Page 2136 - 2152

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 3 | Issue 4

2020

From Privacy to Data Protection in India: Evaluating the Personal Data Protection Bill, 2019

SAMEER KUMAR DWIVEDI[1]

ABSTRACT

The concept of Privacy is a widely accepted legal and moral notion all over the world except for some nations where it has uncertain legal and philosophical foundations and legal backing. In India itself, the much-awaited Personal Data Protection Bill is pending and the Present legal frameworks, such as the IT Act, The Telegraph Act, other Statutes and rules related to this issue are inadequate, in this modernized environment traditional moral concepts such as no intrusion theory and the freedom to act theory, are unable to protect the privacy of an individual. The control of information theory and the undocumented personal knowledge theory are philosophically better accounts but are open to counterexamples. A restricted access theory of privacy is developed and defended but it does not provide any assurance against the state or big players, we cannot say that present legal protections can provide full proof data security in this digital era. So, we need full proof security against all kinds of intrusion in our privacy.

KEYWORDS: *Privacy, Monitoring, Data Protection, Personal Data, PDP Bill 2019.*

I. INTRODUCTION

The concept of privacy has played a large role in legal discussions and judgments during the last century all over the world including India. Privacy is understood in this context as "liberty or freedom to act in personal matters". To understand better how the concept of privacy is philosophically connected in constitutional law we have lots of precedents all over the world by constitutional courts. Data protection is a necessity, it becomes more obvious when the amount of data created and stored continues to grow at an unprecedented rate, coupled with exploitation and mishandling of such data by tech companies and giant service providers e.g. Google, Amazon and other social networking websites and digital service providers without the consent of the individual. The right to privacy is widely acknowledged and well-supported in civilized countries including India and the United States. Many familiar legal and ethical arguments pivot on an appeal to the right to privacy. A charge that a government, a corporation,

[1] Author is a Research Scholar at School of Law & Governance, Central University of South Bihar, Gaya, India. **Sameer Kumar Dwivedi**, thanks **ICSSR, New Delhi** for financial support by awarding **Short-term** Contingency Grant.

 [ISSN 2581-5369]

or an individual has invaded someone's privacy is regarded as a serious matter. The concept of privacy seems so obvious, so basic, and so much a part of our social values, that there may seem to be little room for any philosophical misgivings about it. However, substantial philosophical controversy about the nature of privacy exists. The philosophical debate focuses largely on two major questions: What is privacy? and Can the right to privacy be philosophically justified?[2]

This paper will try to answer these questions as well as all other questions related to this. To safeguard the data available with various agencies, and to curb the trade in data without the user's consent, the Personal Data Protection (PDP) Bill was drafted. This Bill was introduced in the Lok Sabah on December 11, 2019, and pending before the Joint Parliamentary Committee for scrutiny. This Bill was introduced with a futuristic aim to protect the personal data of the individual, to lays down the guidelines and rules for the utilization of data, and to the established data protection authority. In recent, the litigation history of the data protection regime in India can be formally traced back to the petition filed before the Hon'ble Supreme Court by Retired Justice K.S. Puttaswamy. The court has in its a landmark judgment held that *the right to privacy* is protected as

"an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution"[3].

In **K.S. Puttaswamy v Union of India**[4], the Court read the right to privacy to be a fundamental right but with reasonable restrictions, such as

(i) existence of law (ii) legitimate state aim (iii) proportionality.[5]

According to the judgment, the Supreme Court also directed the government to form a data protection law to address the concerns related to privacy in the digital age.

A committee of experts headed by the Justice B.N. Srikrishna, was set up to assess the current scenario of data protection in India, recommend ways to tackle the problems surrounding it and draft a data protection bill, a bill was presented in the year 2018 but after various criticism bill

2 James H. Moor, *The Ethics of Privacy Protection*, (June 2, 2020) https://www.researchgate.net/publication/32961262_The_Ethics_of_Privacy_Protection?enrichId=rgreq9be4abcf1cf8a9d3fe07f736fd6225c2XXX&enrichSource=Y292ZXJQYWdlOzMyOTYxMjYyO0FTOjEwMzA5NTQ2Mzg0MTc5N0AxNDAxNTkxMjgyODE5&el=1_x_2&_esc=publicationCoverPdf

3 Jyoti Panday, *India's Supreme Court Upholds Right to Privacy as a Fundamental Right—and It's About Time,* DEEPLINK BLOG, (June 2, 2020). https://www.e.org/deeplinks/2017/08/indias-supreme-court-upholds-rightprivacy-fundamental-right-and-its-about-time.

