PRIVACY CONCERNS IN THE DIGITAL AGE: THE LEGAL LANDSCAPE OF ELECTRONIC EVIDENCE IN INDIA

Sakshi Sharad Ghadge*

INTRODUCTION

The existence of the human race has been cultivating and evolving through millions of centuries. This escalation has led to numerous innovations in the arena of "**Privacy laws"**. The RIGHT TO PRIVACY has multiple dimensions and can be unfolded in various manners.[1] The inscriptions of the concept of privacy can be enshrined in the *Indian Constitution* under **ARTICLE 21.**[2]

ARTICLE 21[3] safeguards the right to privacy and upholds individual dignity. Recently, concerns have increased regarding the vast amount of personal information stored in computer files. The right to privacy encompasses an individual's control over the collection, use, and disclosure of their personal information.[4] This information can include personal interests, habits, activities, family and educational records, communications (such as mail and telephone records), medical records, and financial records. The presence of computerized data about an individual jeopardize the usual life, especially if the information is inaccurate or misleading.[5] Such data can be rapidly and inexpensively transferred to unauthorized third parties, potentially causing significant harm to the individual. Protection should primarily reconcile these conflicting interests regarding information. In recent times, digitalization in India has shown an evolutionary scope which has led to the use of electronic evidence in the court of law.[6] However, this development in cyberspace has sowed a seed for growing cybercrime, which

*BBA LLB, THIRD YEAR, SYMBIOSIS LAW SCHOOL, PUNE.

[1] Singh, Shiv Shankar. "PRIVACY AND DATA PROTECTION IN INDIA: A CRITICAL ASSESSMENT." *Journal of the Indian Law Institute* 53, no. 4 (2011): 663–77. http://www.jstor.org/stable/45148583.

[2] NDIA C CONST. art. 21

[3] *Ibid*

[4] Supra Note 1

[5] *Ibid*

[6] Duraiswami, Dhiraj R. "Privacy and Data Protection in India." Journal of Law & Cyber Warfare, vol. 6, no. 1, 2017, pp. 166–86. JSTOR

should thereby be protected since the usage of such available data on the internet can led to crimes like identity theft, cyber stalking, fraud etc.

Hence, the data of individuals and organizations should be protected in a way that their privacy is not compromised in any circumstance. However, such personal information of citizens is certainly used if necessary as evidence if necessary in any trial.

RESEARCH QUESTIONS

How does the legal framework in India address the balance between privacy rights and the necessity for electronic evidence in legal proceedings?
What are the key challenges in using electronic evidence in criminal trials while ensuring the protection of individual privacy rights?
What are the legal remedies available to consumers in India when their privacy rights are violated by service providers?
What are the key differences in the legal standards for the admissibility of electronic evidence in India compared to other jurisdictions?

RESEARCH OBJECTIVES

To analyze how the Indian legal framework addresses the balance between privacy rights and the necessity for electronic evidence in legal proceedings.
To evaluate the effectiveness of current laws, such as the Information Technology Act and the Indian Evidence Act, in protecting individual privacy while allowing for the use of electronic evidence.
To evaluate the effectiveness and accessibility of these remedies under current consumer protection and data protection laws.
To identify key differences and potential areas for improvement in India's approach to balancing privacy rights with the need for electronic evidence in legal proceedings.

ANALYSIS

BACKGROUND OVER NECESSITY "EVIDENCES" IN A CRIMINAL TRIAL

An offence is considered to be taken under a criminal trial only when there is a commitment to a crime. Such crime should be defined under the laws in India such as the **BHARATIYA NYAYA SANHITA (BNS).**[7] Although, the burden to prove the accusation made by the prosecution is on the accused to prove his/her innocence. Such a trial requires necessary evidence to support the arguments presented by the accused. These evidences can be documentary evidences, direct evidences, secondary evidences etc.[8] A physical document is considered authentic if it is faithful to the original, uncorrupted, and has a verified history, showing attributes like uniqueness and clarity. Even though electronic evidence is different from paper documents, the rules for authenticating documentary evidence are still important for electronic evidence.[9]

