VOLUME 4 | ISSUE 1

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

ANALYSIS OF THE PRIVACY AND DATA PROTECTION LAWS IN INDIA IN LIGHT OF THE PUTTASWAMY AND AADHAAR JUDGMENTS

- Ayushi Chaurasia[1]

ABSTRACT

The Research paper looks into the evolution of privacy and data protection laws in India. From the judgment of M.P. Sharma v. Satish Chandra and Ors. (1954) where privacy was held to not be a fundamental right to Puttaswamy v. Union of India (2017) where a nine-judge bench unanimously upheld the right to privacy as a fundamental right under Article 21. The research paper will then look into the relationship between the Puttaswamy and the Aadhaar judgment. Since the categorization of right to privacy as a fundamental right, there have been numerous attempts at consolidating a privacy and data protection law. However, till date no legislation is in force. The paper will finally discuss the provisions of the IT Act, 2000 and its Rules that govern data protection in India, while India is waiting for a legislation like EU-GDPR consolidating privacy rights, comes into force.

INTRODUCTION

In an era of technological advancement and digital economy, a massive reliance is placed on data by governments, individuals and corporations alike. The digital world has transformed the human life and made it much easier. It is the data that forms the backbone of the world wide web. The increase in dissemination of information from one corner of the world to another has caused globalization of information. The growth in the digital world based on ever-expanding technology has brought in new key players like blockchain, artificial intelligence etc. While these technologies have immensely improved individual lifestyle, national economies, it has brought with it, its own evils.

Owing to the numerous benefits brought about by technological advancements, the cyberspace today is a common pool used by citizens, businesses, critical information infrastructure, military

[1] Advocate at Supreme Court of India & High Court of Delhi

and governments in a manner that makes it difficult to draw clear boundaries among these different groups. The cyberspace is expected to be more complex in the foreseeable future, with many fold increase in networks and devices connected to it.[2] Information Technology (IT) is one of the critical sectors that rides on and resides in cyberspace. It has emerged as one of the most significant growth catalysts for the Indian economy. The sector has played a significant role in transforming India's image to that of a global player in providing world-class technology solutions and IT business services.[3]

Big data companies harbour massive data which includes personal sensitive data as well of the innocent individuals. The contemporary age has been aptly regarded as an era of ubiquitous dataveillance, or the systematic monitoring of citizen's communications or actions through the use of information technology.[4] It is also an age of 'big data' or the collection of data sets. These data sets are capable of being searched; they have linkages with other data sets; and are marked by their exhaustive scope and the permanency of collection.[5] From knowledge discovery and data mining processes, data can be combined to 'create facts' about an individual; in particular, the likelihood that an individual will engage in a certain type of behaviour.[6] Processing of personal data allows understanding preferences of individuals, which may be useful for customisation, targeted advertising, and developing recommendations. Processing of personal data may also aid law enforcement. Unchecked processing may have adverse implications for the privacy of individuals.[7] Big Data offers specific methods and technologies for statistical data evaluation and in this regard, issues of privacy and customer confidentiality have acquired added prominence on account of the rise of digital tracking and targeted advertising.[8]

As our state becomes an "information state" through increasing reliance on information - such that information is described as the "lifeblood that sustains political, social, and business

[2]Preamble, NATIONAL CYBER SECURITY POLICY - 2013, Ministry of Electronics and Information Technology, Government of India. https://www.meity.gov.in/writereaddata/files/National_cyber_security_policy-2013_0.pdf

[3]*Id.*

[4]*Yvonne Mcdermott*, "CONCEPTUALIZING THE RIGHT TO DATA PROTECTION IN AN ERA OF BIG DATA", BIG DATA AND SOCIETY (2017).

[5]*Id.*

[6]*Martin Kuhn*, "FEDERAL DATAVEILLANCE: IMPLICATIONS FOR CONSTITUTIONAL PRIVACY PROTECTIONS" 172 (2007); *Christina P. Moniodis*, "MOVING FROM NIXON TO NASA: PRIVACY'S SECOND STRAND - A RIGHT TO INFORMATIONAL PRIVACY" [15 YALE J.L. & TECH. 139 (2012)].

[7]LEGISLATIVE BRIEF, "THE DRAFT DIGITAL PERSONAL DATA PROTECTION BILL, 2022, PRS Legislative Research, 30th December 2022.