4 (2017) 10 SCC 641

5 Sinha Amber, *comments to the personal data protection Bill 2019*, THE CENTRE FOR INTERNET & SOCIETY (CIS), (June 2, 2020). https://cis-india.org/internet-governance/blog/comments-to-the-personal-data-protection-Bill-2019.

 [ISSN 2581-5369]

was later presented in 2019 again. This time Bill includes several modifications and changes in scope and intent for creating a framework for "organizational and technical measures" of data processing, introduce "accountability of entities processing personal data", and lay down norms for social media intermediaries and cross border transfer[6].

II. THE CONCEPT OF PRIVACY: A PHILOSOPHICAL LOOK

The concept of privacy has been analyzed extensively by contemporary philosophers. Philosophers, like everyone, have been struck by the broad dissemination and the forceful impact of information technology during the last few decades. Therefore, it is not surprising that most contemporary philosophical accounts of privacy tie it closely to the concept of information. Although control of information is an aspect of privacy, these definitions emphasizing control are inadequate for there are many situations in which people have no control over the exchange of personal information about themselves but in which there is no loss of privacy. Consider some examples[7] Philosophers have offered a variety of justifications of privacy as an important value. Stanley Benn suggests that privacy is grounded in respect for persons. As Benn puts it: "To respect someone as a person is to concede that one ought to take account of how his enterprise might be affected by one's own decisions." This type of justification for privacy is both popular and at least initially plausible. One problem with giving respect for persons as a justification for privacy is that it does not distinguish between times in which privacy is justified and times in which it is not. Apart from PDP Bill, 2019 we have some other laws and regulations to answer the issue related to privacy that are

III. PRESENT REGULATORY FRAMEWORK

In absence of a dedicated data protection legislation India is trying to answer the problems related to this issue by using available law and regulation enacted time to time to answer these type of problem, we will try to evaluate the available laws, rules, and regulation and will also assess the usefulness of these laws, this study will help to disclose whether we need a new law especially dedicated to protecting the personal data and privacy of an individual or the available legislation and provisions are sufficient in this regard.

A. PRIVACY AND DATA PROTECTION LEGISLATION

In the absence of specific legislation, data protection is achieved in India through the enforcement of privacy rights based on a patchwork of legislation, as follows.

6 The Personal Data Protection Bill,2019, s. 26 & 33.
7 Ibid 1

(i) THE INFORMATION TECHNOLOGY ACT (2000) (IT ACT) AND THE INFORMATION TECHNOLOGY (AMENDMENT) ACT 2008[8]

The IT Act contains provisions for the protection of electronic data. The IT Act penalizes 'cyber contraventions' (Section 43(a)–(h)), which attract civil prosecution, and 'cyber offenses' (Sections 63–74), which attract criminal action.

The IT Act was originally passed to provide legal recognition for e-commerce and sanctions for computer misuse. However, it had no express provisions regarding data security. Breaches of data security could result in the prosecution of individuals who hacked into the system, under Sections 43 and 66 of the IT Act, but the Act did not provide other remedies such as, for instance, taking action against the organization holding the data. Accordingly, the IT (Amendment) Act 2008 was passed, which, inter alia, incorporated two new sections into the IT Act, Section 43A and Section 72A, to provide a remedy to persons who have suffered or are likely to suffer a loss on account of their personal data not having been adequately protected.

(ii) THE INFORMATION TECHNOLOGY RULES (THE IT RULES)

Under various sections of the IT Act, the government routinely gives notice of sets of Information Technology Rules to broaden its scope. These IT Rules focus on and regulate specific areas of collection, transfer, and processing of data, and include, most recently, the following:

a. the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules,[9] which require entities holding users' sensitive personal information to maintain certain specified security standards;

b. the Information Technology (Intermediaries Guidelines) Rules,[10] which prohibit content of a specific nature on the internet, and an intermediary, such as a website host, is required to block such content;

c. the Information Technology (Guidelines for Cyber Cafe) Rules,[11][5] which require cybercafés to register with a registration agency and maintain a log of users' identities and their internet usage; and

d. the Information Technology (Electronic Service Delivery) Rules,[6] which allow the government to specify that certain services, such as applications, certificates, and licenses,

[8] IT Act and Rules (Aug 12, 2020) meity.gov.in/content/cyber-laws.
[9] meity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf.
[10] meity.gov.in/sites/upload_files/dit/files/GSR314E_10511(1).pdf.
[11] meity.gov.in/sites/upload_files/dit/files/GSR315E_10511(1).pdf.

