Page 111 - 127 **DOI:** *https://doij.org/10.10000/IJLSI.111060*

INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 3 | Issue 5

2021

© 2021 International Journal of Legal Science and Innovation

Follow this and additional works at: https://www.ijlsi.com/

Under the aegis of VidhiAagaz – Inking Your Brain (https://www.vidhiaagaz.com)

This Article is brought to you for free and open access by the International Journal of Legal Science and Innovation at VidhiAagaz. It has been accepted for inclusion in International Journal of Legal Science and Innovation after due review.

In case of **any suggestion or complaint**, please contact **Gyan@vidhiaagaz.com.**

To submit your Manuscript for Publication at **International Journal of Legal Science and Innovation**, kindly email your Manuscript at **submission@ijlsi.com.**

Data Protection Regulations in India and The Significance of Consent Framework

BHARATH CHANDRAN P S[1]

ABSTRACT

As early as 1988, the UN Human Rights Committee, the treaty body charged with monitoring implementation of the International Covenant on Political and Civil Rights (ICCPR), recognised the need for data protection laws to safeguard the fundamental right to privacy recognised by Article 17 of the ICCPR.

Even though the 21st century has witnessed a tremendous increase in the use of the internet and other related services the laws governing the same were not up to mark. With the world concentrating in the cybersphere, there has been a constant need for legislations that were bound to protect the virtual rights of a person. As people tend to spend more time in the virtual space information has been generated and stored in the form of data.

Every activity we do in the digital sphere generates data, with or without our consent. Similarly, the generated data may be personal or non-personal data. Even with the huge amount of data being collected and processed there have been no specialized laws that focus on the protection of the data. The main question that arises in this regard is the nature of the data collected, the purpose for its collection, the duration for which the data is stored, which entities are provided access to the data, what is done with the data after the specified use and what are the measures in case of breach of these collected data. Countries have been trying to clarify the ambiguity surrounding them by proposing and implementing specialized laws that deal with the aspect of data protection. With the world witnessing a recent trend in the evolution of data protection laws, India has also taken the initiative to come into compliance with the global race by proposing legislation in accordance with the aspect of data privacy and protection.

One of the major factor to be considered is the importance of consent in upholding the digital privacy of a person. There have been several complications revolving around the concept of consent and some of them have been taken into consideration for the purpose of this research.

[1] LLM In IPR & Technology Law, Jindal Global Law School, India

© 2021. International Journal of Legal Science and Innovation [ISSN 2581-9453]

I. INTRODUCTION

Even though the 21st century has witnessed a tremendous increase in the use of the internet and other related services the laws governing the same were not up to mark. With the world concentrating in the cybersphere, there has been a constant need for legislations that were bound to protect the virtual rights of a person. As people tend to spend more time in the virtual space information has been generated and stored in the form of data. Every activity we do in the digital sphere generates data, with or without our consent. Similarly, the generated data may be personal or non-personal data. Even with the huge amount of data being collected and processed there have been no specialized laws that focus on the protection of the data. The main question that arises in this regard is the nature of the data collected, the purpose for its collection, the duration for which the data is stored, which entities are provided access to the data, what is done with the data after the specified use and what are the measures in case of breach of these collected data. Countries have been trying to clarify the ambiguity surrounding them by proposing and implementing specialized laws that deal with the aspect of data protection. With the world witnessing a recent trend in the evolution of data protection laws, India has also taken the initiative to come into compliance with the global race by proposing legislation in accordance with the aspect of data privacy and protection. One of the major factor to be considered is the importance of consent in upholding the digital privacy of a person. While detailed studies have dealt with data protection mechanisms all around the world, there have only been limited study with respect to the importance of consent for the protection of privacy and data of the individual in India. The data protection regulations around the world have laid emphasis on the consent for the purpose of collection and processing of data of the subjects. Even though the proposed legislation in India has been drafted incorporating the consent-based model which is in par with the other legislation revolving around data protection, there have been various criticisms regarding applicability of the model in the Indian legal space. The primary objective of my research would be focused on the importance of the consent framework in the protection of privacy and data of an individual in India. I shall also look into how the consent framework is taken into consideration in the European Union and also dive into the major ambiguities surrounding it. The main objective of this research is to show how the consent based model is best suited for the needs of India and recommend the steps that could be taken to improve the efficiency in the implementation of the consent framework in India.

II. DATA PRIVACY: THE CONCEPTUAL PERSPECTIVES

Privacy: Meaning and Concept

The idea of privacy has a very broad nature in terms of its significance. The concept of Privacy is difficult to determine because it is exasperatingly vague and ambiguous, often meaning strikingly different meanings to different

people.[2] Generally, the nature of Privacy lies in the exclusion of all others from the periphery of a particular individual, whereas, the basis of Privacy rests upon the protection of the 'inviolate personality' of human beings.[3] Although the privacy has an inherently broad nature, there are specific fields in which it is applicable like family privacy, workplace privacy and the emerging area of privacy in the cyberspace. The concept of privacy has become a major issue in the modern world owing to the advancements in the field of information and communications. The technological development that has evolved in the modern society without due regard for its impact on the democratic political system which has led to a condition that threatens to make privacy unachievable.[4]

The term privacy has been derived from the Latin word 'privatus' which means separated from the rest.[5] This simply means to be left alone. The term privacy has seen various implications in various contexts, it differs as per the culture of the people.[6] The meaning of privacy has changed with the change in time, historical concepts, the culture and the prevailing judicial philosophy.[7]

The concept of privacy is not an easy concept to be defined in just words, owing to the fact that its meaning and definition could change from time to time.

