THE SPRING CHRONICLE
We share knowledge

# Privacy and Digital Personal Data Protection Law in India: Some Observations

Author (s): Dr. Vijaykumar Torgal

Category: Humanities & Social Sciences

Date: 07-December-2025

Volume 1, Issue 4, pp 18 – 29, October - December (2025)

https://www.springchronicle.org/home/article/privacy-and-digital-personal-data-protection-law-in-india-some-observations

Human civilization evolved from barbarism to civilized society. This is made possible by the new inventions, technologies, modes of production and system of governance. The agricultural mode of production paved for capitalist system. Capitalism is growing in varied forms such as extractive capitalism, corporate capitalism and so on. This is the result of new networks among individuals, societies and nations. This has brought prosperity to people and nations as well. The civilized world has facilitated systems of rights which are indispensable for humanity to survive in a decent form. Human beings inherit good natural rights which are recognized by the governments. Not only is recognition of natural rights protected and enforced by the governing system. One such right is privacy which is an offshoot of right to life.

**Concept and Dimensions of Privacy:**

Privacy is essential for human existence in civilized manner. This is because humans cannot live an animal existence. It is natural and inalienable right of human beings. Privacy is available to all without any discrimination. It is one of sources of happiness and peace. Autonomy and dignity are foundational principle. Human beings are different physically, biologically, socially and economically. This intrinsic difference is essence of privacy. Thus, heterogeneity presupposes an element of privacy. This difference necessarily entails space for privacy which is nothing but seclusion from others. Privacy in contrast to public is an intimate phenomenon. This brings in

restrictions on privacy since it is not absolute right. It has limitations. Privacy has an instrumental value in the sense it facilitates life, liberty and freedom for a civilized life to fulfill one's desires. Another facet of privacy is dignity. Privacy involves intimacy and autonomy without any discrimination whatsoever. The autonomy of the body and mind is essence of privacy. Privacy postulates private space for individuals. Privacy has three dimensions: spatial, decisional and informational. The spatial is creation of private space whereas personal choices decisional.

The information dimension is retention of personal control over information pertaining to his/her individual. It involves bodily privacy too. (Aadhar Judgement Part I p. 28) The function of privacy is to prevent the public from encroaching and eventually swallowing up private matters (Dorothy J. Glancy). Privacy puts restrictions on public and private actors and entities.

**Evolution of the Idea of Privacy:**

The idea of privacy was conceptualized as right to privacy by Warren and Brandeis in 1890. They distinguished between personal fact/behavior with copyright of any intellectual act. This implies an action of tort for damages in all cases. Even in the absence of special damages, substantial compensation could be allowed for injury to feelings as in the action of slander and libel. '(Warren and Brandies) Aristotle spoke of public sphere and personal sphere by using words 'polis' and 'oikos' respectively. This is the essence of privacy of individuals by distinguishing personal from public sphere. It is an early recognition of privacy. In medieval times J S Mill recognizing privacy said: 'over himself, over body and mind, the individual is sovereign". The libertarian principles sprouted from this assertion including privacy. Jean Austin distinguished 'jus publicum and jus privatum', thus endorsed the notion of privacy. Roscoe Pound, recognizing privacy, said, 'the right to be let alone is a right to enjoy life'. The notion of privacy is essential ingredient of happy life.

**Information Technology and Privacy Challenge:**

Information technology (IT) has revolutionized the world and the life of an ordinary citizen in an unimaginable manner. The computer, internet and the flow of