 [ISSN 2581-5369]

be delivered electronically.

The IT Rules are statutory law, and the four sets specified above were notified on 11 April 2011 under Section 43A of the IT Act.

Penalties for non-compliance are specified by Sections 43 and 72 of the IT Act.

The IT Rules define personal information as any information that relates to a natural person that, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such a person.

Further, the IT Rules define 'sensitive personal data or information' as personal information consisting of information relating to:

a. passwords;

b. financial information, such as bank account, credit card, debit card or other payment instrument details;

c. physical, physiological and mental health conditions;

d. sexual orientation;

e. medical records and history;

f. biometric information;

g. any details relating to the above clauses as provided to a body corporate for the provision of services; or

h. any information received under the above clauses by a body corporate for processing, or that has been stored or processed under lawful contract or otherwise.

Provided that any information is freely available or accessible in the public domain, or furnished under the Right to Information Act 2005 or any other law for the time being in force, it shall not be regarded as sensitive personal data or information for these rules.

B. ADDITIONAL LEGISLATION

In addition to the legislation described above, data protection may also sometimes occur through the enforcement of property rights based on

1. the Copyright Act (1957)
2. the Code of Criminal Procedure (1973)
3. the Indian Telegraph Act 1885
4. the Companies Act (2013)

 [ISSN 2581-5369]

5. the Competition Act (2002)
6. the Consumer Protection Act (2019) in cases of unfair trade practices are also relevant

Finally, citizens may also make use of the common law right to privacy, at least in theory – there is no significant, recent jurisprudence on this.[12]

C. COMPLIANCE REGULATORS

(i) CERT-IN

Under Section 70B of the IT (Amendment) Act 2008, the government constituted CERT-In, which the website of the Ministry of Electronics and Information Technology refers to as the 'Indian Computer Emergency Response Team'. CERT-In is a national nodal agency responding to computer security incidents as and when they occur. The Ministry of Electronics and Information Technology specifies the functions of the agency as follows:

a. collection, analysis, and dissemination of information on cybersecurity incidents;

b. forecast and alerts of cybersecurity incidents;

c. emergency measures for handling cybersecurity incidents;

d. coordination of cybersecurity incident response activities; and

e. issuance of guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response to and reporting of cybersecurity incidents.[7]

(ii) CYBER REGULATIONS APPELLATE TRIBUNAL (CRAT)

Under Section 48(1) of the IT Act 2000, the Ministry of Electronics and Information Technology established CRAT in October 2006. The IT (Amendment) Act 2008 renamed the tribunal Cyber Appellate Tribunal (CAT). Under the IT Act, any person aggrieved by an order made by the Controller of Certifying Authorities, or by an adjudicating officer under this Act, may prefer an appeal before the CAT. The CAT is headed by a chairperson who is appointed by the central government by notification, as provided under Section 49 of the IT Act 2000.

Before the IT (Amendment) Act 2008, the chairperson was known as the presiding officer. Provisions have been made in the amended Act for CAT to comprise of a chairperson and such several other members as the central government may notify or appoint.[8]

12 Aditi Subramaniam & Sanuj Das, The Privacy, Data Protection and Cybersecurity Law Review - Edition 6 ,218, (June 22, 2020) https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-6/1210048/india

 [ISSN 2581-5369]

D. SPECIFIC REGULATORY AREAS

1. FINANCIAL PRIVACY

i) PUBLIC FINANCIAL INSTITUTIONS (OBLIGATION AS TO FIDELITY AND SECRECY) ACT 1983[13]

Under this Act, public financial institutions are prohibited from divulging any information relating to the affairs of their clients except by laws of practice and usage.

ii) THE PREVENTION OF MONEY LAUNDERING ACT 2002[14]

The Prevention of Money Laundering Act (PMLA) was passed in an attempt to curb money laundering and prescribes measures to monitor banking customers and their business relations, financial transactions, verification of new customers, and automatic tracking of suspicious transactions. The PMLA makes it mandatory for banking companies, financial institutions and intermediaries to furnish to the Director of the Financial Intelligence Unit (under the PMLA) information relating to prescribed transactions, and which can also be shared, in the public interest, with other government institutions or foreign countries for enforcement of the provisions of the PMLA or through exchanges of information to prevent any offense under the PMLA.

iii) CREDIT INFORMATION COMPANIES (REGULATION) ACT 2005 AND THE CREDIT INFORMATION COMPANIES REGULATIONS 2006[15]

This legislation is essentially aimed at the regulation of sharing and exchanging credit information by credit agencies with third parties. Disclosure of data received by a credit agency is prohibited, except in the case of its specified user and unless required by any law in force.

