Journal for Re Attach Therapy and Developmental Diversities
eISSN: 2589-7799
2023 August; 6(8s): 966-971

Data Protection And Privacy Framework In India: A Comparative Study

Dr. Palvi Mathavan Puri[1*]

[1*]Assistant Professor, The Law School, University of Jammu.

ABSTRACT
Due to the exponential increase of data and its importance in many facets of our lives in the digital age, data protection is of the utmost importance. Developing an effective data protection and privacy framework is vital for the progress of the country. India has been recognised as the outsourcing hub by countries like UK and US. These countries consider data protection privacy and protection as fundamental right of their citizens. So, it is important for India to have robust data protection and privacy legal policy framework to maintain its competitive position.
This article throws light upon various provisions in Indian laws relating to data protection. A comparative analysis with foreign laws has also been made to understand the lacunas in the Indian laws. The paper shall examine the provisions of the IT Act which only deals with extraction of data, destruction of data, the Copyright Act,1957 and the new Digital Personal Data Protection Act, 2023. India needs to develop its data protection and privacy law, as well as develop a pertinent enforcement mechanisms.

Keywords: Data, Data protection, Privacy, Information Technology Act, 2000, Digital Personal Data Protection Act, 2023.

1. Data Protection : An Introduction

Data Protection refers to the means, process or practice of safeguarding the private/personal information/data of individuals during the process of their collection, storage, and dissemination, and to ensure that they themselves are in control of their information. It is the set of privacy laws that aim to ensure minimum intrusion into one's private life. The term "data protection" was coined in Europe to describe privacy-protective legislation, however, the United States refers to it as data privacy.[1] Article 12 of the United Declaration of Human Rights (UDHR) protects individuals from any arbitrary interference to his private life, his home, his family, and from any attack to his honor and reputation. Thus, every individual is fundamentally entitled to data and privacy protection as it is their human right.
The 21st century is regarded as the information age or the internet age. With the advancement in technology and the internet, data is made easily accessible. Some of the largest countries in the world are data-driven. For example, Ola and Uber are the largest mobility platforms, but own no vehicles; Alibaba is one of the largest retailers having no inventory; Facebook is the largest social media platform, but creates no content. With a humongous amount of information being solicited and disseminated online, a myriad of privacy and data protection concerns have arisen. In 2018, the Department of Justice (DOJ) charged two Chinese hackers for stealing information from 45 tech companies and governmental agencies, including NASA, IBM, and others.[2] Recently, the US Federal Bureau of Investigation and Cybersecurity also accused the Chinese hackers of trying to steal the coronavirus vaccine research.[3] Similarly, many other data breaches have occurred in the past. If such high-profile data of government agencies is not safe, then whose is?
In recent years, we have witnessed a tremendous rise in the use of technology. Ditching the traditional methods, the present generation has shifted towards endorsing online modes of shopping, banking, talking, playing games, etc. Moreover, the trend of keeping our social media profiles up-to-date, exposes the data of every individual to the public at large. Exposing our sensitive information like a credit card, debit card and bank details, mobile number, geographical location, pictures, intimate, private or business chats and calls, interests, financial, educational, family and medical records, travel history, etc., leaves our data vulnerable at the hand of the exploiters. Thus, to avoid exploitation and monitor the efficient flow of data without any infringement of rights, the data protection laws are required. It establishes a mechanism that enables the aggrieved party to seek relief. It also provides guidance and rules for organizations regarding the use of personal data. Data protection laws are important to enable individuals to build trust online by helping to keep the data safe and free

[1] White Paper, < https://www.welivesecurity.com/wp-content/uploads/2018/01/US-data-privacy-legislation-white-paper.pdf> accessed 10 December,2023.

[2] The Verge, <https://www.theverge.com/2018/12/20/18150275/chinese-hackers-stealing-data-nasa-ibm-charged> accessed October, 2023.

