Right to Privacy and Data Protection under Indian Legal Regime

Bandita Das[1] & Jayanta Boruah[2]

Research Article

Abstract

Privacy has emerged as a basic human right across the globe and in India too it has been recognized as a Fundamental Right under Article 21 of the Indian Constitution. Right to Privacy is closely related to protection of data which in this technological and globalized world, has become very difficult to achieve. Further, violation of privacy right by the Ruling majority through discriminatory legislations has also become possible due to lack of legal protection to this Right. In India, this Right was not initially recognized as a Fundamental Right, neither any specific law on data protection for securing the Rights of Privacy of the citizens were enacted. At the same time, there had been many allegations regarding violation of privacy rights both by the Government as well as by the Private Commercial Entities from time to time in India. Such allegations were also placed before the Courts of Law where the Courts had given landmark Judgements including guidelines and rulings. It thus, becomes very important to analyze all these legal developments relating to Right to Privacy and Data Protection in order to understand the extent of security granted by the Indian legal framework to the citizens over Right to Privacy. It has however been found that adequate recognition has been given to the Right to Privacy by the Indian Legal Regime and therefore significant steps were taken to prevent data theft and misutilization of sensitive information, yet a major extent of progressive developments is still needed to enhance the scope of data protection in the contemporary times for securing the Right to Privacy of the Indian citizens.

Keywords: Privacy; Data Protection; Personal Information; Sensitive Information; Confidentiality; and Public Interest

1. Introduction

Privacy means capability of a person or a group of persons to hide information from others as well as to seclude themselves.[3] Besides, it has been recognized internationally as Human Rights

[1] Advocate, Gauhati High Court, dasbandita1993@gmail.com.
[2] Research Scholar, North-Eastern Hill University, Shillong, jayanta.boruah94@gmail.com.
[3] Dr. Payal Jain & Ms. Kanika Arora, "Invasion of Aadhaar on Right to Privacy: Huge Concern of Issues and Challenges", 45(2) *Indian ILR* 33-35 (2018).

under Article 12 of UDHR[4] which provides that everyone has the liberty not to get interfered with his personal privacy, correspondence, family and also not to be permitted to defame its own reputation or honor. Every individual has a right to get safeguards from such intrusion. Privacy is especially acknowledged as a right under international treaties of Human Rights. The ICCPR[5], the ICPRAMW[6], and the UNCRC[7] adopted the same language.[8] For securing this Right of Privacy, Data Protection Laws are required and such laws are called privacy laws, procedure, policies whose objectives is to reduce encroachment on one's privacy that may be caused by the storage, collection, distribution of personal information or data. And Personal data means that information by which one's identity can be known whether it being collected by entity or Government."[9]

The concept of privacy is of old origin, it is a part of Human Rights which is within the human since birth. They cannot be sacrosanct, divisible. It includes right to be left alone, privilege communication, privacy of the body, right to have sexual orientation, right to have family etc. However, it does not include within it the private right, information which is for public interest or in the form of public record. In order to lead a dignified life, privacy is very essential. But with the advancement of innovative technologies and wide use of internet, it becomes very easier to access anyone's data and to share such data to third party which may lead to misuse of data. Moreover, many cybercrime attacks including phishing, virus, ransom ware, hacking, spamming etc. can be seen in our society. So, in order to avoid all such attacks, we need strict Data Protection Laws. Though there are no exhaustive laws in India dealing with data protection, in the absence of such legislations, data protection is enforced under Constitution of India, IT Act 2000, Indian Contract Act, Intellectual Property Laws etc. Furthermore IT (Amendment) Act, 2008 was passed in order to cover all those matters which the original Act failed to do. It also inserted two very important provisions, via- Section 43A and Section 72A that basically talks about liability of body corporate and sanction for revelation of data by infringing a legal contract. Besides many efforts are being taken to protect data like amending

[4] Universal Declaration of Human Rights, 1948, *available at:* Universal Declaration of Human Rights | United Nations (Last visited on Dec. 15, 2020).
[5] International Covenant on Civil and Political Rights, 1966, *available at:* OHCHR | International Covenant on Civil and Political Rights (Last visited on Dec. 15, 2020).
[6] International Convention on Protection of Rights of All Migration Workers, 1990, *available at:* OHCHR | International Convention on the Protection of the Rights of All Migrant Workers (Last visited on Dec. 15, 2020).
[7] The United Nations Convention on the Rights of Child, 1989, *available at:* OHCHR | Convention on the Rights of the Child (Last visited on Dec. 15, 2020).
[8] Rukhmini Bobde, "Data protection and the Indian BPO Industry", 2 *law Rev. GLC*, 79-88 (2002-03).
[9] Vijay Pal Dalmia, Advocates, "India: Data protection laws in India-Everything you must know", *available at:* www.mondaq.com/India/x/655034/data+protection/Data+Protection+Laws+In+India (Last visited on Oct. 21, 2019).

