DATA PROTECTION LAWS IN INDIA - AN ANALYSIS

Alok Kumar Singh, LLM (Criminal Law), Amity Institute of Advance Legal Studies. Noida

ABSTRACT

The famous case of Cambridge Analytica is the landmark case in series of data breach & misusing of data protection law. The same had captured the attention of the public & made questions regarding the validity of laws relating to the protection of data & affinity of the same in the present era. The scandal is so popular that it raised many queries on queries relating to the misuse of private data for psychometric & psychographic analysis. The incident occurred also connects the breach of data, misusage of data & breach of the right of users. Therefore, the European Union General Data Protection Regulation, i.e., GDPR ensured that the company do handle the citizens personal data. With regards to the case of Google Spain, It is also held that the privacy of data shall be regulated after processing the personal & complete information only for legitimate, explicit and specific purpose upon which it is usually to be gathered legally & shall not be processed otherwise. Thus, the article analyses the laws relating to data protection & urge for strong framework.

Introduction

In the National & International Sphere, "Rights", which are inalienable & inherent characteristics of a community of human, have been reduced to a document which is implementable & visible. There are some rights which are mentioned clearly in the documents; on the other hand, there are some which are to be introduced through interpretative tools due to integral linkage with such rights. The most important & acceptable among them is the right to privacy. It also provides the ability for individuals to snoop on others. Right to privacy find out the reference in Universal declaration of Human Right & international Covenant of Political & Civil Right, Convention on Right of Child[1].

The Right to Privacy finds reference in the Universal Declaration of Human Rights & the International Covenant of Political Rights & Civil Rights, and the Rights of Convention on Child. In human life, Privacy right is one of the most important part. In our country, the right is identified as the Integral feature of the Right to freedom of speech & expression and also the right to life & liberty. Each person is eligible for a personal domain, which is free from unjustified interference or surveillance by the state or other actor. Despite prevalent approval of obligations for the protection of privacy, the specific contents of such rights is not fully developed by international human rights protection mechanisms.

The absence of exact expression of the contents of the right had contributed to difficulties in the enforcement & of its application. As privacy right is the right which is qualified, the interpretation of such does raise the challenge with respect to what organises the private sphere & in establishing the notion of the same, which is constituted by public interest. As the occurrence of public interests, the right of human being encroached by the medium of communication. The communication of privacy also concludes that individuals are able to exchange information & ideas in a space which is far from the reach of another member of society, the private sector, & in the end, the state itself. The rights of individuals are only for the exercise of the right of privacy in the system of communication.

The middle of the last century witnessed the documentation of rights that relate to non-interference in the personal life of one. It also acquired significance with the social relations of the technology. Technology is one which has cut across each part of human life. The imposition

[1] *Universal declaration of Human Right & international Covenant of Political & Civil Right, Convention on Right of Child*

in the life of humans by advanced technology has become the phenomenon of each day. It is either by the way of voluntary disclosure or involuntary acquisition of information. The observation potential of a strongest computer system prompted demand for specific rule which governs the collection and handling of private information. The genes of current legislation in the area can be traced by the way of privacy of individuals to the first data protection law in the world. Nowadays, the protection of data is the root of privacy & international phenomenon. The individual is also eligible for Right to protect data if he carries the right to privacy. Due to advancement of time in the field of technology, the protection of data is the much developing area in the coming future.

Data Protection Laws

Data Protection law plays a vital role not only in the country of India, but it plays a role all over the world. In day to day life, there are many devices are which are in work, therefore, the guarantee shall be given to users for their privacy as the same is covered by them is every use. In the present day, mostly each aspect of our communication & privacy is in the hands of some third party. The kingdom or current digitally environment is that mostly every activity which is done by individual involve some sort of exchange of data or other things. Therefore, it may arise the question in our mind on the basis of expectation of privacy which is laid down as the major premise in the view of protection of law. Although the data is used for beneficial purposes, the uncontrolled and arbitrary use of data across the world has raised concerns among a lot of individuals on the basis of privacy and autonomy.

The Judgement was also given by the Supreme Court with such dispute as the subject matter, which led to the recognition of the Right to Privacy as a Fundamental Right.

Expansion of the scope of Current Data Protection Regulation

The protection of data is an important concept not only in a country like India but also across the world. The Data Protection Committee report, which is released on 27th July 2018[2] and Personal Data Protection Bill, 2018, provide the lawful framework & boundary with which the policymakers insight into the protection of individual privacy & personal data in India. The bill also set a high standard mainly after the European Union General Data Protection Regulation, i.e., GDPR, which came into force on 25th May 2018. The most common objective of this bill

