Lex Lexicon
A Reservoir of Socio-legal Discourse

Lex Lexicon Journal

LEGISLATIVE FRAMEWORK OF DATA PROTECTION: A HALT TO THE MISMANAGEMENT OF PERSONAL DATA IN INDIA

By- Ashwin Singh

ABSTRACT

There are innumerable issues faced by the citizens of India due to the unrestricted availability of personal data on the internet. There are no stringent laws or data protection schemes which are implemented to curb this menace. There has been a significant rise in the cybercrimes committed across the world. According to a report of the BBC, the cybercrime sector is the fastest-growing crimes in the world as depicted by a whopping increase of 40% in the organized crimes like credit card and online banking thefts. This has evolved as a 100 billion dollars industry where the minor and major hackers are stocking their claims and are profiting. The physical barriers act as no restrictions in the commission of cybercrimes which may occur at any place in such vast continents. This research paper focuses on the legal framework, which is required for data protection and the different loopholes in the existing framework.

RAPID TRANSFORMATION OF TECHNOLOGY DURING DIGITAL REVOLUTION AND THE SIGNIFICANCE OF DATA PROTECTION

"The digital revolution is more significant than the invention of writing or even printing."[1]

-Douglas Engelbart

[1]Vic Costello, *Multimedia Foundations: Core Concepts for Digital Design* (1st edn. Focal Press 2012)

The 21st century has been a witness to a rise in the wide number of usages of information on the world wide web, which lead to its reference as the 'information age'.[2] The revolution that India has gone through has been away from the spotlight of the international media, unlike the technological advancements in China. The speed and the number by which the standards of the technology in sub-continent have has been astonishing. The existence of large-scale global market players in the economy has resulted in the escalation of the growth rate in the economy to 7-8% with almost 450 million users of the world wide web.[3] Not only has there been a rise in the usage of internet users but there has also been an increase in the usage of the technology by the governmental departments for the purpose of identification of citizens of the country. This brings us to the Aadhaar Card initiative of the government introduced in 2009 by the National Biometric Digital Identity Programme.[4] Apart from this according to the latest report at least 80% of the citizens have a digital bank account on their name because of the *Jan Dhan* Scheme introduced by the Union government in 2014 when Narendra Modi was sworn in as the Prime Minister.[5]Under this initiative, the Unified Payments Interface (UPI) has registered a major chunk of the accounts in 2016 which also lead to the observation that there have been 1.2 billion transactions which have

[2]National Research Council, Computer Science and Telecommunications Board, Committee on Innovations in Computing and Communications: Lessons from History, *Funding a Revolution: Government Support for Computing Research* (National Academies Press 1999)

[3] JatinVerma, *'Data Protection in India'*, (accessed on 10th May 2020) https://www.jatinverma.org/data-protection-in-india

[4] SushilKambampati, '*Aadhaar: the Indian biometric ID system has potential but presents many concerns*' HEINRICH BOLL STIFTUNG, (accessed on 10 May 2020) https://www.boell.de/en/2018/02/07/aadhaar-indian-biometric-id-system-has-potential-presents-many-concerns

[5] Neha Abraham, '*Over 80% Indians now have bank accounts. How many are actually using them*?' THE SCROLL, (accessed on 10 May 2020) https://scroll.in/article/923798/over-80-now-indians-have-bank-accounts-how-many-are-actually-using-them

taken place in the month of November alone.[6] Another prominent use of the digital framework of India has been in the introduction of the Goods and Services

Tax (GST) Network in 2017 which aimed at bringing together all the Small and Medium Enterprises by removing a huge and confusing number of taxes over their head and the initiation of a composite tax system of GST which covers all taxes under one head.[7] The transition of the world towards a digital era has seen a wide range of personal data being fed to various digital platforms for numerous reasons. Almost every single activity which is associated with the digital environment in the present day, some sort of personal data transaction is bound to be involved. There have been establishments of wholly new markets which specifically deal with the extraction, collection and storage of all the personal information of its users for numerous purposes which is considered as the most significant constituent of a business module. It would be a shocking fact to know that the world's largest taxi company Uber, owns no taxis, the world's largest retail business Alibaba, owns no inventory, one of the largest media platforms Facebook, owns no content of itself whereas the world's largest stay provider Airbnb, owns no property or real estate.[8] It is derived that these largest companies in many parts of the world are purely data-driven platforms on which their whole foundation rests. While on the one hand, all such usage of personal data on the world wide web may be significantly useful but it is more vulnerable and prone

