Page: 2879-2916 *URL: www.lijdlr.com*

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

ISSN: 2583-7753

LawFoyer International Journal of Doctrinal Legal Research

[ISSN: 2583-7753]

Volume 4 | Issue 1

2026

DOI: https://doi.org/10.70183/lijdlr.2026.v04.128

THE EVOLUTION OF PRIVACY AS A FUNDAMENTAL RIGHT IN THE AGE OF CYBER CRIME

Tanmay Gujarathi[1]

I. ABSTRACT

This paper examines the development of privacy as a fundamental right in the context of rising cyber-crime and rapid digitalization. In the current digital world, huge amounts of personal data are produced, collected, and processed throughout day-to-day online activities, exposing individuals to increasing risks such as data theft, hacking, phishing, and cyber terrorism. The shocking rise in cyber-crime cases underlines the urgent need for strong legal safeguards to protect personal information and preserve individual autonomy. The paper looks into privacy not only as a negative right of exclusion but as a broad concept deep rooted in dignity, choice, and trust. It critically analyses the judicial recognition of privacy as a fundamental right under Articles 14, 19, and 21 of the Constitution, particularly through the landmark judgment in Justice K.S. Puttaswamy (Retd.) v. Union of India, which affirmed the right to privacy as inherent to life and personal liberty. At the same time, it acknowledges that this right is not absolute and may be reasonably restricted under law. The study adopts a doctrinal and analytical methodology, relying on constitutional provisions, judicial decisions, statutory frameworks, and secondary sources. Further, the paper classifies numerous forms of cyber-crimes and inspects India's divided yet developing legal framework, as well as sector-specific legislation. It critically examines the Digital Personal Data Protection Act, 2023 as a major step toward establishing a comprehensive, rights-based data protection rule, while also recognising challenges relating to application, regulatory transparency, and potential state outreach. The paper concludes that protecting privacy in the digital era requires a balanced approach by combining strong legal frameworks, effective enforcement, technological safeguards, and public awareness, ensuring that privacy remains meaningful in an increasingly interconnected world.

[1] Advocate at Bombay High Court (India). Email: tgujarathi96@gmail.com

 (ISSN: 2583-7753)

II. KEYWORDS

Right to Privacy, Cyber Crime, Data Protection, Digital Personal Data Protection Act, 2023, Fundamental Rights.

III. INTRODUCTION

"Personal Liberty makes for the worth of the human person"[2] - Justice Krishna Iyer

In today's virtual world data is everywhere and available all around us. Some of this data is shared by us voluntarily while others are produced by our day-to-day activities performed online e.g., net banking, online shopping, browsing, etc.[3] The protection of our personal data has suffered threats in recent times due to several issues, primarily with respect to privacy. On one hand, digitization of data has made our work style easy and convenient but on other hand, it has also opened the door for serious threats to the safety of our personal information and other crucial data. As all-over world is facing cyber-crimes like hacking, data theft, cyber terrorism, etc. According to the National Crime Records Bureau, the number of reported cyber-crime cases in India stood at 86,420 in 2023, as per the Crime in India 2023 report released in September 2025. This sharp rise reflects the growing scale of digital offences and underscores the urgent need for robust data protection mechanisms.[4]

Our personal data is being shared by us more frequently than we can ever imagine with Banks, Stores, Websites and Mobile Apps. For instance, people happily share their information like location, age, gender, address and some even more private things like their religious views or sexual orientation when they sign up on dating websites. Considering how crucial such information is, it would be much easier to figure out the identities of these users, and such information can be misused against them later on.

Privacy is a matter of choice and freedom of any individual which includes his or her right to have a choice about what they want to keep a secret and what they want to

[2] Maneka Gandhi v Union of India, AIR 1978 SC 597
[3] Data Protection & Privacy Issues in India, available at: https://elplaw.in/leadership/dataprotection-privacy-issues-in-india/.
[4] National Crime Records Bureau, *Crime in India 2023*, Ministry of Home Affairs, Government of India, published on 29 September 2025, available at: https://ncrb.gov.in

share and with whom. However, the concept of privacy as a right is not exhaustive and rather requires being addressed with another approach, i.e., as trust, where society can benefit from supporting and embracing trust norms among people and between people and data collectors, as this approach recognises that data privacy is not just about restricting information for others but also about regulating its flow by allowing it for some trusted parties. Therefore, it is advisable that at the time of disclosure, both the norms are considered and to further see how we can use the law to improve relationships of trust among parties, thereby, creating a power balance.[5]

A. Research Objectives

The present study seeks to examine the evolution and contemporary relevance of the right to privacy in India within the context of increasing cyber-crime and digitalization. The primary objectives of this research are:

1. To analyse the conceptual development of privacy as a fundamental right under the Indian constitutional framework.
2. To examine the impact of rising cyber-crimes on the protection of personal data and individual autonomy.
3. To critically evaluate the adequacy of existing legal frameworks, including sector-specific laws and the Digital Personal Data Protection Act, 2023.
4. To identify gaps, challenges, and ambiguities in the current data protection regime in India.
5. To suggest measures for strengthening privacy protection in light of technological advancements and emerging cyber threats.

B. Research Questions

This paper attempts to address the following key research questions:

1. How has the right to privacy evolved as a fundamental right under the Indian Constitution?

[5] Ari Ezra Waldman, Privacy As Trust 7 (Cambridge University Press, Cambridge, 2018).

2. To what extent do cyber-crimes threaten individual privacy and data security in the digital age?
3. Are the existing legal frameworks in India sufficient to address modern data protection challenges?
4. What are the strengths and limitations of the Digital Personal Data Protection Act, 2023?
5. How can India balance privacy protection with competing interests such as national security, technological innovation, and economic growth?

C. Research Methodology

This research is doctrinal in nature and is primarily based on secondary sources of data. The study relies on an analytical and descriptive approach to examine the evolution of privacy law in India.

The research includes:

1. Analysis of constitutional provisions, particularly Articles 14, 19, and 21.
2. Study of landmark judicial decisions, including Justice K.S. Puttaswamy (Retd.) v. Union of India and other relevant case laws.
3. Examination of statutory frameworks, such as the Information Technology Act, 2000, SPDI Rules, 2011, and the Digital Personal Data Protection Act, 2023.
4. Review of reports, scholarly articles, and policy documents relating to data protection and cyber-crime.

The methodology is qualitative, focusing on interpretation of legal texts, judicial reasoning, and policy analysis to assess the effectiveness of India's data protection regime.

IV. CONCEPTUAL FOUNDATIONS AND CONSTITUTIONAL RECOGNITION OF THE RIGHT TO PRIVACY IN INDIA

Professor Edward J. Bloustein of New York University School of Law defined privacy as, "One who is subject to intrusion is less of a man and has less of human dignity."[6] Privacy, as a right, is a negative right that denotes a state of exclusion, limitation, and keeping secret from the public at large on the will of the individual whose personal information is involved. It is always understood as a right to exclude others from, in simple words, watching us. However, the privacy is extremely hard to protect in our modern world, and it often suffers because we simply cannot avoid disclosure of our personal information in this technology driven society. Almost every app requires the access to our location, and the moment we give access to any of such information, our privacy is compromised.[7]

The privacy as a right is protected as a fundamental right under Article 14, 19 and 21 of the Indian Constitution as was ruled in the landmark judgment of the case Justice K. S. Puttaswamy (Retd.) v. Union of India.[8] Justice K. S. Puttaswamy who is a retired judge of the High Court, filed a writ petition in 2012, in the Supreme Court against the Aadhar scheme's constitutional validity. The Court held privacy as an inherent right of every individual and an 'inseparable part of human element'.[9] This liberty is not a creation of our Constitution. The Justice K.S. Puttaswamy (Retd.) v. Union of India judgment referred to Kharak Singh v. State of Uttar Pradesh, partially affirming its position that 'life' under Article 21 extends beyond mere 'animal existence,' while expressly overruling its conclusion that the right to privacy is not a fundamental right under the Indian Constitution.

