IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

REGULATION ON ONLINE PROTECTION OF CHILDREN'S PERSONAL INFORMATION IN INDIA

[1] Prachi Mishra, [2] Akhilesh Dureja,

[1] Assistant Professor of Law, [2] Assistant Professor of Law

[1]ICFAI Law School,

[1]ICFAI University, Dehradun, India.

Abstract: The Indian Personal Data Protection Bill, 2019 (PDP Bill), lists out a number of categories of data as "sensitive personal data". While it is a matter of debate whether sensitive personal data should be listed out, or a more dynamic approach is better. Specifically, the need to protect children through data protection laws and policies has increasingly been witnessed in different countries, including India. This article analyses the PDP bill especially with regard to the collection and processing of children's personal data.

***Keyword* – Indian Personal Data Protection Bill, 2019, sensitive data, Children's personal data.**

I. INTRODUCTION

The advancement in technology, especially the digital revolution witnessed in the recent past, has significantly changed the ways in which the world operates. The transformation has had great influence in virtually every sector. Technology and the internet have brought about both negative and positive impacts. One of the major problems that have come with the increased usage of technology includes breach of privacy. This attracts both ethical and legal aspects. There has been an increased data usage from the online sites where people log into for social interaction to electronic storage of data in organizations over the recent past. However, the security of such private date has faced challenges due to the increased exposure and unauthorized access. In response to such challenges, different governments have moved ahead to formulate and pass data protection laws that can protect people from data breach and unauthorized exposure of their personal information. Specifically, the need to protect children through data protection laws and policies has increasingly been witnessed in different countries, including India. Many scholars argue that the need to protect personal data, especially that of children, is essential. In this regard, the enactment of the Indian Personal Data Protection Bill (PDP Bill) of 2019 is one of the most effective legal interventions that the country has taken to protect personal data not only of children but also of adults in the country.

II. OVERVIEW OF THE PERSONAL DATA PROTECTION BILL (2019)

The Indian personal Data Protection Bill passed in 2019 has brought immense contributions to the protection of personal data in India. First, it acknowledges 'personal sensitive data' as something important that should be protected at all costs. The bill was introduced by the Minister of Electronics and Information Technology, Ravi Shankar Prasad in December 11, 2019 . It continues to revolutionize ways in which data is protected in different parts and sectors within the Indian context. The primary aim was to enhance the protection of personal data under the newly formed agency known as the Data Protection Authority.

Applicability: The law is applicable in different ways within the Indian jurisdiction. It governs the process of personal data by the state, incorporated organizations in the country, and foreign organizations that handle personal data of people who live in India. It is important to mention that this law identifies and groups some personal data as 'sensitive.' Such are attended to or processed differently from those that are not. Some examples of personal data where the law applies include financial information, biometric data, caste, and political beliefs, among others. The level of sensitivity of these personal data varies.

The obligation of Data Fiduciary: A data fiduciary, under this act, is the party or individual who has the authority to define how personal data is processed. They make such decisions based on the framework spelled out in this legislation. They also have a mandate to ensure that every transparency and accountability protocol is followed when processing personal data. Another important authority that this legislation gives the data fiduciary is implementing security safeguards. This has to do with the network security measures that are used to ensure that hacking, including phishing which has become quite common recently. The issue of consent in which consent is sought from parents of children under the legal age is also directed towards these entities. Finally, they have the role of instituting grievance redressal mechanisms. Each of these authorities is well-outlined in the PDP Bill of 2019.

Rights of Individuals: The rights of individuals as they handle data and try to seek better ways in which their personal information can be protected and guaranteed have also been defined clearly in this Bill of 2019. The legalization also has spelled individual's right to obtain

information from the fiduciary, to have any incomplete or incorrect personal information rectified, and stop court proceedings if they terminate the consent, they had offered in the change their minds. Each of these rights is important in ensuring that the individuals are protected in the best way possible. The fiduciary is also pushed into ensuring that they protect the rights to privacy of personal data of individuals within the country in the best way possible.

