Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
Special Issue on Art, Design, and Media Convergence in the Digital Era: An Analytical Study of Creative Practices 7(7s)

CYBERSECURITY AND DATA PROTECTION LAWS IN INDIA: CHALLENGES AND PROSPECTS

Gargi Bhattacharya [1]

[1] Research Scholar, PG Department of Law Gauhati University, Jalukbari, Guwahati, Assam

Received 26 January 2026
Accepted 29 March 2026
Published 19 May 2026

Corresponding Author
Gargi Bhattacharya,
Gargi.bhattacharya@outlook.com

DOI
10.29121/shodhkosh.v7.i7s.2026.8201

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

In an increasingly digitized world, the protection of personal data and the assurance of cyber security have emerged as fundamental legal and ethical imperatives. Privacy, long recognized as a core human right, has evolved from the classical notion of "the right to be let alone" to encompass the protection of personal information in digital spaces. This paper examines the evolution of data privacy and protection laws globally and within India, tracing their development from early international instruments such as the Universal Declaration of Human Rights (1948) and the European Convention on Human Rights (1950) to modern frameworks like the OECD Guidelines (1980) and the European Union's General Data Protection Regulation (GDPR). The study highlights the progressive recognition of informational privacy as an extension of constitutional rights under Article 21 of the Indian Constitution, particularly following the landmark judgment in Justice K.S. Puttaswamy v. Union of India (2017).

The paper provides a comprehensive analysis of India's legislative landscape governing data protection, focusing on the Information Technology Act, 2000, its 2008 amendments, and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. It further explores the transformative impact of the Digital Personal Data Protection Act, 2023 (DPDP Act), which represents India's first unified data protection framework emphasizing consent, accountability, and individual rights. The discussion also contextualizes the role of emerging legal instruments such as the Bharatiya Nyaya Sanhita (BNS), Bharatiya Sakshya Adhiniyam (BSA), and Bharatiya Nagarik Suraksha Sanhita (BNSS) in shaping the future of cyber law and data governance.

Ultimately, the paper underscores the necessity for a robust, harmonized, and technology-responsive legal framework that balances individual privacy rights with national security, transparency, and digital innovation in India's evolving cyber ecosystem.

Keywords: Data Privacy, Cyber Security, Legislation, Constitution, India

1. INTRODUCTION

Privacy being a fundamental human right, protects human dignity and other values like freedom of association and freedom of speech. Privacy has emerged as one of the most important human rights of the modern age. [1]

Privacy is recognized around the world in different regions and cultures. It is protected in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and in many other international and regional

[1] Nikolay Omelchenko, 'Protecting Human Rights in Digital Age' in *The Human Being in Contemporary Philosophical Conceptions* 287 https://books.google.co.in/books?id=SvMYBwAAQBAJ accessed 12 March 2026

instruments recognizing human rights. Almost every country in the world includes the right of privacy in its Constitution. The least these provisions include are the rights of inviolability of the home and secrecy of communications. The Courts have identified that right in other provisions, in the countries where privacy is not specifically recognized in the Constitution. [2] Ever since it was first articulated by Justice Brandeis in 1898, the concept of privacy has evolved in the United States. The definition of privacy by Justice Brandeis, "The right to be let alone", has been influential for nearly a century. Further and more sophisticated legal inquiry into the meaning of privacy was encouraged since 1960s, till about 1980s, due to the proliferation of information technology and concurrent developments in the law of reproductive and sexual liberties. In the digital environment of present times, where personal information can be transported and distributed around the world in seconds, the vision of Justice Brandeis of being "let alone" does not suffice to define the concept of privacy. [3]

With the expansion and development of new technical innovations, societies and governments have also come to acknowledge their significance. Strong computer systems' capacity for monitoring has led to calls for particular regulations controlling the gathering and use of personal data.

The word privacy has been derived from the Latin word "Privatus" which means separate from rest. [4] It implies the capability of an individual or group to seclude themselves or information about themselves and thereby reveal themselves selectively. We can interpret privacy as a right of an individual to decide who can access his information, when such information can be accessed and what information they can access.[5] Privacy is not only a human need but also individual's interest with several dimensions. One of these dimensions is privacy of personal data known as 'Data Privacy'. [6]

The first data protection law was passed in Germany in 1970, and this is where contemporary laws in this field got their start. Following the pattern, laws were passed in Sweden (1973), the US (1974), Germany (1977), and France (1978). Ideas about privacy became more complex at the end of year 2000. It reflected the rapid and remarkable advances that thecomputers have made in storage, manipulation, and sharing of data. [7]

The Constitution of India defines privacy as personal liberty in Article 21 as, "Protection of Life and Personal Liberty: No person shall be deprived of his life or personal liberty except according to procedure established by law." Privacy is considered as one aspect of the fundamental rights provided in Part III of the Constitution. Privacy is recognized atan international level as a human right in different dimensions. They are privacy of person, privacy of personal behaviour, privacy of personal communication, privacy of personal data. [8]

2. OBJECTIVES OF THE STUDY

- To examine the evolution and development of laws relating to cyber security and data privacy in India and across the world.
- To analyze the constitutional and statutory provisions governing the right to privacy and data protection in India.
- To evaluate the adequacy of existing legal frameworks and suggest measures for strengthening data protection and cyber security mechanisms.