However, the Right to Privacy, as a fundamental right under Article 21 of the Indian Constitution, is not an absolute right. The exception is that if the breach of privacy is justified by law, then restrictions over this fundamental right are permissible. This will

[6] Ari Ezra Waldman, Privacy As Trust 27 (Cambridge University Press, Cambridge, 2018).
[7] Ari Ezra Waldman, Privacy As Trust 26 (Cambridge University Press, Cambridge, 2018).
[8] WRIT PETITION (CIVIL) NO 494 OF 2012.
[9] Fundamental Right to Privacy, available at: https://www.scobserver.in/court-case/fundamentalright-to-privacy (last visited on Oct 13, 2023).

be discussed in detail further in the chapter related the Indian laws related to data and privacy.

V. CLASSIFICATION OF BREACH OF DATA PRIVACY IN THE MODERN WORLD, I.E., CYBER CRIMES

Cyberspace is a cosmos of limitless knowledge along with unlimited potential threats. There are several kinds of cyber-offences and the offenders that are mentioned below:

A. Types of Cyber criminals

1. **Virus Writers-** These criminals create viruses that are used in order to attack networks, steal data, etc.[10]
2. **Hackers-** these criminals crack into networks with intention to steal and misuse any information that are beneficial to them. There are a few kinds of hackers that are mentioned as below:
    - **Identity Thieves:** These are very common kinds of hackers who steal anyone's personal information like name, address, phone number, account details, etc. and then impersonate their victims to make transactions causing financial loss to the victims. They cause billions of losses to companies and other victims by this technique alone.
    - **Internet Stalkers:** These kinds of hackers usually monitor their victims and acquire their personal information. The motive behind these stalking by cyber criminals can differ based on their interest in the victims. Several times these attacks are for the purpose of bribery, slander, blackmail or all of them at the same time, but sometimes attacks can take shape of even more heinous crimes, sexual abuse and harassments, and rape. These criminals can cause severe emotional distress to the victims.
    - **Phishing Scammers:** These hackers, also known as Phishers, have a strategy of acquiring personal or sensitive data by sending their victims emails, messages, or masquerading as trusted websites such as

[10] Garima Tiwari, Understanding Laws Cyber Laws & Cyber Crimes 51 (Lexis Nexis First edition, 2014).

corporate or government sites. Users may often fall prey to these mails or sites, unsuspectingly giving away their personal information like bank account numbers and passwords, home address, etc. The phishers then either use these sensitive data themselves to commit fraud scams or sell this information to other parties like dark web.

3. **Cyber Terrorists:** These attackers steal sensitive data to corrupt or bring down corporations or even government systems and networks with intentions to harm a nation, its citizen, businesses and economy, etc. Unlike any regular cyber-crimes, these cyber terrorism attacks are well-developed politically motivated, rather than being just for financial gains.

Cyber offences may be systematically classified with reference to statutory frameworks under Indian law. The Information Technology Act, 2000 (as amended) specifically addresses offences such as tampering with computer source documents (Section 65), hacking and unauthorised access (Section 66), identity theft (Section 66C), cheating by personation using computer resources (Section 66D), violation of privacy (Section 66E), and cyber terrorism (Section 66F). This statutory classification provides a more authoritative basis for understanding cyber offences.

Offences such as unauthorised access (commonly termed 'hacking') are criminalised under Section 66 of the Information Technology Act, 2000, while identity theft and impersonation are specifically addressed under Sections 66C and 66D respectively. Similarly, violations of privacy, including capturing or transmitting private images without consent, fall within Section 66E, thereby aligning commonly recognised cyber-crime categories with explicit statutory provisions.

Such classifications must be grounded in enforceable legal provisions. In this regard, the Bharatiya Nyaya Sanhita, 2023, which replaces the Indian Penal Code, supplements the Information Technology Act by addressing allied offences such as cheating, fraud, and forgery when committed through digital means, thereby creating an integrated framework for prosecuting cyber-enabled crimes.

Accordingly, a doctrinal classification of cyber offences in India must adopt a dual framework drawing from the specialised provisions of the Information Technology

Act, 2000 and the general penal provisions under the Bharatiya Nyaya Sanhita, 2023 to ensure both conceptual clarity and legal precision.

B. Types of Cyber Crimes

1. **Data Theft:** Data theft involves stealing of personal sensitive data of any person or organisation. This is an extremely common cyber-crime, which the companies possessing, and handling sensitive information, are often negligent about.
2. **Hacking:** This cyber-crime involves hackers unlawfully accessing any computer system, programs, and network resources with intent to cause damage to any person or corporation by destroying or altering data or affecting computer system and networks.[11]
3. **Spreading Virus:** Virus attacks are another most common cyber-crime which involves simply transferring virus to any system. Through these attacks your data can be transferred to any third party and later it destroys your data from computer.
4. **Spyware:** These are a kind of programs that track and monitor your activities on your computer discreetly, acquiring your personal information like your files, passwords, bank information.[12]
5. **Cyber Bullying:** This involves intentionally causing harm to others by use of electronic devices. This has become quite common with younger generations as these attacks are generally ignored without consequences. However, this can take shape of a dangerous situation like depression and suicides.
6. **Cyber Stalking:** This is a repeated act of harassment of any victim which involves stalking over them through social media and other platforms and even making threats over calls and messages.[13]

[11] Garima Tiwari, Understanding Laws Cyber Laws & Cyber Crimes 64 (Lexis Nexis First edition, 2014).
[12] Garima Tiwari, Understanding Laws Cyber Laws & Cyber Crimes 63 (Lexis Nexis First edition, 2014).
[13] Garima Tiwari, Understanding Laws Cyber Laws & Cyber Crimes 67 (Lexis Nexis First edition, 2014).

7. **Identity Theft:** This is a form of fraud conducted by cyber criminals through impersonation of another person's identity and obtaining sensitive information like credit card numbers and bank details, etc. These crime cause losses in billions.
8. **Email Spoofing and Phishing:** E-mail spoofing is sending e-mail to someone making it look like it was sent by someone else, i.e., disguising as others in order to gain access to accounts and passwords, distributing e-mail viruses. Phishing is an act of sending e-mails disguising as a legitimate enterprise in order to scam the users into giving away their sensitive data that the actually legitimate organisation already has.[14]
9. **Pharming:** It is similar to phishing except that pharming involves redirecting to an illegitimate website even when a user has typed the correct web address.
10. **Email Fraud:** This fraud is rather too broad in ambit, from financial, banking to social, depending on the potential victims. These target victims by way of fraudulent e-mails to send money or personal information.
11. **Cyber Pornography:** This refers to publication and distribution of sexually explicit material that is degrading and abusive in nature, that may tend to corrupt people exposed to it.
12. **Child Pornography:** This is one example of cyber pornography which is related to sexually explicit materials involving children. While pornography per say is not illegal in many countries, but any pornography depicting paedophilia, abuse or sexual activities involving children is illegal in most of the countries.
13. **Online Gambling:** This type of crime is illegal because of its nature as a contract, i.e., gambling, online or otherwise, is a type of wagering contract that cannot be enforced which, therefore, makes such contract invalid and unlawful.

[14] Garima Tiwari, Understanding Laws Cyber Laws & Cyber Crimes 75 (Lexis Nexis First edition, 2014)

14. **Cyber-Terrorism:** This is a major crime that involves hacking, virus distribution, email frauds in order to threaten the national security of a nation, causing harm to its citizens, economy and properties.