the IT Act, Data Protection commission of India, Information technology (Reasonable Security Practices and Procedures and Sensitive Personal Data and Information) Rules, 2011, The Data (Privacy and Protection) Bill, 2019 etc. Perhaps it is not the first time that the Data Protection Bills have been laid before Parliament, long before in 2009 Baijayant Jay, a member of Parliament had laid down a Bill called the Prevention of Unsolicited Telephonic Calls and Protection of Privacy that intended to restrict unwanted telephone calls of individuals or business promoters made to persons, who explicitly showed unwillingness to receive it but despite they made uninterrupted calls. Apart from Baijayant Jay, many of others such as Rajeev Chandrasekhar (2010), Om Prakash Yadav (2016), etc. had introduced Bills in past relating to citizen's data privacy. However, the Bill of 2019 has not been yet enacted.[10] Again, after the privacy judgment declared by the Supreme Court in the case of K.S Puttaswamy, many of the issues came into consideration like validity of Aadhaar Act (Targeted Delivery of Financial and other Subsidies, benefits and services) Act 2016), Section 377 of IPC i.e Consensual homosexuality, etc.

Presently, data either it may be of personal or sensitive is becoming a basis to earn income for those who illegally share data to the third party other than the authorized person. In addition to this, many off shoring business operation are alleged to have been conducted in India wherein person's data are exported by overseas companies. These lead to major threat to privacy.[11] Therefore, this Article will analyze the Indian Legal Framework to find out whether, such framework is sufficient to safeguard the privacy of Indian Citizens or whether there is a need of any new provisions to be adopted? This paper will further focus on some of the International legal instruments adopted by foreign countries to have an understanding about the requirements in Indian legal system for ensuring a higher level of data security in India.

2. Evolution of the Right to Privacy as Fundamental Right in India

Nowhere the Constitution expressly defines the concept of privacy. But in general, what we know about privacy is right of human being to live freely without any disturbances, right not to be interfered as well as right to be left alone. But the problem is that many of the people are exploited from enjoying this right, besides many of them are even not aware that this is their

[10] Kasim Rizvi & Ranjit Rane *"*High time India had a Right to Privacy Law: A private member bill tabled recently tick mist of the boxes that one would expect from a strong data privacy law*", Livemint*, Jul 30, 2017, *available at:* http://www.livemint.com>opinion/EoRER0qfjd1ocT1twFzdVJ/High-time-India-had-a-right-to-privacy-law.html%3ffacat=amp (Last visited on Oct. 21, 2019).

[11] "Data Protection and Privacy Issues in India", ELP, *available at:* www.wlplaw.in (Law visited on Oct. 21, 2019).

right which cannot be prevented from enjoying by anyone. So, in order to aware people of their privacy right which are also Human right, many Declarations and Covenants have been enacted. Moreover, the Indian Judiciary also interpreted privacy right as a fundament right under Article 21 of Part III of the Constitution. Following were the series of Cases which dealt with right to privacy-

MP Sharma v. *Satish Chandra*[12]

The provision of power and seizure in this case was challenged on the basis of transgression of Right to Privacy. However, the higher judicial authority observed that the intention of the Framers of the Constitution was not to limit the power of search and seizure as violation of Fundamental privacy right. Besides, the SC cleared that MP Sharma case did not resolve question relating to Right to Privacy as Fundamental Right under Part III of the Constitution. So here Right to Privacy was not declared as a Fundamental Right under the Constitution.[13]

Kharak Singh v. *The State of UP*[14]

In this case the surveillance under the UP regulation was put in question on the ground that it infringes Fundamental Right under Part III of the Constitution. On hearing this, the Supreme Court struck down Regulation 236(b) because it permitted surveillance by + visit at night and it is a clear violation of ordered liberty and an unauthorized intervention on person's home. However, the other clauses of the Regulation were still legitimate because Privacy was not yet recognized as a fundamental right under the provision of the Constitution and thereby there is no application of Article 21. But J. Subha Rao gave a contrary opinion stating that Privacy is an integral segment of Article 21 even if it was not acknowledged as fundamental right.[15]

Govind v. *State of Madhya Pradesh*[16]

Like in Kharak Singh case, Regulation 855 and 856 of the MP police were again challenged in this case on the ground that State surveillance in the domicile of habitual offenders at night and picking up whom they suspected to be criminals were violation of Right to Privacy. However, SC in this case refused to strike down these regulations holding that domiciary visit at night would not always be an unreasonable restriction on the Right to Privacy. It was the first case where it was held that privacy right cannot be enjoyed in total. There could be fair restriction on the basis of compelling public interest.

---

[12] 1954 AIR 300, 1954 SCR 1077.
[13] Bijan Brahmbhatt, "Position and perspective of privacy laws in India", *available at:*http://www.lawctopus.com/acadomike/postion-perspective-laws-India/ (Last visited on Oct. 22, 2019).
[14]1963 AIR 1295, 1964 SCR (1) 332.
[15] *Ibid*.
[16] 1975 AIR 1378, 1975 SCR (3) 946.