[6] Shreya Nandi, '*UPI clocks 1.2 billion transactions in November'*, LIVEMINT, (accessed on 11 May 2020) https://www.livemint.com/news/india/upi-clocks-1-2-billion-transactions-in-november-11575289390322.html
[7]Vinika D. Rao, '*India's Quite Digital Revolution'* INSEAD KNOWLEDGE https://knowledge.insead.edu/blog/insead-blog/indias-quiet-digital-revolution-12956
[8]Tom Goodwin, '*The Battle Is For The Customer Interface'*, TECH CRUNCH, (accessed on 11 May 2020) https://techcrunch.com/2015/03/03/in-the-age-of-disintermediation-the-battle-is-all-for-the-customer-interface/

to misuse which raises questions on the privacy and autonomy of the personal data.

The analysis of this kind of personal data, has paved the way for the evolution of a specialized science called the 'Big Data' analytics which specifically deals with huge and intricate data. This data analysis may provide significant insight into the social issues in the spheres of food security, health care, urban development and transportation. To support this digital revolution but at the same time to limit the exploitation of personal data in the websites, the government has launched the 'Digital India Programme' which is a set of schemes for the betterment of the netizens.[9] There has been a seamless and limitless disclosure of personal information in public and the private sectors. Even though this data is collected for beneficial purposes, there is a high probability that the data may be wrongly handled due to which it should be subjected to strict surveillance and data profiling. The erosion of any kind of personal data may be a threat to the public and a compromise on national security.

ESSENTIALITY OF A COMPREHENSIVE CYBER LAW

There are innumerable issues faced by the citizens due to the unrestricted availability of personal data on the internet. There are no stringent laws or data protection schemes which are implemented to curb this menace. There has been a significant rise in the cybercrimes committed across the world. According to a report of the BBC, the cybercrime sector is the fastest-growing crimes in the world as depicted by a whopping increase of 40% in the organized crimes like

[9]Nirvaan Gupta, '*India: Data Protection in India'*, MONDAQ, (accessed on 11 May 2020) https://www.mondaq.com/india/privacy-protection/744160/data-protection-in-india

credit card and online banking thefts.[10] This has evolved as a 100 billion dollars industry where the minor and major hackers are stocking their claims and are profiting.[11]The physical barriers act as no restrictions in the commission of cybercrimes which may occur at any place in such vast continents. Currently, India is more vulnerable to cybercrimes due to two main reasons. Firstly, India is

the world's largest outsourced data processing which leads it to be a primary target for all the hackers across the world. Secondly, there are no stringent and comprehensive laws. The Department of Information Technology(DIT) and the Data Security Council of India (DSCI) must act accordingly in regulating the mismanagement of personal data. The finest way through which this problem can be dealt with is by enacting effective legal provisions along with spreading awareness amongst the public and the employees. There is a dire need of rejuvenation of cyber laws to guarantee cybersecurity to the Indian public. Laws are dynamic in nature and should evolve with the change in time and the people. The situation of cybersecurity in India has been so depraved that even the PMO's cybersecurity system has been hacked as announced by the former National Security Advisor MK Narayanan.[12]Just by declaring the cat like a tiger, we cannot justify that the cyber laws in India are in their right place. It is important to note that strong and effective cyber forensics along with a well-secured cyber legislative framework is required to ensure that there are no cyber crimes or data breaches committed. Ranging from credit card details and financial status of a person to the medical history, the BPO and the IT sectors of the country have vital

[10] '*Explosion in Global Cyber Crime*', FAST CASE, (accessed on 12 May 2020) https://www.fastcase.com/blog/explosion-in-global-cyber-crime/
[11] *Id*
[12] Express News Service's Team, '*Chinese hacked PMO computers, says Narayanan'*, THE INDIAN EXPRESS, (accessed on 12 May 2020) http://archive.indianexpress.com/news/chinese-hacked-pmo-computers-says-narayanan/569075/

and personal information which is of utmost confidential nature. This data is stored in the form of an electronic database which may be easily subjected to a data breach. This data may also be accessed by the employees of such companies who may extract personal information and the breach the right to privacy granted to a citizen. There have been a lot of cases in the recent past where high profile companies in India have defaulted in protecting the personal database according

to the data privacy norms. One such incident dates back to December 2018, where India's largest banking company, SBI had left one of its databases unprotected by password leading to the personal information to 420 million people to be exposed.[13] This server is located in the Mumbai city, has exposed the bank account numbers, it's details and phone numbers of various account holders. Such recent incidents, even in the BPO sector, have questioned the data protection system designed by the government.

