A Compendious Analysis: Privacy Protection Laws in India

Akshdeep Gupta & Mahak Gandhi

Pursuing BALLB, Amity Law School Noida, Amity University, Uttar Pradesh

Abstract

Right to privacy is not a common law right but widely recognised under the doctrine of equity and right to democratic justice. Anyone can learn a great deal about this law, from the history of privacy and how, when and where it was derived from, to the current situation. The principles from the privacy protection cases in the United States of America and the laws so formed in the European Union had a big impression on how the Indian privacy bill was developed. The amount of scrutiny that topic of privacy protection had to go through in this country is unmatched. Starting of privacy invasion from the very first cases in 1880s to the famous Puttaswamy case and GRDR & CCPA comparisons today, privacy laws are yet to attain their true place in the society. The aim of the paper is to acknowledge the new laws of privacy as a forward-looking step towards success, it is also important to find a way to eradicate other present loopholes and changes need to be made to improve privacy and the safety of citizens ensuring a more fool proof way. The paper has also discussed on the ways how the privacy is indirectly invaded by the small government departments in which it insists on the special exceptions in the new privacy bill, instead taking the steps to progress towards more complete confidentiality and security. The paper focuses on the how the privacy laws developed over time, taking references from the international legal fraternity and answering the questions of whether the current developments in the privacy laws are leading us to a better or worse form of privacy protection.

Keywords: Right to Privacy, Privacy Protection Laws, Laws of Surveillance, Article 21

1. Introduction

Privacy in a novice sense is defined as '*someone's right to keep their personal matters and relationships secret*.'[1] Privacy & the necessity for it has been prevalent from as long as humankind has been in existence, so even though it was recognized formally in the 19-20th century we can very well say that it is not a neoteric concept or something which has come in vogue recently. While the term privacy may find no straightforward indication in either the Hindu literature or the Islamic literature but it would be altogether be wrong to suppose that in a gregarious society as India, privacy was an alien concept.[2] If we read the dharamsatras, acaras, vedas, smritis & puranas we would observe that man & women started to incorporate the notions of privacy once they realized what is sacred to them and what they would not like to share with anyone. Of course, their actions were not motivated only by privacy but it helps us to understand that the seed of privacy had already been sown. A great example of their ideology is depicted in their division of separate bathing areas for men and women or imposing restrictions to enter one's property.[3] Even the Bible recognizes this concept and preaches that embarrassment & anger are few of the symptoms of violation of privacy and further by the story of Adam and Eve, finds mentions of the inklings of privacy by narrating how they started hiding their private parts with leaves once realization dawned upon them.[4]

If we walk through different civilizations, then studies of various jurists express the diverse stages of privacy practiced from the ancient times to the 19th century. The ancient times portray dominance of the State over the individual's life and hence privacy was almost nil during those times; the medieval times permeated the division of powers where communities were formed for every purpose and monitoring by these groups & socializing for brotherhood was the new norm. Towards the 19th century, socializing gradually helped people to move out and urbanize in the cities for better mental and physical space and for their personal growth. However, urbanization while on one hand saw detachment and

[1]Watts, Privacy and Data Protection in Australia, https://www.w3.org/2018/vocabws/papers/watts-casanovas.

[2] Kiran K. Chauhan, judicial approach to privacy in India, HP University, https://shodhganga.inflibnet.ac.in/handle.

[3] *Supra* at 2.

[4]Bhaerav Achary, Locating Constructs of Privacy Hindu Law, CIS, Dec 29, 2014.

privacy from village monitoring and its people; on the other hand, the cities being crowded led to invasion of this privacy.

As technology progressed interesting invention as that of the newspapers & radio channels made public and private lives and secrecy about them challenging and led to increase in the conscience about the importance of a private actions in daily workings. 'Gossips', 'Word of mouth', 'public notices and announcements' were also widely used for dissemination of any kind of news for awareness which also contributed in killing the private affairs in one's life. In 1890 an article titled 'The Right to Privacy', written by Samuel D. Warren & Luis D. Brandeis which gained great fame as it was first of any document to recognize the dangers to privacy due to technological and societal developments and from this started the awakening of the acknowledgement of how to reduce such threats for smooth advocacy of a private life.[5]

The germination of the seed of privacy was backed up by acknowledgment of the difference between what is public and what should not be made public. Understandably, as civilizations advanced each and everyone wanted some part of their lives to be a private affair and not be made public. Various implications swarm in on the psyche that attempts to examine, classify and categorize in the basket of privacy ranging from the security of private property to security as an exclusive enthusiasm for name and picture, from protection as the hushing up about of one's issues to the security of inside affairs of a willful affiliation or of a business partnership or the security of sexual and familial undertakings, and so forth, the basis for differentiating varies for everyone.[6]

While the European Court of Human Rights and many research scholars assess and assert that defining privacy is not achievable due to its broad contours, a fact which has now become globally accepted is that difference lies in what is viewed as private and what is lawfully ensured as private and hence educating the people about the same has become a pertinent task to preserve their legal rights.[7] In the late years of the twentieth century a few global authoritative documents recognized the privilege to security as an original basic

[5]Adrienn Lukacs, History and Definition of Privacy, University of Szeged, Paris.
[6] *Supra* at 2.
[7] *Supra* at 5.