[2] Data Protection Bill, 2018

is ensuring the development & growth of digital economy with respect to all the change while the personal data is kept secure & protected. The Landmark Judgement should also be noted which includes the famous: "Aadhar Case" of Justice Putta Swamy (Rtd.) vs Union of India[3]. The case also emphasises the protection of personal data indirectly through the safeguard which is being developed by the court under the common law, the natural justice principle & law of Breach of Confidence. Therefore, all rule & policies & regulations commonly which are known as Data Protection Framework provide strong direction for the government, which on the other hand also wish to implement the enforcing of Protection of data, to secure the nation, better control on the receiving, transmitting and to process the data of individual both outside & within the Country. The Supreme Court of India also held in its judgement that privacy is a fundamental right as per Article 21 of the Constitution of India as part of Personal Liberty and the Right to Life. Informational Privacy is enclosed additionally under the scope of Right to Privacy. India shall find the equal balance so as to take the benefit of Right to privacy. India shall find an equal balance in order to take benefit of the data, which is being driven by the eco-system but is subject to fair restriction. There is good potential for directing the world into a digital global economy by making use of the Present strength within the scope of Information Technology. With regard to Protection of Data, India had not enacted any legislation relating to it. Nevertheless, the Legislature amended the Information Technology Act of 2000 to incorporate Section 43A & Section 72A, which provide the right to Monetary Compensation in the Case of disclosure of any personal data.

The forthcoming regulation of the protection of data is the broadened scope of the law by providing a comprehensive Framework of data protection, which is implemented to process the data of individuals & the activities which are carried out both by Private entities & Government.

Key Principles for the Protection of Data in India

The regulation of data protection in the country shall be framed on the basis of th following principles:

- The law must be applicable to both governmental organs and private sector entities.

[3] *Justice Putta Swamy (Rtd.) vs Union of India*

- The law shall be flexible enough to cope with various changes in fields of technology.
- The controller of data shall be held accountable for the data which is being processed.
- The Processing of data in the wrongful sense shall also attract penalty.
- For obtaining the willingness of the citizen, consent is the expression which also indicates the autonomy of humans. Attaining consent shall be genuine & informed.
- Data which shall be collected shall go through the last round of processing & for necessary purposes.

ONGOING EFFORTS TAKEN FOR ACHIEVING THE ABOVE PRINCIPLES

After an absolute analysis of the present data protection regulation, legal experts concluded that the drafted bill had its share of advantages; on the other hand, some parts are cryptic. It was also believed that the bill borrowed various significant parts from the recently implemented Regulation of General Data Protection in countries in Europe. The contours of private data and the territorial reach of law had broadened. The regulations are applicable both in the private sector and public sector, and entities are also subject to regulation. The function of entities is also regulated by law. It does supervise the flow of data across the border & also emphasise the localization of data. The consent of the consumer is required before such processing & the framing of regulation is done in such a way that the examination of the entity is done on the basis of the validity of consent. The regulation also discusses the requirement & necessity for establishing different & independent authorities to oversee & supervise the implementation & enforcement of the law of data protection & impose huge penalties if the violation is caused. The focus is to improve the digital economy in such a way that it is beneficial to citizens & the technological industries.[4]

Constitutional Status

Indian Constitution do have some provision like, “Freedom of Speech & Expression & Right to Life & Personal Liberty. The provision had its effects on the right to privacy as the Fundamental Right. There are various cases which do establish the right to privacy as the

[4] Supra note 1.

fundamental right. This proposition was also connected with the new dimension of the Protection of Data. The Link between Data protection & privacy are interdependent on each other. The right to the protection of data is too closely connected with the information of individuals.

The study of provisions of the constitution is to understand the relation of privacy with explicitly scripted rights along with interpretation granted by the Supreme Court of India. It also explores the issuance of Protection of Data, which is dealt with under various Legislation. Finally, it builds the case to treat the issuance of Data protection for the perspective of Right Based.

As said by Sir John Simmons, the rights of Human Beings are the one which is possessed by Human Beings in all places and at all times, only through the virtue of humanity. They also consist of properties of universality, naturalness, independence from legal recognition or social recognition, inalienability from legal recognition or social recognition, non-forfeit abilities, and imprescriptibly. Thus, the idea for the protection of human right shall always be claimed by human being. Thus, the idea of the protection of rights of human is also the protection of data. The universality & independence of the protection of data is the essential occurrence for individuals. The protection of data also leads to Privacy rights.

The most important significance & illumination discussion is that the protection of data and privacy have different links to each other. The linkage or shadow of various areas which are closely related to such regimes.

The privacy is a concept which is related to seclusion, isolation, and solitude, although it is not alike such terms and is far away from the purely descriptive aspects of privacy, like withdrawing from the corporate sector, influencing others, implying the right to exclusive control of access to the individual empire. The pathfinder of developmental rights as the activism on the part of the courts is also highlighted as a matter of rights.

Such rights of the individual can be acquired naturally, so that the privacy right is also be attain naturally. In the article written by Jurist Herbert Hart, “Are there any natural Rights”? distinguish between special rights and general rights. Where there are special Transactions or Special Relationships, Special Rights do Arise up like contract, promise, or membership in Politics, on the other hand, General Rights belongs to all men that are capable of choice, in the

absence of that special condition that give rise to special right. The perspective that the protection of data is a special right or general right shall be taken into consideration in work.