VI. PRIVACY AND DATA PROTECTION THROUGH VARIOUS OTHER INDIAN LEGISLATIONS

There is infinite amount of data, broadly categorised as public and personal data, flowing around the whole world of platforms, whether digital or non-digital. Data in its raw nature is simply spread-out information. It is when it goes through processing and analysing, in order to convert and process into more usable data, such as geolocation data, health data, financial data, professional data and even browsing data, it can become one of the most powerful tools in the hands of whoever holds it. Data is now being said to be most profitable product as the most valuable companies of the world like, Google, Apple, Microsoft, Amazon, Facebook, etc. operate in the data sector and every nation's power is based on it.[15]

At present, a variety of sectors are dealing in the processing of data, to be precise financial sector, health sector, information technology and telecommunication sector, security and others. All of these sectors are involved in storing and processing data principal's personal information like their photographs, signatures, locations, travel histories, medical information, psychological characteristics, financial details, browsing information and personal preferences, etc. Additionally, with Aadhaar identification and number of personal data like biometrics attached with it, creates a situation where such sectors, whether government or non- government, obtains unmeasurable power over the data principal. The DPDP Act has passed only recently, so the issue that follows this is whether any safeguards were provided to the data principals in order to protect them from any unlawful processing of their data by the abovementioned sectors.

[15] Personal Data Protection Laws in India, available at: https://www.lexology.com/library/detail.aspx?g=08197ebe-aeb4-41d6-a855-ce57a313ea6d

Under this section, we will discuss a number of legal provisions that might be present for protection of data principal's personal data and simultaneously we will determine whether they are sufficient for protection over the new Act of 2023 and what challenges there might be with these provisions. The legal provisions to be discussed are categorised according to their concerned sector, which are as follows:

A. Financial Sector

Before enactment of DPDP Act, 2023, for the purpose of protection of personal information in financial sector, the obligations on corporate bodies were mainly dealt under the Information Technology Act and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (the SPDI Rules), where the SPDI rules provided for various obligations related to data collections and processing. In accordance with the SPDI Rules, personal data would include passwords, financial information such as account details or payment instrument details, physical, physiological, and mental health condition, sexual orientation, medical records and/or biometric information.

We can find other banking related rules and regulations directing to maintain the privacy principle among the data collectors in this sector. We will discuss these laws and regulations below:

1. **Banking Regulation Act, 1949:** The Act talk about confidentiality of information and regulating the data collection, retention and protection. Under the Act, the Tribunal or any other authority cannot compel the Central Government or Reserve Bank to produce any account or document which is considered as confidential.[16]
2. **Insolvency and Bankruptcy Code, 2016 (IBC, 2016):** The code talks about the power of Liquidator to access any information for the purpose of proof and admission of claims and determination of liquidation assets related to corporate debtor. The creditors may also ask the liquidator to obtain and provide them with any financial information of the corporate debtor. [17] The

[16] The Banking Regulation Act, 1949; ss. 34A, 36AI.
[17] Insolvency and Bankruptcy Code, 2016, s. 37

Code further mentions the power of the Insolvency and Bankruptcy Board of India to call for any data relating to insolvency from insolvency professional agencies, insolvency professionals and information utilities, and also publish such data in accordance with regulations. The Board can also specify the manner of collection, storage, and access of the data records by regulation.[18]

3. **Payment and Settlement Systems Act, 2007:** The Act defines a term "trade repository" as a person involved in the work of collection, collation, storage, maintenance, processing or distribution of electronic records or data relating to financial transactions;[19] and the obligations mentioned in the Act also applies to such trade repository.[20] The Act provides the RBI with several power related to the information related to the operation of payment systems. RBI has the power to ask for returns, documents or other information from any system provider related to the function of his payment system.[21] RBI also has the authority to access any information related to any payment system of any system provider[22] and further has power to authorise any officer of Reserve Bank to enter the premises where such payment system is operated and inspect any equipment, documents and call any employee working such premises to furnish any document or other information required by such officer.[23] However, the Act mandates RBI to keep such collected information confidential, except in case where disclosure of such information is necessary for protecting the integrity and effectiveness of the payment system.[24] The Act also obligates the system providers to keep documents or any other information provided by the system participants confidential, unless the disclosure of the information is required under any provisions of the Act, or with express or implied

[18] Insolvency and Bankruptcy Code, 2016, s. 196.
[19] Payment and Settlement Systems Act, 2007, s. 2(1)(r).
[20] Payment and Settlement Systems Act, 2007, s. 34A.
[21] Payment and Settlement Systems Act, 2007, s. 12.
[22] Payment and Settlement Systems Act, 2007, s. 13.
[23] Payment and Settlement Systems Act, 2007, s. 14.
[24] Payment and Settlement Systems Act, 2007, s. 15.

consent of the system participant or under the obedience of an order passed by any court of competent jurisdiction or any statutory authority acting within his power as mentioned by the statute.[25] The Act further provides for punishment of fine not more than 10 lakh rupees in case of violation of Sections 12, 13 and 14 of the Act and imprisonment in case of violation of Section 22 of the Act for not more than 6 months or with fine not exceeding 5 lakh or an amount equal or double the number of damages suffered by such act of such disclosure.[26]

4. **Reserve Bank of India Act, 1934:** This Act was enacted with objective of establishing RBI in order to regulate the issue of Bank notes and securing monetary stability in India. Chapter III-A of the RBI Act talks about the "Collection and Furnishing of Credit Information", in which RBI has the power to collect and furnish the credit information to and from banking companies.[27] However, such Credit information collected or furnished as mentioned under Sections 45C and 45D of the RBI Act shall be treated as confidential and is prohibited to be disclosed unless under certain prescribed circumstances, such as, it is with prior permission of RBI, in public interest, in accordance with the practice and usage customary among the bankers. Courts, Tribunals or any other authority, however, cannot compel the RBI or any other banking companies to disclose the information obtained under Section 45C or furnished under Section 45D.[28] Under Section 18 read with Section 10(2) of the Payment and Settlement Systems Act, 2007, the RBI has been given the power to give general directions and make policies for the purpose of regulating payment systems. In 2018, the RBI, by a written guideline on storage of payment system data,[29] brought the data localisation norms which would require all the local transaction data to be stored by the payment ecosystem entities in the servers located

[25] Payment and Settlement Systems Act, 2007, s. 22.
[26] Payment and Settlement Systems Act, 2007, s. 26.
[27] Reserve Bank of India Act, 1934, s. 45B.
[28] Reserve Bank of India Act, 1934, s. 45E.
[29] Storage of Payment System Data, available at: https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11244&Mode=0

within India. This can be considered as a great step in protection of data of the Indian consumers and national and economic interest.[30]

5. **The Security and Exchange Board of India (SEBI) Act, 1992:** The act was brought into effect to establish the Security and Exchange Board of India, which, under the Act, has the power to call for information regarding the stock exchange, mutual funds or other person associated with securities market, call for information and records from any person including any bank, other authority or Board or corporation relevant to any investigation or enquiry of the SEBI, and call for or furnish information to or from any other authority within India or outside. However, in case of furnishing any information to any authority outside India, it may have to be arranged through an agreement or understanding with such authority with a prior approval of the Central Government.[31] The Act further imposes penalties on persons who fail to furnish the information called for or furnish incomplete or incorrect information. The penalty shall be up to 1 lakh for each day of failure of furnish such information and can go up to maximum 1 crore rupees.[32]
6. **Insurance Act, 1938** along with the **Insurance Regulatory and Development Authority Act, 1999 (IRDA Act):** These statutes deal in the business of the insurance sector. This has always been a data concentrated sector as it functions through significant amount of collection and processing of personal data of customers and employees, which include their health information. The insurance work chain is inclusive of multiple kind of data fiduciaries which includes third-party administrators, third-party broking houses, human brokers and contractual agents, who handle customers and their data on behalf of the insurers. This, consequentially, creates additional distribution of the personal data of the customers. The

[30] Data localisation in India: Significance and economic impact, available at: https://cio.economictimes.indiatimes.com/news/strategy-and-management/data-localisationin-india-significance-and-economic-impact/85292096
[31] The Security and Exchange Board of India (SEBI) Act, 1992, s. 11.
[32] The Security and Exchange Board of India (SEBI) Act, 1992, s. 15A.