However, Privacy could be defined as "*an individual's rightful claim to determine the extent to which he wishes to share himself with others and his control over the time, place and circumstances to be engaged in communication with others, the right to indulge and to participate as he deems fit* ".[8]

III. DIFFERENT DIMENSIONS OF PRIVACY

Local Privacy

It can also be defined as the physical privacy. It mainly deals with the right of an individual to move around in public or private space without being identified tracked or monitored.[9] This conception of privacy includes the right of a person in solitude and the privacy in their own spaces such as office, home etc. [10]

Decisional Privacy

This type of privacy deals with the individuals personal preferences in both the private and public sphere. This concept mainly consists of sensitive information such as sexual preferences,

[2] Arnold Simmel, 'Privacy' (1968) 12 International Encyclopaedia of the Social Science, America: The Macmillan Company and The Free Press 480.
[3] Sangeeta Chatterjee & Dr. Rathin Bandyopadhyay, 'Confidentiality of Information as Right to Privacy: A Comparative Analysis of Indian, U.S. and British Laws' (2017) 1 International Journal of Judicial Sciences 1-16.
[4] S. K. Sharma, 'Privacy Law : A Comparative Study' (1994) Atlantic Publishers & Distributors 1
[5] Harinder Birring, 'An Unreasonable Intrusion Upon Person's Seclusion' (2019) 2 International Journal of Juridical Studies & Research 28.
[6] Sunita Khariwal, 'Parameters of Right to Privacy' (2013) 39 Indian Socio-Legal Journal 129-134.
[7] Ruth E. Gavison, 'Privacy and the Limits of Law'(2012) 89 The Yale Law Journal 421- 471.
[8] Dr.Sanjib Kumar Tiwari, 'Right to Privacy : The Role of Indian Judiciary' (2012) 3 JCC Law Review 10.
[9] Roger Clarke, 'Introduction to Dataveillance and Information Privacy, and Definitions of Terms' (1997) <http://www.rogerclarke.com/DV/Intro.html> accessed 1 June 2021.
[10]Racheal L.Finn, David Wright & Micheal Friedewald, 'Seven Types of Privacy'(2013) European Data Protection: Coming of Age <https://doi.org/10.1007/978-94-007-5170-5_1%3e %20 > accessed 1 June 2021

habits, religious and political views.[11] The people have the right to decide whether their thoughts and decisions are to be displayed in the public or not. This aspect plays a very important role with respect to a person's free will. Infringement of this would result in the curtailing of an individual's autonomy and freedom.[12]

Informational Privacy

Informational privacy mainly includes an individual's personal data such as name, email address, health data etc. An individual has the right to keep knowledge about what information the other person has and would like to maintain a control over that. With the world heading on to a more advanced technological space, the right of a person to be left alone has been much tampered with. Data can be used to identify any individual in the cyberspace. Informational privacy also includes the privacy of communication, that is the right to avoid any interception of personal communication including mail interceptions, telephone or wireless communication interception and access to email messages.[13]

International Character of Privacy

The concept of privacy is not new. The earlier version of privacy was very much limited to an individual's physical right to be left alone. When the world began to shift from a primitive to a more developed and civilized society the concept gained more importance and the social need for privacy has been equally realised in all societies simultaneously.[14] As the right to privacy achieved a wider and more universal sense, various international treaties and conventions included the need to protect the privacy of a person. All these rights have been framed in such a manner that it just includes the basic property of providing safeguards to the private life or the family life, the protection of home and non-interference with the correspondence.[15] The right to privacy assumed the international character with the inclusion of privacy in the Universal Declaration of Human Rights in the year 1948.[16]

Article 12 of the UDHR states that "*no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation and that everyone has the right to the protection of the law against such interference or attacks*."[17]

Though this right is recognised as of international importance in the recent period, the origin of this right is found in the origin of the idea of human rights, in the foundational principles of the British Magna Carta and this has been considered as one of the foundational principles of political democracy.[18] The right to privacy is a fundamental right that is recognized in other

[11] Finn, Wright & Friedewald (n 10)
[12] Clarke (n 9).
[13] Clarke (n 9).
[14] Chatterjee & Bandyopadhyay (n 3).
[15] Althaf Marsoof, 'The Right to Privacy in the Information Era: A South Asian Perspective' (2008) 5 Scripted 3 <https://ssrn.com/abstract=1578222> accessed 1 June 2021.
[16] Universal Declaration of Human Rights 1948 adopted and proclaimed by G.A. Res 217 A (III) December 10, 1948. UN Doc. A/810.
[17] Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR) art 12.
[18] Pierre Juvigny, 'Modern Scientific and Technical Developments and their consequences on the protection of the Right to respect for a person's private and family life, his home and communications,' (1978) Privacy and Human Rights, Manchester University Press 129.

international instruments such as the International Covenant on Civil and Political Rights (ICCPR)[19], European Convention on Human Rights and Fundamental Freedoms (ECHR)[20], the UN Convention on Migrant Workers[21], the UN Convention on Protection of the Child[22] and various other international and national treaties. In a report laid down by the United Nations, there are two major points that have been emphasised, regardless of national borders privacy safeguards should available and that there should be sufficient remedies available in case of violation of the right to privacy.[23] The right to privacy has been given the same importance as other fundamental rights.