3. RESEARCH METHODOLOGY

The present study adopts a doctrinal research methodology primarily based on secondary data sources. It involves an in-depth analysis of constitutional provisions, statutory laws, judicial pronouncements, and scholarly writings related

[2] SN Parikh, *Nature and Scope of the Right to Privacy and the Problem of the Protection of this Right in India: Comparative Perspective to USA and UK* 20 http://shodhganga.inflibnet.ac.in/ bitstream/10603/98806 /11/11_chapter%204.pdf accessed 13 March 2026
[3] Ibid
[4]Karnika Seth, *Computers, Internet and New Technology Laws* (LexisNexis Butterworths Wadhwa 2012) 273
[5]Ibid
[6]Jyoti Rattan, *Cyber Laws & Information Technology* (Bharat Law House Pvt Ltd 2012) 383
[7]Richard Hixson, *Privacy in a Public Society: Human Rights in Conflict* (1987) 3; Barrington Moore, *Privacy: Studies in Social and Cultural History* (1984)
[8]Tim Mather, Subra Kumaraswamy and Shahed Latif, *Cloud Security and Privacy* (1st edn, O'Reilly Media 2009) 145

to cyber security and data privacy. The research relies on books, journals, reports, and online legal databases to interpret and evaluate the existing legal framework governing data protection in India and abroad. Through a qualitative approach, the study critically examines the evolution, adequacy, and effectiveness of current legislations, drawing comparative insights from global data protection regimes to suggest reforms for strengthening India's digital privacy landscape.

4. EVOLUTION OF DATA PROTECTION AS A CONCEPT

1) Ancient Period

The seeds of privacy consciousness were planted in ancient civilizations, though they manifested differently across cultures. In ancient Greece, Aristotle made a fundamental distinction between the polis (public sphere) and the oikos (private household). This division wasn't merely spatial—it represented different realms of human existence. The polis was where citizens engaged in political life, debated public matters, and participated in democracy. The oikos, conversely, was the private domain of family, personal relationships, and domestic affairs. [9]

This Greek conceptualization laid groundwork for Western privacy thinking. The Romans further developed these ideas, creating legal protections for the home as a private sanctuary. The famous principle "a man's home is his castle" traces back to Roman law, which recognized the sanctity of private spaces.

2) Medieval Period

In the medieval period, the information of individuals, which was confined to a small geographic area or community, began to be more accessible as a result of advent of letterwriting, postcards and diaries. Established churches of some societies created and maintained "population records", of events like baptisms, marriages and burials. Capturing and collection of personal data further expanded with the advancement in medicine, law and education.

3) Modern Period

Limitless global transmission of data of all kinds is the status quo in the age of the internet. The phrase 'data privacy' refers to the privacy of information associated with an individual or to the privacy of the contents of electronically transmitted communications, though there are several possible interpretations of the term. [10]

4) Global Scenario of Data Protection

The genesis of data protection laws can be traced back to the late 19th century when American lawyers Samuel Warren and Louis Brandeis published their seminal article "The Right to Privacy" in the Harvard Law Review, describing privacy as "the right to be let alone". This publication marked a pivotal moment in the legal landscape, emphasizing the need for data privacy as technological advancements began to impact personal privacy. [11]

Internationally, the right to privacy gained legal recognition with the United Nations' Declaration of Human Rights in 1948, which explicitly included privacy rights. This was further developed in Europe with the establishment of the European Convention on Human Rights in 1950, which included Article 8, safeguarding an individual's "private and family life, his home and his correspondence". [12]

The legal frameworks continued to evolve with the adoption of the Organization for Economic Cooperation and Development (OECD) Guidelines in 1980, which were among the first international efforts aiming for a harmonized privacy framework. These guidelines laid down principles such as consent, security, and accountability, which are foundational to modern data protection laws. Another significant piece of legislation is the Council of Europe's Convention, 1981 for the Protection of Individuals with Regard to Automatic Processing of Personal Data. This Convention established privacy as a human right recognized in Europe. These regulations together set the stage for the

[9]'The Evolution of Privacy: From Ancient Times to Modern Law' https://philosophy.institute/social-political/evolution-privacy-ancient-times-modern-law/ 5 April 2026

[10]Gail Lasprogata, Nancy J King, Sukanya Pillay and others, 'Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy Through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada' (2004) 4 *Stanford Technology Law Review* 9–10 https://www.sukanyapillay.com/wp-content/uploads/Regulation-of-Electronic-Employee-Monitoring.pdf accessed 5 April 2026

[11]'Data Protection Laws Around the World: A Global Perspective' https://gdprlocal.com/data-protection-laws-around-the-world-a-global-perspective/ accessed 10 March 2026

[12]Ibid

adoption of the EU Data Privacy Directive. [13] In October of 1995, the data privacy concerns of the EU were globalized by implementing an unprecedented regulation known as the EU Data Privacy Directive, viz. EU Directive 95/46/EC ("EU Directive"). [14] The EU Directive takes a firm stance on the importance of protecting personal data by limiting global negotiations regarding data privacy by having effective provisions that maintain a synergy with the European perspective on individual privacy as a fundamental right. [15] Though the EU Directive does not act as binding law on member nations, it is a guiding recommendation, or goal, like all directives issued by the EU, for legislation that should be adopted by each nation. The EU Directive reassures the views of EU on data privacy and confirms that data privacy is a serious concern.

In Asia, the landscape of data protection laws is rapidly evolving. Countries like China, Thailand, Indonesia, and Sri Lanka have recently enacted comprehensive data protection laws. For instance, Indonesia's Personal Data Protection Act includes specific provisions for data processing bases, breach notifications, and the appointment of data protection officers. Similarly, Sri Lanka's Personal Data Protection Act applies both locally and extraterritorially, reflecting a growing trend in the region toward expansive privacy legislation. These laws, however, vary significantly in their specific provisions and enforcement mechanisms, illustrating the diverse approach to data privacy across Asian countries. [16]

5. INDIAN SCENARIO OF DATA PROTECTION

On the backdrop of this global scenario, India is far behind and it lacks a unified regulatory approach to data protection. However, like the United States, India too has sectoral laws governing data protection in particular industries like telecommunications, public financial institutions, and information technology, which are regulated by national legislations. [17] The Telecom Regulatory Authority of India ("TRAI") is a body which protects consumers by making it binding on telecommunications service providers to guard subscribers' privacy whenever national security is not implicated. [18] The Public Financial Institutions Act of 1993 provides for provisions which intend protect confidentiality in bank transactions. [19]

Data Protection laws may be defined as the laws which are enacted for safeguarding and protecting the data.[20] In this section, an endeavour has been made to deal with various laws of India, which play a vital role in the legal regime governing data privacy and data protection.