human right and then other nations followed in their step. Several international conventions and treaties have also made right to privacy a fundamental right. It is in Article 17 of the International Covenant on Civil and Political Rights,[8] Article 12 of the Universal Declarations of Human Rights,[9] Article 7 of the Charter of Fundamental Rights of the European Union[10] and Article 8 of the European Convention of Human Rights [11] - all these treaties explicitly mention that everybody has the appropriate rights and remedies and opportunities for a safe and secure private and family life, home and correspondence to be regarded, and they reserve the privilege to secure themselves against any unlawful obtrusion.[12]

Till now the privacy concerns of the people of India were taken care of under the Information Technology Act, 2000 but with rising issues and mistrust and abuse of power by the authoritarians this Act is proving to be an inadequate law due to which advantage is being taken of the users of data and technology. In light of the above events and with multiplying of business to different countries, rapid mechanization, growing exports and imports and amplification of telecommunication around the world it is imperative that just like other countries, India has also drafted The Personal Data Protection Bill, 2019 and has come up with a subject specific regulation for protection of privacy to protect its citizens from encroachments and wrong use of their sensitive data.

This paper takes us through the history of privacy in India, the developments in India due to which the bill had become a necessity, the problems in the bill drafted and henceforth the analysis and recommendations as to where the bill can be improved for a better implementation.

2. Evolution of Privacy Protection: Sources

The Indian constitution has always looked after the need or welfare of the people. It is considered as a welfare kind of government. So, when the topic such as privacy is

[8] UNGA, International Covenant on Political Rights, Dec 2016, United Nations, https://www.refworld.org/3ae6b3aa
[9] UNGA, UDHR, Dec 2010, 218 A (III), https://www.refworld.org/docid/3ae6b3712c.
10EU, Charter of FREU, Oct 2012, https://www.refworld.org/docid/3ae6b3b70.
11 Council of Europe, Article 8 of the ECHR, Dec 2016, https://www.refworld.org/docid/5a016ebe4.
[12] *Supra* at 11.

discussed, it is always viewed from the point of view of the user or the party whose privacy is in question. For the wide part of history, the USA (United States of America) has been the flag bearer for new regimes in law, primarily due to the fast developments in technology. In fact, for any part of the world a new development in technology always prompts a dilemma for lawmakers that, to which extent it would be right to take the new laws and sanctions. When the early thoughts of privacy were regarding surveillance cases in the USA, the dilemma was whether such surveillance would count as an invasion of privacy.

Laws of surveillance became the basis for many evolutions in the privacy protection for US, in the early years when it was observed that wiretapping does not infringe any rights under the fourth amendment but later Supreme court of US reversed its judgement and stated that expectation of privacy is to be granted safe and secure line to communicate and wiretapping will be allowed only through a judicial warrant in 1967. Meanwhile the growth in technology persuaded the government to draft the new privacy bill as the government believed that law should advance with the advancement in technology. The government also emphasised on the validity and importance of continued adherence to the fourth amendment.

Later in the years the government also stepped forward with new amendments in the privacy protection law when the World Wide Web (www) came into play. The protection of basic rights of privacy of the citizens was taken with a great seriousness and with new developments such as electronic- mail it deemed necessary. With the new law it was made clear that any type of intrusion in anyone's private space will need judicial supervision; from a third-party neutral Judge. The most recent event of privacy law adherence was seen in the case of, using infrared scanner for a home to detect illegal plantation of the Marijuana plant, where the judgement was passed as to banning the scan without judicial order.

In India, the jurisprudence related to 'right to privacy' can be recorded as early as 1880s where the British judge upheld the privacy rights of a pardanasheen women to access her balcony freely as to without fearing the gaze of a neighbour. If it was to be compared to the new world, even today the

Article 21 is the patronage when it comes to dealing with right to privacy. It was read as a vital part of 'personal liberty' under this article but until recent times it was widely believed by the government that fundamental rights would not account in for right to privacy.

It is rightly said that till humans lose something, we do not know the real value of it and take it for granted. The Supreme Court in 1954, for the first time stated that, Right to Privacy is not a fundamental right. *"In the case of MP Sharma v. Satish Chadra, it was observed that, however, free power to search and seizure would dismiss the existence of right to privacy of the, in question, dalmia group, but the makers of the constitution have not envisaged such fundamental right similar to fourth amendment in the US constitution..."*[13]

This was not the only incident where the right to privacy was rejected on such basis. Desire for privacy was recurring and once the topic was out everybody wanted to address it. The court found itself again in the same dilemma in the case of Kharak Singh v. State of Uttar Pradesh, but it was again rejected.

> "*An alleged dacoit was subjected to surveillance and secret picketing of the house, visits at nights, periodical inquiries and verification of movements. The Supreme Court refused to budge and held that there is no fundamental right to privacy but went on to strike down the provision which allowed night visits for violation of 'personal liberty'. The silver lining was Justice Subba Rao's dissent, wherein he said even though the Constitution did not declare the right to privacy to be a fundamental right; it was still an essential ingredient of personal liberty. He went on to say, nothing is more deleterious to a man's physical happiness and health than a calculated interference with his privacy, thereby recording the existence of this right in our post-independence jurisprudence*".[14]

In 1975, in the famous Gobind[15] case, it was upheld that article 21 and the right to privacy will be read together, twelve years later, the right however is not absolute and can be intervened by procedure of law and proper judicial supervision and authority. This was the first time that right to privacy was anywhere acknowledged in the Indian legal sphere.

