VOLUME 23 ISSN 2456-9704

COMPARATIVE ANALYSIS OF INDIA'S DATA PROTECTION NORMS WITH EUROPEAN UNION'S (GDPR) NORMS

By Siddharth Saxena
From School of Laws, UPES Dehradun

INTRODUCTION

Information Technology has been one of the most rapidly growing technology of the recent times. With everyday growing population that uses internet, Information technology has been one of the most used and relevant technologies of the current times. Information technology basically involves the transfer of data at the very basic level to the most complex advanced levels of communication one could ever witness. With the growth comes regulations. Data transferred over the medium or transmission media involves personal data too. In this era of Information Technology, it is quite evident that personal data has to be secured carefully. Certain efforts have to be made to secure your personal information.

To know the requirements of regulations, it is required that what encompasses personal data should be laid out. Any information that can lead to identification of a person over the information technology domain is personal information. The data so collected is personal data. Personal data includes names, addresses, photographs, identification numbers used by the government agencies, date of birth, fingerprints, credit or debit card numbers, vehicle registration plates and IP Addresses to name a few of the examples of what encapsulates personal data. It has to be known that personal data cannot be confined to the above stated examples. Any information that can make the person singled out from the people or pool of people can be said to be an identifier. Therefore, the above stated examples don't really confine what personal data could mean or what would fall into the ambit of personal data. Identifiers are used by companies who track people over their browsing history, their online behavior, how much time they spend on what they spend on. These identifiers are used to make a profile unique to the person whose identifiers are used. Offers shall be shown to these profiles which suit their browsing preferences or their needs. That is what an advertising company would do.

> *"There is little doubt that the growing amount of data will change the world in the coming years in ways that we can scarcely imagine today."*

Personal data usage cannot be confined advertising but it has various other usages too. Policy making involves personal data usage. There have been recent growth in the technology involves that processing of the personal data that can lead to reduction in the wastage of the resources and drastically improve policy making by providing accurate and informative data.

The internet has opened numerous avenues for us and we use a lot of personal information or data on the internet for the companies to collect it and make it an identifier and use it commercially. Therefore, it is evident that there is a need to have a control over your personal data so collected and be known about its use and its implication.

This leads to the incubation of data security and data protection. To define data protection

would be simply to protect data. However, the ambit of this term is quite large. The type of data protection that shall be put to use differs to what data has been it put up to. As such, different types of data require different amount of protection. For example, a person would really want that his personal data over the internet should be secured and he/she should really know the whereabouts of the data tracking done on his/her net surfing session.

Since the ongoing era has seen the rise of various user generated computer systems, like social media, social networking and messaging platforms the amount of personal data that shall be stored in the computer networks has increased drastically. This cannot be simply confined to technological developments but due to the user generated computer platforms stated above.

It has to be also known that this information isn't stored on a single computer or doesn't have single source of data transmission but is send over to different processing environments and techniques that include Cloud Storage etc. These cloud storages are generally stored outside the jurisdiction of the country or have offshore data storages. A breach in such case would result in drastic security threats.

Therefore, it is need of the hour that there should be stringent data protection mechanisms and policies for the protection of any kind of data. The policies should also determine what kind of security shall be given to different kinds of information.

To define data protection,

> *"Data protection is commonly defined as the law designed to protect your personal data. In modern societies, in order to empower us to control our data and to protect us from abuses, it is essential that data protection laws restrain and shape the activities of companies and governments. These institutions have shown repeatedly that unless rules restricting their" "actions are in place, they will endeavor to collect it all, mine it all, keep it all, share it with others, while telling us nothing at all."*[1]

Whatever you do on the internet whether you use a service, buy something online, register for something, schedule an appointment for the doctor, consult a doctor, paying taxes or scheduling a request for server or entering into a contract, you have to give your personal information to the other end. Although, you might not know about it, various companies and agencies use your activity and data to generate identifiers. These identifiers are sold off to different companies. This basically means that your data or identity has been sold over the world without your information and consent.

To bring confidence or trust in the system run by government and different businesses is by making strong data protection regimes that are backed by stringent legislation which help to reduce the surveillance over the individual by both state and business and reduce the exploitation of data.

---

1 https://www.privacyinternational.org/explainer/41/101-data-protection

A strong data protection regime can generate confidence into the system from the users, restrain malpractices and reduce exploitation of data. It is pertinent that governance policies are laid down domestically as well as internationally to make sure that individuals have rights to protect their data, strict regulations are made to be followed by the processing agencies that use personal data which includes state and corporate. A penal regulation is also needed so that a penalty can be imposed against those who breach these regulations and are ineffective in laying down the protections as per mentioned.