Malak Singh Etc v. *State of Punjab & Haryana &ors*[17]

Here the Supreme Court held that where there was no illegal interference, State surveillance exercised within its limit and without violating the Right to personal liberty of the citizen, shall be valid and lawful.

R. Rajagopalan v. *State of Tamil Nadu*[18]

In the case of R.Rajagopalan, the higher judiciary by declaring right to privacy intrinsic in Article 21 of the Constitution has decided that every Indian citizen has the liberty to safeguard his or her privacy whether it may be related to education of child, giving birth to and raising a child, reproduction, decision upon the matter of marriage, family etc. Pertaining to the above matters, no one can publish anything without obtaining the permission of the concerned person, whether it is genuine, complimentary or critical. And if someone does so then it will be clear violation of privacy."[19]

People' s Union for Civil Liberty v. *Union of India*[20]

In this case, the question arose as to the Constitutional validity of telephone tapping on the ground of violating Right to Privacy. The Supreme Court held that Right to Privacy includes talking over telephone and such call can be made by sitting in any place of its own office or at home because telephone conversations itself is an essential aspect of man's life. Therefore, tapping of telephone conversations is a violation of Right to privacy under Article 21. However, the State can tap such conversations if there is a law directing the procedure what to be adopted for the activity of telephone tapping or if it is in conformity of the Rules framed under Telegraph Act.

With this judicial interpretation, different kinds of privacy arose like privacy of telephone conversation, privacy of medical records etc. However, it has not been declared as fundamental right because majority judges in both Kharak Singh and MP Sharma cases held that Right to Privacy is not a Fundamental Right.

But in 2012, a petition was filed by K S Puttaswamy before the Honorable Court questioning the Constitutional validity of Aadhar Act on the ground of violation of privacy. Consequently 9 judges of bench looked upon the new matter i.e. whether the Right to privacy is a fundamental right or not while keeping aside the validity of Aadhar Act which is later heard by bench of 5

[17] 1981 AIR 760, 1981 SCR (2) 311.
[18] 1995 AIR 264, 1994 SCC (6) 632.
[19] "Chapter 4- Legal Framework on Right to Privacy in India", Shodhganga, *available at:* https://shodhganga.inflibnet.ac.in/jspui/bitstream/10603/127846/19/10_chapter%204.pdf. (Last visited on Oct. 23, 2019).
[20] 1997 3 SCC 433.

judges. Thus, in Puttaswamy case, it has been decided by the Supreme judicial authority that Right to Privacy is a fundamental right guaranteed under Part III of the Constitution i.e. intrinsic in Article 21 itself and therein overruled the earlier judgment of Kharak Singh and MP Sharma cases.

Thus, from the above discussion of all the cases, it has been concluded that Right to Privacy is now declared as a Fundamental Right of individuals under the Constitution of India.

3. Issues Relating To Privacy

After the passing of the Aadhaar judgment in respect of privacy, many issues came into consideration viz Constitutional validity of Aadhaar Act, Section 377 of IPC, live in relationship without marriage, etc. which can be briefly analyzed as below-

Aadhaar Scheme

Aadhaar scheme is a welfare scheme launched by the Government in 2009 to give direct benefits to the Indian Citizens. It is a unique identity which is to be used as a proof of identity and also to avail Government welfare services such as LPG distribution, Jan Dhan Yojana etc. Under the Scheme, Unique identification Authority of India (UIDAI) issued a 12 digit number to all individual across India by obtaining demographic information (name, address, sex, etc.) and biometric information (iris scan, finger print etc.).[21]

This scheme was challenged on number of grounds-

First, it was regulated by an executive order and not by Act of Parliament;

Second, data were to be collected by private agencies and there is no provision for data security; and

Third, in case if anybody mis-utilizes the data or is not utilizing it for the purpose for which it has been collected, then there is no provision for prosecution.

Thus, to cover all these aspects, in 2016 a money Bill called as Aadhaar Bill[22] was passed in the Lok Sabha and afterwards becomes an Act. The main aim of the Act is to give legislative support to Aadhaar scheme. After its enactment, a number of notifications were issued for mandatory linking of Aadhaar with PAN, phone number, bank account and other services.

In pursuance of Aadhaar, many petitions were filled challenging its Constitutional validity based on the infringement of privacy before the Supreme Court and it was heard by 5 judges

[21] "Use of Aadhar", Unique Identification Authority of India, Government of India, *available at:* https://uidai.gov.in/contact-support/have-any-question/288-faqs/your-aadhar/use-of-aadhar.html. (Last visited on Oct. 23, 2019).