[13]M. P. Sharma v. Satish C, 1954 AIR 300.
[14]Kharak Singh v. State Of UP, 1963 AIR 1295.
[15]Gobind v. State of MP, AIR 1975 SC 1378.

It is observed that the jurisprudential part of privacy law strengthened even more in the era of post liberalisation. In the case of R. Rajagopal v. State of Tamil Nadu,

"*the Supreme Court dealt with a conflict between the freedom of press and the right to privacy and held that the latter had acquired a Constitutional status, in this case of the infamous gangster from Bangalore, Auto Shanker. A couple of years later in the PUCL case, the court questioned the telephone tapping of prominent politicians and asked the government to comply with strict guidelines for tapping telephonic conversations. The provisions under the Telegraph Act, 1885, and Information Technology Act, 2000, that deals with interception are based on the guidelines issued by the Supreme Court in the PUCL case*".[16]

The laws on privacy protection have given assurance every now and then that we can lead a life without fearing being under surveillance. The issue of privacy has never seen such a challenge as it is being continuously reviewed by the judges and even the decision in the case of MP Sharma is in question whether it is a good law.

Currently, right to privacy enjoys a three pillared support combined given by the *"right to equality (Art. 14), right to freedom (Art. 19), and right to life (Art. 21),"* but it is not absolute so it can be taken away. However, the pillars, so mentioned can only be amended by just and reasonable law (with the exception to the basic structure) which is a primary protection given to us by the Indian Constitution.

Some other important cases on the line are the case of PUCL v. UOI[17], It was held that the voters in India have a right to attain information on the politicians so selected by a fair election, under Article 19(1)(a). The PUCL had filed this case against the law of 1951, which gave full freedom to all the politicians and granted them such freedom that they were not to unveil any private information. The court ordered which overruled the 1951 law and directed that the basic information about the candidates must be made available, so that the voters can make an informed decision and discuss the merits and demerits of the candidates openly.

[16] Rajagopal v. State of TN, 1994 SC (6) 632.
[17] PUCL v. UOI, AIR 1997 SCC 568.

Famous Puttaswamy Case[18], in 2017 the court with the nine- judge bench stated about the privacy right that it will be read under the Constitution of India and this judgement overruled the cases of M.P. Sharma and Kharak Singh, so discussed above. The scenario not only made privacy legitimate but also made it one subject which was faced through the highest level of judicial scrutiny. The judges observed that the "Privacy is the ultimate expression of the sanctity of the individual". The judges also avowed the grounds for the PUCL case. There were mainly five observations made including:

1. Reasonableness test must be adhered to under Article 14 when violation of privacy made with regards to state action.

2. Invasion of privacy under freedoms granted by Article 19 will be observed under the trial for obscenity.

3. Under Article 21, intrusion in one's personal liberty will be tried fairly, and with reason.

4. "Fair, just and reasonable", must be followed when topics such as phone tapping are requested from the judiciary by order, as it not only infringes art. 19 but also rights granted under art. 21, it is to be allowed only when "compelling state interest" is involved.

5. A new test of legitimacy and proportionality was also instituted.

The history of privacy laws is vast, be it accounted for nationally or internationally but the important growth time line can be contained in the abovementioned cases. The current scenario maybe certain or uncertain but the history never changes and thus this is the landmark judgements which has changed the way Indian judiciary views privacy protection forever.

3. New Era Growth in Privacy Protection Laws

Privacy laws have faced more struggle and scrutiny than any other law in the world. In simple terms privacy is an inviolable private space; still there are discussions today which state that need for privacy is a relatively modern phenomenon. This statement may hold

[18] Justice K.S.Puttaswamy (Retd.) v. UOI, (2017) 10 SCC 1.

some truth to itself, but during the last century, with the rapid growth in population, urbanisation, industrialisation and growth of technology the need for privacy and cases of privacy invasion have grown with all the development. Privacy is popularly defined as the right against exposure to public or private matters; matters which are of private nature can easily be distinguished and can be kept in the sheets, there is no doubt in that. However, the matters of individualism have always been the product of collectivism in the pre-dominant patriarchal society like ours, so the revelation of such public information or acts can act as moderation on privacy protection.

The idea of privacy protection, as is very evident from history, has originated from old law of Torts and the constitutional rights. Still, the basic ideology of privacy protection has been borrowed from the American cases and largely from European jurisprudence in the later years of development. Privacy has always been an autonomous zone and never has it been developed as a specific right. The scheme of such protection has always led to a life with no interference in making choices and taking decisions. The constitution of India does not grant any specific right to the citizens in terms of privacy protection till date. In the latest development the Personal Data Protection Bill, 2019 has been presented as after the puttaswamy case. Before this the court in the case of Govind v. State of MP[19], recognised privacy as a penumbral right under Articles 19 and 21 of the Indian Constitution. The Supreme Court in another case asserted that the status constitutional right must be granted to the privacy protection as it is a very basic right and must be enjoyed by every citizen. In the past several police regulations were upheld when compared for the free rights of search and seizure under the Police act.

