Symbiosis Law School, Nagpur Multidisciplinary Law Review
Volume II Issue II (2023), ISSN: 2583-1984 (Online), Pg. Nos. 124-142

UNRAVELLING THE DATA PROTECTION ACT: UNVEILING ARBITRARINESS, VAGUENESS, AND GAPS

Samrudhi Memane*

ABSTRACT

The instant article intends to review the recent Data Protection Act that has been rolled out by the Government. A single reading of the act brings to our notice a lot of fallacies present in the act.

This article majorly focuses on the arbitrariness, vagueness and lawlessness present in the provisions related to the exemption granted by the act to certain governmental authorities and also another provision related to Alternate Dispute Resolution which seems to have been added just for the namesake. The issues with the Act do not take a halt here, it produces further scope for misuse by saying that the guidelines for enforcement of certain provisions will be introduced later. The article has also brought to light the diversion this latest draft has taken from the intent with which this Act was originally decided to be brought into existence.

The author through this article has also attempted to find out ways through which the vagueness can be converted into concreteness, and the gaps that are prone to misuse are filled up in a way that justice will be served to the citizens. Lastly, the author concludes that the question raised initially in the article was actually unanswerable by the current draft Act and there need to be many more detailed provisions to be added to them and avoid any confusion.

***Keywords**: Alternate Dispute Resolution, Arbitrary Exemptions, Safeguards, Vague Drafting.*

* Student, BA LLB (Hons.), National Law Institute University, Bhopal, Email id: samrudhimemane.ug@nliu.ac.in.

UNRAVELLING THE DATA PROTECTION ACT: UNVEILING ARBITRARINESS, VAGUENESS, AND GAPS

Introduction

In the year 2017, the Supreme Court came up with a landmark judgement in the case of Justice K S Puttuswamy (Retd.) v. Union of India[1] and finally recognised the Right to Privacy as a Fundamental Right. Even after this judgement, there were problems revolving Right to Privacy[2] concerning Data breaches, Surveillance, Data Collection and Sharing, Online Tracking, advances in biometric data, Artificial Intelligence and Machine learning and most importantly that all of this lacked regulation. With these issues around privacy, there subsequently arose questions about data. Data in all aspects may be digital or in any other form.

The Justice Srikrishna committee was appointed by the government in 2017 to solve such questions. The committee finally submitted its report[3] in 2018, emphasising citizens' interest. The highlighting aspect of this report was the proposal to draft a Data Protection Bill. The main objective of this bill was to provide the citizens with a "Free and fair digital economy". The Act was modified a little and introduced as the Personal Data Protection Bill, 2019. [4]

When this 2019 draft was sent further to an ad hoc joint parliamentary committee, the committee submitted another version of the same document after additional modifications in 2021. This was published as the Data Protection Bill, 2021.[5] By the time these modifications were processed, the initial idea about protecting the interest of the citizens had moved over to safeguarding the government's interest over the citizens' privacy. This is where the act is being questioned by many. The initial objective of the act was to work on the challenges of privacy that have been arising due to the accelerating technology. However, there were several debates

[1] *K S. Puttaswamy (Retd.) and Anr. V. Union of India and Ors*., (2018) 1 Supreme Court Cases 809.
[2] Pranav M B, "Fundamental Right to Privacy- Four Years of the Puttuswamy Judgment", The Centre for Internet and Society (August, 2021), https://cis-india.org/internet-governance/fundamental-right-to-privacy-2014-four-years-of-the-puttaswamy-judgment.
[3] Justice Srikrishna Committee, "A Free and Fair Digital Economy Protecting Privacy, Empowering Indians" (2018). https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.
[4] The Personal Data Protection Bill, 2019 (Act 373 of 2019) http://164.100.47.4/ActsTexts/LSActTexts/Asintroduced/373_2019_LS_Eng.pdf.
[5] The Digital Personal Data Protection Bill, 2022 https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Protection%20Act%2C%202022.pdf.

ISSN: 2583-1984 (Online)

about the bill due to its drastic diversion from its ulterior objective. As a result of which a parliamentary panel was set up, which propounded 81 amendments to the same. Also, another 12 recommendations were made to build up a "comprehensive legal framework" for the citizens of the digital world. A Joint Parliamentary Committee chaired by Member of Parliament Shri P. P. Chaudhary submitted its report[6] on the same bill on 16th December 2021. The committee which was asked to make the act more comprehensive and beneficial for the people turned out to be arbitrary with its suggestions. The suggestions of the committee have diverged the nature and scope of the bill from its originality.