Analysis of Right Based Approach

The research of approach based on right of protection of data issue can only be done by the way of various law. The objective of such an approach is to analyse the standpoint of protection of the data regime in India. The issuance of protection of data is assumed to be important in later days & the development of Internet-enabled services, which thereafter led to the bud in data processing outsourcing, the function of accounting, the service of call centres, business processes, and various operations of business. However, the technology had been developed for tackling the development of law is also improved. Thus, the protection of data explores how, beyond the information, details & data of individuals & organizations is protected under the law of India, mainly under the Indian Constitution.

The significance is placed on protection, which is available under the Indian Constitution, as it is the basic & ultimate source from where various law derive their force & validity. The following three shall address the constitutional aspect of concern.

1. The rights of privacy for the person interested in cyber space & real space.

2. Mandate freedom of information according to Article 19 (1) (a)[5] of Indian Constitution.

3. Mandate Right to know people at large according to Article 21[6] of Indian Constitution.

Thus, it speaks out for the right to privacy, right to know, Right to Information & Trade Secrets, Intellectual Property, Electronics Government, etc, in various viewpoints. In order to justify the relationship with the right, the research work is done. Further, another gap of this work is that there is no balance b/w data process and information. The approach of right is justified only by the way of discussion with the help of other laws, which are as follows:

Data Protection & Right to Privacy

There is much similarity between Data Protection & Right to Privacy. The protection of data is

[5] Article 19 (1) (a)
[6] Article 21

only possible if privacy intrusion is topped. In particular, informational privacy and privacy law are sharply interrelated with the development of technology. In 1890, in the Right to Privacy, Warren & Brandeis Lament the instantaneous photograph & newspaper enterprise, which is invaded as the sacred precincts of private & domestic life & various mechanical devices that threaten to make good the prediction that" what is whispered in the closet shall be proclaimed from the house-top. These are the genes of matter of privacy. Nowadays, the same is developed by the protection of data. The idea of data protection has various aspects. The various aspect of protection of data as the right like, the access right to data bank, the right to check their exactness, the right to bring them up to date & to correct them, the right to sensitive data secrecy, the right of authorizing circulation, all right when joined together constitute the privacy rights.

Therefore, in the link of "protection of data" & Privacy, Status is too much suitable as the approach which is based on Rights. The advancement of the Right of the Constitution to privacy began in the early 1950s in the context of surveillance of police of accused & domiciliary visits to the home of a person. Such a visit can be done at any time, whether day or night, to monitor the person, whether they are engaged in Suspicious criminal activity or not.

In the Case of **M.P Sharma vs Satish Chandra**[7]**,** it was held by Supreme Court that the argument that seizure & search violated Article 19(1)(f) of Indian Constitution. The court was also in the view that a search done by itself doesn't affect the right to property, although the seizure should affect it, and such was only temporary & was a reasonable restriction on Privacy Rights. Then privacy rights were developed in the sphere of Indian Constitution according to Article 19(1)(a) & Article 21. Right to Liberty under Article 21. The Right to Liberty under Article 21 of the Indian Constitution is also addressed by Justice Subba Rao in the Case of Kharak Singh vs State.

The Supreme Court, in another landmark case, had made developments in the law of Privacy by holding private visits of police & Disclosure Information. Such Disclosures of Information approaches the modern protection of data concerns. In the Case of R Rajagopal vs State of Tamil Nadu, The complainant was the editor, publisher & printer of Weekly magazine in Tamil which is published in Madras and who sought an order stopping the State of Tamil Nadu from

[7] M.P Sharma vs Satish Chandra

interfering with the publication which is authorised of the autobiography of Auto Shankar, the prisoner who is unsafe awaiting the penalty of death that is based on records of the public.

In the case of Jeevan Reddy, J affirmed that the privacy right is the implicit right to life & liberty, which is guaranteed in Article 21 of the Indian Constitution. It is also affirmed by the Court that "Let alone" right for each citizen of the country to safeguard their right to privacy.

Thus, the privacy right had its own way for developing the matter of protection of data. Similarly, both ideas had become a "Matter of Rights" under the Indian Constitution.

Data Protection & Right to Information Act, 2005[8]

Right to Information in India comes with contention that " The Practical Regime of Right of Information for Citizen for securing information under the control of authorities of Public for the purpose of promoting transparency & accountability, for matters which are connected therewith or are incidental to. It is according to the preamble of 2005 Act & Section 2(j) also speak regarding the definition of "Right to Information". Above all, the issue which arose now is whether "the data which is in the custody of public authority is safe or not." The digital data, according to Clause IV of Section 2(j), is presently in doubt.