It is widely observed that the government agencies enjoy full autonomy and many exceptions when it comes to the small business entities, the way of collection of manual data and treatment of non-personal data is a huge defence and there are instances where such small actions are being treated as criminalised actions. The new bill gives the government a way to make such exemptions on a wider scale. The old bill however made such exceptions but in the pursuance of the national security only. The question of necessity and proportionality is being faded and the new authoritative approach can be observed.

[19] Gobind v. State of MP, AIR 1975 SCC 1378.

These government agencies are on the list that enjoys full autonomy and privacy exemptions.

The bill defines certain rights of the individual too, like the rights such as, the right to obtain confirmation from the trustee about the processing of their personal data, where the personal data helps the individual on the financial level, some aspects like ability to request for any corrections, incomplete or outdated personal information, in any government and non-government institution. The other part of the bill about the personal information leads to provisions related to the personal information to any other alternate information to be disclosed by any trustee, this is another characteristic given to the personal information in the bill.

Another most important part of the Puttaswamy case, advised the government to set up authorities for implementation of regulations in the bill. The bill establishes an authority which will work on the data protection which indeed can take action and implement laws in order to protect individual's data and privacy. Such committee will be run by and comprise one chairperson and other six members. Each member is to have at least 10 years of expertise in the matter to deal with the issues in an accurate manner. The individual may appeal to the court against any order given by such committee. This bill also amends the 2000 IT Act and removes any such provision which made businesses pay remunerations for the personal data not protected.

4. Predicaments: Data/Privacy Protection Laws

The rate of growth towards fully realizing that right to privacy is a fundamental right has been one in dribs and dabs, but each case has been directing towards a progressive future. Moreover, it has been observed that each legal case has been a landmark in itself as they arose from grave loopholes in the law or negligent nature of implementation of legal rules or no regulations at all. For a long time the State and few powerful companies kept making profits at the cost of the uninformed public but the advent of global developments and India's jurisprudential advancements functioned as a magnet towards helping to recognize that we still have a long way to go to recognize privacy and protect its various forms and save vis-a-vis the rights of the citizens.

The bill as we have today i.e. The Personal Data Protection Bill, 2019 emancipates from a conflicted nature of precedents which were the outcome of some very famous issues and which were discussed and debated across the country and then finally taken up by the legislature, executive and the judiciary administrators of the nation to address them and formulate the necessary regulations to protect the sanctity of the constitution and the rights granted under it.

We have endless examples of how earlier the voices were raised to protect only the individual's privacy rights and distinct interests such as in the case of Kharak Singh[20] where concerns were raised against the police visits at night or like in the case of People's Union for Civil Liberties v. Union of India,[21] the issue of telephone tapping was debated over or like in Selvi and others v. State of Karnataka and others[22] where attention was drawn towards difference between mental and physical solitude. It is only in the recent years that people have grown to accept that the issue of privacy is a much bigger subject which needs to be protected at a collective level. The famous Adhaar case is one such example here where it was observed that protecting biometric information of the citizens is crucial and that its transfer to any third party should not be conducted without the consent of the effected people. Undoubtedly it is the awareness & the positive tread in the direction of concrete privacy safety legislation which brings us to the present-day Personal Data Protection Bill,2019, however, the bill remains far from being a solution and has become a piece of controversy due to its political undertone and farfetched ideology.

It is no hidden fact that the bill is guided by the principles of General Data Protection Regulation and the Asia-Pacific Economic Cooperation Privacy Framework which itself are facing the issue of senile decay as they originated in the 1970's, hence it widens the gap of reality and data regulation when taken into account from India's practical situation.[23] While countries which already have their laws based on these frameworks have evolved them according to changing times, it is a questionable step when it comes to India firstly

[20] *Supra* at 14.
[21] *Supra* at 17.
[22] S. Selvi v. Karnataka State (2011) 7 SC 263.
[23] Alex J. Wall, GDPR Matchup, Apex Privacy Framework, IAPP (Dec 2019).

due to the dilatory emergence of the Data protection Bill and secondly due to the diverse and rare situations prevailing in the country.

One of the major problems with the bill is the huge amount of weight age it given to the abstract notion of Consent and the authority which is then granted to the other party with accepting such affirmations. Even today when the majority of Indian population is still in shadow about the enforceability of online agreements, the bill dispenses provisions requiring consent without taking into account the previous studies which have suggested that users spend less than 6 seconds to read any e-contract and only 8% read the whole agreement before installing software.[24] Moreover, an American survey of 2018 reveals that 74% of participants of a total of 543 surveyed, preferred quick mode option to skip the policy section and therefore 90% of the total preferred the quick join click wrap method more as it helps to spring towards the main content without much ado.[25]

Regardless of the rules to be complied by data fiduciaries and the penalties in case of violations,[26] on the basis of the changing trend it is observed that the bill portrays consent as a meaningless aspect which instead of a method of protection of data has moreover become a risk by making it a relatively unchallenging task for third persons to procure sensitive information and further only augmenting the preexisting affairs.