The regulations prescribe that the data collected must be adequate, relevant, and not excessive, up to date and complete, so that the collection does not intrude to an unreasonable extent on the personal affairs of the individual. The information collected and disseminated is retained for a period of seven years in the case of individuals. Information relating to criminal offenses is maintained permanently while information relating to civil offenses is retained for seven years from the first reporting of the offense. The regulations also prescribe that personal information that has become irrelevant may be destroyed, erased, or made anonymous.

Credit information companies are required to obtain informed consent from individuals and

[13]http://lawmin.nic.in/ld/PACT/1983/The%20Public%20Financial%20Institutions%20(Obligation%20as%20to%20Fidelity%20and%20Secrecy)%20Act,%201983.pdf.
[14] http://fiuindia.gov.in/pmla2002.htm.
[15] www.cibil.com/sites/default/files/pdf/cicra-act-2005.pdf.

 [ISSN 2581-5369]

entities before collecting their information. For redressal, a complaint can be written to the Reserve Bank of India.

iv) PAYMENT AND SETTLEMENT SYSTEMS ACT 2007[16]

Under this Act, the Reserve Bank of India (RBI) is empowered to act as the overseeing authority for the regulation and supervision of payment systems in India. The RBI is prohibited from disclosing the existence or contents of any document or any part of any information given to it by a system participant.

v) FOREIGN CONTRIBUTION REGULATION ACT 2010[17]

This Act is aimed at regulating and prohibiting the acceptance and utilization of foreign contributions or foreign hospitality by certain individuals, associations or companies for any activities detrimental to the national interest and, under the Act, the government is empowered to call for otherwise confidential financial information relating to foreign contributions of individuals and companies.

2. WORKPLACE PRIVACY

In the present scenario, employers are required to adopt security practices to protect sensitive personal data of employees in their possession, such as medical records, financial records, and biometric information. In the event of a loss to an employee due to lack of adequate security practices, the employee would be entitled to compensation under Section 43A of the Information Technology Act 2000. Other than this piece of legislation, there is no specific legislation governing workplace privacy, although, concerning the workplace, the effect of the Supreme Court judgment on privacy as a fundamental right remains to be seen.

3. CHILDREN'S PRIVACY

Section 74 of the Juvenile Justice (Care and Protection of Children) Act 2015 mandates that the name, address or school, or any other particular, that may lead to the identification of a child in conflict with the law or a child in need of care and protection or a child victim or witness of a crime shall not be disclosed in the media unless the disclosure or publication is in the child's best interest.

4. HEALTH AND MEDICAL PRIVACY

Under the Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations

[16] https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/86706.pdf.
[17] https://fcraonline.nic.in/home/PDF_Doc/FC-RegulationAct-2010-C.pdf.

 [ISSN 2581-5369]

2002 (Code of Ethics Regulations 2002)[18] regulations, physicians are obliged to protect the confidentiality of patients during all stages of procedures, including information relating to their personal and domestic lives unless the law mandates otherwise or there is a serious and identifiable risk to a specific person or community of a notifiable disease.

i) MEDICAL TERMINATION OF PREGNANCY ACT 1971

This Act prohibits the disclosure of matters relating to treatment for termination of pregnancy to anyone other than the Chief Medical Officer of the state. The register of women who have terminated their pregnancy, as maintained by the hospital, must be destroyed on the expiry of a period of five years from the date of the final entry.

ii) ETHICAL GUIDELINES FOR BIOMEDICAL RESEARCH ON HUMAN SUBJECTS

These Guidelines require investigators to maintain the confidentiality of epidemiological data. Data of individual participants can be disclosed in a court of law under the orders of the presiding judge if there is a threat to a person's life, allowing communication to the drug registration authority in cases of severe adverse reaction and communication to the health authority if there is a risk to public health.