The protection of data as per this act is a concern and is being taken care of as a matter of right for the individual. In the case of Bannett Coleman vs Union of India, it was held by the court that it is incontrovertible by freedom of press which meant the right of all citizen to speak, express and publish their views & further, the freedom of Speech & expression include within its compass the right of all citizen to be informed and to read.

In the case of Indian Express Newspaper (Bombay) vs Union of India, it was held by the court, that the prime motive of freedom of speech & expression is that all member shall be able to form their own belief & communicate freely to other. In Aggregate, people's right to know is the fundamental principle involved here.

Thus, the link b/w both contexts can only be made by the judgement of the Supreme Court. In the case of PUCL vs Union of India, it was held that the Right to Information is elevated further

[8] Data Protection & Right to Information Act, 2005

to the status of rights of human, which is important for making governance transparent & accountable.

The Supreme Court also held that in the Indian Constitution, the Right to Information is Inherent according to Article 19. Thus, it is justifiable that the link between both contexts is closely related to the approach based on Rights.

Data Protection & Indian Penal Code

Indian Penal Code had its roots at the time of British Rule in India. In the 1860's, the Formulation of the first introductory draft was done under the Chairmanship of Lord Macaulay. Thus, the relation with the protection of data according to the provisions of the Indian Penal Code is not too much satisfying all of the needs. The Indian Criminal Law does not specifically address the breach of data privacy. Under IPC, the liability of such breach may be inferred from the crimes related. For specimen, Section 403 of the IPC imposes a criminal penalties for dishonest misappropriation of Movable Property for one's own use. When the same comes under the part of the liability of others, then the question arose on the opposite way, that whose rights are to be protected. Section 405 & Section 409 speaks that whoever misappropriates the property of some other person shall be punishable under criminal breach of trust. According to section 378 of Indian Penal Code, No one can dishonestly take any movable property out of the possession of any person without the prior consent of such person, if the same is done by any person, he will be punishable for the offence of committing theft but till date there is not any particular act which is regarding the protection of electronic data. Therefore, there are only two ways to get the protection of legal rights, of which one can be used. All the crimes that are committed are committed against the state only. Therefore, the right of the state to maintain law & order is a serious concern. Indian Penal Code (IPC) penalties are mentioned & in civil action law for damage, including the amount of damage, shall be resolved by the verdict of the jury. The Ideas for mentioning it are too much relevant to address the right issue. The relationship between the protection of data & IPC to address the rights is appropriate. Thus, the state shall also come under the purview of protecting individual data.

Data Protection & Information Technology (Amendment) Act 2008

The Information Technology Act, i.e., IT Act, 2008 and Data Protection, do have their own implication in relation to each other. The objective too clear regarding the matters of protection

of cyber relations. It provides protection against certain the breaches in relation to data from the system of the computer. The Act also comprise provisions for preventing the use of computers unlawfully, Computer Systems, & Data stored in the computers. Various Provisions are also made relating to Protection of Data. Section 43A & Section 72A do clearly mention regarding the data protection.

Information Technology Act 2008 represents a remarkable step toward warring aggregation of crime in the Cyber age. Changes which were introduced in statutory data protection in Indian Law finally ceding to the demand of the US & European nations over the past decade. Service providers are being imprisoned for disclosing personal information in violation of the obligations made under the contract. Further, disclosing the private information makes the perpetrator lawfully liable for paying the damages.

Thus, as a matter of right, the protection of data had given the same status. The development in technology is the matter of main focus given to analyse the EU Data Protection legislation & the stand of the IT Amendment Act, 2008. It also talks regarding the exercise of Data in corporations, such as disclosing, sharing, excess, publication security measures & the penalty in light of the IT Act, 2008. Another Rule of Information Technology 2011 gives the impression of the right concern implication in their provision. The significance of outsourcing business in India & how that may impact business flow from Companies of the European Union.

The regulations which are recently notified related to protecting private data are also discussed in this article & it also examines the Indian Regulation, Contrasting its provision at various points with the Act of 1998, i.e., the UK Data Protection Act. Therefore, the major right base approach is asserted to individuals' right to protection of data.[9]

Data Protection & National Security

In the present era, National Security & Data Protection are of much relevancy. The importance of National Security & agencies of Law Enforcement in each country play a major role regarding the protection of data. In the year 2013, the story came out that their fellow Edward Snowden had released data related to the privacy of the US, i.e. the United States. The situation of Hue & cry arises that there is no privacy at all for individuals. When the data is accessed by

[9] *Research Scholar, Rajiv Gandhi School of Intellectual Property Law, Indian Institute of Technology Kharagpur, West Bengal, India*

an individual and exposed, what kind of privacy shall prevail for such individual? If there is the rise of such a situation, then the country which is developed shall be the most powerful because of the advancement of technology & there shall be no better situation for countries which are developing. National security does not at all play much of a role in the current situation. In order to make parity with such a situation the idea of putting forward the right base approach is too important in nature. In related conditions, law enforcement and national security are excluded from law, or they are accepted broadly for which that access shall be permissible. This is proved in the case of each country, and also in the countries which are much developed in regimes of protection of data.