The implementation of the bill would also see a vulnerable impact on the economic bounds of the data processing firms of the country. The imposition of the bill demands compliances to various terms and conditions, require fulfilling of regulatory requirements at each step, orders for meeting the improvised standards and dictates mandatory conditional processing of data by all the firms in this specific industry as laid down by the government and the data protecting authorities. Moreover, section 15 of the bill iterates that the government and the regulatory authorities may specify more additional regulations and constraints along the way, which reveals that such data processing and regulation costs are not one-

[24] Jeff S., Do Users Read Licenses, (Jan 11, 2011), https://measuring/eula.
[25] Oeldorf H., The Biggest Lie on the Internet, 44th Research Conference on Communication (2016) SSRN: http://dx.doi.org/10.2139/ssrn.2757465.
[26] The PDP Bill, 2019, Sec. 61(6).

time decisions but rather would result in multiplying the compliance cost for the bearers at unexpected times.[27]

Agreed, that under the bill there are exemptions for manual processing by small firms, however it is a tricky situation where exemptions can be availed only after bearing the burden of other compliances like they should be engaged in the process of manually processing their data.[28] While one might see these tariffs as a crucial inclusion in lieu of forward sightedness and developments, it is a fair argument that the magnitude of effect that it would have on small and upcoming firms is incomparable to the dominating powers of the industry and would consequently result in paving a vying path for the budding and small firms.[29] Further the recent 2018-2019 report of Ministry of Micro, Small & Medium Enterprises suggests that in India maximum number of industries is classified as micro level industries,[30] which as history suggests flourish only with the supportive concessional policies of the government. Hence, the effect of this struggling competitiveness & huge economic fee on data processing companies diverts the attention from the original aim which is fairness in the procedures and protection of the data procured.

One of the gray areas of the bill arises from Section 91(2) which says that in order to deliver advanced projected service & schemes the government can lay hands on the personal and non-personal data collected by the data fiduciaries.[31] This subsection creates much uncertainty to the users of the bill and gives the government the opportunity to mould it in their favour. The provision seems to be a paradox to the very agenda of security of information and privacy rules. This section opens a bag of plethora of questions like how the data expropriated would be utilised or whether the data fiduciaries be entitled to receive any incentive in return for the same or what effect will it have on the rights of the people whose data it is or can this section be given effect only on a circumstantial basis or how can this action of government be categorized as crucial step in light of national security?

[27] The PDP Bill, 2019, Sec. 15(2).
[28] The PDP Bill, 2019, Sec. 39.
[29] J. Thomas & D. Bailey, 'Regulating Away Competition,' Marcatus Centre, https://www.mercatus.org/Bailey-Regulation-Entrepreneurship (2016).
[30] Ministry of MSME, GoI, "annual report 2019", https://msme.gov.in/relatedlinks/annual-report.
[31] The PDP Bill, 2019, Sec. 91.

Furthermore, the bill has a very strong undertone of being authoritative i.e. it bends in the favour of the Data Personal Authority & the government more than being consumer friendly or rather an unbiased one. For example, Section 35 of the bill is one such section which lays down that the government agencies can be exempt from the provisions of the bill under various circumstances.[32] It is believed that granting such powers to the government is detrimental because it negates the role of safeguards against government surveillance.[33] This expands the scope of government to excuse the exercise of surveillance by utilizing this section as an excuse. The vast powers given to the Data Protection Authority by way of the provisions seems to be done with the attempt of pulling the strings of the e-commerce trades and other negotiations which involve data processing. It wouldn't be shocking to know that this world's biggest democracy ranks third after Russia and China in surveillance its citizens as confirmed by a UK firm Compritech.[34]

Well, the grounds of India failing in this arena are many but some of the main issues which contribute to such ranking are the Aadhar surveillance where biometric information of millions have been at stake, then the weak data protection bill is also a reason, further government's repeated efforts to monitor Facebook and WhatsApp accounts in the name of tracing threat messages is also a cause, then the rules relating to Closed Circut Tv's are also not very straightforward etc, the conditional exemption on usage of drones by government entities for the Covid-19 related operations for aerial surveillance & photography[35] etc. explains a lot about India scoring a 2.4 out of 5 by falling in the domain of failing to maintain privacy safeguards.[36]

Making the authority an overpower is feared as the governing body can take advantage at the cost of the public at any given time and still turn it around to present it in a way of public good. No rules and checks on these bodies are another concern. It has been seen that

[32] The PDP Bill, 2019, Sec 20.
[33]Aneerudh Barmun, India's Proposed PDPB will be able to Protect Privacy and Promote Growth, Carnegie (Apr 10,2020), https:/carniegeindia.org.
[34]Poul Bichuf, Privacy laws and govt. surveillance: Citizens are safe in which nations? (Oct 16,2019), https:/www.comparetech.com/blog/.
[35] The ongoing illegal use of drones for mass surveillance by the Delhi Police needs to be investigated #SaveOurPrivacy, Internet Freedom Foundation (June 23,2020), https://internetfreedom.in/the-ongoing-illegal use-of-drones-by-the-Delhi-police-needs-to-be-investigated.
[36]Niharika Sharma, India's amongst the world's top three surveillance states, Quartz India, Oct 16,2019 at https://qz.com/india/1728927/indias-among-the-worlds-top-three-surveillance-states.

regulatory bodies who have independent persons as their members tend to provide an unbiased insight and their decisions are welcomed in a much way. The DPA is supposed to refer its draft policies to the government before implementing them,[37] but who is it to say that the government cannot use this provision for their personal gains and ulterior motives. As, revealed by Internet Freedom Foundation in their articles, the government is already involved in ways of discriminatory censorship where the personal and non-personal data of individuals is now being taken into account for verification of facts and detection of misleading statements by common public.[38] The government who was trusted with upholding the citizen's rights are themselves entailing & indefinitely retaining such sensitive personal information without our knowledge and assent and this has become a draconian power in their hand. Hence, the bill doesn't attempt to make anything transparent or creates any scope for open platforms for discussion for the public but only leaves things hanging and in the hands of authorities for the worse.