[8]*Deborshi Bharat*, "DEFINING THE SCOPE OF PERSONAL DATA IN DIGITAL INDIA", S &R Associates, Mondaq (13 July 2023) https://www.mondaq.com/india/privacy-protection/1342060/defining-the-scope-of-personal-data-in-digital-india?login=true&debug-domain=.mondaq.com

decisions" - it becomes impossible to conceptualize all of the possible uses of information and resulting harms.[9] With every click on 'Accept cookies' to access websites to putting a quick tick mark on the 'Privacy policy' when downloading Apps or social media platforms or accessing certain websites, the individuals are unknowingly or helplessly compromising their informational privacy. Social media platforms like Facebook, Twitter, Google which play a crucial role in connecting people, are also one of the biggest captors of personal data.

Governments across the world tap into personal data of citizens and individuals for "surveillance for security concerns." Moreover, the combination of technology with control of data flow has been described as a "tool of enslavement" for society if the power is abused.[10] Thus, private sector and the public sector both are equally guilty of data collection and misuse. In the absence of a concrete data privacy and its protection regime at the national and international level, the future of individual autonomy looks bleak. The GDPR of the European Union is a step in the right direction but needs a similar implementation in India.

PRIVACY – A FUNDAMENTAL RIGHT

In 2017, the Supreme Court of India unanimously and conclusively upheld the right to privacy as a Fundamental Right in the landmark case of K.S. Puttaswamy and Ors. v. Union of India.[11] The nine-judge bench of the Supreme Court thus settled the dust surrounding privacy law in India whereby the uncertainty caused by the decision of an eight-judge bench in M.P. Sharma and Ors. v. Satish Chandra and Ors.[12] still continued to be good law even though smaller bench judgments had upheld the right to privacy as a fundamental right subsequently. The Puttaswamy decision was the first case in more than two decades to be decided by a nine-judge panel. Six judges wrote separate but concurring judgments, which is unsurprising given the landmark nature of the judgment.[13]

Supreme court defined privacy to "*include at its core the preservation of personal intimacies, the sanctity of family life, marriage, procreation, the home and sexual orientation. Privacy also*

[9]*Elbert Lin*, "NOTE, PRIORITIZING PRIVACY: A CONSTITUTIONAL RESPONSE TO THE INTERNET", 17 BERKELEY TECH. L.J. 1085, 1091 (2002) (quoting *Fred H. Cate*, PRIVACY IN THE INFORMATION AGE 5 (1997)); *Christina P. Moniodis*, "MOVING FROM NIXON TO NASA: PRIVACY'S SECOND STRAND—A RIGHT TO INFORMATIONAL PRIVACY" [15 YALE J.L. & TECH. 139 (2012)].

[10]*Robert S. Peck*, "EXTENDING THE CONSTITUTIONAL RIGHT TO PRIVACY IN THE NEW TECHNOLOGICAL AGE", 12 HOFSTRA L. REV. 893, 987 (1983-84).

[11] [(2017) 10 SCC 1].

[12] [(1954) 1 SCR 1077].

[13]MenakaGuruswami, *supra* note 11.

connotes a right to be left alone. Privacy safeguards individual autonomy and recognises the ability of the individual to control vital aspects of his or her life."[14]

The Supreme Court in the judgment stated that privacy is a part of Article 21 which provides for the right to life and personal liberty. Article 21 of the Constitution states that: "*No person shall be deprived of his life or personal liberty except according to the procedure established by law.*" 'Life and personal liberty' include the right to live with dignity as well, as held in the case of Maneka Gandhi v. Union of India, [AIR 1978 SC 597]; Francis Coralie Mullin v. Union Territory of Delhi[15] which stated that "*the right to life enshrined in Article 21 cannot be restricted to mere animal existence. It means something much more than just physical survival.*" While discussing the importance of privacy as a fundamental right, the judgment also explained how human dignity was very much a part of privacy. Thus, any compromise with the right to privacy was against the mandate of not just Article 21 but also Article 14 and Article 19, the Golden Triangle of fundamental rights, i.e. Right to life and personal liberty, Right to equality, and Right to freedom. However, the right to privacy cannot exist without fetters, the reasonable restrictions that apply to Article 14, 19 and 21 are also applicable on the right to privacy. Moreover, the exception to right to life and personal liberty, 'procedure prescribed by law', is a three-pronged test that the procedure must be "just, fair and reasonable".[16]