This article shall give an overview of the same problems created by the draft bill of 2022 which was given for public suggestions and which later took the shape of legislation through The Digital Personal Data Protection Act, of 2023,[7] and in what manner can it be modified to balance out the rights of the citizens and the protection of the security of the nation. The article shall in detail look over the two big issues created by the act separately which are:

1. The arbitrary and unrestricted exemptions granted to governmental agencies, and
2. The ambiguity around the working of the Alternative Dispute Resolution Mechanisms.

Finally, the article shall put forward certain suggestions to resolve these challenges.[8]

The Issue with The Exemptions Granted to Governmental Agencies:

The Draft Bill as under Section 18[9] has granted an exemption to governmental agencies on the ground of national security. The Act has just arbitrarily granted exemptions without thinking about its impact. However, the chances of users' data being misused cannot be ruled completely. Hence, there also needs to be some sought of surveillance. These same clauses have been used even in the final Act of 2023 under Chapter IV.

[6] Joint Committee Report, "The Personal Data Protection Act, 2019" (2021) https://loksabhadocs.nic.in/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Act,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Act_2019_1.pdf.
[7] The Digital Personal Data Protection Act 2023.
[8] Note: Act in this Article would mean the final Digital Personal Data Protection Act 2023, and Bill would mean The Digital Personal Data Protection Bill 2022.
[9] The Digital Personal Data Protection Bill 2022, s 18.

ISSN: 2583-1984 (Online)

The major problem is with the wording or drafting of this section. It is very vaguely drafted and left open-ended to the wide interpretation of the reader, which elevates its likeness to be misinterpreted resulting in misuse.

The section fails to elaborate upon the indeterminate nature of the grounds of exemptions like "public order" as stated in Clause 2(a)[10] of the Bill. Another term which is left very open-ended is "any legal right or claim" as said in Clause 1(a)[11] of section 18 of the draft bill as well. The vagueness created by the terms of this section instead of making the law comprehensible and simple is adding to the confusion and also possible misinterpretation and misuse.

Furthermore, the section failed to encompass the suggestions the Joint Parliamentary Committee gave to improvising this section. The committee had suggested introducing a "just, fair, reasonable, and proportionate procedure" to safeguard against this section's misuse.

The Act states that exemption will be granted to all government agencies from the application of the provisions of the Act. The rationale given behind this is that it has been done to safeguard the sovereignty and integrity of the country and national security. However, a blanket exemption will create a lot of problems in future.

To avoid these possible challenges, either of the following provisions can be adopted instead:

1. There shall be certain provisions yet applicable.
2. There shall be some other authority created for keeping surveillance over governmental agencies.
3. There can be a set of different rules, which are lenient, that can be imposed upon governmental agencies. However, the government shall elaborate upon the rationale of these rules.

Another ambiguity that this section has created is, 'Whether this section would apply to semi-governmental agencies. This can lead to further misuse by many private sector partners of the government. Hence, all provisions of this statute shall be made applicable to all semi-

[10] The Digital Personal Data Protection Bill 2022, s 18 cl. 2(a).
[11] The Digital Personal Data Protection Bill 2022, s 18 cl. 1(a).

ISSN: 2583-1984 (Online)

governmental agencies. Even if there is any minute interference by private agencies, the Act shall be made applicable in its entirety.

Even in the case of governmental agencies, the exemption cannot be given in a blanket form to all. Only in cases where secretive or sensitive information is being processed can there be an exemption granted. A way to resolve the ambiguity, in this case, is to propose certain criteria. The agency shall comply with these criteria, only then can the exemption be granted. The following criterion can be adopted with any additional changes required:

1. Those organizations that deal with the country's security and secret and sensitive information to maintain this security. This term Secretive information shall be defined as something that relates to the Armed Forces, National Security, and Territorial Integrity. The same concerns about National Security have also been elaborated under Article 23 of the GDPR.[12]

2. Those organizations which can maintain a balance between the interest of the state and the privacy elaborated by the Puttaswamy Judgement. This even if seems like a surreal concept can be adapted to a certain extent. The most appropriate way to do so is by classifying information or data in terms of national security, personal data, etc. Additionally, there have already been tests laid down for the same like the test laid down by Justice Nariman in the Privacy Judgement itself. It is stated that,

   "*... when it comes to restrictions on this right, the drill of various Articles to which the right relates must be scrupulously followed. For example, if the restraint on privacy is over fundamental personal choices that an individual is to make, State action can be restrained under Article 21 read with Article 14 if it is arbitrary and unreasonable; and under Article 21 read with Article 19(1)(a) only if it relates to the subjects mentioned in Article 19(2) and the tests laid down by this Court for such legislation or subordinate legislation to pass muster under the said Article."*

[12] Art. 23, General Data Protection Regulation (EU) 2016/679, OJ L 119 (2016), REGULATION (EU) 2016/ 679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL - of 27 April 2016 - on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/ 46/ EC (General Data Protection Regulation) (europa.eu).