In this era of rapid globalization and intensive communication where citizens are being increasingly proactive in voicing out their plights, it is pertinent to bring forward the shortcomings of the Data Protection Bill for better advocacy of our rights so that more insightful and intelligent laws are made and resultantly an end is put to "*severe capacity constraints, highly discretionary & discriminatory powers, and inadequate accountability mechanisms*".[39]

5. Analysis and Review

From the above discussion, it becomes quite clear as to why the bill instead of being a positive sign, has become more of an alarm of caution for data processors and the people whose data is being taken. As the world is becoming more technologically advanced, India is also treading its way to become a full working digital economy. India has seen a progressive rate of growth in its aim to become a safe country for personal data from formation of Justice BN Shrikrishna Committee, for a much larger debate for 'privacy and

[37] The Privacy Data Protection Bill, 2019, Section 50(4).
[38] Surveillance of social media users is not the solution for fake news# Saveourprivacy, Internet Freedom Foundation (June 19,2020), https://internetfreedom.in/legal-notice-becil-tender-social-media-monitoring-tool.
[39] *Supra* at 25.

related concerns', to drafting of the 2019 bill. However, the committee and its discussions and the resultant bill turned out to have major fallouts and hence have created room for healthy discussions and transitions. One of the major causes of eyeing the bill with suspicion is the preceding series of actions of the ruling governments and their attempts at accessing & controlling sensitive personal data of the citizens at the most frivolous issues.

If one sees the Comparitech report on the surveillance strategy of each country, it is apparent even to a layman that India is on the steps of China, the number one country which fails at protecting citizen data and more so aims to invade it. On drawing a comparison chart of Indian privacy policies to Chinese policies, it is seen that just like in China, where ID-cards are mandatory for 16 above aged citizens & biometrics is heavily used, the Indian government has also made incessant attempts to do the same previously by way of mandatory Adhaar. Even after the Aadhar card judgment, the authorities did not stop and have in the wake of COVID-19 pandemic concocted another controversial health application which works by accessing the mobile's Bluetooth and tracks the phone's owner's location 24x7. This Arogaya Setu application which was launched primarily to keep up with corona virus cases to make it easy to trace the disease affected people but was gradually resented against after studies revealed how it uses privacy invasion algorithms and further the government's gradual declarations of making it compulsory for travel and at jobs had revealed their ulterior motives eventually.[40]

It is appalling to know that even when Justice Krishna Committee was constituted for recommendation regarding the data privacy matters, the suggestions of that committee were not taken into consideration while drafting the bill. After the proposed bill came out, it was revealed by Justice Srikrishna (retd.) that the sections related to governmental control on citizen's privacy information were considerably different and he commented that such changes can result in preposterous & perfidious future for the nation. A research committee is one which forwards its solutions and issues by a wholesome study and aims

[40]Aandreu Clarence, India's Aarogya Setu: The Controversy behind tracing app, bbc news, May 16,2020 at https:/www.bbc.com/news/the –controversy-arogya-setu.

at bridging the gap between the citizens and ruling government and hence the government should have adhered to the findings so that accountability related issues do not rise.[41]

While the Indian Privacy Bill is also on similar lines of General Data Protection Regulations, 2016 (GDPR) and the California Consumer Privacy Act of 2018 (CCPA) but it still has scope to be a more inclusive and pragmatic one. The Comparitech report along with the rankings of the countries regarding data surveillance, also states that the top 5 countries which fall in the category of upholding "citizen's privacy the most" have high to medium success rates because they faithfully follow the General Data Protection Regulations, 2016. In order to better comprehend & improve the Data protection bill, 2019 it is imperative to analyse it in a parallel manner with the GDPR bill. The authors in the subsequent paragraphs have put in their observations regarding both the bills and subsequently proposed methods for a more practical way ahead.

The PDPB, with respect to the notice and consent lay down the similar stipulations as that of the GDPR bill. Moreover, under section 23 of the PDPB, the new concept of "Consent Managers" has been introduced which could possibly bring in better division of work.[42] Moreover the PDPB present the consent withdrawal provisions in a broader manner than the GDPR one. Further, the people who have given their consent should be given the onus to decide whether any contractual violation is harming them or not rather than the government making these decisions. This does not mean that boundaries shouldn't be made for the data fiduciaries and data processors, but in order to make the bill more consumers friendly, this step seems fitting.