information and the process have affected the life of every individual enormously. It is shaping and reshaping the lives and activities of society which has posed threats to privacy. The rise of intelligent machines, i.e., computers, can make decisions and create new ideas faster than ever. The implication is that humans are being replaced in many ways. Earlier inventions like radio and printing press were passive agents whereas the IT tools and devices are active agents in human life. The rise in the application of IT in almost every sphere of life has posed serious threat to individual privacy. The concept of information in the IT domain has unique qualities. The information is non-rivalrous which means the use of information by one person does not make it less available to others. The quality of information remains intact in spite of number of users of same information. It is invisible. It enables invasion of data privacy and as such difficult to ct the encroachment on privacy. The system allows easy access to information and same can be stored and even disseminated without any notice. Information travels faster and collection is also fast. Information of large quantity can be collected, stored and transmitted at higher speed. Another feature of information is recombinant, thus, facilitating the data output as an input to generate more data output. This enhances the quality of data and subsequently the value of data too. The digital age has opened a pandoras box as regards data generation. Individuals are generating valuable data constantly which are tracked by the state and non-state actors. The individual's moves, choices, preferences and entire set of behavior patterns are tracked. The data generated even in passive mode of individual with every click on the 'world wide web'. In this web identity process and parameters have changed from hard binary to biometric identity. (Manan Dwivedi, 2025:22). An individual's active engagement as well passive observation allows continuous data generation and outputs. Thus, digital footprints are left behind once the IT device is used by individuals. It reveals human behavior and interactions. The information is collected, processed, and sold, making big data for targeted entities for use and misuse.

**Privacy Jurisprudence in India:**

The advent of IT-enabled operations has penetrated all spheres of human life. The space between private and public sphere is drastically constricted. As a result, the

privacy of individuals is at great risk. Decent and civilized human life is becoming difficult. This process begun with appearance of newspapers as a means of public communication. From there onwards human society is struggling to protect the sphere of individual privacy. The process of protecting privacy is now hastened due to all round application of IT-enabled services. The present ubiquitous application of IT, the necessity of protecting privacy, has gained momentum. Polity and governing systems must protect the right to privacy in recognition of this natural right so that the individual can retain his/herself. Further, the enforcing of this right must be the priority of the government and judiciary. In India, the Right to Life in Article 21 of the constitution has inherent right to privacy. In spite of this, the saga of privacy right is zigzag. In M P Sharma vs Sathi's case, the Supreme Court did not favor this since there is no express mention in Part III of the Constitution. The Supreme Court in Kharak Singh vs State of UP partially recognized this right. It opined that police have no right to domicile visits to habitual offenders' houses. It violated the liberty and dignity of the individual. Following Griswold vs Connecticut and Roe vs Wade cases the Supreme Court of the US, the Supreme Court of India in Govind vs State of MP and others recognized right to privacy. The state can interfere in the right to privacy only on compelling interests of state. The test of state interest is the criteria for encroaching privacy of the individual. The telephone tapping case of 1997 affirmed right to privacy The court held that interception telephone communication contents only through procedure established by law. The landmark judgement of Aadhar in K S Puttaswamy vs Union of India enunciated the privacy jurisprudence. The Supreme Court bench of nine judges unanimously declared the right to privacy as a fundamental right under Article 21. However, it is not absolute right, it is subject to restrictions and limitations.

**The Digital Personal Data Protection Act, 2023:**

The judgements of Supreme Court and fast-growing application of IT services in various spheres of human life compelled for legal structure for the enjoyment of privacy. The result is DPDP Act, 2023. Rules under Act are yet to be finalized. Draft rules are in the public domain for public consultation and feedback. The Act provides for processing digital personal data with an aim to protect rights of individuals to

protect their personal data and need to process such personal data for lawful purposes. The Act is applicable to processing digital personal within the territory of India where the personal data is collected. (Section 3). The data may be digital form, or it is subsequently digitized. The data collected within the territory of India while offering goods and services may be processed outside India. The 'data' means a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means. (Section 2(h)). The individual whom the data relates to is a 'data principal' (Section 2(f)). In case of minor its lawful guardian. The data fiduciary a person alone or in conjunction with other person determines the purpose and means of processing personal data (Section 2(i)). The data fiduciary is obliged to process personal data of Data Principal only after obtaining consent of the Data Principal. (Section 4). The consent of the Data Principal shall be free, clear, specific, informed and unconditional. The Data Principal can access his/her personal data from the data fiduciary and further the identities of said shared entities. (Section 11). Provision has been made for redressal of grievances of Data Principal with Data Fiduciary (Section 13). The Data Principal is bound by this Act not to impersonate and suppress the information. Not make false and frivolous complaints. (Section !5). The Act provides for appointments of consent manager, data processor and data protection officer. The personal data breach means any unauthorized processing of personal data or accidental disclosure, acquisition, sharing use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity. (Section 2 (u)). The penalties for data breach are prescribed in the schedule as per Section 33. The Data Protection Board is provided for adjudicating data breach complaints.