MEANING OF DATA PROTECTION AND DATA PRIVACY

There are two crucial aspects to consider: data privacy and data protection. **Data privacy refers to the conditions, timing, and extent to which a consumer's personal data can be shared and communicated with others.** This personal information may include name, address, ethnicity, phone number, marital status, and more. With the rise in internet usage over the years, the need for robust data privacy regulations has become increasingly urgent. Data protection, on the other hand, involves the legal safeguarding of data against loss, damage, or corruption. With data now being collected at an unprecedented rate, ensuring the protection of this data from unauthorized sources has become a critical issue.

PROVISIONS UNDER THE INFORMATION TECHNOLOGY FOR DATA PROTECTION

SECTION 43A[10] of the ***Information Technology Act***[11] holds a body corporate liable for damages if it negligently mishandles sensitive personal data or information, resulting in wrongful loss or damage. The **Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011,**[12] outlines the

[7] Bharatiya Nyaya Sanhita (BNS), 2023, No. 47, Acts of parliament (India)
[8] Supra Note 1
[9] *Ibid*
[10] Information Technology Act, 2000, § 43 § A, No.21, Acts of Parliament (India)
[11] Information Technology Act, 2000, No.21, Acts of Parliament (India)
[12] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

necessary security measures to protect sensitive personal data, such as financial information, sexual orientation, and medical records.

Under **SECTION 43A,**[13] a body corporate that is negligent in implementing and maintaining reasonable security practices, thereby causing wrongful loss or gain to any person, is liable to pay damages by way of compensation to the affected person. In the case of ***Poona Auto Ancillaries Pvt. Ltd. v. Punjab National Bank,***[14] an amount of Rs. 80.10 lakh was transferred from the complainant's account to a third party without authorization. Upon investigation, none of the ultimate transferees could be located, and it was discovered that the information provided by these transferees to the respondent bank was falsified. The adjudicating officer determined that the respondent bank had been negligent in following security practices and directed the bank to pay Rs. 45 lakhs in damages to the complainant.[15]

Under **SECTION 72A**[16] of the IT Act[17], penalties are imposed for unauthorized disclosure of information. If someone knowingly and intentionally discloses information without the individual's consent, thereby breaching a lawful contract, they can face a fine of up to Rs. 5,00,000 or imprisonment for up to three years. **SECTION 87**[18] under the IT Act, grants the Central Government the authority to make rules. It explicitly states that the Central Government is empowered to create rules, via notification in the official gazette, to implement the provisions of the Act.

RULES FOR DATA PROTECTION UNDER INFORMATION TECHNOLOGY RULES 2011

THE INFORMATION TECHNOLOGY (*Reasonable Security Practices and Procedures and Sensitive Personal Data or Information)* **RULES, 2011**[19], established under **SECTION 87(2)**[20] in conjunction with **SECTION 43A**[21] of the **Information Technology Act,**[22] provide extensive protection for personal data. These rules address fundamental aspects of data protection,

[13] Supra Note 10
[14] Punjab National Bank v. Poona Auto Ancillaries Pvt. Ltd., 2018 SCC OnLine TDSAT 937
[15] Singh, Atul. "DATA PROTECTION: INDIA IN THE INFORMATION AGE." *Journal of the Indian Law Institute*, vol. 59, no. 1, 2017, pp. 78–101. *JSTOR*, https://www.jstor.org/stable/26826591. Accessed 2 Aug. 2024.
[16] Information Technology Act, 2000, § 72 § A, No.21, Acts of Parliament (India)
[17] Supra Note 11
[18] Information Technology Act, 2000, § 87, No.21, Acts of Parliament (India)
[19] Supra Note 12
[20] Information Technology Act, 2000, § 87§ 2, No.21, Acts of Parliament (India)
[21] Supra Note 10
[22] Supra Note 11

including consent, notice, collection limitation, use limitation, rectification, and onward transfer.