The dynamic, technical and all-inclusive nature of the digital revolution in India has made it important for the legislation which deals with data protection to be of equally stringent and comprehensive nature to help reduce the mismanagement of individual personal data. There have three major steps which are taken towards the rejuvenation of the data protection laws in India, which are a combined effort of not only the judicial system but also the government.

(i) A judgement which reincarnated the right to privacy

[13]Prabhjote Gill, '*Biggest data leaks of 2019 that hit Indians'*, BUSINESS INSIDER, (accessed on 12 May 2020) https://www.businessinsider.in/tech/news/biggest-data-breaches-of-2019-to-affect-india/articleshow/72465865.cms

The Supreme Court, in the case of ***K.S. Puttaswamy (Retd.) v. Union of India &Ors.***[14]which constituted a nine-judge bench gave an integral decision declaring the right to privacy as an inherent part of Article 21 of the Indian Constitution. It is declared as an integral component of Part III of the Constitution which constitutes the fundamental rights and the freedoms. It is also held in the judgement that the nature of the Constitution must be dynamic, and it should evolve in order to protect the democratic order which is governed by the rule of law. The Constitution has been interpreted in a different way in many aspects by the courts through its different judgements and law commission reports. It is

noted that the Constitution may not be implemented in the same manner as it was adopted. There has been a constant evolution in the manner in which right to privacy has been interpreted by the court of law, as during its enactment it was a basic right and later it was interpreted as a positive or a negative right.[15] The facet of informational policy of the right to privacy is recognized by the court in this judgement. This right to privacy is not absolute in nature and has some reasonable restrictions which are attached to it. This right can be enforceable against the state and the non-state players. The court also has to avoid any misuse or wrongful interpretation of the right has initiated a test for the same. There are certain conditions which need to be proved for the restriction to be considered valid or invalid. The action must be directed by the law, it must be of some legitimate necessity to the state, the need and the extent to which the state must intervene into the privacy of an individual must be proportionate to each other, and there

[14] K.S. Puttaswamy (Retd.) v. Union of India &Ors., 2017 (10) SCALE 1
[15]Vrinda Bhandari, AmbaKak, SmritiParsheera and Faiza Rahman, '*An analysis of Puttaswamy: the Supreme Court's privacy verdict*', THE LEAP BLOG, (^accessed on 13 May 2020) https://blog.theleapjournal.org/2017/09/an-analysis-of-puttaswamy-supreme.html

must be some limitations in the procedure to restrict the State from misusing its power.

(ii) Responsibility of the State to preserve national security

India is a democratic country with a vast cultural, religious and linguistic diversity which poses a lot of loopholes and problems to the State in many aspects of the economy. Adding to this India's geopolitical factor that is the geographical territory of where it is located, it has raised India's bar to the third rank in the list of countries which are highly prone to cybercrimes.[16] It is the duty of the State to initiate real-time data protection surveillance system to eradicate the internal and external cyber threats and discrepancies. To conduct proper and effective surveillance of the data, the State must be provided with access to all the databases on the IT and BPO centres or any other companies which extract personal information in a large proportion. But in today's advanced digital era, the data centres may be scattered all over the world due to which it has made the task of surveillance complex for the state.

The global advancements in the sphere of privacy jurisprudence and the constitutional developments in India have led India to draft constitutional legislation which guarantees the citizens the right to privacy. A step in that way is the drafting of the Personal Data Protection Bill, 2019 which not only amplified the power of the State in protecting the privacy of the citizens but also diluted the functioning of the companies in extracting the personal data of the citizens.[17] Even though the court in the Puttaswamy Judgement, had held that right to