[22] Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Service) Bill.

of bench viz CJI Dipak Mishra, Justice A.K. Sikri, A.M Khanwilkar, Ashok Bhushan and Justice D.Y Chandrachund. And recently by a majority of 4:1 it has been decided that Aadhaar Act is Constitutionally valid. However, it struck down certain provision like Sec. 57, Sec. 47, Sec. 33(2) i.e Private entities can no longer ask for Aadhaar number and individual can now file complaint against entities and Government for violation of their rights. Among the five Judges, one judge J Chandrachud gave a dissenting opinion that the Act is unconstitutional because it breaches part III of the Constitution. He said that by passing Aadhaar as a money Bill which undermined the Rajya Sabha, made it against the Constitutional scheme and thus it was a fraud on the Constitution.[23]

Section 377 of Indian Penal Code (IPC)

Under IPC, Section 377[24] reflects unnatural sex and the issue relating to Section 377 was first raised before the Delhi High Court by Naz foundation but it was dismissed.[25] However, after 8 years, in 2009 in the Naz Foundation case[26], the HC of Delhi decriminalized homosexuality between consenting adults. But again, in the year 2013, in the case *Suresh Kumar Koushal v Naz Foundation*,[27] it repealed High Court of Delhi's judgment.[28]

Later, on filling many petitions, on July 10 five judges bench headed by CJI Dipak Mishra heard the case again and on Sept. 6, 2018 the bench decriminalized homosexuality by partially striking down the colonial era provisions of Section 377 of IPC.[29] The argument placed by the higher judicial authority is that sexual relations is constituted as privacy right of individuals which is protected under Article 21 i.e. Right to Life and Personal Liberty of the Constitution. However, the State can impose reasonable restriction on the ground of compelling public interest.

---

[23] Soni Mishra, "Justice Chandrachud: The lone dissenting voice in Aadhaar Judgement*", available at:* http://www.theweek.in/..../justice-chandrachud-lone-dissenting-voice-aadhaar-judgement (Visited on Oct. 22, 2019).

[24] Section 377 refers to unnatural sex and says whoever voluntarily has carnal intercourse against the order of nature with any man, women, or animal shall be punished with imprisonment for life, or with fine which may extend to 10 years" Indian Penal Code, 1860 (Act XLV of 1860).

[25] 160 Delhi Law Times 277 (2009).

[26] *Naz Foundation* v. *Union of India*, 160 Delhi Law Times 277.

[27] Civil appeal No. 10972 of 2013.

[28] "Supreme Court decriminalized Section 377: All you need to know", *The Times of India*, Sept 6, 2018, *available at:*http://www.m.timesofindia.com/india/sc-verdict-on-section-377-all-you-need-to-know/amp_articleshow/65695884.cms (Last visited on Oct. 23, 2019).

[29] Krishnadas Rajagopal, "Section 377 will not apply to consensual same-sex acts, say Supreme court", *The Hindu*, Sept 6, 2018, *available at:* http://www.thehindu.com>News>national/section-377-will-not-apply-to-consentual-same-sex-say-supreme-court/article24878751.ece/amp/ (Last visited on Oct. 23, 2019).

4. Indian Legal Framework on Right to Privacy

As of now in India, we know that there is lack of definite legislation that could specifically deal with privacy and protection of data. However, in the absence of such legislation, there still exists a legal framework that though not directly but indirectly deals with privacy and data protection. Apart from the statutory protection, privacy is also being protected under the Constitution of India. So, basically there are two protections by way of which privacy rights as well as personal data can be protected.

1. Constitutional protection
2. Statutory protection

4.1 Constitutional protection

The Constitution does not expressly or explicitly grant privacy as Fundamental Right. It is nowhere pointed out in the Constitution. However, it is intrinsic in Right to Life and Personal Liberty under Article 21[30] of the Constitution and other freedom guaranteed under Part III of the Constitution. Although it has been granted as Fundamental Right in the Puttuswamy case[31] by a nine Judges bench but the right cannot be enjoyed in total. Rational limitation can be forced under Article 19(2) i.e Public Interest, Sovereignty, and Integrity of Nation etc.

Apart from this, Privacy has been made an inalienable right which we possess since our birth. Its relevance can be gauged from the fact that even if the Supreme Court, by its majority decisions held that Right to Privacy is not a Fundamental Right, minority opinions of many judges from the beginning was that Right to Privacy is a Fundamental Right under Article 21 of the Constitution. Thus, we can say that the core of the Constitution is Article 21 because it incorporates within it many rights which are essential to give constitutional recognition to newly emerging rights with the changing need of the society.