The basis for Processing Personal Data: As previously mentioned, the fiduciaries are mandated to process personal data. This can be done under two conditions. It can either be under consent or sometimes even without consent, depending on the nature of that specific personal data .Personal data can be processed without consent under conditions such as when the government wants to offer services to the person if it involves es legal proceedings and under the condition that the case involves a medical emergency that the government seeks to respond to in trying to handle a pandemic.

Social Media Intermediaries: The online interaction and ways in which data is shared across social media platforms are also regulated by this data bill. In the advent of the digital revolution, the need to regulate ways in which people share information online, and the extent to which personal data can be exposed was found to be of critical importance. The government of India has specifically been keen on regulation, social media because it affects political order. The extent to which this bill regulates social media interaction is phenomenal. Most scholars agree that this law has brought sanity and order within the online community where many Indians interact actively on a daily basis.

Data Protection Authority: This is a regulatory body established the bill. It is mandated to perform various roles including protecting individuals when it comes to data processing and information consumption, averting possible misuse of personal data, and enforcing the legislation to ensure that all its components re strictly adhered to. Most importantly, the head of this agency is expected to have over ten years of experience in data protection issues. The authority is also governed by six members with almost equal expertise and experience. However, the decisions that they make or policies they formulate may be appealed against in the Appeal Court. It implies that their word is not final when it comes to data protection despite the fact that they have almost the highest power when it comes to the protection of personal data.

Matters related to Transfer of Data Beyond Indian Borders: The government of India takes seriously matters of data transfer, especially if it is going beyond its borders. First, it should be noted that this allows consensual transfer of personal data outside India. However, this act comes with different conditions that may further make the process more complicated. The government through this legislation insists that even when transferring such data outside the country, a copy of it should remain and be stored in India.

Exemptions: While this act is meant to protect individuals from misuse of personal data and ensure complete data protection, the government of India may suspend the application of various provisions of the legislations part under certain condition. These conditions include situations where national security is at stake and the relations of India with other states within the regional and international landscape, and in preventing incitement that may have been directed towards the state or any other state organ, among other. These exemptions may be exercised directly by the state organs or by the central government.

Offences: The bill specifies various offences that are prosecutable in the court of law. Some of these include:

- Processing and transferring of personal data against the set procedures and policies under the act. Upon conviction, the individual or entity is fined Rs 15 crore .
- Re-dentification or processing of de-identified data is another serious offence under this law punishable with a jail term of not more than 3 years.
- One can also be fiend for not conducting a data audit.

Sharing of Personal Data: The bill gives the government powers to access non-personal data or anonymous through the fiduciaries so it could provide various services to the citizens. However, this should be done based on the available protocols as stipulated in the bill.

Amendments: As has already been mentioned, this particular law was an amendment to the initial Information Technology Act of 2000. It was meant to heighten the level to which data is protect, especially on the regulation of parental consent and exposure of children's personal data online.

III. Children, Online Services and Data Protection based on PDP Bill

The PDP Bill of 2019 has attempted to protect children from exploitation by ensuring that the provisions of the legislation are followed to the latter. First, it requires the data fiduciary to verify an ascertain that the individual in question is a minor who is below the legal age. It is through this that parental or guardian age has to be sought . This particular provision does not apply to individuals who have attained the legal age. However, the bill does not provide detailed information about how this is expected to be done. The most important thing is to entrust the data fiduciary with the role of ensuring this age is confirmed. Nonetheless, there are specification under the regulation on how age verification is done which the data fiduciary is expected to know considering their training. With regards to online services, the regulation also provides for how much personal data of children are processed and determine if any of the personal data can create harm to the specific child. The law further helps in classifying data fiduciaries who handle the commercial website and other online services that deal with children. For instance, the personal data about children may be stored by one group of data fiduciary while the another handle other online services where guardians, for instance, may find help if need be.