[3] Live mint, <https://www.livemint.com/news/world/us-says-chinese-hackers-trying-to-steal-covid-19-vaccine-work-data-reports-11589252247220.html> accessed October, 2023.

from the intrusion of the third party, thus avoiding its misuse, and deter cyber-crimes as much as possible. In 2016, when WhatsApp announced a change in its privacy policy, stating that all the analytics and data including phone numbers, names, location, status, and other details will be shared with Facebook, its parent company. This was challenged by being deceptive and threatening the right to privacy of users. This case is pending before the Supreme Court.[4] Instances like these call for a well-defined data protection regulatory framework.

In many countries across the globe, the enthusiasm towards data protection policies and laws is increasing. This is because increasingly sensitive and personal data is collected by organizations. Therefore, it is important for organizations to safeguard and manage personal information. Some of the countries have already implemented robust data protection laws while some are moving in that direction. Recently, an apprehension in India has emerged regarding the influence of data protection laws passed in other countries. According to Forrester Research (2013), China has effectively no restrictions to privacy and data protection, India has minimal restrictions and Australia has some restrictions. So, a comparative study of these some countries would give some ideas for India to move forward.

2. Objectives of the Study

The objectives of this research paper are as follows:

(a) To understand the legal as well as policy aspects of data protection and privacy in India.

(b) To compare the data protection and privacy policies as well as laws of India with other countries like US, UK, European Union, China and Australia.

(c) To examine the importance of data protection and privacy for India.

3. DATA PROTECTION UNDER THE INDIAN LEGAL FRAMEWORK

India has recently passed a data protection law in 2023. Before that, due to the lack of specific law, data protection in India was realized by the implementation of privacy and property rights. Privacy rights are enshrined in Constitution of India and also covered in the Information Technology Act, 2000. The property rights are covered by Indian Contract Act, 1872; the Copyright Act, 1957; and the Indian Penal Code, 1860. India's Ministry of Communication and Information Technology adopted Privacy rules, called the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (Lok Sabha Secretariat, 2013). These rules necessitate business entities to gather, process, and accumulate personal data. The personal data includes sensitive personal information to fulfill the laid down procedures.[5]

Even though the right to privacy is not explicitly or patently granted by the Indian Constitution, the Indian judiciary, through many precedent cases has recognized this right under the fundamental rights enshrined under Article 21 of the Constitution of India. Realizing the paramount importance of Right to Privacy, the Supreme Court through several cases, including *Kharak Singh v. State of U. P.* AIR 1963 SC 1295; *Govind v. State of M.P.* AIR 1975 SC 1375; *People's Union of Civil Liberties (PUCL) v. Union of India* AIR 1997 SC 568, has declared that the Right to Privacy is an intrinsic, sacred, fundamental and integral component of the Right to Life and Personal Liberty, and a part of the fundamental right enshrined under Part III of the Constitution. Reiterating this decision, the Supreme Court in the landmark Justice *K. S. Puttaswamy v. Union of India*, [2017] 10 S.C.C. 1 judgment also emphasized on the necessity of giving statutory recognition to data protection.[6]

India did not have any specific legislation until 2023 dealing with data protection. However, it had adopted various international conventions and declarations like the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, which recognizes the right to privacy. In India, earlier data protection is achieved by provisions maintained under other existing legislations.

Information Technology Act,2000

The Information Technology Act, 2000 is a single legislation which was brought into existence to provide a legal framework for regulating the entire electronic system including e-commerce, emails, electronic transactions, electronic

[4] Right to Privacy and Social Media, <http://rsrr.in/2018/10/27/right-to-privacy-and-social-media/> accessed October,2023.

[5] Dla Piper (2014). Data Protection Laws of the World. pp. 20-24. URL: http://www.dlapiperdataprotection.com/system/modul es/za.co.heliosdesign.dla.lotw/functions/export.pdf?c ountry=all (Last accessed on: 5th December 2023).