4.2 Statutory protection

In India, the pieces of legislations that deal with data protection in the present context are IT Act, 2000, Indian Contract Act, 1872, Intellectual Property Laws, Credit Information Companies Regulation Act, 2015 etc. which are discussed below in brief:

a. IT Act, 2000

In India, IT Act, 2000 is the first ever IT legislation whose aim is to deal with e-commerce, e-governance and cybercrimes. Besides, it is the legislation dealing with data protection. The purpose of IT Act is to provide protection against infraction of information due to leak of

[30] No person shall be deprived of his life or personal liberty except according to procedure established by law.
[31] Writ Petition (CIVIL) NO 494 OF 2012.

information from computer. It contains various provisions viz. Sec. 65 and Sec. 66 which prevent other from illegally using technology like computer, laptop and information kept their in.[32]

i. Sec. 43 of the said IT Act contains punishment for any destruction of data kept in computer. Under this Section if any person uses computer data in an unauthorized manner or illegally then he will be liable for penalty of 3 years imprisonment or 5 lakhs rupees as fine or with both.

ii. Section 65 provides protection against those who by knowingly or intentionally made alteration, destruction, concealment of any computer source code.

iii. Section 66 whoever make any alteration, damage to information stored in a computer will be held liable for such wrongdoing. Penalties have been provided under these Sections are 3 years imprisonment or fine of Rupees 2 lakhs or with both.

iv. Besides, if any company violates the provision of IT Act, then the managers of the company and directors are in person accountable for the offence.[33]

Later, the 2008 Act[34] has been passed to handle with the matters that the original Act failed to cover and to assist further development of IT and related security concerns. The new Amendment Act gives power to the Indian government under Section 69(A) to prevent intercept, monitor, and decrypt computer system, resources in computer devices and also to block electronic data stored therein. But this came under major controversy and later in the year 2015 it has been declared by the Supreme Court that Section 69(A) under which the government can issue direction to block internet site is Constitutionally valid as there prevails adequate procedural safeguard.[35]

b. Indian Penal Code, 1860

There is lack of direct provision in criminal law for violation of data privacy. However, there are certain crimes from which an inference can be made that there exists penalty for violation of privacy say e.g, Under Article 408 of IPC liability arises out of dishonest misappropriation of movable property.[36]

[32] *Supra* note 13.
[33] *Ibid*.
[34] Information Technology (Amendment) Act, 2008 (Act 10 of 2009).
[35] "Section 69A IT Act to block website constitutionally valid says SC", *Firstpost,* Mar 24, 2015, *available at:*http://www.firtstpost.com/politics>/section-69a-act-block-websites-constitutionally-valid-says-sc-2171293.html/amp (Last visited on Oct. 23, 2019).
[36] *Supra* note 13.

c. Intellectual Property Law

In India, Copyright Act, 1957 deals with matters of copyrighted piracy (theft) and for such piracy impose compulsory punishment which is in proportion to the seriousness of offence. Section 65 of the Act provides that whoever makes use of a computer or an infringing copy of computer program shall be punishable with imprisonment which may extent to 3 years or with fine. Moreover, wherein an author produces a books, records or broadcast program by collecting information from different source by devoting time, money, labor and skill amounting to literally work within the meaning of Copyright Act are protected as being copyright of that person. Thus, the outsourcing parent entity may have recourse under the Copyright Act for any violation occurring to that data bases.[37]

d. CICRA[38]

In India any information relating to credit of individuals is to be collected as per the privacy norms that are mentioned in CICRA regulation. Where there any modification or divulgence of collected information are made by the entities then in such cases, they will be responsible for it as per this regulation Those entities that collected and maintained data are held liable for any possible leak or alteration of their data. In India, to protect the information with respect to credit and tenancy of the companies as well as individuals, a strict structure has been framed by CICRA. This Act also provides stringent principles for information privacy that have been appraised by the RBI.

e. Indian Contract Act, 1872

Among the Indian laws, it is the Indian Contract Act, 1872 which governs contractual terms and agreements of the parties generated by them. Accordingly, if a contract is entered by the parties including in it a confidential or privacy clause i.e. to say disclosure of personal information of individuals only with the permission and consent of those individuals and that too for a purpose or in a manner concurred among the parties. Thus, an individual who disclosed information in an unauthorized manner and by non-complying with the expression stated in the accord be equal to contravention of contract which further results in action for damages. Besides, in an insurance contract an insurance proposal is provided by the insurer where it contains a confidential law pertaining to personal information of the insurer customers. Any disclosure of such information without the prior consent will invite an action for damages on the ground of breach of contractual obligation agreed by them.[39]

---

[37] *Ibid.*
[38] Credit Information Companies Regulation Act, 2005 (Act 30 of 2005).
[39] *Ibid*.

D. Recent Efforts in India towards Data Protection

Due to increase in the instance of data theft and breach of data privacy, the government and the industries were forced to make some sort of efforts for protection of data despite having legalized framework. A few of such efforts are: -

a. Proposed Amendment of IT Act

The Ministry of Communication and Information Technology suggested certain amendments of IT Act, 2000 as regard to protection of information. These suggestions led to the IT (Amendment) Act, 2008 which further incorporated important provisions related to Data Protection i.e Section 43 A and Section 72A. The nature of these provisions is punitive i.e. both criminal and civil. But under the IT Act, this suggested amendment has yet to be enacted into a new set of Rules[40] and as a result a new rules were established named Privacy Rule [41]

Later the Ministry of Communication and Information Technology proclaimed this Rules under Section 87 (I) (06) read with Section 43A, which basically talks about reasonable security practices and procedures that is very essentially required to adopt while handling with sensitive personal data. Non-compliance of these Rules will attract an action under the provision of Section 43A of the said Act which will impose liability to pay compensation. However, its limits have not been fixed.