Privacy is one of the transnationally recognized rights under Universal Declaration of Human Rights (UDHR). Article 12 of the UDHR lays down,

> *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence .... Everyone has the right to the protection of the law against such interference or attacks."*[2]

United Nations General Assembly in December 2016 passed a resolution regarding "Right to Privacy in the Digital Age, GA Res. 71/199" which reinstated past mentions of the General Assembly's contentions on the aspect of privacy. It lays down that,

> *"States must respect international human rights obligations regarding the right to privacy [...] when they require disclosure of personal data from third parties, including private companies."*[3]

The linkage between privacy and data protection is very intrinsic. How person accesses data over the internet and leaves traces of its access all over it. These traces and trackers are used by the companies to make profiling of the users and use these profiles to show them advertisements as per their profiles.

INDIA'S DATA PROTECTION REGIME

EXISTING LEGISLATION

India is the fifth largest economy in the world and it currently doesn't have a stringent specific legislation as per the aspect of data protection is concerned. Although, India does have a national legislation that deals with information technology per se but that doesn't explicitly talks about data protection. It lacks at several aspects of data protection regime and isn't a standalone legislation and has to be coupled with different legislation to effectively exercise its jurisdiction.

The effective implementation procedures that should be laid down are not properly and distinctively laid down. The Information Technology Act, 2000 doesn't proclaim what sensitive data or sensitive information is or even if it has be personal or not. It doesn't define it directly and only lays down the procedure for practicing prudent security and diligence.

Information Technology Act, 2000 deals with the data protection regime under Section 43A & 72A of the Act.[4]

[2] Art.12 UNGA Res. 217 (III) A, Universal Declaration of Human Rights (1948)

[3] Res. 71/199 UNGA, Res. 34/7 Accord Human Rights Council

[4] 43A Information Technology Act, 2000

Section 72A of the Act talks about right to get compensation on improper disclosure of personal information.[5]

Both the sections came into force on 27th October, 2009. The Central Government also laid down the Information Technology Rules, 2011 titled "*Reasonable Security Practices and Procedures and Sensitive Personal Data or Information".* The rules were made to impose subsequent as well as additional requisites on commercial as well as corporate persons in India in relation to the collection as well as the disclosure of the personal information. These rules are somewhat similar to the "General Data Protection Regulations" of the European Union and the "Data Protection Directive" of the European Union.

Every person should have no interference in the matters related to privacy as laid down under the Article 12 of the Universal Declaration of Human Rights.

In India, the landmark judgment by the Hon'ble Apex Court, The Supreme Court of India recognized the right to privacy as a Fundamental Right under Article 21 of The Constitution of India under Part III of the Constitution of India. The Supreme Court in its landmark judgment of *Justice K.S Puttaswami & another Vs. Union of India*[6] *delivered in August 2017 for the first time recognized right to privacy as a part of right to life and right to personal liberty under the Article 21 of the Part III of the Constitution of India. The court also talked about "informational privacy" as well as "informed consent". These two concepts have been held by the court to be of the nature of the face of the right. The court ruled out that every person has a right of privacy and the right to access that information is reserved with the person by the consent of the person. This was the first time Supreme Court had explicitly recognized the right of a person over his or her personal data or information.*

However, Fundamental Rights are enforceable against the state entities not against the private entities. The Supreme Court has held that right to privacy under fundamental rights cannot be enforced against private entities and it would require a legislative framework for a person to enforce these rights over them.

R Chandrasekhar, NASSCOM President has aptly commented on the privacy policy of the country. He says that the sanctity of privacy has a core nexus with the culture of the country and therefore, any measure in regard to the privacy must satisfy the nexus between the social and cultural notion of the nation.

"Notions of privacy have to be encompassed in the form of legislation which is pertinent to the values and social mores in a given country.

The issues around privacy in a country as large as India are complex, and a structured effort has been made to elicit views from different stakeholders over the course of several years. The need now is to bring the formulation process to a close and move this legislation forward," "Chandrasekhar says. In the coming years, a robust privacy law, framed in the context of India's reality,

[5] 72A Information Technology Act, 2000

[6] WRIT PETITION (CIVIL) NO 494 OF 2012

is going to be essential and will form the bedrock of the next digital economy"[7]

J Sai Deepak, a renowned Supreme Court Advocate has talked about how a privacy legislation is need of the hour for the country.