ISSN: 2583-1984 (Online)

Suppose a hypothetical scenario where the State demands that a political organization reveal its membership lists for national security or public order reasons, as was the case in the famous American legal dispute, NAACP vs Alabama.[13] This situation involves the intersection of three constitutional rights: freedom of speech, freedom of association, and the right to life and personal liberty. The Court will need to apply the criteria set out in Articles 19(2) and (4) when considering this issue. Specifically, it must apply the standard established in the case of Arup Bhuyan vs State of Assam,[14] which requires the State to demonstrate a very high level of proximity to violence, equivalent to an incitement to violence, to justify limiting expressive or associative rights in the name of "security of the State" or "public order."

Another example of a similar issue would be if the State imposed restrictions on public protests, citing concerns about public safety or order. This would involve a balancing act between the right to freedom of assembly and the need to maintain public order. The Court would need to apply the standards established in Articles 19(2)[15] and (4)[16] and the judgments of various cases to determine the extent to which the State can restrict these rights.

The Act allows processing data if it is in the interest of the nation and is in accordance with the procedure established by law. But it really does not appear that this phrase, “procedure established by law” has been complied with by the said Act. As elaborated in the case of Maneka Gandhi v. Union of India,[17] “The procedure prescribed by law has to be fair, just, reasonable, not fanciful, oppressive or arbitrary.”

However, while reading the bill, under clause 2(a)[18] of section 18 and the Act under Section 17(4),[19] the phrase used is, “any instrumentality of the state”. By stating this phrase, the govt. is trying to grant complete exemption, because this term would mean all the govt. agencies. In summary, the use of the term "any instrumentality of the state" without clear and precise limitations can lead to arbitrariness and potential abuse of power. It is important to ensure that any exercise of power by the government is based on a clear legal basis and is proportionate to the objective sought to be achieved. Using the term "any instrumentality of the state" to

[13] National Association for the Advancement of Colored People v Alabama, 357 US 449 (1958)
[14] Arup Bhuyan v State of Assam, (2011) 3 SCC 377
[15] INDIAN CONST., 1950, Art. 19 cl.2.
[16] INDIAN CONST., 1950, Art. 19 cl.4.
[17] Maneka Gandhi v. Union and India and Anr., (1978) 1 Supreme Court Cases 248.
[18] The Digital Personal Data Protection Bill 2022, s 18 cl. 2(a).
[19] The Digital Personal Data Protection Act 2023, s 17 cl. 4

ISSN: 2583-1984 (Online)

describe those who exercise power on behalf of the government can be problematic as it can be too broad and arbitrary. This is because it includes a wide range of actors, from elected officials to bureaucrats and law enforcement officers, who exercise power in different ways and to different degrees.

For instance, if the government were to use this term to justify surveillance measures against its citizens, it could lead to the arbitrary targeting of certain individuals or groups without any meaningful justification. Similarly, if the term were used to justify the use of force against protestors, it could lead to excessive use of force and violations of human rights

The sad part is that all of these provisions from the Bill have been included as it is the Act despite multiple suggestions from the public to rephrase them so as to avoid the ambiguity and arbitrariness surrounding them. This shows complete arbitrariness from the side of lawmakers. Hence, the basic principles of natural justice have been ignored while drafting this Act.

The Ambiguity Around Alternative Dispute Resolution Mechanisms:

The bill under Section 23[20] and the Act under Section 29[21] states that if the board thinks it fits, any complaint may be referred for mediation or any other appropriate dispute resolution mechanism. There is nothing more elaborated by the Act. A lot of questions have arisen ultimately, which makes this section ambiguous.

Criteria to decide which case can be referred to Alternate Dispute Resolution:

Firstly, it is not clear what are the criteria to decide which case is to be referred for Alternate Dispute Resolution and which cannot be. It shall be clarified as to who can and who cannot opt for Alternate Dispute Resolution, failing to which it will be left open to the board and then the process can again turn arbitrary and unreasonable.