Provisions relating to sensitive personal data or information (SPD) are contained only under these Rules. SPD incorporates within its data concerning credit/debit card information, password, biometric information (like fingerprint, Deoxyribonucleic acid etc.) as well as physical, mental and physiological health issues etc. Further these Rules elucidate that any information contained in public domain and if it is accessible and available without any cost to general public then such data is not to be stated as SDP.[42]

Further, these Rules explicitly mentioned that the body corporate or any other person on behalf of such body corporate is required to follow rational security procedures or practices in the processing, collecting, sharing of any personal sensitive data or information. If any harm is caused by the reason of violation of information, the corporate body may be made responsible to pay compensation to that person who suffered loss.[43]

---

[40] Latha.R.Nair, "Data Protection Efforts in India. Blind leading the blind*",* 4 *IJLT1* 23-27 (2018).

[41] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rule 2011.

[42] S.S.Rana and Co. Advocates, "India: Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011", *Mondaq,* Sept 5, 2017, *available at:*www.mondaq.com/India/....data.../information+Technology+Reasonable+Security+Pr (Last visited on Oct. 24, 2019).

[43] *Supra* note 9.

In India, these Rules provided a new approach towards data protection laws. There are three groups among which the provisions of these Rules are divided. They are-

i. Body corporate
ii. Information provider
iii. The Government.[44]

Following are the key features of the Rules-

Rule 4 states that the body corporate is under obligation to lay down a privacy policy in their website that would be accessible by the entire provider who shares their information i.e. personal as well as sensitive information. Besides, the policy must contain all the essential details as to what type of data collected, purpose of collection etc.[45]

Rules 5 contain provisions governing collection of information by the body corporate. some of which are explained – first the body corporate shall not collect any sensitive personal information until and unless the provider has given its consent on this behalf and informed him the purpose of its collection. Second, such collection of both personal and sensitive personal data should be for a lawful purpose. Third, that information collected from the provider must only be used for the specified mentioned purpose and shall hold it for a period not longer than it is required. Fourth, the body corporate shall secure the collected information and appoint a grievance redressal body for any disparity arising in between the body corporate and the provider.[46]

Rule 6 states that prior to the disclosure of sensitive information to any third parties, the body corporate is under obligation to obtain consent from the information provider. However, the body corporate can share the information revealed by the provider to the government agencies without its prior consent if there exist a law which gives an order or authorizes to any other third parties or the government agencies to acquire such information from the provider. [47]

As per Rule 8 the body corporate shall adopt and implement reasonable security practices for the purposes of securing data of individuals. This Rule specifically names one of the security practice as ISO security standard but there is no hard and fast rule that one must adopt only this standard. Another code of practices other than the above-mentioned one can be implemented provided that the government must give its approval on the same. In addition to this, there must

[44] Vaibhabi Pandey, "Data protection laws in India The road ahead", *SINGHS AND ASSOCIATE*, pdf (2015).
[45] *Ibid*.
[46] *Ibid*.
[47] *Ibid*.

an independent auditor who is authorized by the government to audit the code on an annual basis.[48]

b. Data Security Council of India

NASSCOM[49] has established a self-regulatory body via- Data Security Council of India so that the industry on its own can develop appropriate data privacy and securities standards as they have more knowledge and experience of the practical commercial issues than that of the government. Besides, it is a non-profit organization having adequate representation of the independent directors and industry specialists. Various organizations like IT enabled services (ITeS) companies, Academic or Research institutions and universities who emerged with data security and privacy protection can also become a member of the DSCI.

The main aims of the DSCI are to promote IT and ITeS companies to develop, monitor and implement high security and data protection standard so that an awareness could be created among the stakeholders and the industrialists about the prevailing issues of privacy and data security. One another objective of the Council is to generate a platform common to all in order to share knowledge about security of information. [50]

c. National Do Not Call services

In the recent past of India, along with the privacy of personal information, personal privacy of telephone number became an issue among the individuals and industries due to variety of telecommunication service provider and easy availability of mobile phones. As a result of it many unsolicited telephone calls came to the persons from the business promoters or individual who do not want to receive such calls. Thus, in order to curb this problem Telecom Regulatory Authority of India (TRAI) establishes a National Do not Call registers wherein the telemarketers cannot call a subscriber whose number is registered.