RULE 3[23] categorizes sensitive personal data to include passwords, financial information, physical, physiological, and mental health conditions, sexual orientation, medical records and history, and biometrics. Biometrics encompass techniques for measuring and analyzing fingerprints, eye retinas and irises, voice patterns, facial patterns, hand measurements, and DNA.

Under **RULE 4**[24], a body corporate must clearly state its policy for handling personal information, detailing the types of sensitive personal data collected, the purpose of collection and usage, and the security practices in place. **RULE 5**[25] mandates obtaining consent for data collection and ensuring data collection is proportional to its purpose. A body corporate must not collect sensitive personal data unless required for a lawful purpose related to its functions. The data should not be retained longer than necessary for performing lawful functions and should be used only for such purposes, thereby enforcing use limitation and confining data retention. **RULE 5(6)**[26] allows data subjects to review and request corrections to their personal data held by the data controller, ensuring individual participation. **RULE 6**[27] requires prior permission from the data subject before disclosing personal data to a third party.

RULE 7[28] permits the transfer of personal information to a third party that provides adequate data protection as envisaged under the rules *(though the term 'adequacy' is not explicitly defined in the rules)*. According to **RULE 4**[29], a body corporate is required to publish its privacy policy on its website.

Upon accessing the websites of **Bharti Airtel Ltd., Vodafone India Ltd., Bharat Sanchar Nigam Ltd. (BSNL), and Mahanagar Telephone Ltd. (MTNL),** it was found that the private

[23] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, § Rule 3, 2011
[24] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, § Rule 4, 2011
[25] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, § Rule 5, 2011
[26] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, § Rule 5 § 6, 2011
[27] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, § Rule 6, 2011
[28] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, § Rule 7, 2011
[29] Supra Note 24

sector service providers had easily accessible privacy policies that detailed the information as prescribed under the rules. However, no privacy policy statement was available on the websites of the state-owned BSNL and MTNL, indicating a lackadaisical approach towards data protection by these service providers and raising questions about the enforcement of these principles.

Under **SECTION 67C**[30] of the **Information Technology Act, 2000**[31], an intermediary may be required to preserve and retain personal information. According to the license agreement between the Government of India and cellular mobile telephone service providers, these service providers are required to preserve billing and accounting records for a period of three years and commercial records related to communications exchanged for a period of one year.[32]

These rules and guidelines also work as a bridge between the "privacy concerns" and "necessary information". Although, when it comes to presenting the information about the individuals concerned in the court of law, the line between them both is quite blurry. Such disparity has led to concerns in regard to the presenting of personal data as evidences.

CONSUMER PROTECTION ACT IN THE LIGHT OF DATA PROTECTION

Personal information, such as an innocuous phone number, can potentially be associated with a unique name, age, gender, financial status, and physical location of a natural person. Under **SECTION 67C**[33] of the ***Information Technology Act, 2000***[34], an intermediary may be required to preserve and retain such personal information. According to the license agreement between the Government of India and cellular mobile telephone service providers, these service providers are required to preserve billing and accounting records for three years and commercial records related to communications exchanged for one year.[35]

[30] Information Technology Act, 2000, § 67 § C, No.21, Acts of Parliament (India)
[31] Supra Note 11
[32] Preservation of Telecom Records, Ministry of Communications & Information Technology, Government of India Aug. 26, 2010, available at: http://pib.nic.in/newsite/PrintRelease.aspx?relid=65325 (last visited on Nov. 15, 2016)
[33] Supra Note 30
[34] Supra Note 11
[35] Singh, Atul. "DATA PROTECTION: INDIA IN THE INFORMATION AGE." Journal of the Indian Law Institute, vol. 59, no. 1, 2017, pp. 78–101. JSTOR, https://www.jstor.org/stable/26826591. Accessed 2 Aug. 2024.