Who will be the mediator or the authority who will help in proceeding with the mediation:

The concerned section additionally states that the board will have the authority to appoint a body or a person who will take up the mediation process. Again, this authority is left to the pure discretion of the board. There is no procedure mentioned concerning these appointments.

[20] The Digital Personal Data Protection Bill 2022, s 23.
[21] The Digital Personal Data Protection Act 2023, s 29 cl. 1.

ISSN: 2583-1984 (Online)

What would be the eligibility for one to be appointed as a mediator:

The section has again left this question unanswered. The phrase used by the section is, "as the board may consider fit", which is open for interpretation. There is no restriction or limitation over who can be fit for this position. This can make these appointments arbitrary. Hence, at times it can be misused and the result of the mediation or any other alternative mechanism will be biased.

Even a rough reading of this under-detailed section will bring up a lot of doubts in mind. The section has been left open to the board entirely, making the process unrestricted-unreasonable, arbitrary, etc. which makes it ultimately go against the principles of natural justice.

The section surely is giving birth to novel and time-saving ideas to solve disputes. It will also ensure the courts from being flooded. However, this can be achieved only when the framing or drafting is doubtless and ascertained. The section shall be reframed to add certain criteria as to which cases can be referred for Alternate Dispute Resolutions. Cases where there is no human hazard involved, disputes that are commercial in nature, etc. should only be made applicable to opt for Alternate dispute resolution mechanisms. Disputes that are even slightly heinous in nature shall not be given this leniency. Such eligibility criteria shall be designed to resolve this issue.

There shall also be another eligibility criteria developed for the appointment of mediators or any other similar authority who will preside over the alternative mode of dispute resolution. This eligibility criterion can be decided based on the current legislation and rules. This will make the process non-arbitrary, reasonable, and accommodative with the principle of procedure established by law.

ISSN: 2583-1984 (Online)

Other Minor Challenges Created by The Act:

Discrimination between offline and online data:

The Act is only talking about online platforms or digital data. Whereas, the idea of the Act has its roots in the landmark Puttuswamy judgement. This judgement talked about privacy not only in the digital arena but in the overall aspect of privacy of the citizens. However, the Act has ignored the fact that data is defined by Merriam-Webster as, "factual information used as a basis for reasoning, discussion, or calculation". Nowhere has been the term digital used here. The Act this way is discriminating between online and offline platforms. The offline platforms would continue to be a hazard and keep up with their unrestricted and harmful practices.

The privacy of the individual is yet compromised, this way the objective of the Act will never be achieved to its fullest.

Issue revolving around deemed consent:

Section 8[22] of the draft bill talks about deemed consent. As stated in the section, a person while giving his/her data to a certain data fiduciary will be assumed to have given consent for the use of the concerned data so given. This means that the person would not have any say when it comes to the circulation of the data, which is one's private space. The possibility of the data fiduciary misusing this data cannot be overruled. Fortunately, while drafting the new Act, the govt. has finally narrowed down the concept of deemed consent to "certain legitimate uses" under Section 7.[23]

The govt. Should frame certain guidelines in respect of these as well, and mention them in the section itself rather than coming up with them differently. The guidelines can be of such nature, that the fiduciary is allowed to utilise the data only for the concerned purpose and dispose of it rightfully after the purpose is fulfilled. Also, if any fiduciary does not uphold these guidelines, a penalty for any other kind of punishment shall be imposed on the privacy violator. This will ensure that the laws are complied with well and that no fundamental rights are endangered.

[22] The Digital Personal Data Protection Bill 2022, s 8.
[23] The Digital Personal Data Protection Act 2023, s 7.

ISSN: 2583-1984 (Online)

The incomplete left provision for transfer of Data outside the country's territory:

Section 17[24] of the Act is yet another patchy provision, which just talks about issuing guidelines. It is stated that about the transfer of data outside the country, the govt. shall be issuing respective guidelines or notify the countries where any data fiduciary will be permitted to transfer data. However, it shall have been mentioned in this Act itself. The problem that may arise in future is that, if the Act is passed now, and the notifications are issued in future, there is no surety that the notification will not be an abuse of the procedure. This abuse of power would happen because for example the guidelines are issued later after the Act passed, and there would be little or no challenge for the same. Secondly, in the meantime in between the passing of the Act and issuing of the guidelines, it is yet questionable as to what rules shall be used by then, the govt. here by using its powers will pass decisions in its favour. The likeliness of the guidelines and the list being arbitrary, and unreasonable cannot be overruled. Similar provisions have also been adopted in the new Act under Section 16.[25]

It can be said that the govt. has done this on purpose to excuse itself from the clutches of the opposition. There is no surety as to on what grounds will countries be included in this list and excluded from this list. A patchy and sketchy left provision cannot result in a well-structured Act.