Act, in case of any investigation and inspection by an investigating officer, requires the insurers, including the service provider, contractor, insurance intermediary, to produce all the account books, registers, documents and other information relevant to the affairs of the insurer in the investigation.[33] Similar power is provided to the Chairperson of the IRDA to call, by a written notice, for any information from any insurer regarding his insurance business and the insurer will be obligated to comply.[34] The IRDA Act obligates the insurers to keep the customers' information confidential by having sufficient measures to protect their interest, and the obligations of the IRDA are applicable to the third-party service providers too.

7. **The Public Financial Institutions (Obligation as to Fidelity and Secrecy) Act, 1983:** This Act puts obligation on the public financial institutions to not divulge any information of their clients' affairs except in case where it is in accordance with law, or practice and usage customary to the institutions, etc. However, the public financial institutions can collect from or furnish to the government, SBI or any subsidiary bank within SBI or any corresponding new bank constituted under Section 3 of the Banking Companies (Acquisition and Transfer of Undertakings) Acts of 1970 and 1980 or any other scheduled bank under the RBI Act, 1934, or any other public financial institutions, where it is for the purpose of its better function.[35]
8. **The Credit Information Companies (Regulation) Act, 2005:** This Act came into force for regulating the credit information companies that collects, maintains and analyses the credit information of companies and individuals. The credit information companies prepare Credit Information Report for individuals based on the data collected, and further generate credit score for individuals.[36] The company or any related institution has to

[33] The Insurance Act, 1938, s. 33.
[34] The Insurance Act, 1938, s. 110C, and IRDA Act, s. 14(2)(h).
[35] The Public Financial Institutions (Obligation as to Fidelity and Secrecy) Act, 1983, s. 3.
[36] Credit Information Companies in India, available at: https://www.paisabazaar.com/creditscore/credit-information-companies-india

adhere to the provisions of the Act and maintain the accuracy of the data collected and protect it from any unauthorised access or disclosure.[37] The Act provides for a specific provision dealing with data privacy, namely, Privacy principles.[38] The provision of privacy principles obligates the credit information company, credit institution and specified users to comply with the said principles in relation to collection, processing, retention, usage and distribution, etc. The provision also mentions that the Reserve Bank may also specify any other guidelines or regulations as it may feel appropriate. The Act also gives the Central Government power to make rules, after consultation with RBI, on matters of level of accuracy, completeness, and protection of data collected.[39]

9. **The Prevention of Money Laundering Act, 2002:** This act provides the regulatory and investigating authorities to ask of disclosure on certain information relevant to determining sources of one's income, assets and evidence that can declare that his or her properties are not involved in money laundering.[40] Under the Act, the Reporting entity, such as banking company, financial institution, intermediaries or any person carrying out designated business, is required to verify its clients and beneficial owner using Aadhaar identification, or passport, or any other valid document. However, in case of verification by Aadhaar credentials, they are not permitted to store the clients' core biometric information or Aadhaar number.[41] Furthermore, the Act talks about obligation of reporting entities to maintain records, furnish such information to the Authority as may be required by him, and procedure and manner of furnishing of such information concerned under Sections 12, 12A and 15 of the Act.
10. **The Income Tax Act, 1961:** This act generally deals in data privacy requirements related to book-keeping and maintaining information in

[37] The Credit Information Companies (Regulation) Act, 2005, s. 19.
[38] The Credit Information Companies (Regulation) Act, 2005, s. 20.
[39] The Credit Information Companies (Regulation) Act, 2005, s. 36
[40] The Prevention of Money Laundering Act, 2002, s. 8.
[41] The Prevention of Money Laundering Act, 2002, s. 11A.

relation with transactions, whether made locally or outside India.[42] The income tax authorities too have to power to call for furnishing of certain personal information, which shall be subject to the provisions and regulations of Information Technology Act and SPDI rules.

B. Health Sector

The Healthcare sector deals primarily in belief of the clients or patients. The patients have to be confident in their healthcare organization. So, the principle of data privacy is an essential part of the healthcare sector too, as the organizations hold several types of personal data of the clients, which include their name, address, records of medical history, psychological or medical profile, and in current times, their Aadhaar details. These types of information are called as Protected Health Information or PHI.

In order to ensure constant and easy access to healthcare, without the breach of trust and privacy of the patients, the protection of their data has to be ensured too. We will discuss what Indian laws, related with healthcare, are there that may also be dealing with the data protection principle.

The Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002 was enforced to give the Medical Council of India (MCI) to govern the conducts of the medical professionals by making regulations of professional conduct, ethics and etiquettes, such as duties of physicians to maintain medical records and upholding the secrecy of their patients. Under Chapter 1, dealing with Code of Medical Ethics, every physician has to mandatorily keep the medical records of their indoor patients for 3 years from the commencement date of their treatment and further have to issue such records within 72 hours, it is requested by the patient, authorised attendant or legal authorities concerned.[43]

In case of failure in maintenance of such records, or furnishing such records to patient, etc. within time, it would constitute a professional misconduct.[44] Under Chapter 7,

[42] The Income Tax Act, 1961, s. 9.
[43] The Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002, regulation 1.3.
[44] The Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002, regulation 7.2.

which is regarding professional misconducts, the registered medical practitioners are obligated to not disclose any secrets related to their patients unless it is required by the court of law by order of the presiding Judge, or where there seems to be a high risk to another specific person or community, or in case of communicable disease, where the medical practitioner has to report to State or local public health officials.[45] There is another obligation of the medical practitioners to not publish the photographs or case reports of their patients in any medical journal, etc. without their consent, which can reveal their identity, and if the identity is not to be disclosed at all, then there is no need for any consent.[46]

In September 2020, the Medical Council of India was dissolved pursuant to the enforcement of the National Medical Commission Act, 2019, and was replaced by the National Medical Commission. Subsequently, the National Medical Commission Registered Medical Practitioner (Professional Conduct) Regulations, 2023 came into force, replacing the earlier Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002.

The new regulations have some similar provisions, but with modifications, as compared to the earlier regulations of 2002, for instance, the duty of Registered Medical Practitioners (RMP) to maintain medical records of their patients for 3 years starting from their last contact for treatment, and if asked for their records by the patients, the same to be provided within 5 days.[47] Moreover, confidentiality under Section 24 of the new regulations is the same as provided by previous regulations under Chapter 7. However, a few additions have been made too, such as, a provision and guidelines for informed consent in their clinical practice, as well as their conduct on social media.[48] A good step has been taken by including specific guidelines in case

[45] The Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002, regulation 7.14.
[46] The Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002, regulation 7.17.
[47] National Medical Commission Registered Medical Practitioner (Professional Conduct) Regulations, 2023, regulation 13.
[48] National Medical Commission Registered Medical Practitioner (Professional Conduct) Regulations, 2023, regulation 19, guidelines 5, 6.

of Telemedicine, for data privacy related to digital records adhering to the provisions of Information Technology Act as well as any other laws related to data protection.[49]

Digital Information Security in Healthcare Act (DISHA), was drafted by the Ministry of Health and Family Welfare (MoHFW) to promote and ensure the data privacy, security, confidentiality, and reliability related to digital health. This draft propose the individuals with several rights, such as right to access their digital health records, change or correct it, right to keep the data confidential, right to seek damages in case of data breach and right to give consent for each use of his or her data along with the right to give or refuse consent for collection, storage, access or disclosure, etc.[50] However, it is important to note that DISHA remains an unenacted draft and is not a law in force. Accordingly, it should be understood as reflecting policy intent rather than binding legal obligations. Its relevance lies in shaping the discourse on healthcare data governance, with many of its principles now subsumed within the broader Digital Personal Data Protection (DPDP) framework.