E. GENERAL OBLIGATIONS FOR DATA PROCESSORS, CONTROLLERS, AND HANDLERS IN PRESENT SYSTEM

The IT Rules provide certain obligations to data processors, Controllers, and Handlers of the data of citizens, these obligations are must create a relationship between data principle and other authorities, the PDP Bill also provide certain provisions of same nature with updated views

(i) TRANSPARENCY

The IT Rules state that all data handlers must create a privacy policy to govern the way they handle personal information. Further, the policy must be made available to the data subject who is providing this information under a lawful contract.

(ii) LAWFUL BASIS FOR PROCESSING

A body corporate (or any person or entity on its behalf) cannot use data for any purpose unless it receives consent in writing from the data subject to use it for that specific purpose. Consent must be obtained before the collection of the data. The IT Rules also mandate that sensitive

[18] http://niti.gov.in/writereaddata/files/1.pdf

 [ISSN 2581-5369]

personal information may not be collected unless it is connected to the function of the corporate entity collecting it, and then only if the collection is necessary for that function. It is the responsibility of the body corporate to ensure that the sensitive personal information thus collected is used for no other purpose than the one specified.

(iii) PURPOSE LIMITATION

Neither the IT Rules nor the IT Act specifies a time frame for the retention of sensitive personal information. However, the IT Rules state that a body corporate or any person on its behalf holding sensitive personal data or information shall not retain that information for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law for the time being in force.

(iv) DATA RETENTION

Section 67C of the IT Act requires that an intermediary preserve and retain information in a manner and format and for such a period as prescribed by the central government.

(v) REGISTRATION FORMALITIES

India currently does not have any legislative requirements for registration or notification procedures for data controllers or processors, and it is a great lacuna in the eye of the law.

F. RIGHTS OF INDIVIDUALS IN PRESENT SYSTEM

(i) ACCESS TO DATA

Rule 5, Subsection 6 of the IT Rules mandates that the body corporate or any person on its behalf must permit providers of information or data subjects to review the information they may have provided.

(ii) CORRECTION AND DELETION

Rule 5, Subsection 6 of the IT Rules states that data subjects must be allowed access to the data provided by them and to ensure that any information found to be inaccurate or deficient shall be corrected or amended as feasible. Although the Rules do not directly address deletion of data, they state in Rule 5, Subsection 1 that corporate entities or persons representing them must obtain written consent from data subjects regarding the usage of the sensitive information they provide. Further, data subjects must be provided with the option not to provide the data or information sought to be collected.

The Supreme Court of India in a nine-judge bench decision in August 2017 in *KS Puttaswamy*

& Ors v. Union of India & Ors[19]also identified the right to be forgotten, in physical and virtual spaces such as the internet, under the umbrella of informational privacy.

(iii) OBJECTION TO PROCESSING AND MARKETING

Rule 5 of the IT Rules states that the data subject or provider of information shall have the option to later withdraw consent that may have been given to the corporate entity previously, and the withdrawal of consent must be stated in writing to the body corporate. On withdrawal of consent, the corporate body is prohibited from processing the personal information in question. In the case of the data subject not providing consent, or later withdrawing consent, the corporate body shall have the option not to provide the goods or services for which the information was sought.

(iv) RIGHT TO RESTRICT PROCESSING

provides for a data principal's right to restrict or prevent continuing disclosure of personal data by the data fiduciary, but only if the data protection authority, through an adjudicating officer, determines that any of the listed grounds for restriction or prevention of disclosure have been found.

(v) DISCLOSURE OF DATA

Data subjects also possess the right to disclosure of the information they provide. Disclosure of sensitive personal information requires the provider's prior permission unless either disclosure has already been agreed to in the contract between the data subject and the data controller, or disclosure is necessary for compliance with a legal obligation.

The exceptions to this rule are if order under the law has been made, or if a disclosure must be made to government agencies mandated under the law to obtain information for verification of identity; prevention, detection and investigation of a crime; or prosecution or punishment of offenses.

Recipients of this sensitive personal information are prohibited from further disclosing the information.

(vi) RIGHT TO COMPLAIN TO THE RELEVANT DATA PROTECTION AUTHORITY

Rule 5, subsection 9 of the IT Rules mandates that all discrepancies or grievances reported to data controllers must be addressed promptly. Corporate entities must designate grievance

[19] http://supremecourtofindia.nic.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf.