[6] https://inforrm.org/2017/09/04/case-law-india-puttaswamy-v-union-of-india-supreme-court-recognises-a-constitutional-right-to-privacy-in-a-landmark-judgment-hugh-tomlinson-qc/

data, and electronic documents. It contains provisions for the prevention of cyber-crimes and unauthorized use or misuse of computers, computer systems, electronic data, by imposing heavy penalties and criminal liability against the offender. Some main provisions dealing with data protection are as follows:
Section 43 provides for penalty and compensation for accessing, downloading, extracting or making copies, disrupting, deleting, destroying, stealing, altering, or causing damage to computer or computer systems, without the prior consent of the individual.
Section 43A provides for compensation for failure or negligence in adopting reasonable security practices and procedures while handling sensitive personal data.
Section 65 provides punishment for tampering with electronic documents.
Section 72 provides penalty for breach of confidentiality and privacy and Section 72A imposes punishment on persons and intermediaries for disclosing unwarranted information by virtue of a lawful agreement.
Thus, the IT Act, 2000 imposes a certain kind of liability and obligation on every person dealing with personal data, to handle such information by adopting reasonable security practices and with care.
Today, 20 years after passing the act, the virtual ecosystem has grown to such an extent that it is involved in every aspect of our lives. However, this act failed to address all the issues. In the year 2008, an amendment was brought to the existing IT Act, 2000. The major highlight was that according to Section 79 the intermediaries would not be held liable for the content or data made available by the third party. However, this protection is not absolute.
In 2011, the Ministry of Communications and Technology notified a set of rules known as the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, whereby it set out rules and procedures to be followed by corporate bodies to ensure reasonable security practices and procedures while handling sensitive information.

The Copyright Act, 1957
According to Section 2(o) of the Copyright Act, computer database and computer programs is protected under the term "literary works". Apart from the landmark Puttuswamy judgment, this was also upheld in the case of ***Burlington Home Shopping Pvt. Ltd. v. Rajnish Chibber & Anr.***[7] Also, Section 63B of the Act provides for punishment to persons who knowingly use the infringing copy of the computer program.

Indian Penal Code, 1860
The IPC, being a very old statute, does not expressly address data protection breaches. However, the liability for data breaches is gathered from related crimes like theft. For example, Section 403 imposes criminal punishment for dishonest misrepresentation of property, including 'data' within the ambit of the word 'property'.

The Personal Data Protection Bill, 2019
Following the ***K. S. Puttaswamy v. Union of India***, judgment, a committee of experts chaired by Justice B.N. Srikrishna was set up, which submitted a report and a draft Personal Data Protection Bill, 2018 after examining the issues related to data protection in India. After making necessary changes, The Personal Data Protection Bill, 2019 was introduced in the Parliament in 2019[8]. The Bill seeks to create a framework to regulate the processing, collection and storage of personal data by protecting the privacy of the individuals. However, the bill has been criticized on the grounds that it fails to provide a clear and detailed roadmap for governance.
It is pertinent to note that despite the existence of the above provisions, India did not have any comprehensive legislation in place till now. To address the trending issue of privacy and data protection, a comprehensive and separate regulatory framework is required to monitor every aspect of that area, fill in the lacunas in law and bring in more clarity on the subject.

Digital Personal Data Protection Bill, 2023
The first draft of the Data Protection Bill came out in 2018. After various rounds of amendment in 2019 and 2021, the Bill was scrapped and replaced with the Digital Personal Data Protection Bill, 2022. The Digital Personal Data Protection Bill, 2023 introduced on 3 August, 2023 and was passed by the Lower House of the Parliament on 9 August, 2023. The Bill has received the Presidential assent followed by official gazette notification and has become a law of the land on 11 August, 2023.
The Digital Personal Data Protection Act, 2023 lays down procedures to process personal data in a lawful manner and thereby empowers and protects the rights of Data Principals. Factors such as accountability, transparency, data

[7] 1995 PTC (15) 278
[8] https://lawtimesjournal.in/justice-k-s-puttaswamy-retd-vs-union-of-india/.

minimization, fairness, accuracy, and lawful processing of personal data have been reflected in the DPDPA. It addresses Data Principals as 'she/her', which is unseen in any Indian Law till date and sets the tone in a new light.
An act to provide for the processing of digital personal data in a manner that recognizes both the right of individuals to protect their personal data and the need to process such personal data and the need to process such data for lawful purposes and for matters connected therewith or incidental thereto.