[16] PTI, '*India ranks 3rd among nations facing most cyber threats: Symantec'*, ECONOMIC TIMES, (accessed on 13 May 2020) https://economictimes.indiatimes.com/tech/internet/india-ranks-3rd-among-nations-facing-most-cyber-threats-symantec/articleshow/63616106.cms?from=mdr
[17] *Govind v. State of Madhya Pradesh,* AIR 1975 SC 1378

privacy is a fundamental right under Article 21 of the Indian Constitution which guarantees right to personal life and liberty, there always existed an ambiguity in the constitutional nature of the right to privacy as a fundamental right.[18] This is because the court had given a totally contrary view in the Supreme Court judgement of ***Kharak Singh v. State of Uttar Pradesh***[19], where it held that the right to privacy is not guaranteed by the Indian Constitution. As a step to eradicate this ambiguity about the right to privacy as a fundamental right, the Personal Data Protection Bill was drafted by the legislature to restrict the power of the businesses from collecting the personal data. The requirements of the Bill must also be satisfied by all the government agencies which will comply with it in a

similar latitude.[20]There have been a significant number of privacy regulations which have been vested into the hands of the government, which greatly undermine the privacy interests. There are certain instances according to this Bill, which require the data to be divided into some additional categories which the BPO, IT and the social media companies will implement. These categories include sensitive information and various means of identification. There has been a dilution of powers of safeguarding the personal data as the government agencies are exempted from the provisions of the Bill. The observation of the functions of the government can be kept in a track by adhering to the procedure described under the Information Technology Act, 2000[21] and the Indian Telegraph Act, 1885.[22]It is left upon the hands of the government according to the provisions of the Bill, to enact the procedure, regulations, and the safeguarding mechanism to

[18] *supra note* 14
[19] Kharak Singh v. State of Uttar Pradesh , AIR 1963 SC 1295
[20] Personal Data Protection Bill 2019, sec. 35
[21] Information Technology Act 2000, sec. 69
[22] Indian Telegraph Act 1885, sec. 5

be implemented upon the agencies.[23]This bill that is enacted gives the government the power to form its rules for proper surveillance and the licence to the government authorities to maintain different safeguards for different agencies.

On the examination of the regulatory powers of the government, DPA and the online companies, they are bifurcated according to the Bill as the nature of each of them is different. The government has the authority to restrict all the social media platforms from the exploitation of the personal data by carrying on a substantial supervisory system which will implement various mechanisms of identity mechanisms.[24]Such companies o social media agencies will be required to register with the DPA as they are considered to be substantial data fiduciaries. But the Bill is flawed with respect to the identity verifications as it is clearly

against the principles of data privacy due to its nature of revealing the identity without keeping the data anonymous. The principle of anonymous identity many often is ignored or unseen due to the data verification on the internet. The DPA has been given a general instruction of rules and regulations which will help in the regulation of the mismanagement of personal data, protect the principles of data protection, ensure that the laws under the Act are fulfilled and promote the significance of data protection among the people of India.[25] The Bill has been drafted in such a way to give authority to the government to fulfil all the obligations for which the Bill has been in existence. The authority to manage cross border data transfer, restrict substantial data fiduciary and the power to develop mechanisms to rebuild data trust among the people are all the functions

[23] *supra note* 20
[24]Personal Data Protection Bill 2019, sec. 26(4), 28(3), 28(4)
[25] Personal Data Protection Bill 2019, sec. 49

of the DPA.[26]These extensive powers that have been adhered to the government and the DPA have led to giving of significant power to regulate online data mismanagement and the social media agencies which process the internet user's data according to their own needs. The preventive measures to contain data breach must be diligently taken by the government and the DPA as it would address all the harms and the mismanagement of the data that may be caused.

(iii) The United States and the European Union Model of Data Protection

The prowess of IT companies in India has always been on an escalating rate since the past decade. Out of the US$ 185-190 billion outsourcing companies in the world, India owns an enormous share of 55% in the Financial year of 2018.[27]All over the world, the countries have adopted contracting models of data protection framework, which is suitable for their individual data structure and outsourcing companies. A comprehensive data protection mechanism can be explicitly observed in the data protection model of the European Union. An individual's dignity and reputation may be protected in most of the cases which seek the protection of the right to privacy as a fundamental right. The right to protection of personal data as well as the right to privacy is protected by the European Charter of Fundamental Rights and are given utmost importance.[28]This advanced data protection mechanism which is formulated by the EU functions by the processing of personal data and the activities which are carried out by the Private companies which include social media and IT companies and also the