"Sai Deepak believes that codifying and legitimizing privacy in some way will start giving the legal apparatus certainty, as these issues continue to proliferate. The first draft need not be perfect, but it at least gives the nation something to work with, he asserts. He urges action, believing that as long as privacy continues to remain in air, these debates will continue to be academic.

Sai Deepak feels it is time to move fast on the legislative front because the multiple ramifications of privacy are becoming evident in our society today. He contends that privacy has largely been treated as an elitist issue, restricted to urban environments. As such, it's not seen as a livelihood issue and therefore is dismissed as being unimportant to the pressing needs of the country."[8]

PERSONAL DATA PROTECTION BILL, 2018

Supreme Court in the landmark judgment of *Justice K.S Puttaswami & another Vs. Union of India*[9] had asked the Government of India to frame legislation for protection of data. The government in turn formed a Committee of Experts under Justice Srikrishina which drafted the first draft bill for the data protection.

The bill comprises of 15 Chapters. It contains 112 Sections, 2 Schedules and 4 Recitals. The bill recognizes the right to privacy as a fundamental right. The bill also considers that protection of personal sensitive data is one of the basic essentialities of the informational privacy. The above concepts were discussed in the landmark judgment of *Justice K.S Puttaswami & another Vs. Union of India*.

The bill intends to provide protection of the personal data of an individual. The bill gives them certain rights that an individual shall enjoy autonomy over their personal data. The bill has discussed fair and reasonable processing by implying where the flow of data and processing of it is appropriate.

The bill also intends to create a relationship between the individual and the organizations which would use his data. The bill intends to create the relationship of trust between them. The bill also lays down the specific rights of the person for the protection of their data.

The bill also lays down various processing parameters for personal data. The bill for the first time discusses transnational transmission of data. It also talks about the accountability of the organizations who process data.

[7] Why India's Cyberlaw Must Rapidly Evolve www.inforisktoday.in, https://www.inforisktoday.in/interviews/indias-cyberlaw-must-rapidly-evolve-i-2617 (last visited Apr 15, 2020)

[8] Why India's Cyberlaw Must Rapidly Evolve www.inforisktoday.in, https://www.inforisktoday.in/interviews/indias-cyberlaw-must-rapidly-evolve-i-2617 (last visited Apr 15, 2020)

[9] WRIT PETITION (CIVIL) NO 494 OF 2012

The bill also creates a penal provision for punishment of unauthorized as well as unfair processing and usage of data. This is for the remedial purposes that a person might have in cases of the action stated above.

The bill also lays down provision for the establishment of a Data Protection Authority that shall overlook the activities of the processing of data.

Some of the **Key Definitions** are laid down under Section 3 of the Bill which include –

1. *"**Personal data** means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information;"*[10]
2. *"**Sensitive Personal Data** means personal data revealing, related to, or constituting, as may be applicable— (i) passwords; (ii) financial data; (iii) health data; (iv) official identifier; (v) sex life; (vi) sexual orientation; (vii) biometric data; (viii) genetic data; (ix) transgender status; (x) intersex" "status; (xi) caste or tribe;(xii) religious or political belief or affiliation; or (xiii) any other category of data specified by the Authority under section 22."*[11]
3. ***"Data principal** means the natural person to whom the personal data referred to in sub-clause (28) relates;"*[12]
4. ***"Data fiduciary** means any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data;"*[13]
5. *"**Processing** in relation to personal data, means an operation or set of operations performed on personal data, and may include operations such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction"*[14]

Section 2 of the Bill lays down the scope. The bill proclaims that the Act shall apply to all the personal data laid down under Section 3 which is collected or disclosed or shared or processed in India. The Act shall be applicable to every person under Indian law whether legal, artificial or living person. The Act shall also apply on foreign organizations if handle or process data in regard to the business carried in India or profile data principals in India.[15]

DATA PROTECTION OBLIGATIONS

Chapter II of the Bill deals with the Data Protection Obligations. The bill places certain obligatory provisions on the data fiduciaries in relation to the data they process. The bill talks about Fair and Reasonable Processing which simply means that the data shall only be processed for the causes which are crystal clear. This shall also mean that the purpose should be legal as well as clear and for which there shall be a reasonable expectation of the data principal. The Bill also talks about the limitation on storage which simply means that data shall only be stored for the time period it is

[10] Section 3(29), Personal Data Protection Bill 2019
[11] Section 3(35), Personal Data Protection Bill 2019
[12] Section 3(14), Personal Data Protection Bill 2019
[13] Section 3(13), Personal Data Protection Bill 2019
[14] Section 3(32), Personal Data Protection Bill 2019
[15] Section 2, Personal Data Protection Bill 2019

reasonably necessary for the cause it is stored for.