C. Information Technology and Telecommunications Sector

The information technology sector is the major sector dealing in the normal, personal and sensitive data of any individual in the country. Technology and Data are interlocked in such a way that the principle of data privacy becomes an interconnected concept too, whether we talk about access, collection, storage, processing or transmission of data. The information technology systems will always be the most responsible for it. Hence, it is essential to discuss the manner in which this sector manages the personal data, what security measures they adopt for data protection and what legal remedies are available to the data owners in case of breach.

1. **The Indian Telegraph Act, 1885**, enacted during British rule, traditionally governed telegraph services and enabled state intervention of communications. However, being a pre-digital statute, it does not address modern data privacy concerns in a practical manner. The prevailing legislation is the

[49] National Medical Commission Registered Medical Practitioner (Professional Conduct) Regulations, 2023, guideline 11.
[50] https://www.pib.gov.in/Pressreleaseshare.aspx?PRID=1578929

Telecommunications Act, 2023, which give permission for interception on grounds such as sovereignty, security of the State, and public order, subject to suggested safeguards. Despite this, distresses continue regarding the absence of consent and the inadequate integration of data protection principles. From a constitutional perspective, the government raises proportionality and oversight concerns, particularly due to the lack of robust independent judicial administration and limited transparency, which may undermine accountability in the exercise of surveillance powers. Accordingly, the 1885 Act serves only as historical context, while the Telecommunications Act, 2023 warrants critical scrutiny for its implications on digital privacy.

2. **Information Technology Act, 2000, along with SPDI Rules, 2011** was the main legislation regarding e-commerce and data protection before the new DPDP Act, 2023 came into existence. Section 43A of the Information Technology Act, 2000 read with Rule 4 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, also known as the SPDI Rules, specifically talks about the protection of Sensitive personal data in possession of a body corporate, by implementing measures to maintain secured procedures, and would be liable for compensation in case of failure of compliance. The IT Act, 2000 defines Sensitive personal data as such information as it may be prescribed by the Government, while the SPDI Rules define it under Rule 3 as any information relating to passwords, physical, physiological and mental health conditions, medical records, financial information, sexual orientation, and biometric information. The IT Act provides for penalty in case of breach by any person, by way of access and download without permission of the data owner, or by damaging, deleting, altering or stealing such data.[51] The Act gives the Controller power to have access to any computer system, data, etc. for the purpose of searching if he has reason to believe that there has been a violation.[52] The punishment for failure of furnishing such data to the Controller has been

[51] The Information Technology Act, 2000, s. 43.
[52] The Information Technology Act, 2000, s. 29.

provided under Section 44 of the Act. SPDI Rules provide for obligation on the body corporate to obtain prior permission from the data owners before disclosing their data to any third party, unless such disclosure is permitted by a contract between them or for the purpose of verification of identity, prevention, detection or investigation of cyber-crimes by the Government agencies. The data obtained by the government agency shall not be published or shared with any other person.[53] The Rules also obligates the body corporate or any person on their behalf to implement reasonable security practices and procedures, and in case of any breach of data, they have to demonstrate that they have implemented such measures and policies.[54]

3. **The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021** was brought with the intention of regulating social media platforms and their conduct regarding digital content. The rules are primarily focused on regulating contents, online safety, and particularly accountability of the social media intermediaries. The Rules provides for due diligence by the intermediaries, for instance, they shall inform their users with the privacy policies, regulations, etc. as well as instructions to not upload, publish, store, or share, etc. any content or information derogatory and invasive of another person resulting in invasion of their privacy, insult, harassment, racism, or other cyber related offences, etc. The intermediary further has to inform its users the consequences of violation of their policies, such as termination of service, etc.[55] The Rules compels the Significant social media intermediaries to enable the identification of the first originator of an information when it is required by a judicial order of a competent court, where such order may be for the purpose of detection, prevention, investigation, prosecution or punishment of an offence harmful to the national sovereignty and integrity, foreign relation or public order. However, the intermediary is not

[53] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, rule 6.
[54] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, rule 8.
[55] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, rule 3.

permitted to disclose the contents of any electronic message, any other information of the first originator or any information of its other users.[56]

VII. DEVELOPMENT OF THE PERSONAL DATA PROTECTION LAWS IN INDIA

The evolution of privacy rights in India reflects a significant transformation, primarily driven by the proactive stance of the Indian judiciary. Over the years, judiciary has played a crucial role in interpreting and expanding the scope of the right to privacy through various landmark cases. These cases have tackled diverse aspects of privacy, gradually contributing to the recognition of privacy as a fundamental right enshrined in the Indian Constitution. The journey has not been without its challenges, particularly with the rapid digitization of personal data and the emerging risks associated with it. This evolving landscape necessitates the establishment of a comprehensive legal framework aimed at safeguarding personal data privacy, highlighting the urgency of the DPDP Legislation in India.[57]

The enforcement framework of the Digital Personal Data Protection Act, 2023 has been substantially clarified through the notification of the Digital Personal Data Protection Rules, 2025 by the Ministry of Electronics and Information Technology in November 2025. The Rules introduce a phased implementation structure, with the immediate establishment of the Data Protection Board of India, followed by staged compliance obligations extending into 2027.

Pursuant to the Digital Personal Data Protection Rules, 2025, Phase I—concerning the establishment of the Data Protection Board of India—has come into immediate effect, thereby operationalising the adjudicatory and enforcement architecture envisaged under the Act. The Rules prescribe a structured, phased compliance roadmap: Phase II, relating to the registration and regulation of consent managers, is scheduled to take

[56] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, rule 4.
[57] Protection of Personal Data, in SECURITY AND PRIVACY IN THE DIGITAL ERA 29, (2016), https://doi.org/10.1002/9781119347750.ch2.

effect in November 2026, while Phase III encompassing full substantive compliance obligations for data fiduciaries will commence in May 2027, thereby affording stakeholders a transitional adjustment period.

The Digital Personal Data Protection Rules, 2025 adopt a liberalised framework for cross-border data transfers, permitting such transfers by default except to jurisdictions specifically restricted by the Central Government through notification, thereby aligning India's regime with a more facilitative global data flow approach.

VIII. JUDICIAL EXPANSION OF DIGITAL RIGHTS: FREE SPEECH, PRIVACY, AND DATA GOVERNANCE

A. Shreya Singhal v. Union of India

A crucial milestone in the evolution of fundamental rights in the digital sphere is the decision in this case, wherein the Supreme Court struck down Section 66A of the Information Technology Act, 2000 as unconstitutional. The provision criminalised the sending of "offensive" or "menacing" messages through electronic communication, employing vague and overbroad terminology.[58]

The Court held that Section 66A violated Article 19(1)(a) of the Constitution, as it imposed unreasonable restrictions on freedom of speech and expression and failed to satisfy the test of reasonable restrictions under Article 19(2). Importantly, the judgment recognised that vagueness in digital regulation can lead to arbitrary state action, thereby indirectly affecting individual autonomy and privacy.

This ruling is significant in the context of privacy jurisprudence as it laid the groundwork for limiting excessive state control over digital communication. By safeguarding online speech, the Court reinforced the idea that digital spaces are extensions of constitutional freedoms, thereby shaping the broader discourse that later culminated in the recognition of privacy as a fundamental right in Puttaswamy (2017).

[58] Shreya Singhal v Union of India (2015) 5 SCC 1.

B. K.S. Puttaswamy (II) v. Union of India (Aadhaar Case)

Following the recognition of privacy as a fundamental right in K.S. Puttaswamy (Retd.) v. Union of India (2017)[59], the Supreme Court in this case, examined the constitutional validity of the Aadhaar scheme.

The Court upheld the Aadhaar framework with certain limitations, while simultaneously laying down critical principles of data protection, including:

1. **Proportionality**: State action infringing privacy must be necessary and proportionate to a legitimate aim.
2. **Purpose Limitation**: Data collected must be used only for specific, lawful purposes.
3. **Data Minimisation**: Only necessary data should be collected.