This international character of privacy is based upon the idea of liberty and the concept of human rights.[24] However, it is at a much later stage that various countries have recognized the right to privacy as being fundamental.

IV. DATA PROTECTION: THE EVOLUTION AND SIGNIFICANCE

Internet and its importance in right to privacy have seen a tremendous increase in the latter half of the 20th century. This is mainly due to the advancements in the field of technology. The surveillance potential of powerful computer systems prompted demands for specific rules governing the collection and handling of personal information.[25] The term of data protection has been derived from the German word "Datenschutz".[26] It is a set of norms that serves a wider range of interest rather than simply the protection of the privacy of an individual, it can be more associated with freedom, autonomy and liberty in a modern societal concept.[27] The first type of data protection regulation in the modern world can be traced back to the Land Of Hesse in Germany in the year 1970.[28] There are two international instruments that play a crucial role in the development of data protection rules around the world, The Council of Europe's (COE) 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data[29] and the Organization for Economic Cooperation and Development's (OECD) Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data

[19] International Covenant on Civil and Political Rights 1966.

[20] European Convention for the Protection of Human Rights and Fundamental Freedoms (1950) ETS 5 < https://www.refworld.org/docid/3ae6b3b04.html > accessed 1 June 2021.

[21] International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families, Resolution 45/158 (1990).

[22] Convention on the Rights of the Child (1989) United Nations, Treaty Series, vol.1577, p.3, <https://www.refworld.org/docid/3ae6b38f0.html> accessed 1 June 2021.

[23] 'Report of the United Nations Special Rapporteur on the Right to Privacy', (A/ HRC/31/64) 8th March 2016.

[24] Chatterjee & Bandyopadhyay (n 3).

[25] David Banisar & Simon Davies, 'Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, And Surveillance Laws and Developments' (1999) 18 John Marshall Journal of Information Technology and Privacy Law 1.

[26] Jayanta Ghosh & Dr. Uday Shankar, 'Privacy and Data Protection Laws in India: A Right Based Analysis' (2016) October -December Bharathi Law Review 54.

[27] Arthur R Miller, 'The Assault on Privacy: Computers, Data Banks and Dossiers' (1971) 69 Michigan Law Review 1389.

[28] Bennett CJ, 'Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States- David H. Flaherty Chapel Hill: University of North Carolina Press, 1989, pp. xxiv, 483' (1990) 23 Canadian Journal of Political Science 605.

[29] 'Convention for The Protection of Individuals with

articulate specific rules covering the handling of electronic data[30]. Even though the various data protection regulations have prescribed different types of models, we can observe that the underlying principles have been the fundamental base of all these data protection regulations [31]:-

- Data should be obtained lawfully
- It should be used only for the specified purpose
- The data obtained should be correct and up to date
- The data should be made accessible to the data subject
- The data obtained should be kept secure
- It should be destroyed after the purpose is completed

With the growing importance of the protection of data, various countries have been trying to incorporate data protection laws in their existing legislations while many other countries have been trying to formulate new and updated legislation that focuses on the protection of data.

Privacy and data protection are distinct legal concepts under the English law but the analysis of the legislative data protection regime would illustrate that the policy makers have ignored their distinctness and viewed them as a single entity.[32] The need for a data protection regime has been viewed as essential due to the ever growing dependence and evolution of computers which resulted in the large scale processing of data.[33] The European Union's laws were not tailored to accommodate the advancements in technology. During the 1970 a committee on privacy was constituted under the chairmanship of Kenneth Younger, but it did not have the effect that the government had hoped for.[34] In response to the report submitted by this committee, the government had formulated plans to extend and improvise the principles regarding the protection of individuals information. This led to the formation of the Data Protection Act, 1984.[35] The law that had been existing in the EU did not have the ability to cater to the needs of this evolving technology. In the year 1998, the government repealed the existing Data Protection Act[36] and the 1998 Data Protection Act came into existence.[37]

This new legislation has been in accordance with the updated guidelines by the European Data Protection Directive.[38] When we glance into the

regard to The Automatic Processing of Personal Data Convention' (1981), Ets No.108 <http/www.coe.fr/eng/Legaltxt/108e.Html> accessed 1 June 2021.

[30] Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data (1981) < https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.html > accessed 1 June 2021.

[31] Banisar and Davies (n 25).