For eg: As written by Dan Svantesson that Australian Law taken together…. provide enforcement of Australian Law & Agencies of National Security with wider access for data of private sector.

The result is that the collection of data & use for national security & enforcement of law purposes is often excluded from oversight applicability to other data processing activity or subjected to a much less transparent standard & oversight regime.

The protection against the authority of an individual is mandatory for examining the approach which is right-based. In such conditions, police are able to track cell phones except in a limited set of time-sensitive situations & emergencies. The updated technologies have given each moment snooping for an enforcement agency, & the geolocation of each individual. The issues are that it discusses cellular location technology, which is used by police for monitoring citizens who use cell phones. Precisely, the commentary will examine cell site, Global Positioning System & Technology of Wi-Fi. Other issues will show that legislation is required in the area because the tracking of cell phones is a universal practice that eventually replaces federally regulated wire-tapping to some degree. Now, to some extent, the encroachment is authentic for national security reasons, but on the other hand, personal privacy-related issues also peep into the door.

The Supreme Court in the case of District Registrar & Collector, Hyd. Vs Canara Bank had contended that the seizure & search by enforcement agencies of any register, book, record, paper, document or other proceeding for the motive of collection of evidences & discovering fraud & omission of stamp duties payable or not of individual come under the situation of infringement, confidentiality & secrecies which shall be maintained.

As per the establishment of Rights, individual liberty, like privacy & protection of rights, is an important phenomenon to tackle the policy of cyber crime & cyber security, which is increasing day to day. Concerns relating to the Protection of data & Human rights are on the common edge. It involves the protection of data and privacy in each country.

In philosophy debate of 'Security vs Privacy' dichotomy 'Interest vs Right' or 'Value vs Value' joint the idea that balance is required according to some weighing rule that limit one in the favour of another. This also provides the ideas of Data Controller, Data, Storage of Data, Data Processer, Proposed Regulation.

Data Protection & Consumer

The relationship of the consumer with the organisation is too vital to articulate the matter of the protection of data. The Calcutta High Court in the case of Shakankarlal Agarrwalla vs State of India held that banker is under strict obligation to maintain secrecy. As per Lord Halsbury' Law of England, the contract b/w banker & his customer that the banker will never share the personal information or any information relating to customer acquire through the keeping of accounts unless the banker is so compelled to do so by order of the Hon'ble Court or the circumstances which give rise to complete the public duty of disclosing information or protecting of the banker own interest if requires, to other customer or third person, until he gain the express or implied consent from such party. Thus, the idea for putting forward relation of banker & customer shall be maintained.

On the other hand, The growth of misuse is increasing daily and mainly due to electronic commerce, data protection is in danger. The issues which are related online are storage, accuracy, collecting, & use of data which is being provided by users of the internet. The major concern regarding it is the fraud of BPO, and all the frauds committed are covered under the provisions of the Information Technology Act. The phenomenon is only due to the relation of customer with authority. If service providers do maintain the policy of privacy, then such a situation can't arise. However, the situation is real, and the authorities are not bothered by such a privacy policy. Enforcement agencies are also not aware of such kinds of violations of rights. The issues of privacy with the protection of data can be satisfied only by a well-equipped right, right-based approach.

While the examination of privilege to data with protection in this age and day, it was held by Hon'ble Justice D.Y. Chandrachud that:

 Protection of Information, which is the feature of privilege to security. The danger to the protection of one at the time of data may start from the state as well as from some non-state on-screen character also. We may also recommend to the Union Government that there is a need to look at & to place into the spot strong systems which are required for assurance of information. The system formation may require progressively cautious & touchy harmony b/w genuine worry of state & interest of Individual.

The real focal point of state may be to ensure national security while it forestalls & examine wrong-doing with empowering advancement & such appearance of information while forestalling the dissemination of one's social government assistance benefit. This is considered by the Union Government as a simple matter of arrangement, whereas it designs intentionally organized systems for the security of information.

Although the Court had been educated by the Union Government, it also established the committee, which is governed by Justice B.N. Srikrishna (Former Judge) and for this reason, such issues shall be managed suitably by the government that has due respect to what had been set out in provided judgement.

 The Privilege to Protection that is asserted by State & Non-State on Screen Characters. Acknowledgements & implementations of such case qua non-state on-screen character can require administrative mediation by the State.

Protection of Data Under Foreign Laws

Various Countries other than India do have their separate laws which are related to the protection of data. Those laws are framed well & are established law, exclusively for the protection of data.