The judgment also struck down or read down certain provisions that enabled excessive data retention or private sector access, thereby reinforcing safeguards against misuse of personal data.

This decision represents the operationalisation of the right to privacy, translating abstract constitutional recognition into concrete limitations on state data practices. It serves as a vital link between constitutional doctrine and legislative developments, directly influencing the framework and principles embodied in the Digital Personal Data Protection Act, 2023.

IX. DIGITAL PERSONAL DATA PROTECTION ACT, 2023: FRAMEWORK, OBJECTIVES AND EMERGING CONCERNS

DPDP Act, 2023 is a landmark piece of legislation that signifies a substantial advancement in the realm of digital governance in India. While it lays a strong foundation for protecting data privacy, it is also essential to identify the gaps that exist within this framework. DPDP Act is designed to regulate the processing of personal data by both government bodies and private entities, with the overarching goal of

[59] *Justice K.S. Puttaswamy (Retd.) v Union of India* (2017) 10 SCC 1

ensuring individual privacy and autonomy in the rapidly evolving digital economy. This comprehensive legislation emerges from extensive deliberations and draws from earlier iterations, notably the Justice B. N. Srikrishna Committee Report (2018) and the Personal Data Protection Bill, 2019 constituted the foundational framework for India's data protection regime, introducing principles of consent, purpose limitation, and data fiduciary obligations. The Act aims to strike a delicate balance between fostering technological innovation and enforcing robust rights-based safeguards that protect citizens' privacy.

The Joint Parliamentary Committee Report on Personal Data Protection Bill significantly reshaped the 2019 Bill by proposing over 80 amendments, including expanded scope, stricter compliance requirements, and broader exemptions for the State, thereby altering the regulatory balance between privacy and governance. However, the Personal Data Protection Bill, 2019 was withdrawn by the Government in August 2022 after prolonged deliberations, primarily due to concerns regarding its complexity, the extensive amendments recommended by the JPC, and criticisms relating to wide-ranging governmental exemptions and compliance burdens.

Subsequently, the legislative approach was recalibrated, culminating in the enactment of the Digital Personal Data Protection Act, 2023, which adopts a more streamlined and principles-based framework, reflecting a shift towards ease of compliance, reduced regulatory fragmentation, and a calibrated approach to State exemptions. The transition from the 2019 Bill to the 2023 Act represents a critical inflection point in India's data protection trajectory, evidencing a deliberate move away from a highly prescriptive regime towards a flexible, implementation-oriented framework informed by prior legislative challenges.

Several elements of the DPDP Act have garnered praise for their potential to enhance personal data protection in India. One notable aspect is the expansion of individual rights, which extends beyond traditional limits of purpose limitation. This enhancement empowers individuals to challenge and oppose potentially harmful Al systems that may infringe upon their rights and freedoms. Such provisions are critical in mitigating the adverse effects of algorithmic decision-making and ensuring that

individuals retain control over how their data is utilized in various contexts, particularly in scenarios involving complex Al systems.

Another significant advancement within the DPDP Act is the introduction of stringent regulations on unrestricted cross-border data transfers. This is a vital step toward establishing data sovereignty and safeguarding the privacy of Indian citizens. By implementing restrictions on government access exemptions, the Act, 2023 effectively addresses concerns surrounding unchecked state surveillance powers that could jeopardize individual privacy rights. Moreover, the law mandates periodic data audits and establishes fiduciary duties for data processors, further reinforcing accountability in data processing practices. This is essential for fostering a culture of responsibility among entities that handle personal data, ensuring they adhere to ethical standards and legal requirements.

The regulatory framework provided by the Data Protection Board, in conjunction with the introduction of stricter compensatory mechanisms, is expected to enhance the enforcement of the law.[60] This oversight mechanism is crucial for protecting individuals' rights and interests, ensuring that data processors are held accountable for any violations or breaches. By establishing a clear process for accountability and redressal, DPDP Act enhances individuals' trust in how their personal data is managed. A particularly commendable aspect of DPDP Act is its rights-affirming orientation, which underscores the importance of user control over personal data. The comprehensive definition of personal data empowers individuals to have a more significant say in the collection, processing, and sharing of their data. The Act emphasizes the principles of fair and reasonable processing, grounded in transparency, accountability, and proportionality. These principles encourage the adoption of ethical data practices across various sectors, promoting a culture of respect for individual privacy.

The provisions aimed at enhancing transparency in automated decision-making systems are especially noteworthy. By ensuring that individuals have access to the

[60] What is Data Protection Board under DPDP Law, LEEGALITY, https://www.leegality.com/consent-blog/data-protection-board

necessary information regarding decisions that significantly impact their lives, the law strengthens due process. This transparency enables individuals to challenge potentially harmful decisions, fostering a more equitable environment in which their rights are respected. The Digital Personal Data Protection Act, 2023 demonstrates a forward-looking approach by establishing a comprehensive framework for the processing of digital personal data, while its scope remains limited to such data and does not extend to non-personal or non-digital data, which currently remain outside a dedicated statutory regime in India, demonstrates its adaptability to emerging technologies and the ever-evolving digital landscape.

DPDP Act, 2023, marks a pivotal advancement in India's legislative framework regarding data protection and privacy.[61] This law introduces a series of comprehensive measures designed to enhance the protection of individual rights in the digital landscape. One of the most notable aspects of Act is the implementation of stricter penalties for violations. These enhanced penalties are a critical component of the law, as they aim to deter non-compliance by organizations that handle personal data. Furthermore, the law extends the breach notification mandate, requiring organizations to inform individuals in a timely manner if their data has been compromised. This proactive approach not only empowers individuals to take necessary precautions but also fosters a culture of accountability among data handlers.

In addition to these measures, the law significantly strengthens the regulatory framework by enhancing the powers of the relevant authorities responsible for enforcement. This empowerment enables regulators to take decisive action against violations and to ensure compliance with the law's provisions. The inclusion of specific safeguards for children's data demonstrates a heightened awareness of the vulnerabilities that minors face in the digital space, while provisions for grievance redressal reflect the law's commitment to addressing individual concerns promptly. Collectively, these elements illustrate a well-rounded approach that seeks to balance

[61] Soumya Banerjee, "Digital Personal Data Protection Act", A Strudel Served Raw! 2024 INT'L J.L. ETHICS & TECH. 85, (2024), https://doi.org/10.55574/mowt9922.

the interests of various stakeholders, including individuals, businesses, and regulatory bodies.

Industry experts have widely recognized the DPDP Act, 2023, as a landmark achievement in asserting India's leadership in the realm of digital rights. Commentators have praised the law for its principled and rights-based approach, which deftly navigates the complexities of individual versus community interests. This balanced perspective is crucial in establishing trust within the digital ecosystem, as it not only protects individual privacy but also recognizes the collective implications of data governance. By fostering responsible data use, the law aims to create an environment where personal data can be managed ethically, thus enhancing user confidence in digital services and technologies.

However, the successful implementation and enforcement of the DPDP Act, 2023, are paramount for its overall effectiveness. While the legislative framework is robust, the actualization of its provisions depends heavily on the capability and resources allocated to the Data Protection Board. It is essential that this regulatory body is adequately equipped to carry out its responsibilities effectively, ensuring that the law's intent is realized in practice. Additionally, the government must prioritize initiatives that raise awareness about the law's provisions and educate both individuals and organizations on their rights and obligations. Such educational efforts are critical for empowering users to navigate the new legal landscape effectively and to understand the implications of their data rights.

The introduction of the DPDP Act, 2023, has sparked a dialogue that includes both commendation and scepticism. While many view the law as a significant stride forward in safeguarding privacy rights within India's burgeoning data economy, certain concerns have emerged regarding its potential limitations. One primary critique pertains to the ambiguity surrounding the criteria for categorizing specific classes of personal data as sensitive. This lack of clarity could inadvertently lead to inadequate protection for data that is particularly vulnerable, thereby undermining the law's objectives.[62]

[62] Ibid.

