh Sinha v. State of Uttar Pradesh, (2019) 8 SCC 1

Deepti Kapur v. Kunal Julka[19], a case involving a pending divorce suit in the family court, was decided by the Delhi High Court in 2020. The crux of the problem was that the husband utilised a compact disc (CD) to record an audio-video of his wife talking to a friend about the husband's family in a defamatory and harsh manner. In her written declaration to the family court, the wife claimed that the conversation was private and that the proof of recording invaded her right to privacy and was taken illegally, making it inadmissible in court.

7. OUTLOOK OF COURTS: INDIAN PERSPECTIVE

Though the right to privacy has not been an integral part of the right to life since its very inception, as a result, the right to privacy has had its own journey and is interpreted by the judiciary system in the below-mentioned cases.

- In the case of P. Sharma and Others v. Satish Chandra[20], the issue was whether the search and seizure in order to collect evidence and complete the trial were violating the fundamental rights of the concerned under Article 19(1)(d) and Article 20(3) and whether such collection and search constituted a breach of the privacy of the individual. In this case, a majority of an eight-judge Constitution bench decided that the right to privacy was not a fundamental right under the Indian Constitution. They also said that search and seizure are necessary to protect social security and that the process of search and seizure is a temporary interference for which there is no need for statutory recognition. It's also stated for the breach of privacy that, at the time of drafting the Constitution, the drafters had no intention to make the power of search and seizure subject to the right to privacy.

- In the case of Kharak Singh v. The State of U.P. & Others[21], the accused challenged the constitutionality of putting him under surveillance for the collection of evidence electronically, even after being acquitted by the court, as it is violating his fundamental right of movement under Article 19(1)(d) and of personal liberty and privacy under Article 21 of the Indian Constitution. It was ruled that night-time domiciliary visits by the officials were unconstitutional, but it upheld the surveillance

[19] Deepti Kapur v. Kunal Julka, 2020 SCC OnLine Del 672
[20] M. P. Sharma and Others v. Satish Chandra, 1954 SCR 1077
[21] Kharak Singh v. The State of U.P. & Others, 1963 AIR 1295

and other regulations as written. Majorly, the court agreed that the Constitution of India does not expressly provide for the right to privacy. Thus, here the infringement was not termed a breach of the privacy of the accused.

- Taking a historical step, the Indian judiciary gave its citizens the verdict in the case of J. KS Puttaswamy (Red.) v. UOI, holding that individuals' "right to privacy" is a fundamental component of their "right to life," which is protected by Article 21 of the Indian Constitution. The victim is also an individual who is entitled to a fundamental right to privacy. Thus, this principle led down here is a fundamental principle that should not be violated unless and until extremely necessary.

- Following the principle of the Puttaswamy judgement, in the case of P. Gopalakrishnan v. State of Kerala and another, there was a conflict between the victim's right and the procedure that is to be followed by the magistrate in sending the police reports and other submitted documents to the accused to conduct a fair trial under Section 207 of the Cr.P.C. However, considering the fundamental right of privacy, the court held that the magistrate can supply the documents to the accused as per Section 207 of the Cr.P.C., except the documents that tend to infringe the right to privacy of the victim.

Therefore, it is quite evident that evidence collect, stored, preserved, seized and search are made should be now done in the ambit of the Indian Constitution as the Right to Privacy is well recognized as an integral part of the Personal Liberty and right to life under Article 21 of the constitution.

8. SUGGESTIONS & CONCLUSION

British jurisprudence has had a significant impact on the Indian legal system, as seen by the applicability of several legal principles. Electronic evidence is accepted in Indian courts, as it is in other nations, and the 'relevancy' criterion is applied. According to the judiciary's interpretation of the cases, the right to privacy is an inherent aspect of one's right to life and

personal liberty, which should not be taken away, and for the fair conduct of proceedings, evidence that violates an individual's privacy should be extended.

However, with the recent acknowledgement of the right to privacy as a fundamental human right, this field of law is projected to improve and trend towards the exclusionary rule of American jurisprudence in situations involving violations of citizens' personal rights in order to acquire evidence. The Puttaswamy decision, as well as the right to privacy provided by Articles 14, 19, and 21, have broadened the scope of illegally obtained evidence. In 2017, the Supreme Court also ruled that the right to privacy is not absolute and that the state may impose reasonable restrictions in order to enforce the law and protect state interests. However, the conditions for getting justice cannot be decreased in order to strike a balance between the right to privacy and the interests of the state. And it cannot be accomplished by jeopardising one's personal liberty and choice. Obtaining and proving evidence in court is an important aspect of criminal law, but doing so at the price of someone's privacy, particularly when it comes to phone tapping and searches, is also an injustice.