The incompleteness of the process of appointing the data protection board of India:

It is surely good to see that a separate Data Protection Board of India will be appointed. However, even this section has been left very sketchy. The bill under section 19[26], while talking about the board and its appointment says that the govt. will be issuing guidelines for these appointments. The same mistake that has been done with other sections of not giving crystal-clear guidelines, has also been committed here.

This means, again not the diverse representatives, but rather the ruling govt. will have the sole power to decide over the guidelines over these appointments leaving a lot more scope for misuse, arbitrariness, unreasonable, etc.

[24] The Digital Personal Data Protection Bill 2022, s 17.
[25] The Digital Personal Data Protection Act 2023, s 16.
[26] The Digital Personal Data Protection Bill 2022, s 19.

ISSN: 2583-1984 (Online)

Even with the new Act, even if they have still provided more details about the Board under Section 18[27] and Section 19[28] about, the discretion has been given to the government to choose these members. This discretion can lead to arbitrariness and hence there shall be certain checks and balances to oversee them.

Powers of the board;

Under Section 18[29] of the bill and Section 27[30] of the Act, the board has been given the power to impose a penalty on non-compliance with the provisions mentioned, however, this is again left to the discretion of the board. The only limit mentioned is in Section 25[31] where it is stated that the penalty imposed shall not exceed Rupees Five hundred crore, which is a lot. Even after changes made to the Act in relation to penalties, they are exorbitant and there is no rationale given for the amount of penalty.

Although there can be severe offences where the penalty imposed needs to be this high, it cannot be overruled that the board would impose a hefty fine on a small offender as well. And in such a case the person is likely to go for an appeal or review with the court as given the opportunity under Section 22[32], hence the courts would be flooded with cases. Again, the main motive behind the establishment of the board of lessening the burden of the courts would be futile.

The majority of the fallacies seen are arising due to poor drafting of the bill. The phrases have been left open-ended leading to ambiguity. Also, it won't be wrong to say that there has been a lot of laziness expressed in the drafting when it came to constructing eligibility criteria or guidelines concerning different provisions. The majority of the provisions of that Act state that the central govt. shall be releasing guidelines over the same. I don't know if it was done deliberately to exercise arbitrariness and avoid opposition or is just mere procrastination.

[27] The Digital Personal Data Protection Act 2023, s 18.
[28] The Digital Personal Data Protection Act 2023, s 19.
[29] The Digital Personal Data Protection Bill 2022, s 18.
[30] The Digital Personal Data Protection Act 2023, s 27.
[31] The Digital Personal Data Protection Bill 2022, s 25.
[32]. The Digital Personal Data Protection Bill 2022, s 22.

ISSN: 2583-1984 (Online)

International Scenario Over Personal Data Protection:

According to the recent report[33] from UNCTAD "Data Protection and Privacy Legislation Worldwide" over 137 out of 194 countries had legislation in place concerning data protection. India has also been included in the list of these 137 countries, however, the fact that the legislation has not yet been enforced is ignored. Still, it is seen that the majority of the nations around the world have laws in force about data privacy, and India has still been clinging to the drafting work.

The world has been inspired to develop such legislation by the European Union's General Data Protection Regulation (GDPR)[34] enacted in 2018. Especially after the effect that this legislation had on the modifications in WhatsApp terms and conditions helped people across the globe understand the significance of this legislation. The story goes such that when WhatsApp recently announced changes in its policy, they were not made applicable in the member countries of the European Union due to GDPR's stringent approach. Subsequently, countries felt a sudden urge to make such Acts for safeguarding the interest of their citizens. The EU's General Data Protection Regulation (GDPR) is considered one of the most comprehensive data protection laws in the world. India can look at the GDPR's provisions on data subjects' rights, data protection officers, and extraterritorial applicability as models for its data protection law.