6. LEGISLATIONS GOVERNING CYBER SECURITY AND DATA PROTECTION IN INDIA

India has come a long way in its quest for achieving a hassle-free and citizen-oriented legal framework in the field of information technology. Though there is a need for drastic reforms in this area of laws, it would be interesting to see the journey and evolution of Indian laws in the field of information technology and data protection.

1) The Constitution of India

Though the Constitution of India is not a legislation in strict sense of the term, it is the framework within which all laws made by the legislature of India are required to operate. The Constitution is thus the cornerstone on which all laws are founded.

Article 21[21] and Right to Privacy

[13]Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data [1995] OJ L281/31, art 28

[14] Ibid

[15]Directive 95/46/EC, art 1(1)

[16]'Data Protection Laws Around the World: A Global Perspective' https://gdprlocal.com/data-protection-laws-around-the-world-a-global-perspective/ accessed 12 March 2026

[17]Information Technology Act 2000; see also Recovery of Debts Due to Banks and Financial Institutions Act 1993

[18]Telecom Regulatory Authority of India Act 1997

[19]Recovery of Debts Due to Banks and Financial Institutions Act 1993

[20]Vaibhavi Pandey, 'Data Protection Laws in India: The Road Ahead' (ICCA) http://www.mondaq.com/india/x/408602/data+protection/data+protection+laws+in+india+the+road+ahead accessed 12 March 2026

[21]Constitution of India, art 21

Though the Constitution of India does not contain a provision granting a general right to privacy, it has been recognized by the Indian judiciary as implicit in Article 21 and Article 19 (1) (a) [22] of the Constitution in many cases. The scope and ambit of the right of privacy or right to be left alone was considered by the Supreme Court in R. Rajagopal v. State of T.N. [23] during 1994. In this case the right of privacy of a condemned prisoner was in issue. By interpreting the Constitution in light of case laws from the United Kingdom and United States, it was held that though the right to privacy was not enumerated as a fundamental right, it could certainly be inferred from Article 21 of the Constitution. In another significant case People's Union of Civil Liberties v. the Union of India, [24] it was held by the Supreme Court that tapping a person's telephone line violated his right to privacy, unless it was required in the gravest of grave circumstances such as public emergency. [25]

It is provided under Article 21 of the Constitution of India that "No person shall be deprived of his life or personal liberty except according to procedure established by law." However, 'right to privacy' is not specifically recognised by the Constitution of India as a fundamental right. [26] Article 21 of the Constitution guarantees every citizen the fundamental right to life and personal liberty which has been interpreted by the Indian courts, to include the right to privacy. This right further extends to data in electronic forms, which is specified by the Indian courts in the terminology 'informational privacy. [27]

Hon'ble Supreme Court, in the case of Justice K. S. Puttaswamy (Retd.) v Union of India, [28] dealt with Right to privacy in detail which is popularly known as the 'Aadhaar card case'. In this case, the Aadhar card scheme was challenged on the ground that collecting and compiling the demographic and biometric data of the residents of the country to be used for various purposes is a breach of the fundamental right to privacy embodied in Article 21 of the Constitution of India. [29] On the backdrop of the ambiguity in prior judicial precedents on the constitutional status of right to privacy, the Hon'ble Supreme Court referred the matter to a constitutional bench consisting of nine judges.

In the landmark judgment, the Supreme Court upheld the Constitutional validity of the Aadhar Act and made it clear that Right to privacy is included in Article 21 of the Constitution. Going a step ahead, it was also held by the Supreme Court that informational privacy is an important facet of Right to privacy. This terminology of 'informational privacy' necessarily implies the privacy of individual's information, i.e. data.

Article 19(1) and Right to Privacy

In State of Uttar Pradesh V. Raj Narain, [30] the Supreme Court held that it is not in the interest of the public to 'cover with a veil of secrecy the common routine business of the State and it is the responsibility of the official to explain and the justify their acts. It is the chief safeguard against oppression and corruption. [31]

The right to impart and receive information is an important and intrinsic facet of the right to freedom of speech and expression as guaranteed under 19 of the Constitution. [32] Every citizen of India has a right to use the best means of imparting and receiving information. It is the duty of the State to respect the fundamental rights of the citizens, and the State is also under an obligation to ensure conditions under which the right can be meaningfully and effectively enjoyed

[22]Constitution of India, art 19(1)(a)
[23]*R Rajagopal v State of Tamil Nadu* (1994) 6 SCC 632
[24](1997) 1 SCC 318
[25]Shyamkrishna Balganesh and Niranjan Maitra, 'Cryptography, Privacy and National Security Concerns' in *Law Relating to Computers, Internet and E-commerce* (2nd edn, 2001) 377
[26]Economic Laws Practice, 'Data Protection and Privacy Issues in India' https://elplaw.in/wp-content/uploads/2018/08/Data-Protection-26-Privacy-Issues-in-India.pdf accessed 12 March 2026
[27]Vidushpat Singhania, 'Is There a Database Right to Protection in India?' https://www.lakshmisri.com/News-and-Publications/Archives/Publication/Is-there-a-database-rightprotection-in-India accessed 12 March 2026
[28]*KS Puttaswamy v Union of India* (2017) 10 SCC 1
[29] Ibid
[30]1975 SCR (3) 333
[31](1975) 4 SCC 428
[32]Pravin Dalal, 'The Needs and Modes of Data Protection' http://www.electroniccourts.in/ privacylawsindia/?author=2 accessed 12 March 2028

by one and all. At the same time, Article 19(2) [33] permits the state to make any law in the interest of sovereignty and integrity of India, the security of state relations with other state and thereby impose reasonable restriction on the exercise of rights conferred by Article 19(1)of the Constitution. Thus, the data protection rights have to be tested against principles of Article 19(2) in a given case and the facts and circumstances of each case will govern the availability of this right.