Justice D.Y. Chandrachud who authored the majority judgment in the Puttaswamy case stated that privacy was a natural right of humans which are inalienable.[17] The state does not bestow natural rights and thus the state cannot take them away as well. They exist equally for all individuals irrespective of class or strata, gender or orientation.[18] Further, "*privacy is described as the right to be let alone. The concept is founded on the autonomy of the individual. The ability of an individual to make choices lies at the core of the human personality. The autonomy of the individual is associated over matters which can be kept private. The integrity of the body and the sanctity of the mind can exist on the foundation that each individual possesses an inalienable ability and right to preserve a private space in which the human personality can develop.*"[19]

---

[14] Para 323, Justice K.S. Puttaswamy and Anr v. Union of India and Ors [AIR 2017 SC 4161] ("Puttaswamy judgment").
[15] [(1981) 1 SCC 608].
[16] District Registrar and Collector v. Canara Bank, [(2005) 1 SCC 496]; State of Maharashtra v. Bharat Shanti Lal Shah, [(2008) 13 SCC 5]; Gobind v. State of M.P., [(1975) 2 SCC 148].
[17] Para 42, *supra* note 12.
[18] Para 46, *id.*
[19] Para 297, *id.*

Thus, summarizing the words of Justice DY Chandrachud, the right to choose, right to dignity and right to autonomy, come as a part and parcel of the right to privacy. The notion of privacy enables the individual to assert and control over the human element which is inseparable from the personality of the individual.[20] Privacy recognises the autonomy of the individual and the right of every person to make essential choices which affect the course of life.[21]

While explaining the importance of this crucial Fundamental Right, the Supreme Court referred to the International Standards that India had to abide by i.e. Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR). 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. Everyone has the right to the protection of the law against such interference or attacks.*" The Supreme Court also observed that India did not object to the provision of privacy under the ICCPR and hence was bound by law to implement it under Article 51 and Article 253 of the Indian Constitution.

Right to privacy is essentially a 'personal right' as opposed to a 'community right' and the primary goal of the Constitution is the socio-economic welfare of the community as a whole, as given in the Directive Principles of State Policy (DPSP). In fact, shortly after independence, and being acutely aware of its post-colonial heritage and institutional origins from a British federal court, the Supreme Court of India became deeply invested in protecting the collective rights of all Indians from state negligence by crafting socio-economic rights, like food, education, livelihood, and even a clean environment, through a rather expansive interpretation of Article 21.[22]

However, community rights do not trump personal rights as the Preamble itself starts with "*We the people*" which can be interpreted to include each and every member of the society. Moreover, Article 21 is also a personal right *in rem* where every person has the right to live freely unless some reasonable procedure under the law says otherwise. Even though the majority of the laws are focussed on improving the socio-economic conditions of the country, the Constitution has been adopted by the people cumulatively. Hence, the individual rights of the citizens are equally important as the community rights. The basic spirit of our Constitution is to provide each and every person of the nation equal opportunity to grow as a human being,

[20] Para 297, *id.*
[21] Para 127, *id.*
[22] MenakaGuruswami, *supra* note 11.

irrespective of race, caste, religion, community and social status.[23] The individual lies at the core of constitutional focus and the ideals of justice, liberty, equality and fraternity animate the vision of securing a dignified existence to the individual.[24]

The judgment further approved the test of proportionality as originally stated in the case of Modern Dental College & Research Centre v. State of Madhya Pradesh and Ors.[25], in order to balance the right to privacy with the interest of the state. There are four sub-components of proportionality which need to be satisfied. They are:

1. *"A measure restricting a right must have a legitimate goal.*
2. *It must be a suitable means of furthering this goal.*
3. *There must not be any less restrictive but equally effective alternative (necessity).*
4. *The measure must not have a disproportionate impact on the right holder (balance)"*

Thus, this test shall ensure right to privacy while balancing the right of the individuals with the sovereign right of the state to protect its territory for ensuring peace and tranquillity.