[26] Personal Data Protection Bill 2019, sec. 60(2)(b), 60(2)(c), 60(2)(f), 60(2)(j), 60(2)(k)
[27] *supra note* 9
[28] Chris Jay Hoofnagle, Bart van der Sloot, Frederik, ZuiderveenBorgesius, '*The European Union general data protection regulation: what it is and what it means'*, TAYLOR & FRANCIS ONLINE, (accessed on 13 May 2020) https://www.tandfonline.com/doi/full/10.1080/13600834.2019.1573501

Government entities. But along with all these restrictions, they have certain exceptions which include public order, national security, defence emergencies, etc. Apart from this framework, there was an enactment of the General Data Protection Regulation of the EU initiated from 25th May 2018 which has created certain conditions for the transfer of data from the EY to a non-EU country. There are two conditions out of which either of them needs to be satisfied. Firstly, it should pass the adequacy test, or it must satisfy all the contractual clauses that are in accordance with the guidelines for transferring sensitive data. This responsibility of transferring such enormous amounts of data is undertaken by the standard contractual clauses, but it has become a practically impossible task for India to monitor such huge numbers of economic activities and the enlarging environment of data protection which leads it to greatly differ from the EU's model of data protection. Even though the contractual clauses are effectively drafted, enforcement of such clauses in the absence of an effective regulatory framework is a mammoth task. Only if the adequacy test is positively fulfilled by

India proving that it has a strong data protection mechanism which is effectively implemented, the threat to cybersecurity can be suppressed. The European Commission has taken up the job of analysing the data protection framework which is followed in India, the rights of data protection under the legal statutes, the effective implementation of such laws, the adequate authority for data protection, the powers guaranteed to such an institution, the satisfaction of the significant international policy obligations and review of the prior mentioned criteria.[29] After undertaking all these steps, it declares whether a particular

[29]Malavika Raghavan, BeniChugh & Nishanth Kumar, '*Effective Enforcement of a Data Protection Regime*' (2019) DVARA RESEARCH WORKING PAPER SERIES, (accessed on 13 May 2020) https://www.dvara.com/research/wp-content/uploads/2019/12/Effective-Enforcement-of-a-Data-Protection-Regime.pdf

country is considered adequate or not. Even though India has not yet entered the list, many countries like Argentina, the United States, Israel, Canada and New Zealand have been termed as adequate with effective data protection system. India should take progressive steps towards framing a strategical data protection framework which is in accordance with the EU model of Data Protection.

According to the US model of Data Protection, the privacy of an individual is protected from the government, which is termed as liberty protection. There is no definite and comprehensive set of data protection laws in the US, as discussed in the EU. There are no elaborate laws which mitigate the cyber threats against the use, assembly and exposure of the data. The mechanism towards data protection is different for the public and the private sector as it varies according to its nature. The Electronic Communications Privacy Act and the Privacy Act are broad and enormous legislation which control the authority and the activities of the government to regulate personal information. The laws in accordance with the private sector are drafted in a sector-specific manner like the Federal Trade Commission Act (FTC).

DATA PROTECTION MECHANISM THROUGH THE LENS OF PREVALENT AND PROPOSED LEGAL FRAMEWORK

Privacy is such a term which is frequently confused with confidentiality and secrecy, but technically it refers to the usage and exposure of personal data which belongs to private individuals. An individual's personality can be established through his private information because of which the Indian Courts which also

includes the Apex Court have ruled that the right to privacy is an integral part of Article 21 of the Constitution which provides for the right to life and personal liberty, which is the backbone of the fundamental rights.[30] The right to privacy is now considered as a substantial part of the judicial system, which is of utmost importance and can only be compromised for compelling reasons like national security, defence and public order and morality. In the case of ***Govind v. State of MP***[31], the Apex Court has held that right to privacy is a fundamental right which is a part of the right to freedom of speech and expression and the right to life and personal liberty. The right to privacy is an umbrella term which includes the privacy of marriage, family, childhood and procreation. There are certain exceptions to these rights, which include the situations of national interest and emergency. This case was elaborated in a more structured manner and covered a different aspect in the case of ***R. Rajagopal v. Union of India***[32]**,** where the Apex

Court deciding that the right to privacy is a part of Article 21 of the Indian Constitution, has also expanded the scope of this right to a tortious liability apart from being a part of fundamental rights. Nobody can publish any matter about a person's family, procreation, child-bearing, marriage and other intricate personal matters until and unless:

(i) He or she has put themselves into such a situation or a controversy or has consented to such a publication.