The issues to be noted as regards the DPDP law are at two levels. Firstly, at the level of the Act and its functional efficacy with reference to inadequacies in protecting the digital personal data, thus leading to violations of privacy. Secondly, at the larger context of socio-political and economic levels, especially in the framework of technological sovereignty.

**Critical Analysis of the DPDP Act:**

The Digital Data Protection law, by identifying the data principal notion has accorded the individua; a pivotal role in the legal schema. The Act revolves around this and his/her interests. It enables respect for the protection of privacy. The personal data of data principal is an asset of the data principal. Further, the data fiduciary and his obligations in maintaining and protecting personal data is delineated. The process of consent and remedies for breaches in the data protection are provided. A legal right is created. A speedy disposal of cases of data breaches is ensured by fixing a timeline for disposal. The Rule 18 (9) time duration of six to nine months is prescribed for disposal of cases.

In contrast to the General Data Protection Regulation, 2016 (GDPR) of European Commission the Indian law is soft in digital data protection particularly transfer of data to other countries. The Indian law permits data transfer to other countries freely except the countries prohibited by the government. The GDPR prescribes safeguards for transfer of data from EU countries to others. The EU has laid down a condition that adequate level of protection is necessary in the countries where the data is being. Further, by applying appropriate safeguards data can be transferred. The data transfer must be through binding corporate rules so that any violations are dealt appropriately. This kind of robust data protecting framework is absent in the Indian law.

The DPDP Board is provided for adjudicating cases of breaches of data by the data fiduciary. The effectiveness of the Board is dependent upon the following structural factors:

1. Procedure for appointment of Chairman and Members of the Board
2. Salary and terms of service conditions
3. Qualification of Chairman and members
4. Removal of Chairman and Members of the Board.
5. Restrictions on the powers of the Board

The central Government is empowered to appoint the Chairman and Members of the Board as per Section 19 (2). The salary, terms and service condition is to be prescribed by the Central Government. These are not to be varied to their advantage during their service. The term of office is two years. The qualification prescribed are ability, honesty and integrity and possessing special knowledge in the fields of data governance, administration of law, digital economy and so on. The qualifications are so broad that anyone having some knowledge or experience in the above areas are eligible. The Central Government is empowered to remove the Chairman and Members of the Board also they are eligible for reappointment. Central Government has complete sway over the Boards composition. The autonomy and independence required for these kinds of institutions particularly fourth branch institutions is missing. It has become handmade institution of the central Government.

The Board in Section 27 (3) must modify, suspend, withdraw or cancel its direction on the request made by the offended person and on the direction of the Central Government. This is a critical section where in the flexibility and dilution is introduced in the Boards orders. Thus, the central government's overreach has made the Board a gullible adjudicating body.

The Board acts as a civil court as per code of civil procedure. The Boards decisions are appealable before the Telecom Regulatory Authority of India. The civil courts are barred from entertaining any suit or proceedings in which the Board is empowered under the Act.

The Act is silent on compensation to the aggrieved party. The adjudicating officer appointed under the IT Act,2000 is divested the powers. These powers are now vested with the Board but without power to order compensation to the affected party for suffering the breach of personal data. (Alok Prasanna Kumar,2025: 11). Thus, the Act is soft as regards data transfer to other countries, lack of powers in compensating the victims of data breach. The orders of the are subjected to modifications on request. The autonomy and independence of the Board is compromised. The Act stands to strengthen the government more than the victims of data breach.