THE AADHAAR ACT AND PRIVACY CONCERN

The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 ("Aadhaar Act") was challenged on the ground of violation of privacy because of the collection of biometric and retina and iris data, amongst other data by the state. It was contended that the imposition of Aadhaar for availing beneficial services was violative of right to privacy and would make the state totalitarian. Linking the biometric data with bank account and PAN Card was apprehended to be a way of mass surveillance to monitor day-to-day activities of the individuals. The privacy concerns were the potential tracking of citizens and influencing their behaviour in the long run by the state and stifling dissent by citizens or groups. There was also a fear of theft of data by non-state entities and its potential misuse in the absence of adequate data protection measures taken by the government. The constitutional bench of Supreme Court upheld the Aadhaar Act to be constitutional and not violative of the right to privacy[26] as established in the Puttaswamy decision. The court relied heavily on the

[23]Justice K.S. Puttaswamy and Anr. vs. Union of India (UOI) and Ors. [(2019) 1 SCC] 1 at Page 23. ("Aadhaar judgment")
[24]Kesavananda Bharati v. State of Kerala [(1973) 4 SCC 225].
[25] [(2016) 7 SCC 353].
[26]Puttaswamy judgment, *supra* note 12.

Puttaswamy judgment before concluding that the privacy of individuals would not be compromised by the Aadhaar Act.

CURRENT DATA PROTECTION REGIME IN INDIA

The current privacy and data protection regime is governed by the provisions of Information Technology Act, 2000 ("IT Act")(as amended in 2008) and its Rules. It states that in case the company or firm handling digital sensitive personal data is negligent in its conduct and fails to maintain reasonable security practice or procedure, resulting in loss or unlawful gain, it will be liable to pay compensation to the affected person.[27] Also, any person who has secured access to personal data of other individuals in the form of electronic records, books, correspondence, etc. and he shares it with another will be liable to imprisonment of maximum of two years or a fine which may extend to one lakh rupees.[28] Right to privacy has been ensured against a person or intermediary who receives personal information under a lawful contract providing for service, and discloses the personal information to a third party in breach of the contract with the intention to cause wrongful harm or wrongful gain, with a punishment for up to three years imprisonment or fine of Rupees five lakhs or both.[29]

Interception, monitoring or decryption of digital information could be done by the Central or State government in the interest of sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence.[30]

Information Technology (Intermediaries Guidelines) Rules, 2011, were implemented in 2011 but have now been superseded by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 which were published on 25th February, 2021. These rules were modified subsequently in 2022 and latest on 06.04.2023.[31] These Rules ensure privacy of individuals from the acts of intermediaries and service provider. Social media intermediary has been defined as "*an intermediary which primarily enables online interaction*

[27] Section 43A of the Information Technology Act, 2000.
[28] *Id* at Section 72.
[29] *Id* at Section 72A.
[30] *Id* at Section 69.
[31] INFORMATION TECHNOLOGY (INTERMEDIARY GUIDELINES AND DIGITAL MEDIA ETHICS CODE) RULES, 2021 (updated 6th April 2023) ("Intermediary Guidelines") https://www.meity.gov.in/writereaddata/files/Information%20Technology%20%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20%28updated%2006.04.2023%29-.pdf.

between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services."[32]

The Rules provide that intermediaries including social media intermediary, significant social media intermediaries and online gaming intermediaries are required to publish their privacy policy and user agreement on its website or apps in English or any language of the 8th Schedule.[33] The privacy policy and user agreement are also required to mention obligations of the users of such platforms to prevent them from publishing data belonging to another person without their consent, or is defamatory, infringes trademark, etc. or violates any law for the time being in force. The users would be required to not share misleading information intentionally but which may be reasonably perceived as fact.[34] Privacy was further protected by preventing the users from disseminating software virus, impersonating another person or publishing defamatory content with the purpose of harassing another entity for financial gains.[35] The users would also be required to prevent from publishing anything that threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign States or public order.[36] Finally, the intermediary was mandated to its users every year about its right to terminate user's access in case of non-compliance with rules and regulations, privacy policy or user agreement.[37] *Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011* ("SPDI Rules") provide for digital privacy and sensitive data protection in India. Sensitivepersonal data or information consists of passwords, financial information, health condition, sexual orientation, medical records and history, biometric information that has been provided to a service provider or body corporate legally.[38] Information that is freely available under right to Information Act, 2000, or any other law will not be classified as sensitive personal data. The word biometric includes "the technologies that measure and analyse human body characteristics, such as 'fingerprints', 'eye retinas and irises',