Despite providing one of the strongest mechanisms for consumers to enforce claims related to breaches of contracts or torts, the **Consumer Protection Act, 1986**[36], has seen limited success in addressing data protection issues. In fact, one of the early cases involving personal data under this Act resulted in a highly contested dispute and, to some degree, judicial mishandling.[37]

A deficiency in service can result from faults, imperfections, shortcomings, or inadequacies in the quality, nature, or manner of performance. In telecommunications, connectivity issues are considered faults or shortcomings in service. However, this might not apply directly to the use of personal information gathered during service provision. The handling of personal data may be part of the performance if telecom providers include data protection in their privacy policies. In this case, the privacy policy can be viewed as part of the contract between the data subject and the data controller.[38]

In the case of ***Nivedita Sharma v. Bharti Tele Ventures,***[39] the complainant was troubled by unsolicited marketing calls from banks and financial institutions. A complaint was filed against Bharti Tele Ventures, ICICI Bank Ltd., and American Express Bank Ltd. The Delhi State Consumer Disputes Redressal Commission concluded that these banks had obtained the complainant's telephone number and financial details from the telecom provider without authorization or the complainant's knowledge or consent. The commission ruled that both the telecom service provider and the entities that acquired the information were guilty of deficiency in service and unfair trade practices.

As a result, the commission imposed a joint penalty of Rs. 50 lakhs on the banks and telecom providers, with an additional penalty of Rs. 25 lakhs to be shared between the banks. The complainant was awarded Rs. 50,000 as compensation. Furthermore, the commission issued a general order entitling any consumer suffering from such nuisances to a minimum compensation of Rs. 25,000 upon approaching the commission. This order was subsequently challenged before the High Court of Delhi in the case ***Cellular Operators Association of India v. Nivedita Sharma.***[40]

[36] Consumer Protection Act, 1986, No. 35, Acts of Parliament (India)
[37] Supra Note 34
[38] *Ibid*
[39] Nivedita Sharma v. Bharti Tele Ventures, 2007 (1) CPJ 186.
[40] Nivedita Sharma v. Cellular Operators Assn. of India, (2011) 14 SCC 337

DNA PROOFING IN EVIDENCE

DNA is the biological material that contains all the genetic information within living organisms, including humans. The ability of human body cells to replicate themselves is due to the presence of the DNA "blueprint" in the chromosomes within each cell's nucleus. Each human cell contains 23 pairs of chromosomes in its nucleus, with one half of each pair inherited from each parent at conception. Although the majority of the information stored in human DNA is common to all humans, certain information is unique to each individual. Only identical twins share identical DNA.[41]

The proper utilization of DNA samples necessitates expertise in molecular biology, population genetics, and statistics. The generation of DNA profiles requires biochemical proficiency.[42] However, several hazards are associated with DNA testing, including the potential mixing of samples prior to testing, mishandling that leads to contamination either during sample collection or later in the laboratory, and contamination with bacterial, viral, or other human or nonhuman DNA at the crime scene. Additionally, testing small samples can complicate the process and render further verification impossible. There is also a risk that the test itself may be conducted incorrectly.[43]

COMPARATIVE STUDY

COMPARATIVE DISPOSITION IN REGARD TO EVIDENCE

In the United States, issues have primarily arisen concerning unlawful search and seizure by the police. The U.S. Supreme Court has ruled that, regarding federal crimes, the Fourth Amendment's[44] search and seizure clause prohibits the admissibility of evidence obtained illegally.[45] In recent years, this principle has been extended. Prior to 1961, the U.S. Supreme

[41] Singh, Subhash Chandra. "DNA PROFILING AND THE FORENSIC USE OF DNA EVIDENCE IN CRIMINAL PROCEEDINGS." *Journal of the Indian Law Institute*, vol. 53, no. 2, 2011, pp. 195–226. *JSTOR*, http://www.jstor.org/stable/43953503. Accessed 3 Aug. 2024.
[42] . Bernard Robertson and G.A. Vignaux, "Expert Evidence: Law, Practice and Probability" (1992) 12 Oxford Journal of Legal Study
[43] National Research Council, DNA Technology in Forensic S Hence, 53-54 (Washington, DC; National Academy Press, 1992)
[44] The Fourth Amendment reads: "The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures shall not be violate….."
[45] Weeks, v. United States, 232 U.S. 383 (1914)