Section 8 under the Chapter lays down the provision for giving the Notice. Data Fiduciaries shall have to give notice to the data principal that shall contain different types of mandatory information. These requisites include-

1. Reason for Collection of Data.
2. Details of the Data fiduciary as well as the data protection officer which includes identity etc.
3. Data principal's right to withdraw his consent and the procedure of it.
4. Details of any transnational transmission of data.
5. Grievance Redressal Procedure.

Grounds for Processing of Personal Data

Chapter III of the Act deals with the grounds of processing of personal data.

The Act talks about consent. The consent here in after mentioned shall be free[16], informed, specific, clear and meaningful. The consent shall have the capability of withdrawal. The individual can withdraw their consent at their own will.

Section 13 of the Act gives power to the Legislative bodies – State Legislatures and Parliament to process the personal data if it is requisite for their functioning. The state shall also have the power under the Act to process the personal data so collected for any function that is authorized by the law.

The chapter also lays down several parameters that have to be satisfied to process personal data. These include-

1. Public Interest
2. To prevent or detect any illegal activity
3. Whistle blowing acts
4. To safeguard network as well as intelligence security

The above parameters are a few to name under the Act.

GROUNDS FOR PROCESSING OF SENSITIVE PERSONAL DATA

Chapter IV deals with the grounds that related to the processing of the sensitive personal data that is collected by the data fiduciary.

Chapter IV lays down under various sections what are the grounds where the processing of the sensitive personal data shall be done. It lays down that such data shall only be processed on the consent of the individual. It shall be processed to carry out functions of the state. It can be also done to execute the order of any court or tribunal or in compliance of the law. Personal Sensitive data can also be processed for situation that require immediate action.

The consent here in discussed shall be according to the Chapter III of the Act.

PERSONAL & SENSITIVE PERSONAL DATA OF CHILDREN

Chapter V of the Act deals with the personal and sensitive personal data of children.

Section 3(9) of the Act lays down the definition of child.

> *"Child" means a data principal below the age of eighteen years;*[17]

[16] Section 14, Indian Contract Act, 1872

[17] Section 3 (9)

The Act lays down safeguards to process personal data of the children. The act also lays down that during such processing, interest of the children shall be paramount.

Section 23 lays down that age verification and parental consent shall also be core to the processing of personal data of the children.
The act also lays down that the DPA (Data Protection Authority) under this act shall be empowered to notify the data fiduciaries that provide services to the children or collect their personal data that they are not allowed to profile, track or monitor the behavior or enable targeted advertising to the children or any data processing that may have the ability to cause harm or damage to the children.

RIGHTS OF DATA PRINCIPLES

Chapter VI of the Act lays down the rights of data principals.

1. Right to Confirmation and Access – Individual have the right to get to confirmation regarding the processing of data, summary of data which is going to be processed or is processed & summary of work that data fiduciary does.
2. Right to Correction of Information
3. Right to Data Probability- Individual can ask for personal data to be received in readable format or to be transmitted to other data fiduciary.
4. Right to be Forgotten- Individual has the right to restrict or deny the continued disclosure of data. The right has to be enforced through Adjudicating Officer. It shall only be applicable if the data fiduciary violates the right to free speech & right to have information of any individual,

TRANSPARENCY & ACCOUNTABILITY MEASURES

Chapter VII of the Act imposes several Transparency and accountability measures on the data fiduciary.

1. Implement policies to ensure safeguard of privacy and enabling it in all practices and systems
2. Take prudent steps to maintain transparency.
3. Notify Authority in case of data breach
4. Undertake DPIA(Data Protection Impact Assessment), Data Audit
5. Appoint DPA to carry out regulations mentioned under the Act
6. Make procedure and mechanism to carry out grievance redressal.
7. Implement security mechanism.

TRANSFER OF PERSONAL DATA OUTSIDE INDIA

Chapter VIII of the Act talks about cross border transfer of personal information. The act has talked about data localization as well as Trans national data transmission.

Section 40 talks about restrictions on trans national transmission of personal data.[18]
Section 41 of the Act talks about the conditions that are required for data transfer in cases of cross border transfer of personal data.[19]

This chapter talks about consent, contractual obligations, trans national transmission of data and central government powers and duties. The chapter also talks about effective law enforcement of existing laws as well as the act.