[30]People's Union of Civil Liberties (PUCL) Vs. Union of India, (AIR 1997 SC 568)
[31] Govind v. State of MP, 1975 SCR (3) 946
[32] R. Rajagopal v. Union of India , 1994 SCC (6) 632

(ii) The matter published is extracted from a public records document which is open to be published which does not include cases of kidnapping, rape and abduction.

(iii) In cases where the person is a public servant, and it is necessary to publish certain personal information in the discharge of his or her official duty.[33]

(i) Safeguards under the Information Technology Act, 2000

There are certain situations during which the data in the computer systems experience threat due to the lack of proper safeguards. These safeguards are provided under the IT Act, 2000. The unauthorized usage of the computer system and the mismanagement of data stored in such systems is curbed due to the prevalence of adequate provisions in the aforementioned Act.

Any person who illegally and without any permission uses transfers or manipulated the data stared in the computer system is personally liable for such an act under the provisions guaranteed in the Act.[34]The quantum of liability or

punishment is adequately determined by the criteria of 'best efforts' and 'knowledge'. But the section has no mention of the liability of internet service providers, social media entities managing data or any outsourcing company which are involved in collection of data. Due to this reason, the section does not govern the Acts of outsourcing or internet service providers for the distribution and the processing of the data. Henceforth, according to this Section the, if there is any personal information provided by the data outsourcing company or the

[33] Kumar Sumit, '*A Case Study on R. Rajagopal alias R.R. Gopal and Another Vs. State of Tamil Nadu*', LEGAL SERVICES INDIA, (accessed on 14 May 2020), http://www.legalservicesindia.com/article/435/A-Case-Study-on-R.-Rajagopal-alias-R.R.-Gopal-and-Another-Vs.-State-of-Tamil-Nadu.html>
[34] Information technology Act 2000, sec. 79

service provider to a third party, it may not be held liable if they are successful in proving that they had no knowledge about the breach of data privacy and that such an offence was not committed under his purview.[35] It is also interesting to note that if there is any data breach on violation which is committed by a company, the employee who is responsible for such an act is made liable for the offence irrespective of the act which may be negligent or intentional.

The state of intention for committing a breach of data is not taken into consideration while a data breach is committed, and there are no criminal penalties that are imposed due to the committing of a breach. If a computer code is intentionally destroyed, modified or concealed, Section 65 of the Act offers protection. If any information on a computer system is deleted, altered or destroyed it is considered to be an offence under Section 66 of the Act. If any of the offences given above are committed, then a penalty of $440,000 may be imposed or imprisonment of up to three years may be imposed.[36]Irrespective of the damages which are assessed in that particular case, any breach of privacy with regards to personal information may lead to a maximum penalty of up to $222,000.

AMENDMENTS ADDED TO THE IT ACT, 2000 FOR STRINGENT CYBER SECURITY LAWS

Section 43 A was inserted in the IT Act by the Information Technology (Amendment) Act, 2008, which was passed by the legislature and came into force on 27th October 2009. The power conferred to the Central Government by Section 87 of the IT Act, 2000 have to be read with Section 43A of the Amended IT Act

[35]Devansh Saxena, '*Position and Perspective of Privacy Laws in India'*, LAWCTOPUS, (accessed on 13May 2020) https://www.lawctopus.com/academike/position-perspective-privacy-laws-india/
[36]Information technology Act 2000, sec. 65, sec. 66

as mention in the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.[37]

According to this Section in the amended Act, if a corporate entity which is in possession, regulates and functions a certain sensitive personal data and is negligent in handling that data without maintaining a proper reasonable security system and procedures, which may lead to the causing of wrongful gain or loss to the person, then the person who is affected from such activity can claim compensation from the corporate entity.[38]The sub-clause of this particular section explains the scope of the term body corporate contending that it is a wide term which includes a firm, company, association of people, sole proprietorship any of which may be engaged in any finding of commercial or professional activities.[39]The term 'reasonable practice and procedures' is also used in the Section, which includes are those mechanisms which prevent the unauthorised access, modification, deletion or destruction of personal information. Such specifications must have been mentioned in the:

1. Agreement between the parties
2. According to any statutory law in force during the commission of the act and if there is no specific agreement between the parties, then the data must be protected according to the guidelines that may be prescribed by the Central Government.[40]