UNITED KINGDOM LAWS[10]

[10] *Nicholas D. Wells, Poorvi Chothani and James M. Thurman, Information Services, "Technology, and Data Protection," The International Lawyer, Vol. 44, No. 1, International Legal Developments Year in Review: 2009 (2010): 355-366.*

The Data Protection Act (DPA) in the U.K. was framed in the year 1984 by the U.K. Parliament and was repealed by the DPA in 1998. The act was basically formed to provide due protection & privacy to the personal data of individuals in the UK. This act do cover data which is used for identifying living person. The same includes birthday, anniversary dates, telephone numbers, fax numbers, e-mail, addresses, etc. It only applies to data which is intended to be held or is held on computers or various equipment that are operated automatically in response to instructions given for such purpose or is held in a relevancy filling system.

According to the Act, the person & organization that stores personal data shall register with the commissioner of information, the appointment of which had been done as official of government to oversee the whole act. The act further restricts the collection the data. The personal data can only be obtained for one or more lawful purposes, & cannot be processed further in any manner incompatible with such purposes. The personal data shall be relevant, adequate & non-excessive in relation to the purpose for the same they are used for processing

USA LAWS

Both the European Union & U.S. focus on enhancing the protection of the privacy of their own citizens. However, the U.S. take various other approaches to privacy as compared to the European Union. The Sectoral Approach, which relies on mixed legislation, self-regulations and regulation, is adopted by the United States. In United States, on the basis of importance and utility, the grouping of data is done into various classes. Then, the various degrees of protection are awarded as the classes are separated.

There are many acts which have been passed to stabilize the protection of data law in the U.S. The Privacy Act was also passed in 1974, which provides for establishing standards for when it is reasonable and justifiable for government agencies to compare data in various databases.

The Electronic Communication Privacy Act was also passed in order to restrict the interception of electronic communication & prohibit access to store data when the consent of the user is not obtained.

Afterwards, The Children's Online Privacy Protection Act was passed by the US Congress in October 1998, which required Website operators to obtain consent of parents before the

information is obtained from children, & Consumer Internet Privacy Protection Act requires an ISP to get permission from Subscriber before the information is disclosed to third parties.

On the other hand, the federal laws which are in existence are not sufficient for covering a wide range of issues & making a new digital environment with no threat to personal privacy. The Government of United States is also reluctant for imposing regulatory burden on activities relating to Electronic Commerce which may hamper the development & had looked for answer in self-regulation.

Protection of Data under Indian Law[11]

Indian Constitution under Article 21 provides the provision or law related to Privacy. The interpretation of the same was not found sufficient for providing utmost protection of the data. Efforts are made by the Legislature of India to support the protection issues related to computer systems under the Information Technology Act, 2000 in the year 2000. The Act also contains many provisions that protect the data that is stored. Indian Legislature in the year 2006 introduced the bill called "The Personal Data Protection Bill" to provide the protection of private information of individuals.

Under the Information Technology Act, 2000

Section 43

The Section helps in providing protection against unauthorised access to computer systems and imposes a huge penalty of up to Rs. 1 crore. Extracting the data, downloading data on an unauthorised basis & copying the data are covered under this section. Section 43(c) also imposes a penalty for the unauthorised introduction of computer viruses or contaminants. Section 43(g) provides a penalty to assist the un-authorised access.

Section 65

The Section deals with the Source Code of the Computer. If any person intentionally conceals, alters, destroys or causes another to do shall suffer the penalty of imprisonment or a fine, which

[11] Beitz (2004): 196, Simmons (2001

may be up to Rs. 2 lacs. Therefore, this section provides protection against the tempering of documents on a computer.

Section 66

This section deals with the protection against hacking by other persons. According to Section 66, Hacking is defined as the act with intention of causing the wrongful loss to any person or with knowledge that some loss or damage shall be caused to any person & information which is present in computer system may be destroyed, altered, or deleted or the value or utility of the same may get diminish. Section 66 imposes the penalty for imprisonment for up to 3 years or a fine, which may be up to Rs. 2 Lac or both.

Section 70

This section deals with providing protection to the data which is stored in the system which is protected. Protected Systems are the computer systems, computer networks or computers to which the concerned government, by issue of gazette information in the official gazette, declares it as the protected system. Any attempt to secure access to such a system in contravention of a provision of Section 70 will make a person liable for punishment, which may be imprisonment extendable to ten years & also be liable for a fine.

Section 72

This section deals in providing the protection against breach of confidentiality & privacy of data. According to section 72, any person upon whom power is conferred under Information Technology Act & rules for securing the access to any electronic book, record, register, document of any material disclosed to any third person shall be liable to imprisonment extendable to two years or with fine extendable to Rs. 1 lac or both.

Law of Contract

In the modern world, the corporate sector completely relies on contract law as a very important and useful means used to protect the information of the companies. The companies are engaged in entering into several agreements with other clients, companies, partners, agencies for keeping the information secured to the extent they required to secure. Agreements like non-disclosure agreements, non-circumvention agreements, user license agreements, etc. are

entered, which are highly confidential & various clauses such as arbitration clauses; privacy clauses are used to move legally if any dispute relating to a contract arises.