1. The Bill protects digital personal data that is the data by which the person may be identified.
2. The Bill also seeks to introduce data protection law with minimum disruption while ensuring necessary change in the way data fiduciaries process data; enhance the ease of living and the ease of doing business; and enable India's Digital economy and its innovation ecosystem.
3. The Bill is concise and saral, i.e. simple, accessible, rational and actionable law, as it use plain language, contains illustrations, contains no provisos and has minimal cross referencing.
4. The Bill provides for the following rights of the individuals such as, right to access information, right to correction and erasure of data, the right to grievance redressal and the right to nominate a person to exercise rights in case of death or incapacity.
5. The Bill also safeguards the personal data of the children only with the parental consent. The bill does not permit processing which is detrimental to wellbeing of children or involves their tracking, behavioural monitoring or targeted advertising.
6. The exemption provided in the bill are for notified agencies, in the interest of security, sovereignity, public order, for achieving research, archiving or statistical purposes, to enforce legal rights and claims, to perform judicial or regulatory functions, for approved merger, demerger etc., to locate defaulters and their financial assets.
7. The main functions of the Board includes, to give directions for remediating or mitigating data breaches; to inquire into data breaches and complaints and impose financial penalities; to refer complaints for alternate dispute resolution and to accept voluntary undertakings from data fiduciaries; and to advise the Government to block the website, app etc. of a data fiduciary who is found to repeatedly breach the provisions of the Bill.

4. DATA PROTECTION UNDER FOREIGN LAW

In 2017-18 a 10% increase was seen in the number of countries that enacted data privacy laws covering the public and private sectors and meeting the standards of international agreements. Many countries have also replaced their existing laws. There has been an awakening among countries worldwide, whereby they have started moving towards stronger and globally pervasive laws relating to the trending issue of data privacy.[9]

European Union
The European Union, which is a union of 27 countries, recognizes the Right to Privacy as a fundamental right. Article 8 of the Charter of Fundamental Rights of the European Union specially provides for the protection of personal data. The introduction of the General Data Protection Regulation (GDPR) in May 2018 is a notable change and represents a positive framework in the data protection regimes. It adopts a rights-based approach while dealing with the free movement of personal data with the union. The regulation is comprehensive legislation that seeks to strengthen and protect the privacy rights of the individuals in the member countries. The Regulation is very strict and imposes heavy fines, which prioritizes the affected countries to comply with the terms. The Data Protection Law Enforcement Directive 2018 is an EU legislation, parallel to GDPR which deals with the regulation and processing of personal data used by law enforcement authorities. It controls data that falls outside the ambit of GDPR. Countries like Brazil, Japan, UK, South Korea, Thailand, and many more have incorporated Data Privacy laws similar to the GDPR. This highlights the success of the regulation.

United Kingdom
The UK has a dedicated Data Protection Act in place. To implement the GDPR, the UK government enacted the Data Protection Act, 2018 which regulates and controls how private information should be used by business and governmental organizations. It puts a restriction on the collection of data and provides that data should be collected only for lawful purposes. The Act lays down 'data protection principles' which must be followed.

The United States of America
The US courts in ***Olmstead v. United States***[10], 277 U.S. 438 (1928) held that the right to privacy is the right to be left alone. In the case, Justice Louis D. Brandeis stated that this was the most comprehensive rights granted by the maker of

[9] https://en.wikipedia.org/wiki/Privacy

[10] *Olmstead v. United States*, 277 U.S. 438 (1928)

the US Constitution. However, similar to India, the US too does not have single principal legislation dealing with data protection. The data is categorized into various groups based on their importance and utility, and each group has been conferred with different degrees of protection. Several federal and state laws regulate consumer privacy and data protection on a sectoral basis. Some of these include the Gramm Leach Bliley Act for the protection of personal data and Non-public Personal Information (NPI) in the banking and finance sector; Health Insurance Portability and Accountability Act (HIPAA) which governs the data in the health insurance sector; Children's Online Privacy Protection Act (COPPA) which protects the privacy of children below 13 years of age, and regulates the collection of their personal data; Driver's Privacy Protection Act (DPPA) which protects the individual's motor vehicle records. Similarly, there are hundreds of other legislations in the US governing the data of each sector. In the year 1974, the US Privacy Act was passed to safeguard the privacy rights of the individual by creating ethical, justifiable, and reasonable standards with regard to data held by the government agencies.