Though the right to information is indisputably a fundamental right, it is always subject to the reasonable restrictions. Right to information is a facet of "right to speech and expression" as provided in Article 19(1)(a). Right to know has set a transparency and determines accountability in the working of public department. Implementation of Right to Information Act, 2005 has led to reduction in corruption in public departments. [34]

7. OTHER STATUTES GOVERNING DATA PROTECTION AND CYBER SECURITY

The primary set of legislations governing data privacy in India are the Information Technology Act, 2000 (the "IT Act") and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011114 (the "Privacy Rules").Another primary legislation governing data protection and cybersecurity in India is the Digital Personal Data Protection Act, 2023 (DPDPA), which came into effect on August 11, 2023. This act establishes a framework for processing digital personal data, focusing on individual privacy rights and lawful data processing.The DPDPA is India's first comprehensive data protection legislation, aiming to regulate the collection, use, and disclosure of digital personal data.

"Sensitive Personal Data or Information" ("SPDI") Rules is a subset of Indian laws regulating the processing of personal information. As per SPDI Rules, sensitive personal data or information comprises of, amongst other things, information relating to passwords, financial information, medical records, sexual orientation, and biometric information. Non-sensitive personal information is still an unregulated area in India. Due to the vagueness of consent under the Indian legal framework, the requirement for consent often creates chances of implied consent. The applicability of Indian laws is not clear, when it comes to conferring extraterritorial jurisdiction on the courts of law. For example, if a citizen of India shares his personalinformation with a company in the USA, while he is travelling in the USA, it is questionable whether the IT Act or the Privacy Rules would apply to such collection of information or the breach of privacy of such citizen and his personal data. [35]

On this backdrop, it is necessary to deal with the IT Act and the Privacy Rules in detail.

1) Information Technology Act, 2000.

The preamble of the Information Technology Act, 2000 provides its aims and objectives as under:

"An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as electronic commerce, which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto."

Government's Power to Interfere with the Personal and Professional Data

Section 69[36] of the IT Act provides as under: "If any person or officer authorized by the Government is satisfied that it is necessary or expedient so to do in the interest of sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, for reasons to be recorded in writing, by order,

[33]Article 19(2): Nothing in sub-clause (a) of clause (1) shall affect the operation of any existing law, or prevent the State from making any law, in so far as such law imposes reasonable restrictions on the exercise of the right conferred by the said sub-clause in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence.

[34]Aman Deep Kaur, 'Right to Know – Constitutional Perspective' http://www.legalservicesindia.com/article/ 1743/Right-to-Know-Constitutional-Prospective.html accessed 12 March 2026

[35]Pillsbury Winthrop Shaw Pittman LLP, 'Data Protection Laws in India' https://www.lexology.com/library/detail.aspx?g=818a8528-f387-4ccd-b42f-080ea58ffe34 accessed 12 March 2026

[36]Section 69 - Power to issue directions for interception or monitoring or decryption of any information through any computer resource.

can direct any agency of the Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in anycomputer resource."

Thus, Section 69 provides for interception and monitoring as well as decryption for the purpose of investigation of cybercrimes. This is an absolute intrusion in the privacy of an individual. The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, have also been notified by the Government of India under the abovementioned Section 69. These Rules deal with the blocking of websites. These powers of interception are certainly required to be curtailed by means of defining the ambit and limit of the intrusion.

Penalty for Damage to Computer, Computer Systems, etc.

Section 43[37]of the IT Act, imposes a penalty without prescribing any upper limit, for doing any of the following acts: "If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network;

1) accesses or secures access to such computer, computer system or computer network;
2) downloads, copies or extracts any data, computer database or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
3) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
4) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;
5) disrupts or causes disruption of any computer, computer system or computer network; f. denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means; (g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;
6) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network, he shall be liable to pay damages by way of compensation to the person so affected.
7) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;
8) steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage." [38]

This provision is an endeavour to address almost every possible infringement of privacy of an individual or entity by others. The legislature has tried to consider several possible instances of breach of data privacy. However, the biggest challenge in India is the procedural lapse of time and the lack of technical expertise amongst the judiciary and law enforcement agencies. Due to these challenges, it is necessary to make provision of a legal framework which shall address these technological issues more effectively and efficiently.

8. TAMPERING WITH COMPUTER SOURCE

Section 65 [39]of the IT Act lays down as under:

"Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up tothree years, or with fine which may extend up to two lakh rupees, or with both." [40]

[37] Section 43 - Penalty and compensation for damage to computer, computer system, etc
[38]Ibid
[39]Section 65 - Tampering with computer source documents.
[40] Ibid

Computer Related Offences

Section 66[41] provides that:

"If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both"

Thus, this provision provides for punishment for a class of offences and is an effective mechanism providing imposition of fine as well as imprisonment. However, the criticalanalysis of Section 43 made hereinabove is applicable to this Section as well.

Penalty for Breach of Confidentiality and Privacy

Section 72 [42]of the IT Act makes provision for penalty for breach of confidentiality and privacy. The Section provides that:

"Save as otherwise provided in this Act or any other law for the time being in force, if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both."

Thus, even a lawful access to confidential information, followed by unlawful disclosure is made punishable under this Section. This is an effective provision which prevents unlawful disclosures of the confidential information, which is sought lawfully.

2) Information Technology (Amendment) Act, 2008

The IT Act was originally enacted with an intention to provide legal recognition to e-commerce transactions and to impose sanctions on the misuse of computers. It had no specific and express provisions governing the security of data. Individuals who intercepted in the computer systems of others could be prosecuted and punished under Sections 43 and 66 of the IT Act, however, other effective remedies were not provided by the IT Act, e.g., provisionsto initiate legal action against the corporates holding the personal data of its consumers were not clear.

Therefore in order to address the newly emerging concerns of the digital revolution in India, the IT (Amendment) Act, 2008 was enacted, which, inter alia, incorporated two new and effective sections into the IT Act, Section 43A and Section 72A[43], to protect and to provide remedy to persons who have suffered or who are likely to suffer a loss on account of their personal data not having been protected with adequate and lawful compliances.