Another appreciative country is Iceland, which at times has also been referred to as the Switzerland of Data,[35] which made the country draft one such legislation[36] long before the world felt so. It was in 2000 that Iceland enacted its Data Protection Act,[37] and it has been quite effective since then due to its approach to balancing out restrictions and rights. the legislation survives on the sole condition of "unambiguous and informed consent". India while drafting its final legislation shall focus on this aspect of unambiguity because the most intriguing

[33] United Nations Conference on Trade and Development, "Data Protection and Privacy Legislation Worldwide" 2022 https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.
[34] General Data Protection Regulation, Regulation (EU) 2016/679, European Parliament and of the council, 2016 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.
[35] Gaedtke F. "Can Iceland become the 'Switzerland of data'?", Al-Jazeera (Reykjavik, Iceland, 30 December 2014) Can Iceland become the 'Switzerland of data'? | Features | Al Jazeera.
[36] Act on the Protection of Privacy as Regards the Processing of Personal Data, No. 77/2000, Govt. of Iceland Government of Iceland | Act on the Protection of Privacy as regards the Processing of Personal Data, No. 77/2000.
[37] Act on the Protection of Privacy as Regards the Processing of Personal Data, Act. No. 77/2000, Iceland. https://www.government.is/Publications/Legislation/Lex/?newsid=fadb4b17-f467-11e7-9423-005056bc530c.

ISSN: 2583-1984 (Online)

problem with the current legislation is its ambiguity which has been elaborated upon initially in this article.

Like India, even China recently rolled out its draft bill and invited general public opinions over the same. The country already has a couple of pre-existing legislations concerning privacy laws, however, through the recent draft they aim to amalgamate all of them which seems to be a sensible idea because it is often seen that overlapping legislation can bring terrible outcomes in terms of interpretation. The novel outcome of this collaboration of laws and incorporation of some more is to enhance the protection of personal data by levying hefty fines, the appointment of data protection officers, etc. Even India can amalgamate its data protection, and privacy laws and also seeing that AI has been entering each one of our lives, the focus shall be also upon the regulation of the same.

Another progressive effort was made by the Chilean government through an amendment to its Constitution to entail the protection of data or data privacy as a Human Right. In India, the Right to Privacy has already been considered a Fundamental Right and Data Privacy should be an integral part of it.

The United States of America does not have a Federal Law for data protection however certain states do have their legislation relating to it. One such example is the California Consumer Privacy Act (CCPA)[38] which highly seems to be inspired by the European Union's General Data Protection Regulation. It is astonishing to see that even after the infamous Facebook-Cambridge Analytica Scandal[39] that happened in 2016 the country did not make any efforts to construct one such law for safeguarding the interest of its citizens. In brief, the scandal was such that, the personal data of millions of Facebook users was collected by Cambridge Analytica (a British Consulting Firm) and then "misused" for the Presidential Campaign of Donald Trump in 2016. However, after progressive steps from California, other states like Texas, Washington, New York, Virginia, Connecticut, Florida, Alabama and Illinois have put acts in place, however, they are yet to be enacted. India should learn from this mistake and

[38] California Consumer Privacy Act, 2018 https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

[39] "Facebook-Cambridge Analytica Data Scandal", ICMR (2018) https://www.icmrindia.org/casestudies/catalogue/Business%20Ethics/BECG160.htm.

ISSN: 2583-1984 (Online)

formulate and enact this law as soon as possible to avoid any such scandals relating to data leakage.

Brazil has a plethora of legislation[40] relating to data protection. It has a General Data Protection Law enacted in 2018 and another 40 different legislations which govern data. India on the other hand does not have even one proper legislation. But it is better to have a single comprehensive legislation rather than multiple of the same type, as that would lead to one provision contradicting the other.

South Africa has the Protection of Personal Information Act (POPIA)[41] in place to ensure the data privacy of its citizens. The Law is quite Comprehensive, Stringent, and rigorous.

In the Middle East,[42] Qatar was the first country to enact data protection legislation in 2016. Today Bahrain and Saudi Arabia have data protection laws in place. However, the data protection laws of Saudi Arabia have highly relied on Sharia Law. The data protection Laws of Qatar and Bahrain were highly influenced by the European Union's General Data Protection Law. Both of these nations aim at being major data hubs and have hence made efforts by enacting such laws which would build confidence in data fiduciaries and attract investors. India being a secular nation would surely avoid this mistake of bringing religion into law.

Even Canada had implemented its Personal Information Protection and Electronic Documents Act (PIPEDA)[43] which is in line with the European Union's General Data Protection Law and also seems to be complying with the six Global Privacy Principles.[44] India while drafting its legislation shall take into consideration these Six Global Privacy Principles.