China

China has not passed a wide-ranging data protection legislation. So, the provisions of data protection and privacy originate from multitude of laws and regulations. China has effective pronouncements that form the basis of data protection. Examples include: Decision on Strengthening Online Information Protection passed in December 2012, National Standard of Information Security Technology passed in February 2013. These pronouncements intend to protect information security; defend the interests and legal rights of citizens, legal bodies and other organizations; and guard public interest and national security. It is noteworthy that in China, the decision has same effect as the law. In addition, there are some provisions in various legal instruments that covers certain aspects of privacy and data protection, such as, Article 253 of the Criminal Law, provisions on Telecommunication and Internet User Personal Information Protection, Consumer Rights Protection Law etc.

Australia

In Australia, data protection and privacy policies are the mix of federal and state governments legislation. The Australian government Federal Privacy Act 1988 and the Principles of Privacy apply to all Commonwealth Government agencies, Australian Capital Territory Government agencies and private sector companies with a minimum annual turnover of AUD 3 million. Australian states have data protection legislations, such as Information Privacy Act, 2014 by Australian Capital Territory, Information Act, 2002 by Northern Territory, Personal Information Protection Act, 2004 by Tasmania, Privacy and Personal Information Protection Act, 1998 by New South Wales (NSW), Privacy and Data Protection Act, 2014 by Victoria, Information Privacy Act, 2009 by Queensland. There are some other legislations that influence the data protection and privacy for specific data or activities. They are Telecommunications Act, 1997 by Commonwealth, National Health Act, 1953 by Commonwealth, Health Records and Information Privacy Act, 2002 by NSW, Health Records Act, 2001 by Victoria, Workplace Surveillance Act, 2005 by NSW Under Privacy Act, an organization could be individual, partnership, body corporate, unincorporated association or even a trust.

5. Analysis of Data Protection Legislation of India with Other Countries

On comparing India with the other developed countries like the UK, the US, and the EU countries, we find that all the developed countries have adopted their personalized strategies for addressing their data privacy issues. Each country has endorsed a separate approach to enact the data protection laws, after considering the utility value in their country. The US has adopted a sectoral approach to make data protection more efficient by regulating the flow on a sector-to-sector basis. However, this patchwork system of legislations may sometimes overlap or contract one another.

When we analyze the Data Protection laws in India and the EU countries, we find a couple of loopholes. The very obvious difference is the absence of a comprehensive data protection legislation in India. The Personal Data Protection Bill, 2023 is still at a very nascent stage. Even though India does have provisions under the different acts, it lacks efficiency and effectiveness due to the absence of a dedicated and detailed framework to address the issue. As data breach issues have been increasing day by day, the need for dedicated legislation also increases. Moreover, the terms and provisions are very ambiguous. For example, there is no clear demarcation between 'personal' and 'sensitive' information. Also, the term 'data' under the IT Act, 2000 is only restricted to computer-based data. In 2015, in the case of ***Shreya Singhal v. Union of India***[11], Section 66A of the IT Act was struck down on the grounds that it was vague.

Another issue with the Indian laws is the inadequacy and insufficiency of penalties. The penalties are mostly monetary in nature, which fails to have a deterrent effect. However, when we look at the EU's GDPR, despite a few loopholes, it is effective as it is concise, and directly addresses the issue at hand. The high fines and stringent punishments help as a deterrent to future offenses.