d. Personal Data Protection Bill, 2019

Another recent effort towards data protection is the introduction of a Bill[51] on December 11, 2019 in the Lok Sabha by Mr. Ravi Shankar, Minister of Electronics and Information Technology, the main objects of the Bill were to draft a data protection regime to recognize current issues and possible statutory protection.[52] And this is not the only Bill introduced, prior

[48] *Ibid*.
[49] The National Association of Software and Services Companies, *available at:* https://www.britanica.com/topic/National-Association-of-softwae-and-service-companies (Last visited on Oct. 25, 2019).
[50] *Supra* note 40.
[51] Personal Data Protection Bill 2019.
[52] The Personal Data Protection Bill, 2019' *available at*: http://www.prsindia.org>billtrack (Last visited on Oct. 23, 2019)

to this in the year of 2017 and 2018 also Bills pertaining to data protection were introduced in the Parliament.

One of the important features of the Bill is that it entrusts obligation on the data intermediary to execute security measures so as to ensure that the collected data are secured. He/she is under obligation to inform individual within the fixed time about any breach of data. Besides data protection officer are created under the Act to redress grievance, DPPA[53] is also formed with a motive to appeal. This authority has the power to take action discretionary against data collector or processor. The Bill also authorized the DPPA to punish, monitor, and order damages for any kind of harm caused to individuals from any acts of the Government or private institution"[54]

Under the provision of the Bill, the individual can file complaint against private entity and the Government for violation of privacy. Moreover, another feature of the Bill is that- to process any kind of information whether sensitive or personal, one must require to obtain affirmative consent from the individual whose information, the entity or the Government is seeking for. The Bill made all offences within its ambit punishable and also increased the monetary and imprisonment penalties for all existing breaches. Apart from this, there is certain provisions like-Sec. 10, Sec. 14 and Sec. 36 which clearly depict the importance of the Bill. But the problem is that the Bill is yet to be enacted. However, we can say that this Bill is a significant step towards data protection and can also be called as effective and excellent legislation to protect data if it would become an Act in future.

6. Need of Specific Privacy Laws

Despite of existing legal framework and efforts made by government, the existing legislations are not efficient to provide with safeguards to personal privacy rights and protect data. Moreover, there are number of loopholes which can be seen in the existing laws like IT Act, Rules of 2011 etc. Some reasons demanding special laws can be briefly enlisted as follows-

Loopholes in existing legal framework

a. These proposed amendments in the IT Act i.e insertion of Section 48A and Section 72A could not make any new alterations into the original IT Act because whatever comments are given by the Standing committee to the Ministry of Parliamentary affairs, they are just received by them further no application is made.

[53] Data Privacy and Protection Authority.
[54] *Ibid*.

b. Besides, the proposed amendment, it does not deal with matter of data protection such as handling of sensitive personal data, what safeguards should one adopted in the process of collecting data, processing of personal information etc...

c. The Rules that were promulgated by the MCIT[55] named as "2011 Rule, under Section 87(2) (06) read with Section 43A basically deals with sensitive data and information. They are applicable only to body corporate or person located within India.

d. They do not take into account State authority within its scope. Besides not complying with the rules invoke Section 43A which will further provide for both liability and compensation to be paid. However, to what extent or limit, it is not fixed yet.

e. In terms of Rule 4 of 2011 Rules, the Private sector service provider (i.e a body corporates) like the Vodafone India limited, Bharti Airtel Limited are required to issue its privacy policy on its websites. However, few State-owned sectors are alleged to have not published their privacy policy on their websites. Thus, there is no availability of any statement pertaining to privacy policy on their website which indicates weak approach of service provider towards data protection and thus question arises as to enforcement of the principles.[56]

f. Since 2011 Rule deals with the sensitive data or information (SPDI) which includes password, medical records, biometric information etc. Therefore, there exists less regulation on non-sensitive information in India. Apart from this, Indian laws grant limited extra - territorial jurisdiction and also their applicability remains uncertain in certain situations. For Example- It is questionable whether the IT Act or the privacy Rules would apply to a US company that collects Indian citizens SPDI when such person is travelling to US.[57]

Besides, some other limitations that make the Indian legal framework weak in protecting data are as follows-

a. "No comprehensive law on private right.

b. No proper classification as to private, public and sensitive information.

c. Lacking of proper procedures for creating processing and transmitting and flowing of information.

d. No proper guidelines that can define the term Data Quality, proportional and Data Transparency.

[55] Ministry of Communication and Information Technology.
[56] *Ibid*.
[57] Atul Singh, "Data Protection: India in the information Age," 59 *JILI* 78-84 (2017).

e. Lacking of legal framework to deal with the issue of cross-country flow of information.[58]

Thus, from the above lacunas or loopholes in the existing legal framework as mentioned above, it can be said that there arises a need of specific law on Privacy and Data protection immediately. Further it also becomes essential to have a comprehensive Data protection law due to vast increase in customer service amongst corporate entities which acquire various personal information of their customer. However, such increase in various information technologies, web services, internet in the global space, and increase in BPO (Business process outsourcing) operators, it become paramount to have stringent law on data protection that could deal with both the flow of data across national borders as well as to provide adequate safeguards for protecting the flows of data.