EXEMPTIONS

Chapter IX of the Act talks about certain situations where the provisions of the bill

[18] Section 40, Personal Data Protection Bill 2018

[19] Section 41, Personal Data Protection Bill 2018

wont apply. The provisions that shall not apply would for data processing in certain specific conditions.

Chapter lays down certain conditions or purposes where Chapter I to VIII will not apply –

1. Section 42 – Security of the State
2. Section 43 – Prevention, Detection, Investigation & Prosecution Of Contraventions of Law.
3. Section 44 – Legal Proceedings by Court or Tribunal.
4. Section 46 – Personal or Domestic Purposes
5. Section 47 – Journalistic Purposes.

It has to be noted that all sections under the above mentioned chapter will not apply except Section 4 and 31 of the Bill.

Above Mentioned exemptions aren't absolute and certain sections shall be exempted by the Data Protection Authority (DPA) for the Purposes of Research, Archiving or Statistics as laid down under Section 45. The Sections that shall be exempted include Section 4, 31 and 33.
Section 48 also talks about that above mentioned sections shall not be applicable for manual processing by entities which are small.

DATA PROTECTION AUTHORITY OF INDIA (DATA PROTECTION AUTHORITY OF INDIA)
Chapter X of the Bill talks about the composition and establishment of a Data Protection Authority.

Section 49 lays down the composition of Data Protection Authority.

Data Protection Authority of India shall include –

1. One Chairperson
2. Six Whole Time Members

These members shall be appointed by 3 member committee that shall comprise of

1. Chief Justice of India or any Judge of Supreme Court.
2. Cabinet Secretary
3. Expert in the field of Information Technology.

These members shall satisfy the condition of professional experience of at least 10 years.
Section 51 talks about their tenure and salaries. This provision also talks about ensuring integrity of the office.

1. Tenure – 5 years or 65 Years of age whichever is earlier;
2. Cannot hold office of government or any data fiduciary till 2 years of holding the above mentioned office.

Section 52 talks about the conditions of the removal of the members which include –

1. Insolvency
2. Physical or Mental incapacity
3. Moral Turpitude
4. Public Interest
5. Conflict of Interest

Section 60 to 66 provides Data Protection Authority Of India powers and functions.

1. Section 60 – Monitoring & Enforcement of the Act which includes – taking action in data breaches, monitoring data audit reports and trans national data transfers, spreading awareness, conducting enquiries with same powers as that of a civil court as

mentioned under Civil Procedure Code, 1908
2. Section 61 – Issue Codes of Practice
3. Section 62 – Issue directions or guidelines to data fiduciaries and make sure they are complied with.
4. Section 63 – Can ask data fiduciaries to give information.
5. Section 64 – To conduct inquiries in violation of the Act.
6. Section 65 – Take actions based on inquiry
7. Section 66 – Conduct search and seizure
8. Section 68 – Adjudication wing.

PENALTIES AND REMEDIES

Chapter XI of the Act lays down penalties and remedies for the violation of the provisions of the act.

1. 5 Crore rupees or 2% turnover for violations of data security and data audits.
2. 15 Crore Rupees or 4% turnover for violation under Chapter II to V
3. 10 Lakh rupees for violation under Chpater XI
4. 20 lakh rupees on failing to submit reports etc.
5. 2 crore rupees on non-complying with Authority directives.
6. Any data principal can seek compensation who suffered damages.

APPELLATE TRIBUNAL

Chapter XII of the Act talks about Appellate Tribunal.

Section 79 lays down that the composition and establishment of Appellate Tribunal lies with Central Government. The Appellate Tribunal shall hear any appeal from Adjudicating Officers or Authority.

Supreme Court of India shall hear the appeal against the order of the Appellate Tribunal.

OFFENCES

Chapter XIII of the Act talks about offences under the Act.

It also lays down that all offences shall be cognizable and non bailable and investigation shall be conducted in accordance with the CrPC 1973.

Following are offences-

1. To obtain, transfer or sell personal data.
2. To obtain, transfer or sell sensitive personal data.
3. To re identify and process deleted personal data.
4. Offences committed by State and Corporate Entities.

The Bill also contains some transitional provisions that contain the procedure that shall be followed if the act is enacted and in force. The act also aims to amend Information Technology Act, 2000 and shall omit 43A and give power to Central Government. The Act shall also amend Right To Information Act, 2005 to remove contrary provisions to the Bill.