[32] Ashwini Sival & Ghulam Yazdani, 'Comparative Analysis of the Legal Framework Related to Data Protection in India USA and UK with special reference to inter country Problem of Outsourcing' (2017).

[33] Chris Reed & John Angel (Editors), 'Computer Law – The Law regulation of Information Technology'(6th Edn, Oxford University Press 2007).

[34] Reed & Angel (n 33).

[35] Data Protection Act 1984 c. 35 <http-/www.hmso.gov.uk/acts/acts1984/1984035.htm>

[36] DPA 1984 (n 35).

[37] Data Protection Act 1998 c. 29 <http/www.hmso.gov.uk/acts/acts1998/ 19980029.htm>

[38] European Union, Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 24 October 1995

jurisdiction of the European Union it is evident that the main piece of legislation that was in par with the technological developments was the Data Protection Act of 1998.[39] The act does not explicitly mention privacy but in practice, it provides a way in which the individuals can enforce control over the information that concerns them.[40] The act gave rise to a legal obligation to be followed by anyone that holds and process data. One of the major differences that the 1998 act had over the old data protection act of 1984 was that the principles that were laid down in the previous legislation were not mandatory. " There were eight basic principles upon which the Data Protection Act of 1998 was based upon:-

- Principle 1- Fair and Lawful- The information to be contained in personal data shall be obtained, and personal data shall be processed, fairly and lawfully
- Principle 2- Purposes- Personal data shall be held only for one or more specified and lawful purposes
- Principle 3- Adequacy- Personal data held for any purpose or purposes shall be adequate, relevant and not excessive in relation to that purpose or those purposes
- Principle 4- Accuracy- Personal data shall be accurate and, where necessary, kept up to date
- Principle 5- Retention -Personal data held for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes
- Principle 6- Rights- There shall be certain rights the individual is entitled to
- Principle 7- Security - Appropriate security measures shall be taken against unauthorized access to, or alteration, disclosure or destruction of, personal data against accidental loss or destruction of personal data
- Principle 8- International Transfers - Personal data should not be transferred outside the EU unless the country it is being transferred to can ensure adequate protection of the data in order to maintain the rights and freedoms of data subjects and their personal data." [41]

V. CURRENT LEGISLATION ON DATA PROTECTION IN INDIA

Even though India does not have a specialised data protection regulation as of now, it has incorporated the framework for the protection of data in the Information Technology (Amendment) Act of 2008.

Section 43-A: Compensation for Failure to Protect Data : The Act lays down that "*Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body*

<https://www.refworld.org/docid/3ddcc1c74.html> accessed 1 June 2021.

[39] DPA 1984 (n 35).

[40] Sival & Yazdani (n 32).

[41] Data Protection Act 1998 Schedule 1 Part I, < https://www.legislation.gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf > accessed 1 June 2021.

corporate shall be liable to pay damages by way of compensation to the person so affected."[42]

Section 72-A: Punishment for disclosure of information in breach of lawful contract: "*As otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of a lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both*."[43]

Even with these legislations governing the Indian cyberspace they had been heavily criticized for the fact that even though Indian technological space has evolved into a much-developed sphere the laws and regulations dealing with it has been of such a nature that it had been implemented at the onset of the internet era. This current legislation that provides the legal framework for privacy protection has been said to be ineffective and outdated, the need to implement a much stronger and stringent policy has been emphasised by the Supreme Court of India while deciding the Puttuswamy case.[44] For achieving the purpose of having a strong regulatory framework for data protection in India, a committee was constituted under the chairmanship of Justice B.N Srikrishna, which in turn led to the formulation of The Personal Data Protection Bill.[45] The significance of the regulatory bill in India would be discussed in detail in the coming chapters.

VI. UNDERSTANDING THE CONCEPT OF CONSENT

What is consent?

Consent can be defined as the voluntary acquiescence to the proposal of another person.[46] In simple words, it can be said to be the actual willingness of a person to do something. It is important to notice that the word consent can be seen in several legal scenarios.

Consent Under Contract Law

The Indian Contract Act mainly deals with provisions relating to types of contract, the essentials of a valid contract and many other provisions that deal with a contract.[47] Section 13 of the contracts act gives the definition of consent, it states that two or more persons are said to be in consent when they agree upon the same thing in the same sense.[48] If there is no consensus ad idem on the material terms of the contract, the contract is said to be void. In section

[42] The Information Technology (Amendment) Act 2008, s 43(A).
[43] Information Technology (Amendment) Act 2008, s 72(A).
[44] *Justice K.S. Puttaswamy (Retd) v Union Of India* [2017]10 SCC 1.
[45] Personal Data Protection Bill 2019 <http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf > accessed 1 June 2021.
[46] 'Consent', *West's Encyclopedia of American Law, Edn 2* (2008) < https://legal-dictionary.thefreedictionary.com/consent > accessed 1 June 2021.
[47] The Indian Contract Act 1872.
[48] The Indian Contract Act 1872 s.13.

14 of the act, free consent is defined. It states that the consent is said to be freely given when there is no scope of coercion, undue influence, fraud, misrepresentation or mistake.[49] So in order to satisfy the definition of a valid consent, these are to be taken into consideration.