Section 10A[44] was inserted in the IT Act for dealing with the validity of contracts formed through electronic means. It lays down that "contracts formed through electronic means shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose." [45] It is a revolutionary step in the evolution of evidentiary jurisprudence, since it has widened the scope of documentary evidence.

The IT Amendment Act, 2008[46]substituted and inserted the following important provisions:

1) Section 43A - Compensation for failure to protect data.
2) Section 66 - Computer Related Offences.
3) Section 66A - Punishment for sending offensive messages through communication service, etc. [47]
4) Section 66B - Punishment for dishonestly receiving stolen computer resource or communication device.
5) Section 66C - Punishment for identity theft.

[41]Section 66 - Computer related offences.
[42]Section 72 - Penalty for breach of confidentiality and privacy.
[43]Section 72 - Penalty for breach of confidentiality and privacy.
[44]Section 10A - Validity of contracts formed through electronic means, inserted by Act 10 of 2009, (w.e.f. 27/10/2009).
[45] Ibid
[46]The Information Technology (Amendment) Act, 2008, Act 10 of 2009, which came into effect on 27/10/2009.
[47]Section 66A was struck down by Supreme Court's Order dated 24/03/2015 in the *Shreya Singhal vs. Union of India*, AIR 2015 SC 1523.

6) Section 66D - Punishment for cheating by personation by using computer resource.
7) Section 66E - Punishment for violation for privacy.
8) Section 66F - Punishment for cyber terrorism.
9) Section 67 - Punishment for publishing or transmitting obscene material in electronic form.
10) Section 67A - Punishment for publishing or transmitting of material containing sexually explicit act, etc, in electronic form.
11) Section 67B - Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc, in electronic form.
12) Section 67C - Preservation and Retention of information by intermediaries.
13) Section 69 - Powers to issue directions for interception or monitoring or decryption of any information through any computer resource.
14) Section 69A - Power to issue directions for blocking for public access of any information through any computer resource.
15) Section 69B - Power to authorize to monitor and collect traffic data or information through any computer resource for cyber security.
16) Section 72A - Punishment for disclosure of information in breach of lawful contract.
17) Section 79 - Exemption from liability of intermediary in certain cases.
18) Section 84A - Modes or methods for encryption.
19) Section 84B - Punishment for abetment of offences.
20) Section 84C - Punishment for attempt to commit offences.

3) Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, which are more popularly known as the Sensitive Personal Data (SPD) Rules, were notified by the Ministry of Communications and InformationTechnology (Department of Information Technology) on 11th April, 2011 vide Notification No. G.S.R. 313(E). Main highlights of the SPD Rules are as follows: [48]

1) By issuance of a Press Note132 on 24th August 2011, it was clarified by the Ministry of Communications and Information Technology that the SPD Rules were applicable to a body corporate or any person located within India. Thus, while addressing the issues relating to cyber security involving cross-border transfer of data, the question of applicability and jurisdiction of these Rules pose a great hurdle.
2) Rule 3 of the 2011 Rules the types of information which is to be treated as 'sensitive personal data'. This information, inter alia, includes information relating to passwords, credit/debit cards, biometric data such as DNA, fingerprints, voice patterns, etc. This information may be used for the purpose of authentication or to determine physical, physiological and mental health condition, etc. It is further clarified that any information, which is freely available or accessible in the public domain, shall not be construed to be 'sensitive personal data'.
3) Rule 4 provides that a body corporate seeking sensitive personal data must draft a privacy policy and make it easily accessible to people who are providing the information. The privacy policy is required to be clearly published on the website of the body corporate and it is further required that such privacy policy should contain details about the type of information that is being collected, the purpose for which such information has been collected and the reasonable security practices that have been undertaken to maintain the confidentiality thereof.
4) The guidelines that are required to be followed by a body corporate while collecting information are provided in Rule 5 of the 2011 Rules.133 These guidelines impose following duties on the body corporate:

[48]Ministry of Communications and Information Technology, 'Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011' http://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf accessed 12 March 2026

- Body corporate needs to obtain consent in writing, i.e. in physical or electronic mode, from the person(s) providing information to such body corporate. The consent must be obtained before collecting such sensitive personal data. The electronic mode of consent is included by the Press Note issued by the Ministry of Communication and Information Technology, which is mentioned hereinabove;
- The body corporate must not collect the information otherwise than for lawful purpose and unless it is necessary for the purpose for which it is collected. The body corporate must use the information so collected only for the purpose for which it is collected, and it must not retain the information for a period longer than it is required for such purpose.
- The body corporate should ensure that the person(s) providing such information are aware about the fact that the information is being collected, the purpose for which it is collected and the names and addresses of the agencies and recipients, who will be collecting and retaining the information;
- The body corporate must not retain the information longer than the time which is required for using the information for the purpose for which it is collected or for the time which is otherwise required under any other law for the time being in force;
- An opportunity must be provided by the body corporate to the person providing such information, to review the information provided and make corrections, if required;
- An option must be provided by the body corporate to the person(s) providing information, to not provide the information sought, if the person so desires;
- The body corporate is duty bound to maintain the security of the information provided; and
- A grievance officer must be designated by the body corporate. The name and contact details of such grievance officer must be published on the website. The officer shall be responsible to expeditiously address grievances of information providers and must resolve the same with a maximum period of one month.