COMPARISON BETWEEN EUROPEAN UNION'S GENERAL DATA PROTECTION REGULATION AND INDIA'S PERSONAL DATA PROTECTION BILL

European Union had passed a set of regulation back in 2016 and adopted it in April 2016. The European Union has adopted a resolution from 1995 which was an outdated data protection regulation. This data protection regulation aims and carries regulations that find requisite to be complied with for business to ensure protection of data

which is personal and privacy of the citizens of European Union for the transactions they do inside European Union member states. The regulation also aims to bring regulations towards the transmission of personal data outside the European Union member states.
The conditions mentioned under the General Data Protection Regulation (General Data Protection Regulation) are to be abided and same across the 28 European Union member states. A company will have to abide to General Data Protection Regulation and it will be in compliance with 28 European Union member states.

General Data Protection Regulation of European Union is one of the most admired and most widely accepted model law across the globe. Since it has wide scope, companies usually want that this should be the only data protection regulation compliance they should comply with. However, with different data protection regimes coming up for different countries it has become evident that there should be a model law. Hence, General Data Protection Regulation of European Union is considered as one of the model law.

Most of the Data protection regimes in the world have considered General Data Protection Regulation as one of the basic model laws for data protection. As such, most of them have been inspired and are off shoots of General Data Protection Regulation.

India's Personal Data Protection Bill 2019 has inspired itself from the General Data Protection Regulation of European Union more or less. With some of the basic model regulations same as that of General Data Protection Regulation. However there are certain regulations that beg to differ with the General Data Protection Regulation. Although the model law of Personal Data Protection Bill is same as that of General Data Protection Regulation and the aim is same with data protection for India yet it begs to differ at various provisions and gives a broader outlook towards evolving data protection regimes.

India's Personal Data Protection Bill differs at various levels and is discussed below under various heads-

JURISDICTION

General Data Protection Regulation of European Union applies to 28 European Union member states or process data form the European Union. General Data Protection Regulation shall also apply if the processing is done in the context of European Union. In context here means process personal data in respect of offering goods or services or collecting data from persons in European Union.

Personal Data Protection Bill of India has the same scope however the definition is broader with respect to General Data Protection Regulation. Personal Data Protection Bill includes an entity within its jurisdiction even if it uses a processor in India. A processor might be used by the company as 3rd party means.

However, PDBP under section 2(A) (c) gives powers to the central government to exempt such businesses or such processing activities. PDBP has a broader scope when it comes to jurisdiction, however, central government has wide authority regarding exemptions of certain provisions.

SUBJECT MATTER

While both of the data protection regimes deal with personal data, General Data Protection Regulation includes automated or non-automated processed data whereas Personal Data Protection Bill doesn't.

General Data Protection Regulation and Personal Data Protection Bill don't apply to personal data processed for personal uses as well as used by law enforcement agencies. However, Personal Data Protection Bill allows processing in the interest of investigation, prevention, detection or prosecution of any offense in the court of law while General Data Protection Regulation doesn't.

Personal Data Protection Bill gives wide set of powers to the Government. Personal Data Protection Bill also allows the central government to compel the disclosure of anonymous data collected that may or may not comprise of personal data.

DEFINITION OF PERSONAL DATA

General Data Protection Regulation talks about personal data as in the reasonable likelihood that the data might lead to identification of a natural person[20] whereas Personal Data Protection Bill defines personal data as data which would directly connect or indirectly identify an identifiable trait or attribute.

While General Data Protection Regulation on the other hand talks about flexibility in the scenario Personal Data Protection Bill doesn't.

General Data Protection Regulation also doesn't encapsulate whole data under personal data but only the one which attributes to identifiable features of the person. Personal Data Protection Bill on the other hand puts every data under personal data which may or may not be defined or derived or expressly within the scope of the definition.

Personal Data Protection Bill grants wide powers to the DPIA to lay out a definition of anonymization which may or may not broaden or the contrary narrow the scope of the definition of the above mentioned aspect.

DEFINITION OF SENSITIVE PERSONAL DATA

General Data Protection Regulation defines Sensitive Personal Data as the special categories of personal data which includes racial origin, political opinions, memberships, genetic data, health, sexual orientation etc.

Personal Data Protection Bill includes the above mentioned categories and it has an added category of financial data as well that includes credit cards, debit cards etc.

Personal Data Protection Bill also allows the government to consult with Data Protection Authority Of India to make additional categories of sensitive personal data.

RELEVANT PARTIES

General Data Protection Regulation names Controller as authority, agency or any other body that processes data. Processor who processes data and data subject as the one whose data is processed.