7. Conclusion and Suggestions

Thus, in India Right to Privacy has evolved as a Fundamental Right due to several interpretations made by the Judiciary. But if we notice our present scenario then we will find a vast technological development due to globalization. And with this development of technology, the question that comes to our mind is that whether we have privacy in our life or not? This right constitutes a very important element to lead a dignified life, to make a decision of own and to develop ourselves and thus such right becomes very important.

As we can see in today's world technology is becoming a part of our life, it benefitted us to a large extent but at the same time it became a threat because with the development of technology many problems like cybercrimes, data theft, misuse of data, etc. came in front of us, which has a direct link to our privacy. As we know, that at present we have to share our personal information or data to a party whether it may be a Government or private entity in order to avail any kind of services, while sharing such information nay increase the risk of data theft or misuse of data because in India there is a lack of adequate Data Protection Laws even though it has certain legislations which though not directly but in an indirect way is dealing with Data Protection. Some of which are IT Act, Criminal Law, Intellectual property law etc. When such information is leaked or misused by third party illegally then it can be treated as 'Breach of Privacy'. Moreover, many loopholes could be seen in the existing legislations like for internet the provider of service, data intercessors are not answerable for any infraction of data

[58] Shrikant Ardhapurkar, "Privacy and Data Protection in Cyberspace in Indian Environment", *available at:* https://www.researchgate.net/publication/50273874/Privacy-and-Data-Protection-in-Cyberspace-and-Inda-Environment (Last visited on Oct. 25, 2019).

processing if they proved that such data was processed without their knowledge, so in order to give protection to data privacy we need a stringent Data protection Law.

As we know that the Supreme Court upheld privacy as Fundamental Right intrinsic in Art 21 of the Constitution. But only by holding this view is not sufficient because one should be aware of their right, he should know the alternative that if such rights are transgressed then one can move to the Higher Authority for redressal. If they were not known they may be left out unredressed. Thus, people can develop or lead a dignified life only when they are well known of their rights. Earlier only personal privacy was taken into consideration but with the passage of time, data privacy must also be taken into account. Thus, the Government should adopt such efficient mechanism which can alert them to take action as quickly as possible. Besides this, legislatures should enact certain rules, regulation or laws which can give assurance that the collected data are secured. The database where the information is stored should be circumscribed with tight security that even for the experts it becomes impossible to access it, whereby it can be accessible only by those who have the authority to access and that too for the welfare of the people. Further only those authorities that collect process and stores data should be made more responsible. Besides, in any law there must contain provision of penalty i.e monetary and imprisonment that too so high that the unauthorized one thinks twice before mishandling data of individuals.

As an alternative to the collection of biometric information, few experts have suggested shifting to smart cards which would be an optional one. Smart cards which require pins will demand citizen's conscious co-operation during the identification process because biometric permitted to recognize individuals even if they don't agree to get identified. Once smart cards are disposed, nobody can use them to identify any individual. Adopting smart cards would completely eliminate or at least reduce the peril of criminals and terrorists, foreign government utilizing the database of biometrics to identify Indians.

References

Apar Gupta, "Balancing online privacy in India", 6 *IJLT*, (2010).

Asok Kini, "Aadhaar the summary of majority (4:1) judgement", pdf.

Credit Information Companies Regulation act, 2005

Dr Payal Jain &Ms Kanika Arora, "Invasion of Aadhaar on right to privacy: huge concern of issues and challenges", 45 (2) *ILR* (2018).

Indian Penal Code, 1980

Intellectual Property Law

Kalyani Menon Sen, "Aadhaar: wrong no, or big brother calling", 11(2) *socio-legal rev.* 85 (2015).

Latha. R. Nair, "Data Protection Efforts in India. Blind leading the blind". 4*IJLT1*,23-27.(2018).

Rukhmini Bobde, "Data protection and the Indian BPO industry, 2 *law Rev. GLC,*79-88(2002-03) nlu.5

Shiv Shankar singh, "Privacy and data protection in India: a critical assessment", 53 *JILI,* 683(2011).

Shraddha, "What impact the recent right to privacy judgement will have on existing law", April 24, 2018.

Subhajit Basu, "Policy- making, technology, and privacy in India" 6 *IJLT* (2010).

The Constitution of India, 1950

The Indian Contract Act, 1872

The Indian Copyright Act,1957

The Indian Evidence Act, Act, 1872

The Information Technology (Amendment) Act, 2008

The Information Technology (Reasonable Security Practices and procedures and sensitive personal data or information), Rules, 2011

The Information Technology Act, 2000

Vivek Baid and Shyam Panday, "Privacy on the internet-protected by legislation" *1lawRev. GLC* 14, 21-23(2001-02)