**Dataveillance and Data Colonialism:**

The IT revolution has enormously changed the life of human beings. The society, polity, economy and other sectors of life have been under the influence of IT tools and design. This has enabled better in terms of improved facilities, infrastructure, information and communication at a high speed. The IT industry has become new power centre in national and international politics and governance. The economic activities like market transactions and forces are enormously affected by the IT tools and programmes. The sports, culture and even to some extent religion is not spared in this revolution. The IT has facilitated in networking with people, activities and processes which were compartmentalised prior to the influence of IT. In this process identity and identifications have gained prominence and have become central to our social, legal and digital lives. (Manan Dwivedi 2025:22). Further, the 'quintessential Identity plays a significant role and is necessary for access, security as well as verification in the everyday lives of millions of citizens' (Manan Dwivedi 2025:22).

Of late, the IT sector is further revolutionised by the AI. The AI tool is being exploited by private entities to enhance their efficiency and profit. The Google tries to centralise all information at one place, the Amazon wants to become the world shop for all things, and all social spheres are connected by Facebook. This kind of monopolisation of activities leads to dataveillance. It is a surveillance of person's activities by studying activities such as transactions of credit cards, UPI based finances services, mobile phone calls and internet usage.

The China pioneered the AI technology with their 'New Generation AI'. This is followed by all other nations. Russia and US are also in forefront of this technology. In India Modi in January 2018 declared that: 'the one who control the data will control the world' (available at www.mea.gov.in/speeches-ststements). The data is basic ingredient of AI. Data on people's health, education, skills, luxuries are required to arrive at patterns. On this people are targeted for marketing, controlling, security and surveillance. In today's world this data is used to influence the minds of people in certain ideologies. The data generated on these activities is exploited by the data giant companies for all sorts of controlling activities. The AI driven economic activities lead

to data colonialism. In the 18th and 19th centuries the land was prime source of colonialism whereas in the present world it is data. Whoever controls data will control the human beings and natural corollary of this is political and economic control. The data colonialism is created out of Silicon Curtain. 'The Silicon Curtain is made of code, and it passes through every smart phone, computer, server in the world'. (Yuval Noah Harari,2024:375) Nexus p. 375). The code on smart phone determines the data flow and based on this algorithm run human life. The Ai will demand unprecedented levels of truth and self-discipline. (Yuval Noah Harari, 2024: 387). It is easier to hide illicit AI lab than illicit nuclear reactor. Further, AI have multiple usage-civilian, military, market, health, education. Sports, politics, governance religion and so on. Presently, AI is being used prominently by private entities for profit and market capture. But once state and government use AI in a full scale it may lead to humans may lose their democratic tools and practices. It leads to algorithmic citizen in which citizenship depends upon algorithmic inferences rather than law, rights and engagement with political system and government. (Goswami,2025:11). Thus, based on one's eligibility, visibility and inclusion algorithms decide citizenship. (Goswami, 2025:11). The algorithm-based system takes over monitoring humans. In a world where humans monitored humans, privacy was the default. But in a world where algorithmic based system monitors humans it may become possible for the first time in history to completely and annihilate privacy (Yuval Noah Harari, 2023: 241).

**Difficulty in Legally Catching up with Galloping AI innovations:**

Locating privacy in this emerging situation is difficult one. The data pertaining to human beings is accessed stored, transferred, processed and reprocessed once such data passes through AI operated system. Under such a situation data privacy is difficult to identify, regulate and control. Regulating the data flow from unprecedented surge in IT/AI innovations in the digital personal data spectrum is difficult and challenging. This is because 'the people who lead the information know far more about underlying technology than the people who are supposed to regulate it' (Yuval Noah Harari, 2024:225). The journey of DPDP law suffices this.