Consent Under Criminal Law

In the area of criminal law, consent is used as a means of defence. There is no proper definition of consent in the criminal law. It generally means something that is done with intention or purpose. In the Indian Penal Code, we can observe that there is a section that deals with what does not amount to consent. Section 90 deals with *" Consent known to be given under fear or misconception —A consent is not such a consent as it intended by any section of this Code if the consent is given by a person under fear of injury, or under a misconception of fact, and if the person doing the act knows, or has reason to believe, that the consent was given in consequence of such fear or misconception;*

or Consent of insane person —if the consent is given by a person who, from unsoundness of mind, or intoxication, is unable to understand the nature and consequence of that to which he gives his consent; or

Consent of child—unless the contrary appears from the context, if the consent is given by a person who is under twelve years of age".[50]

Consent plays a very important role when it comes to criminal law, it decides the fact whether a person is innocent or criminal, for example, consent of a women over 18 years to an act of sexual intercourse makes it no offence, but without such consent, the act becomes very serious offence, that is, an offence of rape.[51]

Consent Under Data Protection

Personal information is an important currency in the new era. The monetary value of data is beyond anyone's expectation and the corporates of the world have been trying to harvest and benefit from it.[52] The corporates have viewed this as a source of income and have invested a huge deal of money in the software and technology that could be used to collect this information.[53] For keeping a check on these issues various countries have come forward with the legislations that protect the data of the individual. In this chapter, we are mainly focused on the data protection laws in the EU and India and the importance that consent of the data subject has to the data protection laws.

When we look into the data protection laws all around the world it is very much evident that the word "Consent" plays a very important role. The purpose of data processing is enormously dependent on the framework surrounding consent. If a data of an individual is processed by a data controller, the first question to be raised is whether the consent of the data subject was taken

[49] The Indian Contract Act 1872 s.14.
[50] The Indian Penal Code 1908 s.90.
[51] B.M Gandhi, '*Indian Penal Code'*, (4th Edn Eastern Book Company, 2017).
[52] Jennifer Sullivan & Christopher Jones, 'How Much Is Your Playlist Worth?' (WiredNews, March 1999) <http://www.wired.eom/news/technology/o,1282,32258,oo.html> accessed 1 June 2021.
[53] Paul M. Schwartz, 'Property, Privacy and Personal Data' (2004) 117 Harvard Law Review 2056.

or not. Once the data controller obtains the consent of the data subject he is free to process that data.[54] For the purpose of this research we would be dealing with consent under data protection and analysing the various consent mechanisms that have been integrated into the data protection frameworks mainly in India and the European Union.

VII. THE DATA PROTECTION FRAMEWORKS

The General Data Protection Regulation

The GDPR is the European Union's comprehensive data protection framework. It came into force on 25th May 2018 as an umbrella legislation to safeguard data privacy in the European Union.[55] The regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.[56]

The regulation has defined the term consent as "consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".[57] The regulation has given further conditions relating to consent and stresses on the specific provisions that should demonstrate records for proving consent from the data subject, the prominence and clarity of the consent requests, the right of the data subject to withdraw consent and whether the consent was freely given.[58] The EU GDPR has given great significance to the consent framework. It aims to give a high standard for consent. The consent being freely given is a very deciding factor under the GDPR for the lawful processing of personal data.

Consent generally means giving the data subject a genuine choice whether to accept or reject the terms and conditions and if the individual does not have a real choice then the consent is said to be invalid. The underlying factor is that people should be able to refuse consent without any detriment and withdraw their consent with ease at any time.[59] The GDPR is clear on the part that the consent should not be bundled up with any condition of service unless it is necessary to do so.[60] Recital 43 of the GDPR signifies that "Consent is presumed not to be freely given if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance".[61] A very detailed analysis of the GDPR with respect to the consent frameworks have been discussed in the coming chapters. However, this is not applicable in all cases there are at times the consent is valid even

[54] Rahul Mathan, 'Beyond Consent: A New Paradigm for Data Protection' (2017) <http://takshashila.org.in/wp-content/uploads/2017/07/TDD-Beyond-Consent-Data-Protection-RM-2017-03.pdf> accessed 1 June 2021.
[55] General Data Protection Regulation [2018] OJ L127/01.
[56] GDPR, Subject matter.
[57] GDPR Art 4(11).
[58] GDPR Art 7.
[59] Information Commissioner's Office, "What is a valid Consent?" <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/> accessed 1 June 2021.
[60] What is a valid consent? (n 59).
[61] GDPR Recital 43.

if it is bundled with a precondition the only factor is that the data controllers could provide a valid justification for this.

The Personal Data Protection Bill 2019

The Indian government after the landmark judgement in Justice KS Puttuswamy's case[62] appointed a committee under the Chairmanship of Justice B N Srikrishna to study and formulate a comprehensive data protection framework for India. This has led to the formulation of the Personal Data Protection Bill in India.[63] The bill has been deeply influenced by various data protection regimes in different jurisdictions especially the EU's GDPR and Asia-Pacific Economic Cooperation (APEC) Privacy Framework.[64] Currently the bill is under the consideration of the Joint parliamentary committee and is expected to come into existence in the near future.