When it comes to the legal rules of Data Processing, it is observed that as differed from the GDPR Bill, the PDPB does not recognise 'legitimate interests' as grounds for data processing to the data processors who determine the relevant purposes but instead introduces the term 'reasonable purposes' in its place and these purposes will be determined by the Data Processing Authority.[43] The very step of giving DPA the role &

[41]Suresh Kumar, An evaluation of the role and working of parliamentary committees of India, Jamia Hamdard University, http://hdl.handle.net/10603/12212.
[42]The PDP Bill, 2019, Sec 23.
[43]The Privacy Data Protection Bill, 2019, Clause 15.

power to decide the rationality is in itself an objectionable idea as it can lead to restricting the type of activities authorized under this provision. [44]Under this arena of processing of personal data, Sec 12 of the PDPB seems to be rather overpowering provision for the government which could result in detrimental for the public as it does not require consent and only enumerates rather open-ended conditions when this consent wouldn't be needed.[45]

The PDPB, for storage of data moves on different lines from those of the GDPR. Under section 9 of the Indian privacy law, the data needs to be deleted once the purpose has been exhausted and explicit permission of the data principal is required to seek any extension.[46]

It is observed that while this measure might seem as a good privacy protector way, it is not very practical. This might result in deleterious repercussions as it would mean utilizing the technology for the same thing over and over again. Collection of data is a perpetual process which combined & processed with artificial intelligence produces new results for the authorities. Hence, instead of storing the consented data and rather deleting it only adds to the cost of the processors.[47]

Moving to the provision of breach notifications, the GDPR provides a 72-hour window to the DC's to inform the supreme authority of the breach of personal data.[48] However, it is only when the data principles are affected negatively to a great extent that the Data Processing Authorities are to be informed. Furthermore, the data fiduciaries are entitled to update the data principles about such breach only at the discretion of the Data Processing Authorities.[49]

While in terms of security and adherence to rules, both the GDPR and the PDPB present a similar thought process, the difference lies in the modus operandi. Under the Privacy data protection bill, only few specified firms are supposed to undertake the data protection impact assessment (DPIA) under specified circumstances that too at the discretion of the

[44]Kurt Wimmer, Gabe Maldoff and Diana Lee Covington & Burling, COMPARISON: Indian Personal Data Protection Bill 2019 vs. GDPR, International Association of Privacy Professionals (2020).
[45]The PDP Bill, 2019, Sec 12.
[46]The PDP Bill,2019, Sec 9.
[47]*Supra* at 25.
[48] General Data Protection Regulations, 2108, Articles 19,33, 34 and 55.
[49]Ratul Roshun and Sreenidhee Srinivasan, EU analysis: GDPR,2016 and the PDPB,2019, mondaq , Mar 13,2020 at https:/www.mondaq.com/913076.

DPA, as opposed to the GDPR where all DC's have to undertake DPIA's and maintain records of the same.[50] However, what we can probably learn from the GDPR is that we should make the conditions for conducting DPIA broader so that such necessary assessments bring in lucidity in the system.

The data localization and the cross border data transfer also require mention here as they form a pivotal role in the privacy field.[51]While there are no restrictions on transfer and processing of personal data outside India, but the sensitive personal data on the other hand requires explicit consent and can only in special conditions be processed outside India under the supervision of the DPA or the government.[52] This differs minutely from the GDPR where the compliance provisions are comparatively of a broad spectrum and less strict.[53]

It is apparent that a comparison with the GDPR makes it easier to conclude that the PDPB is not all diabolical. Be that as it may, the huge magnitudes of data being accessed and exchanged, the burgeoning of inventions, the mushrooming of rapid digital connections and the birth of unknown imperils alongside make it next to impossible to settle on any one plan of action for the best outcome. The PDPB sets forth many bracing provisions of which one such refreshing concept is that of the Data Sandbox, which is a paramount step of the authorities to boost the start-ups and the already existing firms to indulge in technologically advanced practices. As rightly said by Arun Prabhu of Cyril Amarchand and Mangaldas, about the same that this step of the government has been in the wake of balancing innovation needs of the country along with the privacy concerns of the citizens and consequently this would definitely result in a high yielding output for the nation.[54] Further glancing at the grievance and Redressal mechanisms provisions, one will learn that the GDPR does not provide any specific time period for addressing the grievances[55] while the

[50]*Supra* at 36.
[51]*Supra* at 50.
[52]The PDP Bill, Sec 34.
[53]GDPR, Art 44 and 48.
[54]Yuvraj Maleek, data rules exemption to companies, business standard, Dec 12, 2019 at https:/www.Business-Standard.com/article.119121100027_1.html#:~:text=The%20government%20has%20proposed%20that,rules%20for%20a%20limited%20period.&text=According%20on%20such%20requests.
[55]General Data Protection Regulation,Article 38,57,77,78,79 & 80 along with recital 97.

PDPB bill lays down a 30 day window for the addressing any issue.[56] This grievance and Redressal limited time period is a very thoughtful and a very suitable provision when the Indian socio-economic factors and past precedents are taken into account.