[11] *Shreya Singhal v. Union of India* AIR 2015 SC 1523

6. Importance of Data Protection and Privacy in India

Many developed countries have taken a lead in data protection and privacy. India has emerged as a top choice for global outsourcing (Clutch, 2021)[12]. India has clearly benefitted from outsourcing. In a survey conducted by Statistic Brain Research Institute (2015), 26% of Chief Financial Officers (CFOs) favor India for their company's outsourcing needs. The surveyed companies have cited economic, political, and cultural incentives for choosing India. Companies have also been impressed with India's pro-business and entrepreneurial climate. India's historical trade ties to the United Kingdom and United States also play an important role (George and Gaut, 2006). India also possesses low-cost and highly qualified workforce with English speaking capabilities and advance educational standards. India's steady democratic government, independent institutions, advances in Information Technology as well as convenient geography which is suitable for around the clock work makes it possible for companies to seek outsourcing to India as a preferred destination (Chandra and Narsimhan, 2005). However, it is important to note that the global competition for outsourcing is increasing. Countries like Indonesia, Estonia, Singapore, Bulgaria, Philippines etc. are giving a tough competition to India. Moreover, countries in Europe and United States consider privacy a fundamental right. So, it is a need of the hour that India should toughen its data protection and privacy laws. It is also important that India should encourage the companies to self-regulate. India needs to address the loopholes in its data protection and privacy laws to address the concerns of American and European companies about their data protection and privacy. India needs to assure its outsourcing clients that cost effectiveness of outsourcing would not be diluted by the additional costs of handling customer data privacy apprehensions, in case of a breach.

CONCLUSION

India has made the progress in data protection and privacy by putting in place various legal and policy measures. The main findings from this research regarding data protection and privacy in India are:

(a) Privacy and property rights conferred under the Indian legal-policy framework provides a certain amount of data protection and privacy.
(b) There are multitude of laws in India which protects certain aspects of data protection and privacy. These laws include the Constitution of India; Information Technology Act, 2000; Indian Contract Act, 1872; Copyright Act, 1957; and Indian Penal Code, 1860.
(c) India has also developed privacy rules for business entities to manage personal data.
(d) There is not a single comprehensive legal-policy framework in India to address data protection and privacy.
(e) The penalties prescribed under the existing Indian laws are not enough to deter the cyber-criminals.
(f) The existing Indian laws mostly applies to state- and state-owned enterprises.
(g) The existing Indian laws does not address finer details of data protection and privacy. For example, lack of distinction between data protection and database protection under Copyright Act, 1957.

It is clear that India has certain limitations in its data protection and privacy legal-policy framework. India seems to be doing better than countries like China, however not as good as Countries like Australia, US, UK. The shortcomings of data protection and privacy in India visà-vis foreign countries are:

(a) India does not have a National Data Protection Authority like Privacy Commissioner in Australia.
(b) Unlike SPAN Act, 2003 of Australia; there is no legal-policy framework in India to address the data protection and privacy issues related with electronic marketing.
(c) Unlike Australia, there are no laws and regulations in India to manage cookies, location data or behavioral advertising.

A comprehensive legal policy framework to address data protection and privacy issues is need of the hour in India. Such legal and policy framework can be vital to sustain investor confidence. This is especially true for foreign investors, which send large volume of data to India for managing their back-office operations. Data protection can play an important role in outsourcing arrangements. These arrangements delegate an Indian company with a foreign company's confidential customer data, trade secrets etc. Since, outsourcing by foreign companies' plays a significant role in contributing to the Indian economy. So, it acts as an added incentive for India to strengthen its legal-policy framework to address its data protection and privacy concerns.

Data breach and privacy concerns have been constantly on a rise. This calls for the enactment of comprehensive laws regarding the same. After analyzing the laws of India with a few developing countries, we have found out that those countries have comprehensive data protection legislation in place. However, India severely lags behind in this area which hampers its position in the international commercial regime. The Indian laws are inadequate and insufficient in dealing with the plethora of threats associated with personal data, which is a matter of great concern. A nationwide holistic and dedicated legislation is the 'need of the hour'. Major inspiration can be drawn from the GDPR, which provides to the point and detailed regulations regarding data protection. Stringent penalties should be imposed to provide a better deterrent.

[12] Clutch (2015). Top Outsourcing countries. URL: https://clutch.co/top-outsourcing-countries (Last accessed on: 2December 2023).