The Personal Data Protection bill[65] is a robust legal framework which sets the procedure for the collection and use of personal information. The most important feature of this bill is it's wide scope of applicability. The PDP Bill contains provisions for the processing of personal data by the government, companies incorporated in India and foreign companies that deals with the personal data of individuals in India.[66] The bill proposes to set up an authority called 'Data Protection Authority' to protect the interests of data principals, prevent any misuse of personal data, monitor and ensure enforcement of the provisions of this Act and to promote awareness about data protection .[67]

The data fiduciary is under the obligation to ensure that the data collected and processed are accurate and stored only for the period necessary for satisfying the purposes of data collection and also will be accountable for all compliance requirements under the bill.[68] The law also provides that data fiduciaries could only retain and use the collected data until the purpose of collection have been met.[69] The bill also provides an detailed analysis on the rights that are available to the data principal.[70] The data principal can ensure that the data that have been collected on them has been processed and if processed, a summary of the processing that have been undertaken should be made available to the data principal on their request.[71] The data principals have been given the right to complete their data, update or correct data that have been undertaken for processing.[72] Another important feature that the data principal is entitled is the right to portability, it means that if the data has been processed by automated means, the data subject is entitled to receive the processed data in a structured and commonly used format that could be understood.[73] There are provisions under the act that enables the data principal to

[62] *Justice K.S. Puttaswamy (Retd*) (n 44).
[63] PDP Bill 2019 (n 45).
[64]Alex Wall, 'GDPR Matchup: The APEC Privacy Framework and Cross-Border Privacy Rules' (2019) <https://iapp.org/news/a/gdpr-matchup-the-apec-privacy-framework-and-cross-border-privacy-rules/. > accessed 1 June 2021.
[65] PDP Bill 2019 (n 45).
[66] PDP Bill 2019 (n 45).
[67] PDP Bill 2019 Chapter IX.
[68] PDP Bill 2019 s.8.
[69] PDP Bill 2019 s.9.
[70] PDP Bill 2019 Chapter V.
[71] PDP Bill 2019 s.17.
[72] PDP Bill 2019 s.18.
[73] PDP Bill 2019 s.19.

prevent or restrict further processing of their data under certain conditions.[74] The data fiduciaries are under obligation to prepare a privacy by design policy that would enable them to foresee errors and flaws in their security and privacy measures in order to ensure that the data that are collected would be secure.[75]

The provisions laid down in the bill clearly indicate the power of the central government to exempt any of its agencies from the application of this act.[76] The bill also lays down provisions for exemptions of class of research, archiving, or statistical purposes from the application of any of the provisions of this Act.[77] On implementation, it will apply to all enterprises across India other than those specifically exempted and this would include any enterprise that uses automated means to collect data.[78]

This legislation in India therefore adopts a comprehensive data protection mechanism that would successfully monitor and regulate the collection and processing of personal data. It not only sets obligations on the data fiduciaries but also gives the data principals certain rights that would help in the betterment of this legal framework.

The Consent Framework in India

The most important principle that has been envisaged in the Indian data protection framework is the requirement of consent of the data principal. For any data fiduciaries that are collecting and processing personal data it is absolutely important to note that unless free, informed and specific consent is obtained they are barred by law to process such data. The framework does not define the word consent as such, but it states that consent means consent referred to under section 11 of the act.[79] Under the provision, it is given that the personal data shall not be processed by the data fiduciary unless consent is given by the data principal.[80] The bill explicitly mentions when the consent given by the data principal shall be valid and notes down various prerequisites to be followed by the data fiduciary for the legal processing of data.

"*Under this framework it is given that the consent of the data principal shall not be valid, unless such consent is*—

(a) free, having regard to whether it complies with the standard specified under section 14 of the Indian Contract Act, 1872

(b) informed, having regard to whether the data principal has been provided with the information required under section 7;

(c) specific, having regard to whether the data principal can determine the scope of consent in respect of the purpose of processing;

(d) clear, having regard to whether it is indicated through an affirmative action that is meaningful in a given context; and

(e) capable of being withdrawn, having regard to whether the ease of such withdrawal is

[74] PDP Bill 2019 s.20.
[75] PDP Bill 2019 Chapter VI.
[76] PDP Bill 2019 s.37.
[77] PDP Bill 2019 s.38.
[78] PDP Bill 2019 s.39.
[79] PDP Bill 2019 s.3(10).
[80] PDP Bill 2019 s.11(1).

comparable to the ease with which consent may be given." [81]

The bill also aims to categorize certain data as 'sensitive personal data'[82], and special position is given to them while undergoing data processing. The sensitive data's can only be processed by the data fiduciaries by informing the data principal of what sensitive data may be processed and should obtain specific consent for it.[83] The PDP bill also lays down strict provisions for the data fiduciaries for processing of personal data and sensitive personal data of children.[84] The law provides that while processing data that are related to children the data fiduciaries are required to verify the age of the child and obtain specific consent from the parents or legal guardian before collection and processing of these data.[85] It is evident that there has been a certain provision in the law that includes data to be processed even without consent. This includes processing by the state[86], by data fiduciaries for employment purposes[87] and other purposes the central government may deem fit.[88]

The legislation makes it crystal clear that the data fiduciaries cannot exploit the data principals on the claim of bundled conditions, even if the data principal does not consent to a type of data being processed, the data fiduciaries cannot use them to lower the performance of the service that has been promised.[89] The proposed legislation also includes that in case of any discrepancies the burden of proof to show that the data principal has given the consent would be on the data fiduciary.[90] It is interesting to note that the proposed bill has made consent an important factor that would give the data principal more control over their data. By giving consent to what data is shared there is a significant possibility that the gap that exists between the data principles and data fiduciaries would be reduced.