Personal Data Protection Bill on the other hand aligns with General Data Protection Regulation and names Controller as data

[20] Recital 26, General Data Protection Regulation

fiduciary, Processor as Data Processor and Data subject as Data Principal.

GENERAL PRINCIPLES

General Data Protection Regulation sets out its general principles as-

1. Lawfulness
2. Purpose
3. Data Minimization
4. Accuracy
5. Storage Limitation
6. Integrity and Confidentiality
7. Accountability[21]

On the other hand, Personal Data Protection Bill has very specific principles when it comes to lawfulness of processing. It lays down its general principles as –

1. Specific, clear and lawful purpose [22]
2. Fair and Reasonable manner.[23]
3. Connected to the Purpose [24]
4. Collected to the extent necessary for the purpose.[25]
5. Accuracy [26]
6. Non retention[27]
7. To comply[28]

When it comes to Personal Data Protection Bill, the general principles are very specific than General Data Protection Regulation and require accuracy to be assessed. Moreover, storage limitation provisions as compared to General Data Protection Regulation, Personal Data Protection Bill has more specific storage limitation provisions.

LEGAL BASIS TO PROCESS PERSONAL DATA

General Data Protection Regulation lays down six lawful basis to process personal data-

1. Consent
2. Performance
3. Legal Obligation
4. Interest
5. Life protection
6. Public interest.

Personal Data Protection Bill on the other hand includes the same 6 but adds the 7th basis as "reasonable purposes". Reasonable puposes include detection, prevention, investigation, whistleblowing, etc that shall be specified by the regulations.

Coming to health and safety Personal Data Protection Bill has narrow scope as compared to General Data Protection Regulation.

CONSENT

Personal Data Protection Bill mentions valid consent as –

1. Free
2. Specific
3. Informed
4. Clear
5. Capable of withdrawal.

Personal Data Protection Bill also lays down that data fiduciary can penalize the data principal if they withdraw the consent without any valid reason.[29]

The above are one of the major heads of comparison.

General Data Protection Regulation also talks about the processing when there is legitimate

[21] Article 5, General Data Protection Regulation
[22] Section 4, Personal Data Protection Bill 2019
[23] Section 5(a), Personal Data Protection Bill 2019
[24] Section 5(b), Personal Data Protection Bill 2019
[25] Section 6, Personal Data Protection Bill 2019
[26] Section 8, Personal Data Protection Bill 2019
[27] Section 9, Personal Data Protection Bill 2019
[28] Section 10, Personal Data Protection Bill 2019
[29] Section 11(6), Personal Data Protection Bill 2019

interest of the controller without consent of the person where they have to document the reasons. Personal Data Protection Bill permits Data Protection Authority Of India to specify what are the reasonable purposes which include public interest, reasonable expectations etc. In comparison, Personal Data Protection Bill has stringent provisions than General Data Protection Regulation when it comes to reasonable purposes. Data Protection Authority Of India has the power to define what reasonable purposes or legitimate interest would be.

When it comes to processing of sensitive personal data, General Data Protection Regulation and Personal Data Protection Bill align closely. Both have to rely on explicit consent. Data Protection Authority Of India can under Personal Data Protection Bill can say reasonable purpose for processing of sensitive personal data.

When it comes to children, General Data Protection Regulation lays down its consent age as 16 whereas Personal Data Protection Bill age of consent is 18. Personal Data Protection Bill is stringent when it comes to interests of the children as it requires verification of age before the consent is taken. Moreover, Personal Data Protection Bill includes automated and non-automated processes unlike General Data Protection Regulation.

When it comes to right of access, General Data Protection Regulation and Personal Data Protection Bill are broadly similar. Under both of them, personal data has to be provided free of cost.

When it comes to right of portability, General Data Protection Regulation and Personal Data Protection Bill are similar. Personal Data Protection Bill is broader as it isn't limited to processed under certain circumstances.

When it comes to right to be forgotten, Personal Data Protection Bill gives two right unlike General Data Protection Regulation – Erasure and disclosure of data and places the responsibility on Data Protection Authority Of India unlike General Data Protection Regulation who puts it on controller.

General Data Protection Regulation doesn't talk about DPA Registration whereas Personal Data Protection Bill does require significant data fiduciaries to register themselves with Data Protection Authority Of India. These shall inform Data Protection Authority Of India regard to volume, company revenue etc.

Personal Data Protection Bill requires all DPAs to submit their data protection impact assessment to the Data Protection Authority Of India for review which is not there under General Data Protection Regulation.