The agreements made help them for smooth running of the business. BPO companies also implemented processes such as BS 7799 & ISO 17799 standard of information, which are used for managing security and also restrict the quantity of data which is made available to employees of BPO & Call centres.

Indian Penal Code

Indian Penal Code does impose punishment for wrong, which is expected to occur till the last decade. But IPC fails to incorporate within itself the punishment for a crime relating to data, which has become the order of the day.

The Personal Data Protection Bill, 2006

The bill had been introduced on 8th December, 2006 in Rajya Sabha upon the footprints of Foreign Laws. The main motive of the bill is to provide the protection of private data & information of the individual which is collected for a particular purpose by one organization & preventing its usage by another organisation for commercial purpose or other purposes & also entitle the individual for claiming compensation or damage due to the disclosure of private data or information of the individual without the consent & for matter connected with act or that are incidental to this Act. The provisions which are contained in the act are related to the nature of data which is being obtained for specific purpose & quantum of data for obtaining such purpose. The controllers of data had been proposed for appointment to look upon the matter related to the violation of the above act.

Conclusion

Presently, the Personal Data Protection Bill, 2019 is framed in corollary to EU i.e., European Union's GDPR (General Data Protection Regulation) also set in Lok Sabha. The bill also addresses the major concerns which are raised by the makers of the law. The Personal Data Protection Bill, 2019, which is drafted specifically focuses on placing consent as the most important aspect of the bill & also includes provisions relating to the localisation of Data & it also made its regulation stringent on the Processing of data. The bill also addresses the issue of

Processors of Data. Therefore, the bill should be awaited by the individuals to become the law, thereby having stronger legislation that will form the concept of privacy jurisprudence.

The analysis of various themes highlights the protection of data, which has been treated as a right from various perspectives. Subjects such as Right to Privacy, Right to Information, Information Technology, Indian Penal Code Corporate Affairs, & consumers were given special emphasis for accepting the fact of protection as the right. The main objective of the problem is to strengthen the outlook for the protection of data as the right in the age of technology. There is an increase in technology day by day, so to maintain this phenomenon, the protection of data is required to protect the liberty of individuals. The other objective of this research is to establish the privacy right & protection of data right as the fundamental right & after analysis; it is justifiable to treat it as a right. The institutional status for the protection of data can provide a consistent approach to the protection of data. In order to give standard features for protecting the data as the right of the individual, the facet of protection of data such as processing, storage, access, and data collection must provide a together platform in the legal framework.

The awareness of the right-based approach to the protection of data & privacy is to spread unanimously worldwide.

On the comparison of the laws of India with those of other developed countries, an analysis of the exact laws of India can be done. Data are not of the same utilities & importance; they vary from one another based on their utility. Therefore, we do require different framework categories of data having separate utility values, like those of the United States. Further, the provision of the Information Technology Act also deals basically with data extraction, destruction of data, etc. Corporate sector does not get all protection of data through which ultimately forces them into entering into different private contract for keeping their data secured. Such Contracts do have the exact enforceability as the contracts in general.

However, a lot of efforts were made for having the protection of data as a different discipline; then also, Indian Legislature left some lacunas while the bill was framed in the year 2006. The bill was wholly drafted as per the structure of the United Kingdom Data Protection Act, whereas today's requirement is the comprehensive Act. Therefore, it can be recommended that the arranged draft on the basis of United States laws related to the protection of data be much more favourable to today's requirements.

As it is one of the most apprehensive topics of discussion in the modern world, Indian Legislatures are, therefore, required to frame more rigid & exhaustive laws for data protection, which require qualitative efforts rather than quantitative.

Reference

1. Puttaswamy v. Union of India, 2017 (10) SCALE 1.

2. Google Spain SL v. Agencia Española de Protección de Datos Case, C-131/12

3. Supra note 1.

4. The Right to Privacy in the Digital Age, U.N.Doc.A/RES/68/167 (2003), Preamble.

5. A. Awya & C. Mulei, An Outline of Media Legal Education Program-Sheria (1998).

6. Hartford Casualty Ins. Co. and the Acara case (1991),216 § 59.

7. Research Scholar, Rajiv Gandhi School of Intellectual Property Law, Indian Institute of Technology Kharagpur, West Bengal, India.

8. Assistant Professor, Rajiv Gandhi School of Intellectual Property Law, Indian Institute of Technology Kharagpur, West Bengal, India.

9. Prakash Shah, "International human Rights: A perspective from India," Fordham International Law Journal, Vol. 21, Issue 1, Article 3, (1997): 24- 38

10. Article 12, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." Accessed October 21, 2016

11. http://www.un.org/en/documents/udhr/, Article 17 (1), "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation." Accessed October 21, 2016,

12. http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspxArticle 16 (1) No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, or correspondence, nor to unlawful attacks on his or her honour and reputation. Accessed October 21, 2016,

13. http://www.ohchr.org/en/professionalinterest/pages/crc.aspx.

14. Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," Harvard Law Review, Vol. 4, No. 5 (1890): 193-220

15. Article 21 & 19 (1)(a) of the Indian Constitution, See also Udai Raj Rai, Fundamental Rights and their enforcement, PHI Learning Private Limited, New Delhi, (2011) p.19. See also Kharak Singh v. The State of U.P. and Ors. AIR 1963 SC 1295

16. UNESCO, Global Survey on Internet Privacy and Freedom of Expression, (2012): 51.

17. S.K. Sharma, Privacy Law: A Comparative Study (Atlantic Publishers & Distributors: 1994)

18. Austin, Lisa Michelle, "Privacy law and the question of technology." Ph.D. Thesis, University of Toronto; 2005, ProQuest Dissertations and Theses.

19. David Flaherty, "Protecting Privacy in surveillance societies", University of North Carolina Press, (1989).

20. Lee A. Bygrave, "Privacy and Data Protection in an International Perspective," Stockholm Institute for Scandinavian Law, (2010).

21. Nicholas D. Wells, Poorvi Chothani and James M. Thurman, Information Services, "Technology, and Data Protection," The International Lawyer, Vol. 44, No. 1, International Legal Developments Year in Review: 2009 (2010): 355-366.

22. Section 2 (o) of the Information Technology Act, 2008 provides "Data" means 'a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, and punched tapes) or stored internally in the memory of the computer"

23. Further on the origins of "Datenschutz", Smitis, S. (ed.), "Bundesdatenschutzgesetz, Nomos Verlagsgesellschaft, Baden-Baden," 6th edition, (2006): 62–63.

24. Lutha R Nair, "Data Protection Efforts in India: Blind leading the Blind?," The Indian Journal of Law & Technology VOL 4 (2008).

25. Bygrave, L.A., "Data Protection Law: Approaching Its Rationale, Logic and Limits," Kluwer Law International, The Hague / London / New York (2002).

26. Westin, A.F., "Privacy and Freedom," Atheneum, New York (1970); Miller, A., "The Assault on Privacy: Computers, Data Banks and Dossiers," University of Michigan Press, Ann Arbor (1971). The title of Westin's seminal work, Privacy and Freedom, is a case in point. Indeed, as pointed out further below, "privacy" in this context has tended to be conceived essentially as a form of autonomy – i.e., one's ability to control the flow of information about oneself

27. Supra Note 13.

28. Supra Note 13.

29. Handbook of European Union Data Protection laws, Accessed October 21, 2016, http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protectionlaw-2nd-ed_en.pdf.

30. Secretary of Health and Human Services, Shalala made recommendations to Congress on the Confidentiality of Individually-Identifiable Health Information on September 11, 1997.

31. Rebecca Vesely "Cop-friendly Approach to Handling Medical Data," Wired News 12 (September 1997) Accessed March 20, 2014, http://www.wired.com/news/news/politics/story/6824.html.

32. Article 19 (1) (a) of the Indian Constitution

33. Article 21 of the Indian constitution.

34. R Rajagopal v. State of Tamil Nadu AIR 1995 SC 264; Sharda v. Dharampal, AIR 2003 SC 3450; District Registrar and Collector v. Canara Bank, (2005)1 SCC 496; State of Karnataka v. Krishnappa AIR 2000 SC 1470; State v. N. M. T. Joy Immaculate, AIR 2004 SC 2282; X v. Hospital Z AIR 1999 SC 495; Kottabomman transport Corporation Limited v. State Bank Of Travancore and others, AIR 1992 Ker. 351; Registrar and Collector, Hyderabad and Anr. v. Canara Bank Etc AIR 2004 SC 935;

35. In a case, The CPIO, Supreme Court of India v. Subhash Chandra Agarwal and Anr. the Information Technology Act 2008, laid down the Definition of 2(f) "information" means 'any

material in any form, including records, documents, memos, e-mails, opinions, advices, press releases, circulars, orders, logbooks, contracts, reports, papers, samples, models, data material held in any electronic form and information relating to any private body which can be accessed by a public authority under any other law for the time being in force'.

36. It has held that in a case of Ram Jethmalani & Ors v. Union of India, (2011) 8 SCC 1. "Right to privacy is an integral part of right to life, a cherished constitutional value and it is important that human beings be allowed domains of freedom that are free of public scrutiny unless they act in an unlawful manner. Revelation of bank account details of individuals, without establishment of prima facie grounds to accuse them of wrong doing, would be a violation of their rights to privacy. State cannot compel citizens to reveal, or itself reveal details of their bank accounts to the public at large, either to receive benefits from the State or to facilitate investigations, and prosecutions of such individuals, unless the State itself has, through properly conducted investigations, within the four corners of constitutional permissibility."

37. Beitz (2004): 196, Simmons (2001)

38. H L A Hart, "Are There Any Natural Rights?" The Philosophical Review Vol 64, NO 2 (1955): 175-191,

39. Ibid, pp.183-188.