The journey begun with the judgement of K S Puttaswamy vs Union of India in Aadhar case (Anurag Sourot and Deepali Kushwaha,2025: 7359). It recognised the Right to Privacy as a fundamental right. Justice B N Krishna Committee was set up by Government of India on July 31st, 2017, to make recommendations on the data protection. This Committee submitted draft personal data protection bill18. The Personal Data Protection Bill, 2019 was introduced in the Lok Sabha on December 11, 2019. It was referred to Joint Parliamentary Committee (JPC) for detailed examination and recommendation. The JPC along with recommendations submitted revised bill on December 16th, 2021. This Bill was withdrawn from Parliament in August 2022 to accommodate latest developments in data protection sphere. Hence, a new draft Bill was prepared. It was released for public consultation from stakeholders in December 2022. The Cabinet approved the Bill on July 5, 2023. It was passed in both the Houses of Parliament in August 2023 and received the Presidents assent and officially gazetted it. The Rules under this Act are prepared and placed in the public domain in January 2025 for public consultation and feedback. From August 2023 till now the law has not come into force. The Rules are yet to be finalised. This is the state of present law, whereas the AI is revolutionising the IT sphere almost every minute. It appears that regulators are struggling. Under such a situation the privacy of an individual personal data is at stake. It looks that the legal digital personal data protection exercise is precariously grappling with incessantly unleashing AI revolution.

**Technological Sovereignty and Governance:**

The world is changing fast innovations in IT sector. The global order whether economy, politics, international relations, war and peace all are determined by the inventions and innovations in the field science and technology. It was so in the previous centuries but now it is more pronounced. The international market, trade, finance, politics and governance are inherently affected by the development's technology. Whether it is bilateral or multi-lateral international relations the technology plays bigger role and the outcomes are dependent upon it. In this scenario the issue privacy and personal digital data protection law needs to be examined.

The world order that emerged after second world war is replaced. Now it is multi polar world. The new nations have emerged. During the Second World War there were hardly 50 countries now it is 193. The forces of neo liberalism and globalisation have created strong international market and trade. The economies have opened at international level. Thus, 'the economies have become global but politics and legal system remains national and local' (Deepak Nayar, 2025:44). Implications of this is that national governance mechanism needs to cope up with transnational economies with the help of national regulations. The effectiveness of national laws is contestable. This is because of technological sovereignty. The technological sovereignty entails technological security. The key element in the concept of 'technological sovereignty is primacy of state power in the sphere of regulating relations related to methods of transforming the interacting world' (Prikhodo 2022, quoted in Jawahar Bhagwat and K S Zaikov, 2024:10). The 'technological sovereignty is the ability and freedom to choose to create or acquire, as well as apply, develop and use commercial purposes, technologies necessary for industrial innovation' (Grant,1983: 239-270). In the light of this India needs to achieve technological sovereignty in core strategic technologies (nuclear, space, defence), critical digital technologies (Semiconductor, telecommunications, electronics), emerging technologies (AI, quantum computing and drones), and biotechnologies. (Jaishankar and Sirkar 2024s quoted in Jawahar Bhagwat and K S Zaikov, 2024 :11). One more facet is storage of digital data locally within the country. For instance, it is estimated that the India generates 20% of global data but it can hardly store three percent. (Indian Express Editorial 21-10-2025) It means around 97% of digital data is stored outside India. The technological sovereignty expects closing this gap in the interest of national security and privacy. The dependency on other countries for the development of essential technologies hamper the governance capabilities. Countries which control critical raw materials and technologies write the rules of global economic governance (Berg et al, quoted in Jawahar Bhagwat and K S Zaikov,2024: 12). The country's regulatory system in the fields of high-end technologies depends upon the technological sovereignty. Hence, appropriate data privacy and protection is imperative in the context of growing sage of AI. The challenge is how to control the flow of data across borders at individual,

company and country level in the light of privacy requirements. The regime of digital personal data protectional law is initiated in India and how this will help to protect and promote right to privacy will be seen only after its full-scale implementation. The effectiveness of its enforcement will be known after its actual operation. The individuals availing the law in case of breach of privacy needs to be assessed.

## Author (s)

**Dr. Vijaykumar Torgal**
Retired KAS Officer
Dharwad