5) It is interesting to note that Rule 6 of the 2011 Rules makes it mandatory upon a body corporate to seek prior permission of the information provider before disclosing suchinformation to a third party, but no such permission is required when the information is disclosed by the Government, as required by law or when it is disclosed by any third party pursuant to a lawful order. [49]
6) The nature of reasonable security processes and procedures that are required to be implemented by body corporates are provided under Rule 8. One of such standards is the international standards, IS / ISO / IEC 27001. These standards are required to be implemented by a body corporate to maintain data security. It is further provided under Rule 8 that the body corporate should carry out an audit of reasonable security practices and procedures through a certified auditor, at least once a year or whenever the body corporate undertakes significant upgradation of its process and computer resources. [50]
7) It is also made clear by the Ministry in the Press Note that "a body corporate providing services relating to collection, storage, dealing or handling of sensitive personal data or information under contractual obligation with any legal entity located within or outside India is not subject to the requirement of Rules 5 & 6. Body corporate, providing services to the provider of information under a contractual obligation directly with them, as the case may be, however, is subject to Rules 5 & 6." [51]

4) Right to Information Act, 2005

Preamble of the Right to information Act, 2005 (the "RTI Act") provides as under:

"An Act to provide for setting out the practical regime of right to information for citizens to secure access to information under the control of public authorities, in order to promote transparency and accountability in the working

[49]Ibid
[50]Ibid
[51] Press Information Bureau, 'Clarification on Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 under section 43A of the Information Technology Act 2000' https://pib.gov.in/newsite/erelcontent.aspx?relid=74990 accessed 12 March 2026

of every public authority, the constitution of a Central Information Commission and StateInformation Commissions and for matters connected therewith or incidental thereto."

The RTI Act confers a right to know upon the citizens of India and equips them with a lawful right to access the information held by Government and governmental bodies. It can be said that the right to Information and right to privacy are complementary and supplementary to each other. In fact it is expected that they should not be the rivals of each other but should cohabit as the two sides of the same coin. However, a conflict is often found between the two rights, which is contrary to their nature. The conflict often occurs when the State exceeds in the exercise of its powers in withholding the information possessed by the State or in intruding over the privacy of the citizens under the garb of its lawful authority. Globally, more than 110 countries have recognised the right to information and right to privacy and have adopted the principles of privacy and right to know in their national laws. As many as fifty countries across the globe have guaranteed the right to Information in their Constitutions. [52]

5) Bharatiya Nyaya Sanhita (BNS)

The Bharatiya Nyaya Sanhita (BNS) addresses various cybercrimes, including those related to data protection, in conjunction with the Information Technology (IT) Act, 2000 and the Digital Personal Data Protection Act, 2023.

Under the IPC, Section 66A (before it was struck down) dealt with offensive messages through communication service, while Section 67 penalizes the publishing or transmission of obscene material in electronic form.Additionally, the BNS introduces more comprehensive provisions aimed at modernizing the approach towards cybercrimes, reflecting the need for updated legislation in line with technological advancements.The BNS sections related to cyber laws emphasize offenses such as identity theft, cyberstalking, and data breaches, ensuring stricter penalties and greater protection for individuals in the digital realm. [53]

Here are some key sections of the BNS that relate to data protection and associated cybercrimes: [54]

- Section 303: This section deals with theft, including data theft. It defines theft as dishonestly taking movable property (which can include data) without consent and specifies punishments of up to three years imprisonment, a fine, or both.
- Section 316: This section criminalizes breach of trust involving data, where a person entrusted with property (including data) dishonestly misappropriates or converts it to their own use. Criminal penalties for breach of trust may apply concurrently with the remedies available under the Digital Personal Data Protection Act (DPDP Act).
- Section 317: This section pertains to receiving stolen property, including stolen mobile phones, computers, or data. Punishment can be imposed even for the possession of such property by third parties.
- Section 318: This section addresses various types of fraud, including password theft, creation of bogus websites, and cyber frauds. Punishments vary based on the gravity of the offense.
- Sections 336-338: These sections deal with digital forgery and identity theft. They cover offenses like email spoofing, online forgery, and creating false documents or electronic records with intent to harm reputation or for the purpose of cheating.
- Section 356: This section penalizes defamation, including sending defamatory content through email, with imprisonment and fines.

6) The BharatiyaSakshyaAdhiniyam (BSA)

Before the BharatiyaSakshya Adhiniyam, 2023[55], the Indian Evidence Act, 1872, governed the admissibility of evidence, including electronic records. Adhiniyam has widened the scope of the general applicability of the BSA via Section 1(2), as compared to the old Indian Evidence Act, 1872.BharatiyaSakshyaAdhiniyam (BSA) has significantly expanded the scope of the terms 'evidence' and 'documents'.

[52]'Global RTI Rating and its Flaw' http://www.iasparliament.com/interviews/upsc-interviewmaterials/global-rti-rating-and-its-flaw-51 accessed 12 March 2026

[53]Pratibha Singh Khushwala, 'Data Privacy in India: Laws, Security, and Responsibilities' https://www.linkedin.com/pulse/data-privacy-india-laws-security-responsibilities-advocate-hpe1c accessed 12 March 2026

[54]Bharatiya Nyaya Sanhita, 2023

[55]Bharatiya Sakshya Adhiniyam, 2023

Section 2(d) defining the term "document" has significantly increased its ambit by using the term 'any other means' as a mode of expression, description or recording. Moreover, by its very definition documents are meant to include electronic and digital records. Illustratively, electronic records on server logs or any documents on your laptop are documents and can be used as evidence.

Section 2(e) of the Bharatiya Sakshya Adhiniyam defines the term "evidence" (the old Section 3 of The Indian Evidence Act, 1872). The new definition includes electronically given statements as oral evidence (e.g. statements by a witness via video conferencing) and electronic or digital records as documentary evidence. [56]

7) Bharatiya Nagarik Suraksha Sanhita(BNSS)

The Bharatiya Nagarik Suraksha Sanhita (BNSS) does not have specific sections directly addressing data protection, as it is a procedural law for criminal matters, not a data privacy act. However, its provisions on the recording and use of electronic evidence, such as Sections 105 and 185(2), are relevant to data privacy by dictating how digital information (video and audio recordings) is collected and managed during investigations.