VIII. IS THE CONSENT-BASED MODEL THE RIGHT APPROACH FOR INDIA ?

Comparative Analysis of the Consent Model

European Union's GDPR has been known to be the benchmark model when it comes to a data protection framework. It has been known to address several known and also potential issues that may arise in the near future.[91] The Indian data protection framework has been drafted taking into consideration various existing data protection regimes all around the world. While analysing the PDP bill it is clear that the committee has followed a very similar framework that completely resonates the European law.[92] The Srikrishna committee report has specifically mentioned that the importance of notice and consent, they were of the view that

[81] PDP Bill 2019 s.11(2).
[82] PDP Bill 2019 s.3(36).
[83] PDP Bill 2019 s.11(3).
[84] PDP Bill 2019 s.16.
[85] PDP Bill 2019 s.16(2).
[86] PDP Bill 2019 s. 12.
[87] PDP Bill 2019 s. 13.
[88] PDP Bill 2019 s. 14.
[89] PDP Bill 2019 s.11(4).
[90] PDP Bill 2019 s.11(5).

[91] 'India's Personal Data Protection Bill vs. GDPR'(oneDPO, 10 December 2020) <https://www.onedpo.com/indias-personal-data-protection-bill-pdp-vs-gdpr > accessed 1 June 2021.
[92] Deva Prasad & Suchithra Menon, 'The Personal Data Protection Bill, 2018: India's regulatory journey towards a comprehensive data protection law' (2020) 28 International Journal of Law and Information Technology 1–19.

"the notice and choice framework to secure an individual's consent is the bulwark on which data processing practices in the digital economy are founded."[93]

The consent based approach that has been an integral part of the PDP bill is inspired form the GDPR framework. As discussed in the previous chapters, provisions relating to the need for consent has been the foundation under which processing of data would take place. Both the framework requires that the withdrawal of the consent by the data subject/ data principal should be as easy and hassle-free as giving the consent. The language under which the consent framework in PDP is given is much more comprehensive than under the GDPR and offers much more clarity on the issue that may arise if the data principal withdraws consent without taking proper measures. The consent requirement for processing of personal data is very much identical in both the framework, for sensitive personal data the PDP prescribes the need for specific consent. It has included various additions to the consent mechanism in GDPR, these include the availability of multiple languages and the inclusion of any other information that the authority may deem fit.[94] There has also been the introduction of a 'consent manager' in the Indian framework. A consent manager may be a data fiduciary whose main responsibility is to assist the data principals in managing their consent.[95] Thus when the data principal needs to exercise their rights regarding the confirmation, correction, updation or to withdraw the consent, they can either directly or with the help of this consent manager do such tasks.[96]

Major Drawbacks in the Consent Model

The significance of the consent based model has been widely accepted and India has drafted its data protection framework taking into consideration this acceptance. The consent from an individual has been one of the most important factors that facilitates the collection and use of data by the data processing entities. However, in a country like India the effectiveness of the consent based model have begun to raise doubts. The committee report by Justice Srikrisha has also taken a note of how the consent in the modern world of internet seems to be broken.[97] The report goes on to say that consent forms is a very complex in nature, "*Consequently, individuals do not read them; even if they attempt to, they might not understand them; even if they understand them, provisions to give meaningful consent in a granular fashion are absent"*.[98] Even though the committee reports clearly states the consent based model has been followed

[93] "Report of the Committee of Experts under the Chairmanship of Justice B N Srikrishna," (India: Ministry of Electronics & Information Technology, Government of India, July 27, 2018) <https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf. > accessed 1 June 2021.

[94] India's Data Protection Bill vs. GDPR (n 91).

[95] 'Personal Data Protection Bill, 2019: Considering Consent And Offences' (MEDIANAMA, 29 January 2020) <https://www.medianama.com/2020/01/223-pdp-bill-2019-consent-and-offences-views/> accessed 1 June 2021.

[96] Personal Data Protection Bill,2019: Considering Consent and Offences (n 95).

[97] Report of the Committee of Experts under the Chairmanship of Justice B N Srikrishna, (n88).

[98] B. W. Schermer, 'The crisis of consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection' (2014) 2 Ethics and Information Technology 16.

taking into considerations all these lacunas, they have not been able to pinpoint the changes they have taken to effectively enable this model.