[32] Rule 2(w) *Id.*
[33] Rule 3(a) *Id.*
[34] Rule 3(b)(vi) *Id.*
[35] Rule 3(b)(vii)(ix) *Id.*
[36] Rule 3(b)(viii) *Id.*
[37] Rule 3(c) *Id.*
[38] Rule 3, INFORMATION TECHNOLOGY (REASONABLE SECURITY PRACTICES AND PROCEDURES AND SENSITIVE PERSONAL DATA OR INFORMATION) RULES, 2011 ("SPDI Rules") Ministry Of Communications And Information Technology (Department of Information Technology), Notification (11th April, 2011). https://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf

'voice patterns', 'facial patterns', 'hand measurements' and 'DNA' for authentication purposes."[39]

Corporate bodies that collect personal data and sensitive personal data are obligated to publish on their website the privacy policy in clear and easily accessible terms, the kind of sensitive personal data collected, the purpose and usage for it, disclosure of information and taking reasonable steps to keep the information secure.[40] Consent is essential in writing in order to collect sensitive personal information and that the service provider or body corporate should collect it only for a necessary and lawful purpose.[41] Rule 5 further states that the data should be used only for the purpose for which it is collected and should not be retained for longer duration than necessary. The information provider should also have the power to review the information so provided and make changes if it is found to be inaccurate or deficient.[42] Withdrawal of consent can be done by an information provider at any step in a written manner and thus the body corporate shall have the option to not provide goods and services for which information was sought [Rule 5(7)]. Rule 6 provides that the disclosure of sensitive personal information can be done by a body corporate only with prior approval from the information provider or if provided under a lawful contract.

However, in matters of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences, the government can ask for sensitive personal information by stating the purpose in writing to the body corporate. Rule Seven provides for the transfer of sensitive personal information outside the country. Transfer may be possible when the corporate body sending the information is aware that the location where the information is being sent to, adheres to the same data protection standards as in India, or it can also be done when the provider specifically gives his consent. Reasonable security practice and procedures involve implemented security practices and standards and implemented comprehensive documented information security program.

MOVING TOWARDS A NEW DATA PROTECTION LAW

Since the Puttaswamy judgment in 2017, multiple efforts have been taken at strengthening privacy and data protection laws in India. B.N. Srikrishna Committee on Experts was constituted in August 2017 in order to look into the privacy laws and come up with a draft bill.

[39] Rule 2(b) *Id.*
[40] Rule 4 *Id.*
[41] Rule 5 *Id.*
[42] Rule 5(6) *Id.*

The Committee submitted its Report and the draft Bill to the Ministry of Electronics and Information Technology (MeitY) on July 27, 2018.[43] The recommendations of the Committee in brief were:

1. Establishment of an Authority to oversee compliance of data protection law.
2. Fiduciary relationship between service provider and the individual wherein an individual who parts with his personal information and requires the service provider and the consequent obligation of the service provider to use it for authorised purpose only. Obligations of service providers were to not abuse data, inform individual about data collection and to act fairly and reasonably.
3. The definition of personal and sensitive personal data was introduced. Personal data was defined as any data from which the identity of the person can be directly or indirectly identified. Sensitive personal data included passwords, financial information, biometric and genetic data, religious and political affiliation, sexual orientation or anything as notified by the Authority.
4. Consent was made the essence for personal data collection and for processing by service providers.
5. Exceptions where consent was not needed were state welfare, compliance with the law or court order, in the necessity to save a life, in certain employment contracts when consent of employer may be unreasonable.
6. Individuals had the right to access, confirm and correct data, they had the right to transfer and right to be forgotten and to object to automated decision making, data processing and portability.
7. Transfer of personal data outside country was possible only when authorised by the Central Government or the Authority.
8. Grounds for processing sensitive personal data were consent; if function was necessary for any Central or State legislature or for the state to provide benefit to society; as required by law or in compliance of any judgment.
9. Offences and penalties for personal data breach extended up to five crore rupees.