Moreover, while the emphasis on obtaining valid consent for data processing is commendable, the mechanisms for individuals to withdraw consent could be improved. Simplifying these processes would enhance user-friendliness and facilitate greater user control over personal data, which is crucial for the practical application of the law. Sec. 4 & 5 of the DPDP Act outlines these procedures, yet they still pose challenges for users seeking to exercise their rights.

Another contentious issue is the requirement for data localization, which has been the subject of intense debate. Critics argue that the compliance costs associated with data localization could be prohibitively high for businesses, particularly small and medium enterprises, without necessarily providing demonstrable security benefits. This raises concerns about whether the law will impose undue burdens on businesses while failing to enhance the overall security of data.

Furthermore, the provision allowing the government to exempt entities from certain core regulations through consultative rulemaking has elicited apprehension among authorities. Experts caution that this could establish a troubling precedent for diluting privacy safeguards. Specifically, sec. 16 of Act, 2023 raises questions about the circumstances under which such exemptions may be granted and how they might undermine the law's overarching objectives.

The penalty structures outlined in the law have also drawn criticism for their perceived favouritism towards large technology firms, potentially diminishing the law’s effectiveness in holding these companies accountable for data breaches and violations. Delving deeper into the specifics of the DPDP Act, it becomes evident that the law does expand the grounds for processing personal data without consent. While this expansion serves various operational needs, it also necessitates rigorous oversight to prevent abuse and to safeguard individual privacy rights.

Additionally, the mandates for data portability and the restrictions on cross-border data transfers introduce vital protection for users. However, there remains an ongoing need for further alignment with international standards to ensure comprehensive protection and facilitate global data flows. This harmonization is crucial as the digital

landscape increasingly transcends national borders, requiring cohesive strategies to address privacy concerns effectively.

Concerns have also been voiced regarding exemptions for public interest processing and the handling of sensitive data, such as biometric and financial information. These discussions highlight the intricate balancing act that policymakers must navigate, weighing the need for security and public interest against the imperative to protect individual rights. DPDP Act, 2023, while ambitious in its aims, illustrates the complexities and challenges inherent in crafting effective data protection legislation that addresses the diverse needs of a rapidly evolving digital economy. As the law unfolds, it will be essential to monitor its implementation and make necessary adjustments to ensure that it meets its objectives of safeguarding privacy while fostering innovation and growth.

At the heart of the DPDP Act, 2023 is its commitment to creating a rights-based approach to data processing. This shift is not merely a regulatory formality; it signifies a deeper recognition of the importance of ethical considerations in handling personal data. By emphasizing individual dignity and freedom, the Act aims to empower citizens and ensure that their rights are protected against potential misuse of their data. This empowerment is particularly relevant in today's digital landscape, where data breaches and unauthorized surveillance can undermine public trust in digital services. The incorporation of lessons learned from previous iterations of data protection legislation enhances the robustness of this new law, positioning it as a proactive measure rather than a reactive one.[63]

However, the real effectiveness of the DPDP Act, 2023 hinges on the successful operationalization of its enforcement and grievance mechanisms. The law outlines various rights and protections for individuals, but these provisions must be effectively implemented to make a tangible difference in the lives of citizens. This necessitates the establishment of well-capacitated institutions capable of enforcing these regulations. Without the necessary infrastructure, the law runs the risk of remaining

[63] JAYA THAPA -, Data Privacy Vis- A- Vis the Digital Personal Data Protection Act, 2023, 6 INT'L J. FOR MULTIDISCIPLINARY RSCH., (2024), https://doi.org/10.36948/ijfmr.2024.v06i103.23530.

a theoretical framework that lacks practical impact. Moreover, increasing awareness about data protection rights among citizens and stakeholders within the digital ecosystem is essential for fostering a culture of compliance and respect for individual privacy.

While the DPDP Act, 2023 is commendable for its ambitious vision and ethical underpinnings, it is important to acknowledge that legislation alone cannot guarantee the desired regulatory outcomes. The on-ground impact of this law will depend significantly on ecosystem capacity building, which involves enhancing the skills and resources of institutions responsible for enforcing data protection. Sound regulation-making is also vital, as it sets the parameters within which businesses and other entities operate. Additionally, sincere implementation of the Act's core principles is essential to ensure that the rights it enshrines translate into meaningful protection for individuals.

The global implications of the DPDP Act, 2023 are noteworthy as well. As data protection becomes a universal concern, there is an increasing need for cross-jurisdictional harmonization of regulations. "The United Nations Convention against Cybercrime, adopted by the United Nations General Assembly on 24 December 2024 (Resolution 79/243), underscores the importance of establishing a cohesive global framework for addressing data privacy and cybersecurity challenges.[64] The DPDP Act's alignment with such international initiatives underscores India's commitment to engaging in a broader dialogue on data protection, emphasizing the need for collaboration across borders to effectively tackle issues that transcend national boundaries."

As an adopted international instrument opened for signature on 25 October 2025 in Hanoi, the Convention reflects ongoing global efforts to harmonise cyber laws and strengthen cross-border cooperation, with 74 States having signed as of March 2026. However, the effectiveness of the Convention will depend on its entry into force, which requires 40 ratifications; as of March 2026, only Qatar has ratified the

[64] United Nations Convention against Cybercrime, GA Res. 79/243, UN GAOR, 79th Sess. (24 December 2024)., https://doi.org/10.1016/s1353-4858(01)01201-6.

Convention, indicating that its operational impact remains contingent on broader state ratification. India must closely monitor the progression of the Convention towards entry into force and assess alignment of its domestic data protection framework, including under the Digital Personal Data Protection regime, with emerging international cybercrime and data governance standards.

India's journey toward establishing a comprehensive data protection framework has been intricate and continuously evolving, marked by persistent challenges and an increasing recognition of the necessity for robust legal structures in the digital era. "The interplay of constitutional principles, legislative measures, and judicial interventions has profoundly influenced the nation's data protection landscape, underscoring the urgent need for a coherent and effective strategy to safeguard personal data. Despite the existence of several laws and regulations addressing various facets of data protection, most notably IT Amendment Act, 2008 and its accompanying Rules from 2011, India has grappled with significant challenges in developing a comprehensive, rights-based data protection regime."

However, recent developments indicate a pivotal shift toward a more robust and internationally aligned data protection framework. The landmark "Supreme Court" judgment in the Puttaswamy case, which affirmed the fundamental right to privacy as a constitutionally guaranteed right, has significantly influenced the discourse surrounding data protection in India. This judgment underscored the importance of privacy in the context of data usage and set the stage for the drafting of the PDP Bill, 2019. This bill sought to address the pressing need for a comprehensive legal framework that not only protects individual data rights but also responds to the challenges posed by the digital landscape.

Moreover, India's data protection framework must navigate the complex interplay between data privacy and competing interests such as national security, economic growth, and innovation. "Striking a balance between protecting individual rights and fostering an environment conducive to technological advancements is essential for realizing the full potential of the digital economy. This balancing act will require a

nuanced approach that recognizes the diverse stakeholder interests involved in data governance."

In this context, India's aspiration to become a global leader in the digital economy necessitates alignment with international data protection standards. "Efforts to achieve adequacy status with the EU's GDPR and to foster cross-border data collaborations will be critical for India's engagement in the global data economy. The success of India's data protection regime will depend not only on legislative measures but also on fostering a culture of privacy awareness among the public. Empowering individuals to exercise their data rights through sustained efforts in digital literacy, public education, and the establishment of user-friendly mechanisms for accessing, correcting, and controlling personal data is crucial."