In India where the digital literacy may be found to be low, the consent based approach may face some difficulties especially when the corporate entities would follow an approach of take it or leave it method while formulating their privacy policies.[99] Another major drawback that could be expected is over dependence on the mechanism of consent which may led to consent fatigue. In the previous times when we consent to the collection and use of our data, it is expected to be in a static environment but that is not the case today, the technologies have become interoperable and the data that is collected may pass through various entities which would be hard to keep track of.[100]

In the case of the Internet of things and the new technologies, the effectiveness of the consent model is very much under doubt. " *Many IoT devices do not have screens and communication with users and rely instead on lights or sounds or haptic feedback; text notifications to mobile phones may also be leveraged in the absence of direct device feedback occasioned by the desire to create aesthetically pleasing devices, which may in turn result in opacity about device functionality."*[101] The use of IoT enabled devices by the technology giants would hinder the smooth functioning of the consent mechanism and in turn would disrupt the collection of data and complicate the data protection framework.[102] Indian legislation does not require consent for the collection of non-personal data, with the rise of Artificial intelligence and machine learning, it has been possible to link these non-personal data and convert them to personal and sensitive personal data.[103] This would in turn led to a situation where the mechanism that has been adopted may seem to be inadequate and ineffective against the transforming technologies.

Suggestions & Recommendations

The immediate need and importance of a robust data protection framework in a jurisdiction like India had led to the drafting of the Personal Data Protection Bill 2019. The bill have been known to integrate various importance features that are absolutely necessary for a diverse country like India, however in the previous chapter we have discussed in detail the various drawbacks that have been arisen out of it. One of the major drawback that have been widely criticised is the effectiveness of the consent model in a country like India. For such a framework to be effective in India, it is important to note that the awareness about the consent in data protection and privacy should be given utmost importance. The consent model that have been incorporated in our upcoming data protection regulation would indeed make the citizens have more control over

[99] Ananth Padmanabhan and Anirudh Rastogi, 'Big Data' in Davesh Kapur and Madhav Khosla (eds), Regulation in India: Design, Capacity and Performance' (Hart Publishing 2019) 251.
[100] Mathan (n 54).
[101] Lachlan Urquhart & Tom Lodge, 'Demonstrably Doing Accountability in the Internet of Things' (2019) 27
International Journal of Law & Information Technology 27.
[102] Prasad & Menon (n 92).
[103] Mathan (n 54).

the data that is shared to the data controllers. However one of the major problems that the consumers face is the complex and not so user friendly terms and conditions and privacy policies that the various companies have hosted in their websites. A normal person would not tend to read all these documents before consenting to avail the service. For the consent model to be implemented in a more effective manner the companies should be mandated under law to provide easy and clear privacy policies that would be not lead to confusions or unnecessary hardships to the customer using their services.

Another important aspect is that the citizens of the country should be made more aware of the rights that have been vested with them by these regulations. Without making the citizens aware of these rights it is impossible to achieve the purpose for which these data protection framework have come into existence in the first place. Considering the circumstances in India where many major legislations have been outdated with respect to the advanced technological growth, there should be a constant monitoring system by which all the legislations that play a crucial role in the cyberspace should updated and be kept in pace with the advancement of technology. The consent framework in the PDP bill which has not yet been implemented in the Indian legal space should come into existence considering the advent of new technologies such as the Internet of Things and should be able to identify and overcome the obstacles relating to these new technologies.

IX. CONCLUSION

The modern world have witnessed a widespread and tremendous growth in the field of technology. Looking back to a few years the major difference we could note is that today's technology have been evolving at a much faster pace. The legislations that have been undertaken to curtail and regulate these fast moving technologies have not been able to achieve its purpose. This has been mainly due to the delay in implementing the laws and when such laws are implemented the technologies would be far more complex and advanced for these laws. The present pandemic situation all around the world has led to a situation that calls for an even higher dependence on internet and related its technologies. Students all around the world have been pursuing their education through online mediums, the daily work and other activities of the people have been just limited to the cyber space. While the whole world is engaged in all these activities, the need for the protection of the people and their data online has reached paramount importance. This is where the purpose of privacy and data protection laws comes into existence.

Various countries around the globe have been successful in implementing and regulating measures that enable a sophisticated protection of the data and privacy of their citizens. In the case of India, the framework for the protection of the data have been drafted and is still under the consideration of the Indian Parliament. Even though India has been late to this aspect and that the framework data protection is yet to be implemented, it could be said that the provisions

included in the bill been well drafted after considering the conditions of the country. The main framework that deals with the consent in the bill has been prone to criticisms by various experts stating that the digital literacy of our country is very low and is not possible in a country like India. However, I am of the opinion that the consent based model would empower the citizens with more control over their data. The government should implement measures to ensure that the citizens are well aware of their power and rights when it comes to data sharing and the protection from illegal processing. This regulation should be more concentrated towards the data fiduciaries and strict and efficient means should be deployed to ensure that the data fiduciaries operate in compliance with the regulatory framework. It is very important to note that even after implementing the said legislations, there should be timely and prominent updates to these legislation in order to make it compactable with the ongoing and upcoming technological advancements.

*****