Personal Data Protection Bill requires a privacy to design policy which might relate to development of policies unlike General Data Protection Regulation which leaves it in the hand of controller to give flexibility.

Personal Data Protection Bill requires significant data fiduciaries to submit their audit to auditors who are approved by the Data Protection Authority Of India whereas General Data Protection Regulation contains no such requirements.

When it comes to Data Localization, General Data Protection Regulation has no

requirements for it. Personal Data Protection Bill on the other hand, talks about data localization of critical personal data in India by making and storing a copy of such data in India.

Personal Data Protection Bill has new provisions that ask data fiduciary to hand over the anonymized data to be de anonymized in consultation with Data Protection Authority Of India. General Data Protection Regulation has no such provision. Personal Data Protection Bill also brings Social Media Intermediaries under its ambit whereas General Data Protection Regulation doesn't.

General Data Protection Regulation authorizes National DPAs & EDPB to issue guidance which is non-binding. Personal Data Protection Bill on the other hand authorizes Central Gov. Central Government to make rules and intervene under Annex A. The central Government directions are binding.

The major difference that lies in General Data Protection Regulation & Personal Data Protection Bill is the application in relation to authorities. General Data Protection Regulation only applies to public entities. Different entities are subject to different framework as respect to their local laws.

Personal Data Protection Bill on the other hand is applicable to both private and public entities. Central Government can however exempt a public authority over various reasons which include sovereignty, security, public order etc. [30]

Although, Personal Data Protection Bill is based on the model law i.e. General Data Protection Regulation yet it differs on various grounds and brings out novel provisions in to the application which are game changing. Personal Data Protection Bill has contrasting features when it comes to grounds such as DPA registration, auditing etc.

Personal Data Protection Bill tries to bring out a change in the existing framework of India which has outdated data protection laws which aren't standalone or specific. Coming from that, Personal Data Protection Bill is definitely a revolutionary legislation.

CONCLUSION

Information Technology has been one of the most rapidly growing technology of the recent times. With everyday growing population that uses internet, Information technology has been one of the most used and relevant technologies of the current times. Information technology basically involves the transfer of data at the very basic level to the most complex advanced levels of communication one could ever witness. With the growth comes regulations. Data transferred over the medium or transmission media involves personal data too. In this era of Information Technology, it is quite evident that personal data has to be secured carefully. Certain efforts have to be made to secure your personal information.

The internet has opened numerous avenues for us and we use a lot of personal information or data on the internet for the companies to collect it and make it an identifier and use it commercially. Therefore, it is evident that there is a need to have a control over your personal data so collected

[30] Section 35, Personal Data Protection Bill 2019.

and be known about its use and its implication.

Since the ongoing era has seen the rise of various user generated computer systems, like social media, social networking and messaging platforms the amount of personal data that shall be stored in the computer networks has increased drastically. This cannot be simply confined to technological developments but due to the user generated computer platforms stated above.

Therefore, it is need of the hour that there should be stringent data protection mechanisms and policies for the protection of any kind of data. The policies should also determine what kind of security shall be given to different kinds of information.

A strong data protection regime can generate confidence into the system from the users, restrain malpractices and reduce exploitation of data. It is pertinent that governance policies are laid down domestically as well as internationally to make sure that individuals have rights to protect their data, strict regulations are made to be followed by the processing agencies that use personal data which includes state and corporate. A penal regulation is also needed so that a penalty can be imposed against those who breach these regulations and are ineffective in laying down the protections as per mentioned.

Supreme Court in the landmark judgment of Justice K.S Puttaswami & another Vs. Union of India had asked the Government of India to frame legislation for protection of data. The government in turn formed a Committee of Experts under Justice Srikrishina which drafted the first draft bill for the data protection.

General Data Protection Regulation of European Union is one of the most admired and most widely accepted model law across the globe. Since it has wide scope, companies usually want that this should be the only data protection regulation compliance they should comply with. However, with different data protection regimes coming up for different countries it has become evident that there should be a model law. Hence, General Data Protection Regulation of European Union is considered as one of the model laws.

Although, Personal Data Protection Bill is based on the model law i.e. General Data Protection Regulation yet it differs on various grounds and brings out novel provisions in to the application which are game changing. Personal Data Protection Bill has contrasting features when it comes to grounds such as DPA registration, auditing etc.

Personal Data Protection Bill tries to bring out a change in the existing framework of India which has outdated data protection laws which aren't standalone or specific. Coming from that, Personal Data Protection Bill is definitely a revolutionary legislation.

*****