- Sections related to data collection and management: [57]
- Section 105: Mandates the recording of searches and seizures through audio-video means.
- Section 185(2): Requires the audio-video recording of searches conducted by a police officer, with the proviso that such recordings are preferably made using a mobile phone.
- Definition of "audio-video electronic means" (Section 2(a)) and "electronic communication" (Section 2(i)): These definitions clarify the scope and methods of digital recording and communication, including the use of mobile phones, computers, and other electronic devices for processes like evidence collection and transmission.

8) Digital Personal Data Protection Act (DPDP Act) 2023

Overview and Objectives of the Act:

The Digital Personal Data Protection (DPDP) Act of 2023 is India's first comprehensive framework for regulating digital personal data. The act focuses on safeguarding individual privacy while ensuring that organizations can process data lawfully for legitimate purposes. It outlines the rights of individuals (Data Principals) and the responsibilities of organizations and Government entities (Data Fiduciaries) that handle personal data.The Act governs the processing of digital personal data within India. It also applies to organizations outside India if they process the digital data of individuals within India in connection with offering goods or services. However, it does not cover data used by individuals for personal or domestic purposes, nor does it apply to data that is already made public by law.[58]

The law is founded on seven core principles:[59] The law is founded on seven core principles that guide the processing of personal data. First, it emphasizes consent and lawfulness, requiring that personal data be processed only for lawful purposes and with the explicit consent of the individual. Secondly, the principle of purpose limitation ensures that data is used solely for the specific purpose for which it was collected. The principle of data minimization mandates that organizations collect only the minimum amount of data necessary to achieve that purpose. Further, the principle of accuracy places a responsibility on Data Fiduciaries to ensure that the data they process remains correct and up to date. In addition, the storage limitation principle restricts the retention of data to only as long as it is required for the intended purpose. The law also incorporates a security principle, requiring Data Fiduciaries to adopt reasonable safeguards to protect personal data from breaches and unauthorized access. Finally, the principle of accountability ensures that Data

[56]'Decoding Bharatiya Sakshya Adhiniyam 2023: Comparative Insights and Study with Indian Evidence Act 1872' https://www.lexisnexis.in/blogs/decoding-bharatiya-sakshya-adhiniyam-2023-comparative-insights-study-with-indian-evidence-act-1872/ accessed 12 March 2026
[57]Bharatiya Nagarik Suraksha Sanhita 2023
[58]Digital Personal Data Protection Act 2023
[59]Ibid

Fiduciaries are held responsible for compliance with the Act and for any violations that may occur. Key definitions under the Act further clarify the scope and application of these principles.

Key Definitions Under the Act:

Data Fiduciary:

Entities responsible for collecting, storing, and processing digital personal data are defined as data fiduciaries and have defined obligations. These include: (a) maintaining security safeguards; (b) ensuring completeness, accuracy, and consistency of personal data; (c) intimation of data breach in a prescribed manner to the Data Protection Board of India (DPB); (d) data erasure on consent withdrawal or on the expiry of the specified purpose; (e) the data fiduciary having to appoint a data protection officer and set up grievance redress mechanisms; and (f) the consent of the parent/guardian being mandatory in the case of children/minors (those under eighteen years of age). [60]

Data Principal:

"Data Principal" means the individual to whom the personal data relates and where such individual is— (i) a child, includes the parents or lawful guardian of such a child; (ii) a person with disability, includes her lawful guardian, acting on her behalf; [61]

Consent Manager:

"Consent Manager" means a person registered with the Board, who acts as a single point of contact to enable a Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform; [62]

Rights and Duties of Data Principal: [63]

An individual whose data is being processed (data principal), will have the right to:

1) obtain information about processing
2) ii. seek correction and erasure of personal data,
3) iii. nominate another person to exercise rights in the event of death or incapacity, and
4) iv. grievance redressal

Data principals will have certain duties. They must not:

1) register a false or frivolous complaint, and
2) ii)furnish any false particulars or impersonate another person in specified cases. Violation of duties will be punishable with a penalty of up to Rs 10,000.

Obligations of Data Fiduciaries:

The entity determining the purpose and means of processing, (data fiduciary), must:

1) make reasonable efforts to ensure the accuracy and completeness of data,
2) build reasonable security safeguards to prevent a data breach,
3) inform the Data Protection Board of India and affected persons in the event of a breach, and
4) erase personal data as soon as the purpose has been met and retention is not necessary for legal purposes (storage limitation). In case of government entities, storage limitation and the right of the data principal to erasure will not apply.

Penalties and Enforcement Mechanisms: [64]

[60]Anirudh Barman, 'Understanding India's New Data Protection Law' https://carnegieendowment.org/ research/2023/10/understanding-indias-new-data-protection-law accessed 12 March 2026

[61] Digital Personal Data Protection Act 2023 https://www.meity.gov.in/static/uploads/ 2024/06/2bf1f0e9f0 4e6fb4f8fef35e82c42aa5.pdf accessed 12 March 2026

[62] Ibid

[63]Digital Personal Data Protection Bill 2023 https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023 accessed 12 March 2026

[64]Vajiram Editors, 'What is the Digital Personal Data Protection (DPDP) Act 2023?' https://vajiramandravi.com/ current-affairs/dpdp/ accessed 12 March 2026

Penalty for Infringement:

The Act does not impose criminal penalties for non-compliance. The financial range could range from as high as Rs 250 crores to a data fiduciary or data processor to as low as Rs 10000 to a data principal (the owner of data).

Establishment of a Data Protection Board of India (DPBI):

1) It will function as an impartial adjudicatory body responsible for resolving privacy-related grievances and disputes between relevant parties.
2) As an independent regulator, it will possess the authority to ascertain instances of non-compliance with the Act's provisions and impose penalties accordingly.
3) The appointment of the chief executive and board members of the Data Protection Board will be carried out by the central government.
4) An appeal against any order of the DPBI shall lie with the High Court. The High Court could take up any breach Suo moto.
5) No civil court shall have the jurisdiction to entertain any suit or take any action in respect of any matter under the provisions of this Act and no injunction shall be granted by any court or other authority in respect of any action taken under the provisions of this Act.