 [ISSN 2581-5369]

officers for this purpose, and the names and details of said officers must be published on the website of the body corporate. The grievance officer must redress respective grievances within a month from the date of receipt of said grievances.

IV. TECHNOLOGICAL INNOVATION AND PRIVACY LAW

There are no marketing restrictions on the internet or through email. Because India has no comprehensive data protection regime, issues such as cookie consent have not yet been addressed by Indian legislation. The IT Rules provide reasonable security practices to follow as statutory security procedures for corporate entities that collect, handle, and process data and these also apply to the use of big data. Unfortunately, no specific guidelines exist for the use of big data and big-data analytics in India.

The proposed PDP Bills,2019 also seeks the establishment of a Data Privacy and Protection Authority for regulation and adjudication of privacy-related complaints and disputes. The draft Data Protection allows for a data principal to complain to the data protection authority if it is unreasonably hindered by the data fiduciary in the exercise of its rights

(A) RECENT ENFORCEMENT CASES

As is evident from the above, India has no distinct legislative framework to support litigation in the areas of privacy, cybersecurity, and data protection. There has been no significant litigation in this area in the recent past. It is to be hoped that with the passage of the draft Data Protection Bill, 2019, into law and a clearer definition of rights in this sector, the enforcement of rights will become both more active and more stringent.

Karmanya Singh Sareen & Anr V. UOI & Ors[20]

This case was filed before the High Court of New Delhi in the public interest by two university students against WhatsApp, Facebook, and the Union of India (through the Department of Telecommunications (DoT) and the Telecom Regulatory Authority of India (TRAI)). After its acquisition by Facebook, WhatsApp updated its privacy policy in August 2016, stating that it would now share a limited amount of user information with Facebook for optimized advertising and networking suggestions. The petitioners contended that this change in policy compromised the privacy of the users of WhatsApp. On 23 September 2016, the High Court of New Delhi passed an order directing WhatsApp to 'scrub' all user data collected before 25 September for users who chose to opt-out of the service before this date. For users choosing to continue to make use of the service, the High Court directed that only data collected after 25 September

[20] W.P.(C) 7663/2016, https://indiankanoon.org/doc/138689631/

could be shared by WhatsApp with Facebook and its group companies. The Court also directed DoT and TRAI to examine the feasibility of bringing WhatsApp (and other internet-based messaging applications) under a statutory regulatory framework, ordering that these respondents must take an appropriate decision on this matter 'at the earliest'.

This decision is significant in that it is the only emphatic recognition of the right to privacy for individuals that our jurisprudence has seen in the past few years, other than the landmark Supreme Court judgment striking down Section 66A of the IT Act in 2015.

In 2017, the petitioners filed an appeal before the Supreme Court challenging the order of the High Court. The petitioners impugned the directions of the High Court and sought directions of the Supreme Court since, according to the petitioners, the policy formulated by WhatsApp was unconscionable and unacceptable. The Supreme Court is still hearing the matter and it seems unlikely that the controversy will be resolved this year.

K S Puttaswamy & Ors V. Union of India & Ors[21]

In KS Puttaswamy & Ors v. Union of India & Ors, and litigation that followed it, the constitutional validity of the Aadhar Act scheme was challenged because it was ultra vires to the Constitution and violated the rights of every citizen. The matter was initially heard by a three-judge bench, which referred it to a five-judge bench. However, owing to previous judgments by larger benches of the Supreme Court, a nine-judge bench was constituted to address the issue of whether privacy was a fundamental right guaranteed under the Constitution. The nine-judge bench issued a unanimous decision holding privacy to be a fundamental right of every citizen of the country, with qualified riders. The judgment acknowledges neo-libertarian values, such as the right to be forgotten, and will go down as a landmark judgment. The challenge to the constitutional validity of the Aadhar Act itself is still pending and a judgment of the Supreme Court in this matter is expected soon.

V. EVALUATING THE PERSONAL DATA PROTECTION BILL,2019

Every legislation has certain affirmative as well as debatably controversial aspects that are meant to be scrutinized. This PDP Bill also contains various clauses which intend to strengthen the protection and prevent misuse of data. Union Minister Ravi Shankar Prasad highlighted this by emphasizing the importance of utilizing ‘anonymized data’.[22] for policy innovation during the presentation of the PDP Bill in the Parliament.[23] The Bill aims to protect "Personal

[21] http://supremecourtofindia.nic.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf.
22The Personal Data Protection Bill,2019, ss. 3, s.3.
23 Lok Sabha refers Personal Data Protection Bill to joint panel; Prasad says 'anonymized data' should be available for policy making”, Business Standard, (December 12, 2019). https://www.business-standard.com/article/news-

Data"[24] relating to the identity, characteristics trait, attribute of a natural person and "Sensitive Personal Data"[25] such as financial data, health data, official identifier, sex life, sexual orientation, biometric data, genetic data, sex status, intersex status, caste or tribe, religious or political beliefs.