As India lays the groundwork for forward-looking, globally aligned data governance frameworks, the focus must shift to the effective implementation of existing laws, ongoing policy refinement, and institutional capacity building. Public awareness initiatives are essential to educate citizens about their rights in the digital space. Proactive cybersecurity measures and global cooperation will further bolster India's data protection efforts. Emerging technologies, such as Al, IoT, and biometric systems, necessitate sophisticated "techno-legal" strategies that promote innovation while safeguarding individual rights against potential violations.

"Facilitating international data flows will be vital, but it must occur within a framework that incorporates robust cross-border privacy safeguards. Strengthened enforcement mechanisms and more substantial penalties for non-compliance will enhance accountability among data processors and controllers." Above all, India must enshrine individual privacy and ethical data usage as non-negotiable pillars of a truly empowering and inclusive digital transformation. With the DPDP Act serving as a guiding framework, the collaboration between public and private sectors, along with genuine political and bureaucratic will, positions India to emerge as a global leader in rights-based technological advancement and cross-border data governance.

The outlook for data protection and privacy in India is promising. The nation stands ready to craft a unique model that upholds constitutional values while harnessing the

transformative power of data for social and economic development.[65] "The DPDP Act represents a significant leap forward in this endeavour, yet its successful implementation and enforcement will be the true measure of India's dedication to protecting personal data in an increasingly digital age. By embracing a rights-based approach, aligning with global standards, and cultivating a culture of privacy, India has the potential to emerge as a leader in data protection, effectively balancing individual rights with the myriad opportunities and challenges presented by the digital economy."

X. SUGGESTIONS AND RECOMMENDATIONS

In light of the analysis undertaken, the following suggestions are proposed to strengthen the protection of privacy as a fundamental right in the digital age:

1. **Strengthening Institutional Frameworks:** The Data Protection Board must be adequately empowered, independent, and well-resourced to ensure effective enforcement of the DPDP Act, 2023.
2. **Clearer Regulatory Guidelines:** Ambiguities regarding sensitive personal data, consent mechanisms, and government exemptions must be clarified through detailed rules and guidelines.
3. **Enhanced Judicial Oversight:** Surveillance and data interception mechanisms should be subject to stricter judicial scrutiny to ensure compliance with the principles of necessity and proportionality.
4. **Data Protection Awareness:** Nationwide awareness programs should be conducted to educate citizens about their data rights, consent, and remedies in case of breaches.
5. **Strengthening Cybersecurity Measures:** Mandatory data security standards and regular audits should be enforced across sectors handling sensitive personal data.

[65] DATA SEC. COUNCIL OF INDIA, DATA PROTECTION CHALLENGES IN CLOUD COMPUTING: AN INDIAN PERSPECTIVE: STUDY REPORT (2010).

6. **Simplification of Consent Withdrawal:** Mechanisms for withdrawal of consent must be made user-friendly and accessible to ensure real control over personal data.
7. **Alignment with Global Standards:** Indian data protection laws should be harmonized with international frameworks such as GDPR to facilitate secure cross-border data flows.
8. **Special Protection for Emerging Technologies:** Regulatory frameworks must address risks arising from AI, IoT, and big data analytics through sector-specific guidelines.

XI. CONCLUSION

The development of privacy as a fundamental right in India is a sign of substantial constitutional and legal breakthrough in the digital era. From being an implicit aspect of personal liberty to its explicit recognition as a fundamental right in Justice K. S. Puttaswamy (Retd.) v. Union of India, the law of privacy has gone through a transformative journey. This shift indicates the emerging recognition that in an era dominated by data-driven technologies and increasing cyber-threats, the protection of personal data is inseparable from the protection of human dignity, autonomy, and liberty.

The rapid increase in cyber-crimes, varying from data theft and identity fraud to cyber terrorism, has exposed the vulnerabilities in-built in digital ecosystems. While technological developments have enhanced efficiency and connectivity, at the same time increased risks to individual privacy. In response, India has developed a multi-layered legal framework, put together sector-specific regulations and important acts like the Information Technology Act, 2000. However, these fragmented measures often proved inadequate in tackling the difficulties of modern data processing and cross-border data flows.

The enactment of the Digital Personal Data Protection Act, 2023 symbolises a significant step toward beginning a comprehensive and rights-based data protection system in India. By highlighting consent, accountability, transparency, and individual empowerment, the Act seeks to balance the competing interests of innovation,

governance, and privacy. At the same time, the concerns surrounding implementation challenges, regulatory ambiguities, and potential state overreach highlight that legislative reform alone cannot ensure effective data protection.

Eventually, the future of privacy protection in India depends not only on strong legal frameworks but also on efficient implementation, institutional capacity, technological safeguards, and widespread public awareness. As India continues to integrate into the global digital economy, it must strive to harmonize domestic laws with international principles while preserving its constitutional values. A collaborative approach involving the State, private entities, and citizens is essential to foster a culture of privacy and trust.

In conclusion, safeguarding privacy in the age of cyber-crime is an ongoing and dynamic process. It requires constant adaptation to emerging technologies and threats, ensuring that the fundamental right to privacy remains meaningful, enforceable, and resilient in an increasingly interconnected world.

XII. BIBLIOGRAPHY

A. Primary Sources

1. Legislation

- Constitution of India, 1950
- Information Technology Act, 2000
- Information Technology (Amendment) Act, 2008
- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
- Digital Personal Data Protection Act, 2023
- Digital Personal Data Protection Rules, 2025
- Bharatiya Nyaya Sanhita, 2023
- Indian Telegraph Act, 1885
- Telecommunications Act, 2023

- Banking Regulation Act, 1949
- Reserve Bank of India Act, 1934
- Payment and Settlement Systems Act, 2007
- Insolvency and Bankruptcy Code, 2016
- Securities and Exchange Board of India Act, 1992
- Insurance Act, 1938
- Insurance Regulatory and Development Authority Act, 1999
- Public Financial Institutions (Obligation as to Fidelity and Secrecy) Act, 1983
- Credit Information Companies (Regulation) Act, 2005
- Prevention of Money Laundering Act, 2002
- Income Tax Act, 1961
- National Medical Commission Act, 2019

2. Cases

- *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) 10 SCC 1
- *K.S. Puttaswamy (II) v. Union of India* (2019) 1 SCC 1
- *Kharak Singh v. State of Uttar Pradesh* AIR 1963 SC 1295
- *Shreya Singhal v. Union of India* (2015) 5 SCC 1

3. Reports & Government Documents

- Justice B.N. Srikrishna Committee Report on Data Protection (2018)
- Joint Parliamentary Committee Report on Personal Data Protection Bill (2021)
- National Crime Records Bureau, *Crime in India 2023* (2025)
- Ministry of Electronics and Information Technology, Government of India, DPDP Rules Notification (2025)

- Ministry of Health and Family Welfare, Draft Digital Information Security in Healthcare Act (DISHA)

B. Secondary Sources

1. Books

- MP Jain, *Indian Constitutional Law* (LexisNexis, latest edn.)
- V.N. Shukla, *Constitution of India* (Eastern Book Company, latest edn.)
- Justice Y.V. Chandrachud et al., *Privacy and the Indian Constitution* (Oxford University Press)

2. Journal Articles

- Edward J. Bloustein, 'Privacy as an Aspect of Human Dignity' (1964) 39 NYU Law Review 962
- Upendra Baxi, 'The Supreme Court and the Right to Privacy' (various publications)
- Gautam Bhatia, 'State Surveillance and the Right to Privacy in India' (2016)

C. Online Sources

1. Ministry of Electronics and Information Technology (MeitY), Government of India – https://www.meity.gov.in
2. Reserve Bank of India – https://www.rbi.org.in
3. Securities and Exchange Board of India – https://www.sebi.gov.in
4. National Crime Records Bureau – https://ncrb.gov.in
5. Supreme Court of India Judgments Portal – https://main.sci.gov.in

D. International Instruments

1. United Nations Convention against Cybercrime (UNGA Resolution 79/243, 2024)