[37]S.S. Rana & Co. Advocates, '*India: Information Technology (Reasonable Security Practices and Procedures And Sensitive Personal Data Or Information) Rules, 2011*', MONDAQ, (accessed on 13 May 2020), mondaq.com/india/data-protection/626190/information-technology-reasonable-security-practices-and-procedures-and-sensitive-personal-data-or-information-rules-2011
[38]Information technology Act 2000, sec. 43A
[39]Information technology Act 2000, sec. 43A (i)
[40]Information technology Act 2000, sec. 43A (ii)

The term of the contract should include the extent and the mechanism of security that they are going to implement to the disclosing parties, and the damages that need to be paid to them in case of negligence of the opposite party. There is no specific definition that has been given by the amended Act for the term 'sensitive personal data', but it is mentioned that any data that may be deemed fit by the Central Government after consulting the professional associations or bodies.

By the benefit of power which is granted by the IT Act, only a limited amount of information can be obtained under Section 72 whereas the insertion of Section 72A which is initiated by the amended Act, the scope of this section has been made wider as it even applies to the exposure of personal information of an individual.[41] But this information can be accessed even though without consent only in conditions of a lawful contract and through the power granted by the IT Act, 2000 for the revealing of any information. Under Section 72A, the term intermediary is defined. There are certain people who collect, store and transfer certain data on behalf of another person for the purpose of record. These people may include internet service providers, network service providers, telecom service providers, search engines, online e-commerce websites, online transaction sites and cyber cafes. All these people come under the purview of this section.

When we comparatively analyse the Indian laws to the laws of the developed countries, we can observe a requirement for a proper framework of cyber laws. The UK, for the purpose of guaranteeing its citizens data privacy and protection

[41] '*State of Privacy'*, PRIVACY INTERNATIONAL, (accessed on 14 May 2020) https://privacyinternational.org/state-privacy/1002/state-privacy-india

from data breaches, has the existence of the Data Protection Act, 1988.[42]The Act has certain provisions that if a person or an institution is dealing with the storage and transfer of personal data, they need to get registered with the information commissioner, which will, in turn, lead to the appointment of a government official who will supervise the functioning of such activities to prevent any breach of the Data Protection Act.

The data collected is restricted by the provisions of this act. If a specific data is collected in furtherance of certain lawful purposes, then it is not compatible with the data to be used for any other purpose other than the purpose for which it was collected. The data which is collected must be adequate, related and should not be in excess of what is need for which it has to be analysed.

(ii) Measures against data breaches under the Indian Penal Code, 1860

Under the legislation which govern the Criminal Law of India, there are no provisions for addressing the issue of data privacy. Under the IPC, the offence of data breach must be associated with a crime listed under the Code. One such instance of the provisions that can be used is Section 403 of the Indian Penal Code, where the person can be held liable for a penalty for criminal misappropriation or even for the conversion of a moveable property for another person without his consent into our own use.

(iii) Cyber security under the field of Intellectual Property Rights

If a copyrighted matter is pirated there is a mandatory punishment which is prescribed by the Indian Copyright Act depending on the commission and the gravity of the offence. If a person makes a copy of copyrighted computer software

[42] '*What is Data Protection Act*?' EXPERIAN, (accessed on 14 May 2020) https://www.experian.co.uk/business/glossary/data-protection-act/

without authorization, on the infringement of such copyright, a punishment of minimum 6 months and a maximum of 3 years is provided under Section 63B of the Indian Copyright Act. The minimum amount of fine which may be imposed is $1,250 whereas the maximum fine which can be imposed is $5,000. This maximum fine is imposed for a conviction for the second time or a subsequent conviction along with an imprisonment of one year to a maximum imprisonment of three years.

CONCLUSION

The main concern for the Indian judicial system is the lack of stringent and effective privacy protection laws in India as compared to the laws of other developed countries. This concern has been specifically bothering the foreign countries which work with India in business organisations and share confidential information with the country. Even though there are no statutory laws in favour of the cyber data protection systems, the Indian industry as well have begun the process of sensitising the government and the masses regarding the importance of privacy. Further, with regulators like the Reserve Bank of India providing for strict privacy norms in certain areas, it seems that India is taking a huge step towards privacy norms. It is being felt by all concerned that a dedicated data protection law would give further impetus to not only the outsourcing industry but to the Foreign Direct Investment Policy at large.