In a nutshell, the Bill continues to require that Personal Data[26] be processed fairly and reasonably while guaranteeing the protection of the privacy of the Data Principal[27], for purposes that are associated and consented to by the Data Principal, or purposes incidental or connected thereto[28]. The Bill also discusses the key changes relevant to private Data Fiduciaries[29]. The Bill has also made certain changes to the provisions relating to the processing[30] of Personal Data by Central and State Governments.

Section 2[31] of the PDP Bill proposes its applicability for processing of personal data that has been collected, disclosed, shared or otherwise processed within the territory of India;

(a) By the government, any Indian Company, any citizen of India or any person or body of persons incorporated in India, and

(b) Foreign companies dealing with personal data of individuals in India.

The special provisions contained in Chapter IV of the Bill provide for the processing of personal data and sensitive data of children. According to this section, data fiduciaries handling data of children shall process it only after verifying the age of the child and after obtaining consent from the child's parent or guardian. Business and commercial sites or online services focused on kids or who process huge volumes of personal information that belongs to children have been characterized under the Bill as Guardian Data Fiduciaries. Such fiduciaries are banned from monitoring or targeting advertisements at children unless they are providing counseling or child protection in which case, they shall be exempt from seeking verification.[32]

Chapter V of the PDP Bill gives Indian citizens several rights like the Right to Confirmation

ani/lok-sabha-referspersonal-data-protection-bill-to-joint-panel-prasad-says-anonymized-datashould-be-available-for-policy-making-119121200044_1.html.
24 Supra 6
25 The Personal Data Protection Bill, 2019, ss. 36., s.3.
26 The Personal Data Protection Bill, 2019, ss.28, s.3.
27 The Personal Data Protection Bill, 2019, ss. a, s.5
28 The Personal Data Protection Bill, 2019, ss. b, s.5.
29 The Personal Data Protection Bill, 2019, ss. 13, s.3.
30The Personal Data Protection Bill, 2019, ss. 31, s.3.
31 The Personal Data Protection Bill, 2019, s.2.
32 The Personal Data Protection Bill, 2019, s.16.

 [ISSN 2581-5369]

and Access[33], Right to Correction and Erasure[34], Right to Data Portability[35] , and Right to be forgotten[36]. These rights permit citizens to seek information from the data fiduciary and processing companies of processing that their data which has been or is being subjected to, seek correction for inaccurate or outdated data, to ask for the transfer of data to other data fiduciaries, and limit the continuing divulgence of their data by the fiduciary.

Another feature of the Bill is the appointment of the Data Protection Officer as a state of contact for complaints and grievances of information and data principals. This makes it simpler for data principals to get their interests with a data fiduciary addressed.[37]

Chapter X of the Bill also lays out the penalties and compensation for potential offenders under the Bill. Offenders who process or transfer personal data without consent and falls in a manner that violates the Bill will be fined with either INR 15 crore or 4% of the annual turnover of the company, whichever is higher and Offences regarding the failure to conduct data audits are punishable with a fine of INR 5 crore or 2% of the data fiduciary's annual turnover, whichever is higher.[38]

The PDP Bill shall not apply to the processing of anonymized data, other than the anonymized data or other non-personal data to enable better targeting of delivery of services or formulation of evidence-based policies by the Central Government.[39]

This bill is on the path to the GDPR[40] which is widely accepted, and considered as a model of privacy and data protection law in all over the world, the GDPR makes it mandatory to comply the provisions of it by all service providers in the European Union, whether the service provider is a European company or not. Data protection is the process of protecting the personal and sensitive information of citizens and preventing it from misuse. The quote is newly popularized which states 'Data is the new oil' and highlights the power that data holds.