Court had not applied any prohibition on the admissibility of illegally obtained evidence under the "due process" clause of the American Constitution.[46]

The U.S. Supreme Court's rationale for excluding such evidence includes the deterrence of constitutional violations, emphasizing that the exclusion of illegally obtained evidence is necessary to compel adherence to constitutional guarantees by removing any incentive to disregard them. The Court warned that a government's failure to observe its own laws, or worse, its disregard for its foundational charter, could lead to its swift downfall. By 1949, only seventeen states had adopted the exclusionary rule, but by 1961, when the landmark Mapp case was decided, about half of the states had embraced the rule. However, the Mapp decision has not been extended to civil and non-criminal proceedings. For instance, in ***United States v. Janis***[47], the Court ruled that the exclusionary rule did not apply to an Internal Revenue Service proceeding, a civil action, even when the illegal search was conducted by local police. The Court noted that extending the exclusionary rule in such a manner would hinder the enforcement of valid laws and render relevant and reliable evidence inadmissible. [48]

CONCLUSION

In conclusion, the task of balancing privacy rights with the necessity for electronic evidence in legal proceedings within India is both intricate and dynamic. As the reliance on digital data intensifies in legal contexts, the legislative framework, notably the **Information Technology Act** [49]and its accompanying regulations seeks to safeguard personal data through rigorous standards and penalties for non-compliance. Nevertheless, challenges remain in ensuring the authenticity and admissibility of electronic evidence while protecting privacy.

A comparative examination with international practices, such as the exclusionary rule in the United States, reveals divergent approaches to evidence admissibility and privacy protection. Although India has made significant advancements in data protection, inconsistencies in enforcement, exemplified by cases like ***Nivedita Sharma v. Bharti Tele Ventures***[50], highlight the need for ongoing refinement of legal norms and practices. The overarching challenge is to

[46] Wolf v. State of Colorado, 338 U.S, 25 (1949)
[47] United States v. Janis , 428 U.S. 433 (1976)
[48] Jain, S. N. "ADMISSIBILITY OF ILLEGALLY OBTAINED EVIDENCE." *Journal of the Indian Law Institute*, vol. 22, no. 3, 1980, pp. 322–27. *JSTOR*, http://www.jstor.org/stable/43950696. Accessed 3 Aug. 2024.
[49] Supra Note 11
[50] Supra Note 39

achieve a harmonious balance between the imperative of utilizing electronic evidence and the imperative of upholding stringent privacy safeguards, thereby ensuring that legal proceedings serve both justice and individual rights.

BIBLIOGRAPHY

CASES

Punjab National Bank v. Poona Auto Ancillaries Pvt. Ltd., 2018 SCC OnLine TDSAT 937

Nivedita Sharma v. Cellular Operators Assn. of India, (2011) 14 SCC 337

Weeks, v. United States, 232 U.S. 383 (1914)

Wolf v. State of Colorado, 338 U.S, 25 (1949)

United States v. Janis, 428 U.S. 433 (1976)

STATUES

Bharatiya Nyaya Sanhita (BNS)

Information Technology Act, 2000

Consumer Protection Act, 1986

JOURNALS

Jain, S. N. "ADMISSIBILITY OF ILLEGALLY OBTAINED EVIDENCE." *Journal of the Indian Law Institute*,

Singh, Subhash Chandra. "DNA PROFILING AND THE FORENSIC USE OF DNA EVIDENCE IN CRIMINAL PROCEEDINGS."

Bernard Robertson and G.A. Vignaux, "Expert Evidence: Law, Practice and Probability" (1992) 12 Oxford Journal of Legal Study

Preservation of Telecom Records, Ministry of Communications & Information Technology, Government of India