As other nations across the world have seemed to be inspired by the General Data Protection Act of the European Union, India has not been an exception. Even India's Personal Data

[40] "Data Protection Laws of the World", DLA PIPER (January 2023) Law in Brazil - DLA Piper Global Data Protection Laws of the World (dlapiperdataprotection.com).
[41] Protection of Personal Information Act 2013, Republic of South Africa, No. 37067 Protection of Personal Information Act (www.gov.za).
[42] Privacy Solved, 'Data Protection Is Trending In The Middle East' Data Protection is Trending in the Middle East – PrivacySolved.
[43] The Personal Information Protection and Electronic Documents Act 2000, Canada S.C. 2000, c.5 Personal Information Protection and Electronic Documents Act (justice.gc.ca).
[44] Art. 5, General Data Protection Regulation (EU) 2016/679, OJ L 119 (2016), REGULATION (EU) 2016/ 679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL - of 27 April 2016 - on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/ 46/ EC (General Data Protection Regulation) (europa.eu).

ISSN: 2583-1984 (Online)

Protection Act, 2019 appeared to be reflecting numerous provisions of the GDPR.[45] However, the recently released draft has been shortened from 98 sections to 30 sections, the majority of which focuses on the data principles and fiduciaries and their rights and obligations.

Data protection laws are a matter of sudden awareness, especially due to the Covid Situation when our entire lives were solely dependent on data. There were also several triggering incidents like the modification in the WhatsApp rules,[46] and many more digital scandals that led to the birth of a sudden urge by different countries to build up data protection laws. However, the subject being a little debatable, most of these legislations are yet in the drafting process.

Therefore, a very small number of countries do have definite and well-structured laws on the same issue. The main obstacle to making these laws definite is that technology is continuously evolving. There is always something new rising every day. However, this obstacle shall not be seen from this viewpoint. It was even with the constitution that the same problem was predictable because humans are dynamic beings. Hence there shall be efforts made by countries to adhere to basic human rights and concerned fundamental rights.

Additionally, the primary reason behind the debates over these laws is the inaccurate and poor drafting. If the drafting work is done hassle-free, the law would likely be ambiguity-free. Hence the countries along with the rights shall also focus on drafting because in future the courts decide their opinions based on interpretations. India through these legislations from other jurisdictions shall consider the part where positive outcomes have rolled out and avoid mistakes that have been done by them.

Suggestions

This article has brought into light different lacunae projected by the bill as well as the act. However, only putting forth problems won't suffice. Along with locating problems we also need to find out suggestions for the same. The following are a few solutions that the author would like to implement to correct the Act's flaws.

[45] Vikram Jeet Singh, 'Lessons Learned in Data Regulation: A first look at India's new Data Privacy Act' (2022) 'Lessons Learned' in Data Regulation: A first look at India's new Data Privacy Act - Lexology.
[46] Nate Lanxon, 'Why WhatsApp's New Privacy Rules Have Sparked Alarm', Bloomberg QuickTake WhatsApp's New Terms of Service and Privacy Rules Spark Moves to Rivals - Bloomberg.

ISSN: 2583-1984 (Online)

Granting exemptions procedurally:

The exemption provided by the Act to governmental agencies should not be in a blanket form. It cannot be unrestricted or it would lead to arbitrariness and be against the principle of procedure established by law.

As also suggested earlier, the government must mark out certain criteria for these exemptions. The criteria can be such that exemption would be granted only to those governmental agencies which deal with secret information related to the country's security, Intelligence Agencies, etc. However, there cannot be a complete blanket exemption. The best way is to set up different bodies and make another set of rules for these agencies to govern. A complete exemption will undoubtedly lead to a situation of lawlessness.

The criteria need to be very stringent, non-flexible, and unbiased. The govt. in this case should not say like always that it would release such a notification later, but should rather add it in the main provision itself. Because by saying that it would be done shortly, a lot of scope is left for the law to be misused in the meantime.

Problem with Semi-government agencies:

No semi-governmental agencies shall be granted exemption in the slightest form as there appears to be a private intervention. Semi-governmental agencies shall be treated like any normal data fiduciary.

Ambiguity around Alternate Dispute Resolution:

The provision relating to Alternate Dispute Resolution (ADR) can be easily resolved if the section is more detailed and elaborated. The provision needs to entail the types of cases that can be entertained through ADR. Also, further information as to the authorities who can take over such mediation should be provided.