VI. RECOMMENDATION & SUGGESTIONS

PDP Bill 2019 gives the government access to non-personal data as well. This has drawn criticism from Justice B N Srikrishna himself. According to him, non-personal data should

33 The Personal Data Protection Bill, 2019, s.17
34 The Personal Data Protection Bill, 2019, s.18.
35 The Personal Data Protection Bill, 2019, s.19.
36 The Personal Data Protection Bill, 2019, s.20.
37 The Personal Data Protection Bill, 2019, s.30.
38 The Personal Data Protection Bill, 2019, s.66.
39 The Personal Data Protection Bill, 2019, s.91.
40 General Data Protection Regulation is a modern regulation of European Union on the protection of personal data of a natural person with regard to the processing of personal data and on the free movement of such data, (July 20, 2020) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

 [ISSN 2581-5369]

have been addressed in a different Bill and not be included with personal data because it gives the government the right to seek any non-personal data from companies. This clause allows the government to access business data, including data on intellectual property, business strategy, and mergers and acquisitions, that may not be personal data but necessary from a business point of view[41]. The exemption given to government agencies under Section 35[42] is likely to send a negative message to the global investor network, it must be answered.

Another concern is regarding the selection and composition of the Data Protection Authority. The selection of the DPA is dependent on the Central Government only. The chance of government's direct interference will decrease the reputation, this issue needs to be solved.

The 2019 Bill also does not include the principles of necessity and Section 36 of the Bill provides provision for "Exemption of certain provisions for certain processing of personal data" which lay down criteria that prove the situations necessary to provide access to government agencies of personal data of individuals. In this situation, the principle of proportionality requires by the authorities to strike a balance between the means used and the intended aims. Such an exception raises concerns to State Surveillance of personal data, it will raise another serious debate on state interference by the use of privacy legislation, because the moto of this legislation is "to protect the individual's right" and by this clause, the new legislation will provide a chance to hamper the privacy of individual itself.

VII. CONCLUSION

There is no doubt that India urgently needs to take a keen look at its poorly regulated digital spaces and at the virtual activities of individuals, private organizations, and governmental authorities alike. The several agencies performing cybersecurity operations in India, such as the National Technical Research Organisation, the National Intelligence Grid, and the National Information Board, require robust policy and legislative and infrastructural support from the Ministry of Electronics and Information Technology, and the courts, to enable them to do their jobs properly. The EU's General Data Protection Regulation may provide an impetus for India in this regard, particularly not only concerning cross-border information flow but the protection of data and enforcement of cybersecurity in its new data protection regulation. While it seems that the government is concerned and keen to bring about change in this sector, the Personal Data Protection Bill is an attempt to balance the conflicting interests of the Government and other stakeholders on one hand and the rights of individuals on the other. It is said to bridge

41 Key Changes in the Personal Data Protection Bill, 2019 from the Srikrishna Committee Draft, (July 2, 2020) https://sflc.in/key-changes-personal-data-protection-bill-2019-srikrishna-committee-draft.
42 The Personal Data Protection Bill, 2019, s.35.

 [ISSN 2581-5369]

the gap caused by absentia of legislation extending statutory protection to data and for the prevention of internet misuse. This Bill intends to provide a framework that is essential to address digital privacy on the internet through checks and balances to preserve the trust between said individuals and the entities that have access to their personal data. The clause of essential rights in Bill which provides power to individuals to restrict the use and disclosure of their personal data by a data fiduciary has the potential to empower individuals against its misuse.

However, in its current state, concerns are raised because of a lack of accountability attached to the access given to the Central Government and its agencies in the PDP Bill,2019. Justice BN Shrikrishna said "they have removed the safeguards. This is dangerous. The government can at any time access private data or government agency data on the grounds of sovereignty or public order, this has dangerous implications."[43] He also mentioned this Bill will turn India into an Orwellian State[44]. Observing these statements and various Exclusion of the principles like necessity and proportionality from the Bill also perpetuates the unconstitutional practice of allowing the government access to personal data without appropriate safeguards in place and can violate the fundamental right to privacy, to make this regulation full proof and acceptable by the public these all serious issues must be answered properly.

*****

43 Megha Mandavia. *Personal data protection Bill can turn India into 'Orwellian State: Justice BN Srikrishna*, The Economics Times, (Dec 12,2019), https://economictimes.indiatimes.com/news/economy/policy/personal-data-protection-bill-can-turn-india-into-orwellian-state-justice-bn-srikrishna/articleshow/72483355.cms?from=mdr

44 Orwellian sate means a political system which tries to control every part of people's lives. Dicitionary.cambridge.org. (2020).

 [ISSN 2581-5369]