[43] Report Summary, "A FREE AND FAIR DIGITAL ECONOMY", PRS Legislative Research; Bill Summary, "THE DRAFT PERSONAL DATA PROTECTION BILL, 2018" https://prsindia.org/files/bills_acts/bills_parliament/1970/Srikrishna%20Committee%20Report%20Summary_For%20Upload.pdf

Personal Data Protection Bill, 2019 was presented before the Parliament. The Bill was drafted on the recommendations of the Srikrishna Committee. The Bill was placed before the Joint Parliamentary Committee (JPC). The Bill was later withdrawn from the Parliament. In November 2022, the Ministry of Electronics and Information Technology released the Draft Digital Personal Data Protection Bill, 2022 for public feedback.[44] Currently, the Personal Data Protection Bill 2022 has been approved by the Cabinet but is pending before the Parliament.

Meanwhile, the Explanatory Note to the 2022 Draft Bill which accompanied the draft's release in India, specified that the law would apply to digital personal data only – in recognition of the rising role of the internet and increased 'digitalization'. Nevertheless, this is the first time that Indian law has clarified, both in terms of nomenclature and scope, that the proposed data protection framework is restricted to digital data only.[45]

Key Features of the Draft Personal Data Protection Bill, 2022:

a. Unlike the previous versions of the Bill, the 2022 Draft Bill has been extended to entities situated abroad which collect the personal data of citizens of the country, along with entities (data fiduciaries) located in the country or parking their data outside the country. (Section 4)
b. Section 7 provides for consent to be freely given, informed, specific and unambiguous. It can be withdrawn at any time. Once the data principal requests for the removal of personal data, the data fiduciaries are bound to remove it within reasonable time.
c. Under Section 9, data principal's rights include obtaining information, seeking correction of the personal data held by the data fiduciaries. (Section 13)
d. A new feature added in the Draft Bill is nominating someone to exercise their rights in case of death or incapacity. Amongst the duties of data principals, no frivolous complaints are to be made and no submission of false or fake information to the data fiduciaries. Impersonation by data principals is also prohibited.
e. The data fiduciaries have the duty to ensure correctness and completeness of data and to ensure reasonable security safeguards to protect the personal data. It also has the duty to

[44]THE DRAFT DIGITAL PERSONAL DATA PROTECTION BILL, 2022, Ministry of Electronics and Information Technology, November 18, 2022.
[45]*Deborshi Bharat*, "DEFINING THE SCOPE OF PERSONAL DATA IN DIGITAL INDIA", S &R Associates, MONDAQ, (13 July 2023) https://www.mondaq.com/india/privacy-protection/1342060/defining-the-scope-of-personal-data-in-digital-india?login=true&debug-domain=.mondaq.com

inform the Data Protection Board and the data principals, in case of breach of safety measures.

f. The draft provides for a provision wherein the tracking or behavioural monitoring of children by data fiduciaries could not be done for the purpose of custom or targeted advertisements. Moreover, they shall not collect personal data of children which may be 'harmful' to their interests.

Key Issues with the Draft Personal Data Protection Bill, 2022:

a. There are several issues with the 2022 Draft of the Data Protection Bill. Right to be forgotten and right to data portability both are absent in the bill. Srikrishna Committee had mooted the idea of right to be forgotten to be incorporated in the Bill. But at the same time, the Committee noted that this right ought to be balanced with other's rights and interests so that exercise of one's right does not deprive the right of another.

b. The Draft Bill provides for the need of the consent of the legal guardian of a child. (A child being described in the Act as an individual under the age of 18). This will have an impact on anonymity as the data fiduciary will have to verify the age of everyone signing up for its services.[46] Moreover, treating a seventeen year old as a child is a bit too drastic.

c. The Draft bill gives the power to the Government entity to retain the data beyond the prescribed period i.e. till the fulfilment of purpose for which the personal data is acquired. This goes against the test of proportionality under the right to privacy as held in the Puttaswamy judgment. Using the above exemptions, on the ground of national security, a government agency may collect data about citizens to create a 360-degree profile for surveillance. It may utilise data retained by various government agencies for this purpose. This raises the question whether these exemptions will meet the proportionality test.[47]

d. Some provisions of the Bill provide differential treatment between public and private data fiduciaries in matters of consent and the time period for holding data. This goes against the fundamental right of Equality. The Bill provides for 'deemed consent'. This has been given a wider ambit to include providing assistance and services during breakdown of 'public order', 'public interest' and for 'fair and reasonable purpose'. Since these words are vague, it gives the government an advantage. Even in matters of commercial nature such as