Other Provisions:

Citizen's Rights: Under data principal rights, individuals also have the right to information, right to correction and erasure, right to grievance redressal, and right to nominate any other person to exercise these rights in the event of the individual's death or incapacity.

Interplay Between Digital Personal Data Protection Act (DPDP) Act, 2023 and Information Technology Act:

The Digital Personal Data Protection Act, 2023 (DPDP Act) and the Information Technology Act, 2000 (IT Act) in India have a complementary yet distinct interplay, with the DPDP Act replacing specific sections of the IT Act, such as Section 43A and the related rules, and establishing a comprehensive framework for digital personal data protection. While the IT Act deals with a broad range of cybercrimes, electronic commerce, and digital signatures, the DPDP Act focuses specifically on the processing of digital personal data, outlining consent requirements, data principal rights, and data fiduciary obligations. The DPDP Act provides for a tiered enforcement mechanism with a Data Protection Board and imposes penalties for non-compliance. [65]

9. CONCLUSION

In the digital era, where information has become a vital asset, ensuring the protection of personal data and maintaining cyber security are essential for safeguarding individual rights and national interests. The study reveals that while India has made significant progress through the enactment of the Digital Personal Data Protection Act, 2023, challenges remain in implementation, awareness, and enforcement. The recognition of the right to privacy as a fundamental right under Article 21 marks a pivotal constitutional advancement, yet the evolving nature of technology demands continuous legal adaptation. A strong, transparent, and accountable data governance framework—harmonized with international standards—is imperative. Effective coordination among stakeholders, robust enforcement mechanisms, and digital literacy are crucial to uphold citizens' informational privacy while promoting innovation and secure digital growth in India.

10. SUGGESTIONS

- Comprehensive Awareness Programs: Launch nationwide initiatives to educate citizens, organizations, and government officials about data privacy rights and cyber security practices.
- Capacity Building: Strengthen the technical and legal expertise of law enforcement agencies, judiciary, and regulatory bodies to handle cybercrime and data protection cases effectively.

[65] Aishwarya Agrawal, 'Digital Personal Data Protection Act 2023' https://lawbhoomi.com/digital-personal-data-protection-act-2023/ accessed 12 March 2026

- Robust Implementation of DPDP Act, 2023: Ensure the effective enforcement of the Digital Personal Data Protection Act through clear guidelines, periodic audits, and accountability measures.
- Establishment of a Specialized Data Protection Authority: Empower the Data Protection Board of India with greater autonomy, resources, and enforcement powers.
- Stronger Cyber Security Infrastructure: Develop advanced cyber security frameworks and encourage public-private collaboration for real-time threat monitoring and response.
- Data Localization and Sovereignty: Mandate secure data storage within national boundaries to safeguard against unauthorized foreign access.
- Periodic Legislative Review: Continuously update laws to address emerging challenges posed by artificial intelligence, cloud computing, and cross-border data flows.
- Promotion of Ethical Data Practices: Encourage organizations to adopt privacy-by-design principles, transparent consent mechanisms, and responsible data processing standards.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

A Thomas, 'Global Standards for Data Protection: Lessons for India' (2020) 8 Asian Journal of Legal Studies 132
Ananya Mehta, 'Right to Privacy in the Digital Age: A Constitutional Perspective' (2022) 58 Indian Journal of Constitutional Law 84
Apar Gupta, Internet Law and Policy in India (LexisNexis 2017)
Arif Khan, 'Cyber Security and Legal Framework in India: An Analytical Study' (2021) 9 International Journal of Law and Technology 45
Brian Craig, Cyberlaw: The Law of the Internet and Information Technology (3rd edn, Pearson Education 2019)
Chris Reed and John Angel, Computer Law: The Law and Regulation of Information Technology (8th edn, Oxford University Press 2022)
Deepa Raghavan, 'Informational Privacy and Fundamental Rights: An Indian Perspective' (2022) 14 Indian Bar Review 51
Durga Das Basu, Introduction to the Constitution of India (24th edn, LexisNexis 2022)
KS Puttaswamy, Right to Privacy: The Landmark Judgment (Universal Law Publishing 2018)
Neha Patel, 'Challenges in Enforcement of Cyber Security Laws in India' (2023) 15 Journal of Law, Technology and Society 59
PK Sinha, Cyber Security and Global Information Assurance (Wiley India 2020)
Parag Diwan and Shammi Kapoor, Cyber and E-Commerce Laws (Bharat Law Publications 2020)
Pavan Duggal, Cyberlaw: The Indian Perspective (4th edn, Universal Law Publishing 2023)
Priya Banerjee, 'Balancing Privacy and Security: A Comparative Study of Data Protection Regimes' (2020) 12 Journal of Cyber Law and Policy 97
RK Singh, Data Protection Law in India: An Analytical Study (Thomson Reuters 2021)
Reema Dutta, 'Interplay between Information Technology Act and Data Privacy Rules in India' (2021) 19 Indian Journal of Law and Governance 88
Ritu Sharma, 'Evolution of Data Protection Laws in India: Challenges and Prospects' (2023) 65 Journal of the Indian Law Institute 112
Rodney D Ryder, Guide to Cyber Laws (3rd edn, Wadhwa and Company 2021)
S Mukherjee, 'Impact of Digital Personal Data Protection Act, 2023 on Privacy Jurisprudence in India' (2024) 17 National Law Review 126

SR Bhansali, Information Technology and Cyber Law (2nd edn, Central Law Publications 2022)
SV Joga Rao, Law Relating to Information Technology and Cyber Crimes (Snow White Publications 2020)
Talat Fatima, Cyber Crimes (2nd edn, Eastern Book Company 2016)
Upendra Baxi, The Future of Human Rights (3rd edn, Oxford University Press 2019)
Vakul Sharma, Information Technology: Law and Practice (4th edn, Universal Law Publishing 2021)
Vivek Gupta, 'Cyber Crimes and Judicial Response in India' (2021) 10 NUJS Law Review 76