Also, there shall be clarity about the eligibility and appointment of such presiding authority. There also be detailed information as to what would happen if the results of the mediation are either non-fruitful or unagreeable to any one of the parties. Also, the question as to what would happen in such a failure of the ADR process is left unanswered.

ISSN: 2583-1984 (Online)

Seeing that the provision is just a few lines, it cannot be expected that it would be unambiguous. The section needs to be more detailed. It shall embody the following requirements:

i. Criteria for cases that can be referred to Alternate Dispute Resolution. The criteria need not be definite. Understandably, it shall be based on the facts and circumstances of each case. However, this cannot be an excuse to produce arbitrariness and sole discretion of the board. The gravity of the matter shall be taken into consideration.
ii. The process of appointment of the person or persons presiding over the ADR process shall be elaborated upon. There shall be a definite eligibility criterion in this case. The provision should elaborate as to what will be the aftermath of the ADR process.

Conclusion

After a thorough study of the Data Protection draft bill and the Act thereafter, it is understood that the legislation is very prone to be misused widely. The poor drafting has additionally contributed to this foreseen misuse.

The Act also fails to be in line with some basic principles like "procedure established in accordance to law". Most of the decisions are at the discretion of the board that will be established which at times may make the process arbitrary and unreasonable. There are no necessary safeguards laid down. The Act needs to be modified in such a way that it confines these basic principles and protects the rights of the citizens which was the initial and main objective behind the drafting of this legislation.

As even pointed out initially, the Act has diverged from its main intent and moved towards safeguarding the governmental or statutory interest over the interest of the citizens. Democracy is a government that is built by the people, however, the Act in this instant case by favouring governmental rights over the rights of common individuals is going against these principles of democracy.

Many terms need to be redesigned or redrafted as has been highlighted earlier. The terms have been left so broad and open-ended that an individual can interpret them in his favour and endanger the rights of several.

ISSN: 2583-1984 (Online)

Many opine that these fallacies are due to the hurry made in bringing the legislation into place. However, it cannot be ignored that this Act has been in construction since the Puttuswamy Judgement. There has already been quite a lot of time spent on this issue of data privacy, and by then many individuals had to suffer. A lot of countries that had started their drafting after India have already got their respective legislations in place and are also working well.

If the legislature prefers individual rights over its rights and the importance of the words that have been used in the draft, the Act would be good enough to avoid any confusion. Also, there needs to be attention paid to the questions regarding the promises that the Act has made regarding the issuance of different guidelines, not in one but in a plethora of provisions. Such spaces between the provisions can lead to further misuse and distortion of the objective. The guidelines should be added in the provision itself so that there is no ambiguity left.

Moreover, the delay that has been happening in the enforcement of a data protection Act is leading to a failure of the government in guarding the Fundamental Rights of its citizens. Several have already suffered due to this delay.

Another thing that may be helpful if implemented in the Act is by checking the lacunae in the laws that the other countries have framed and what bad outcomes have brought. The Indian government can priorly check upon it, to avoid any such mishap. Even many landmark cases can be referred to.[47] Even catena of cases has helped lawmakers in different countries to frame the laws following them and avoid any such cases in future beforehand. India can also consider this, as it will help further in strengthening the legislation.

Privacy at times is a requisite for one's dignity and even this is a fundamental right recognised under Article 21[48] of the Constitution. Lawmakers need to take into consideration these basic rights of an individual and bring into effect a modified law on data protection at the earliest. There have already been many times that an Act has been produced and rejected.

The government after so much criticism shall take into consideration the changes suggested. The suggestions stated in these articles are not mere suggestions but are absolute requirements. In the absence of which the law will be of no use, it would be more confusion, misuse, and violation of rights, and subsequently, lead to flooding of the courts.

[47] Suneet Sharma, 'Top 10 Privacy and Data Protection Cases of 2021', The International Forum for Responsible Media Blog Top 10 Privacy and Data Protection Cases of 2021: A selection – Suneet Sharma – Inforrm's Blog.
[48] INDIAN CONST., 1950, Art. 21.

ISSN: 2583-1984 (Online)

It won't be wrong to conclude that the Act is in reality rather than protecting the rights of the citizens safeguarding the government's interest. The Act needs to be reframed in detail and the main objective behind the Act needs to be brought to the notice of the lawmakers. The legislators need to relook at the core intention that the propounders of such regulating legislation had and reframe this draft legislation by it, or else the vision or objective behind this Act will never be achieved.

ISSN: 2583-1984 (Online)