[46] Legislative Brief, "THE DRAFT DIGITAL PERSONAL DATA PROTECTION BILL, 2022", PRS Legislative Research, 30th December 2022.
[47] *Id.*

mergers and acquisitions, corporate restructuring transactions, credit scoring, recovery of debts and prevention and detection of fraud, the public fiduciaries will have deemed consent.

e. The autonomy of the Data Protection Board in questionable as the procedure for the constitution of Board has not been provided for in the Draft. Government may prescribe that in the Rules. Since the Central government will play an important role in appointment of members of the Board, there may be doubts regarding its autonomy.

f. The state has been exempted from fiduciary duty. As these obligations do not apply, a data breach at the National Crime Records Bureau or the Unique Identification Authority of India need not be reported as per the mechanism under the Bill. Data collected by police for the investigation and prosecution of one offence may be utilised for other purposes. Similarly, where personal data is processed to enforce legal rights or claims (for example, the right to food under the National Food Security Act, 2013), the obligation to ensure the accuracy and completeness of data will not apply.[48]

CONCLUSION

Information technology is a complex concept that is prone to elusive harms. While it is impossible to escape the digitalisation of the world, thus actions can be taken to ensure that the ills of information technology can be curbed. Invaluable personal data and sensitive personal data of individuals is prone to data-theft, misappropriation, impersonation and fraud causing irreparable loss to them. The privacy of the individual has to be accorded the highest importance in this digital age. In the landmark case K.S. Puttaswamy and Ors. v. Union of India, (2017) a historic decision was given by a nine-judge bench of the Supreme Court. It is this judicial imagination of privacy that is important not only to an individual's self-determination but also to a constitutional democracy's endurance that makes K.S. Puttaswamy especially significant.[49]Therefore, it has established a binding precedent on all Courts, unless it is overruled by an even larger bench. It is also of wide significance because by putting the right to privacy at the heart of constitutional debate in the world's largest democracy, it is likely to provide assistance and inspiration for privacy campaigners around the world.[50]

[48]*Id.*
[49]MenakaGuruswamy, supra note 11.
[50] "PUTTASWAMY V. UNION OF INDIA (I)", Global Freedom of Expression, Columbia University https://globalfreedomofexpression.columbia.edu/cases/puttaswamy-v-india/

Judiciary has a major role to play in safeguarding the privacy rights of citizens in absence of measures taken by the government regarding introducing reforms in legislations. If the judiciary is going to play a role in understanding data privacy interests and balancing power between citizenand government, it is time to assess the doctrine further.[51] Merely holding the right to privacy as a fundamental right does not end the task of the judiciary, it is only the beginning of ensuring the safeguarding of citizens' rights. Moreover, by judicial innovation, rights of the individuals within the wide ambit of privacy must be protected by the courts at all costs.

Policymakers in India are at a crucial juncture around framing a personal data protection legislation and experimenting with different models of data governance. It is imperative that these frameworks and models be firmly centred around the protection and preservation of the privacy and data protection rights of Indians, both from private and public entities.[52] It is about time for India to enact a data protection legislation which balances the interests of the individuals, private entities and the government. The ultimate balancing between security of state and security of individual in the state is at stake. In conclusion, given that India is positioned as one of the largest data markets in the world, a comprehensive data protection and governance regulation will certainly influence and greatly contribute to the evolution of the global data governance landscape.[53]

[51] *Christina P. Moniodis*, "MOVING FROM NIXON TO NASA: PRIVACY'S SECOND STRAND—A RIGHT TO INFORMATIONAL PRIVACY" [15 YALE J.L. & TECH. 139 (2012)]

[52] Centre for Communication Governance, "COMMENTS ON THE REPORT BY THE COMMITTEE OF EXPERTS ON NON-PERSONAL DATA GOVERNANCE FRAMEWORK, 2020", available at <https://ccgdelhi.org/wp-content/uploads/2020/09/CCG-NLU-Comments-to-MeitY-on-the-Report-by-the-Committee-of-Experts-on-Non-Personal-Data-Governance-Framework.pdf>

[53] *Shruti DvivediSodhi ,BansariSamant and Tushar Sinha*, "THE JOURNEY OF INDIA'S DATA PROTECTION JURISPRUDENCE", Lexology https://www.lexology.com/library/detail.aspx?g=57720842-f709-4dd4-947b-44c3c6e4ed10