It is not that the government is benighted about the data concerns and privacy issues but their empirical workings of the past have been such which make the citizens question their actions. Only recently the Broadcast Engineering Consultants India Limited (BECIL) requested for tenders for their new project of "Solution & Services related to fact verification and disinformation detection".[57] The very purpose of their project was atrocious as it was to be informed about the online disinformation campaigns & related news & dissent against the government by individuals on their social media platforms and to establish an archive for such repeated offenders. This was then opposed by various institutions and they were also served with a legal notice by the Internet Freedom Foundation as this step of the authorities highlighted discriminatory censorship, violated the fundamental rights like right to privacy, freedom of speech, freedom of association.[58]

The protectionist policy approach adopted by the authorities for the sake of protecting data in the name of national security, state integrity or any related purposes are rather flexible terms which can be molded and utilised in any manner to further their purpose.[59] Not only the Indian companies but the Silicon Valley entities like Facebook & Amazon, operating in India have also criticised regarding the stricter policies proposed.[60] The aim of balkanization of internet of the Indian government invites the possibility of domino effect and consequently might trigger the possibility of back lashing at the Indian start-ups in these times of massive globalization and rapid competitiveness in the International and domestic markets and may affect the exchange of cross border data.[61]

[56]The PDP Bill, Clause 32(2).
[57] BECIL: legal notice to it about its tender for employee tracking watches at https:/internetfreedom.in/legalnoticetobecilagainstmasssurvelliencesystem.
[58]*Supra* at 57.
[59]Kareeshma Melhrotra, the debate around PDP Bill, The Indian express, dec 8,2019 at https:/indianexpress.com/article/explainedall-6053016.
[60]Karan Dweep, Indian data privacy charting on its own, The New York Times, 11 Nov, 2019 at https:/www.nytimes.com/technology/onitsownpath.html.
[61] *Supra* at 39.

Up till now it has been the Information Technology Act, 2000 and its amendments of 2008 wide its Section 43A and 72A which governed the dealing and processing of sensitive personal data and breach of contractual obligations respectively.[62] "However, as we move towards being a developed nation with expansive international trade relations and digitalised transactions we needed a robust framework in order to prevent foreign surveillance, continuous hacks in our Indian databases and access of sensitive personal data by arbitrary authorities".[63] Henceforth, an all-rounder, comprehensive roadmap is required to integrate compliance measures & stringent policies along with an equipped & well trained regulatory bodies and law enforcement agencies for a powered enforcement of the Privacy Data Protection Bill, 2019 in order to avoid possibilities of violation of the most basic rights of the citizens.

6. Conclusion

Privacy as a fundamental right is a versatile and complex concept, which can be deduced from the above discussion. This involves maintaining personal privacy, the privacy of a personal life, sex, orientation and even intimate moments of a closed house. This gives and protects the rights and demands to be left alone. It not only gives oneself the freedom to control their own lives but also gives them self-determination to make their own decisions regarding any matter without interference. The right also lets people and society grows on its own pace especially for such a diverse society like ours. The definition of privacy fits all the aspects of fundamentalism and thus should at least be a fundamental freedom. Legal jurisprudence continuously evolves and has lately included privacy of sexual intimacy therefore it is high time that we as a society also recognise it publically and give it liberty to take its due course. The latest development was that Indian judiciary decriminalised adultery (Joseph Shine case) [64] which was long outstanding, as if observed from an international prospective, as it was an ancient belief, based on sexual privacy. The time has also come to criminalize the rape in marriages that silences a woman's sexual intimacy and sexual freedom. The ability of state and non-government agencies has significantly

[62] Bhumesh Verma,Sayantan Dey, Ujjwal Agrawal, Student Researcher Corp Comm. Legal, (2020) PL (CL) February 74 at https://www.scconline.com/blog/post/2020/02/06/evolution-of-data-privacy.
[63] *Supra* at 62.
[64] Joseph Shine v. Union of India, 2018 SCC On Line SC 1676.

improved. Unauthorized leaks, burglaries, and other cybercrimes have made databases vulnerable. In this context, the technology-neutral privacy bill was submitted in 2012 by "Justice A.P. Shah Commission." [65] Depending on the increasing requirements, different countries have established different legal frameworks such as the Data Protection Act, 1998 in the United Kingdom, the Private Electronic Communications Act, 1986 in the United States, etc.

The technology we use today be it our phones or be it any other device contains a huge amount of such private data, for which we fear invasion. Our justice delivery system is yet to declare a separate part of law to regulate the Artificial intelligence laws and issues related to privacy protection of personal data. Though we do have an Information Technology Act, but the current need of the hour is to attain such autonomy that we can protect our data on state and individual level from national and international invasions. In 2018, "*Justice BN Krishna Committee released a white paper to ask opinion of general public for such laws.*"[66] The current need is for a law which is specific and which has a perfect outlined implementation and strict sanctions. New privacy protection bill 2019, thus indulges in many such topics which became a hotwire in the privacy protection system. The need of the people and the encouragement to protect their private information from the public domain has primarily and has been a focal reason for these developments. However, even after pros and cons, the bill contains important aspects such as consent, reasonable purpose, the processing of personal information only with consent. We can hope that the bill will be recognized as law in the next budget session.

[65]Anunya Chulroborty, accountability principles-9 data privacy principles, Aug 25,2017, https:/www.news18.com/righttoprivacyfundamentalreport.

[66] Reeshikesh T. Krishnan, Under the chairmanship of Justice B. N. Shrikrishna- A fair & free digital economy, Jul 28,2018, https:/meaty.gov.in/freeandfaireconomy/Committee_Report