One of the major issues related to this new law is the age verification mechanism challenge that it brings. Some experts maintain that online services that relate to much younger generations may require better age verification strategies to ensure that the law is enforced positively in efforts to protect children more and enhance their wellness. The law has specifically been categorical on the use of PUBG, gaming app that is not only played in India but also other regions across the world . However, in order to positively effect this law, it would be important to recheck the age consent concerns that have been raised by many commentators including parents and other stakeholders.

Some experts maintain that age of consent in India, however, is higher in India than other countries where such games and other online services provided. This is specifically true to the United Kingdom and the United States. In the last two countries, children as young as 13 years are allowed to provide consent to access various online services including violent games . However, the case is entirely different in India, perhaps, because of the countries strong and conservative orientation to traditional cultures. Others have maintained that this has been facilitated by the recent law which gives data factories are even greater role in regulating online services involving minors. It is further noted that the new bill is advocating for what can be described as consent manager system in the endeavor to improve online and data-related services for the young generation. It is also insisting that the information consent system should be dropped completely because of the numerous problems that it has been causing over the past. However, the new proposal may take time to implement and successfully put it into practice because: 1) What the role of consent managers will be is not clear and 2) the age verification mechanism is not clearly defined.

IV. Effective Age-Gating Mechanism

Age verification also known as age-gating is an important aspect that should critically be considered when discussing the question of data protection and the safeguarding of personal data, especially among children. This discussion is even more relevant when considering the best option through which online services can best be delivered to the young ones. There is no doubt that implementing the bets age-gating mechanism has been a major, on-going problem which may not resolved by simply enforcing this bill . Rather, it requires supporting policies and concerned efforts from other relevant factions. Most experts have proposed that implemented knowledge-based tests may be the best solution that India can use to resolve this major concern. This may be done on different ways. One of the most popular one is to use arithmetic tests which may show the age of the person trying to consent. It is more accurate and effective in ensuring that people's age is easily identified and responded to appropriately.

V. Guardian Data Fiduciary and its Effectiveness

Chapter four of the bill broadly discusses the role of guardian data fiduciary in enhancing the overall process of data protection and online service provision among minors. First, their role is not to track and monitor children's activities online. Specifically, their role is nothing close to engaging in any activity that may put the children in harm. This particular part of the provision is meant to prevent cases where Google and You Tube was fined for engaging in an advertising putting children at risk. However, only data fiduciaries who offer essential services like counselling and child protection services may be allowed to handle such personal data. This, raises the question of whether guardian data fiduciaries are playing any significant role in their work towards online protection of children. The PDP bill of 2019 is very categorical on what penalty should be applied when the guardian data fiduciaries fail to perform or extend their duties beyond what is defined. For instance, they face a fine of INR 15 crore.

VI. Does Chapter IV of PDP Bill Protects Children Adequately?

One of the greatest questions to reflect on when discussion children's data protection ii whether the fourth chapter is enough. Many scholars are of the idea that a lot of more protection is required to successfully protect personal data of children and ensure that children are safe when using online services. The processing of their data should be protected through even more effective measures and policies that are more focused on tehri plight and risks. From the discussion, it is determined that Chapter Four of this act serves two wide purposes. The first role of this section is to age verification is positively implemented in a way that benefits the child targeted. Age verification is unquestionably a critical issue in this discussion that cannot be ignored. Second, it seeks to protect children from unnecessary or unwarranted monitoring and tracking of young children for purposes of advertisement and other commercial reasons as witnessed in the case of YouTube and Google recently. While these roles are commendable, a few more critical issues come out which need to be reviewed and addressed.

First, the role of guardian data factory is not well addressed. It seems to be a critical issue that is being ignored by this law. The obligation they are assigned seems confusing and many of them may end up getting prosecuted for ignorance . Some perspectives have insisted that it would be more meaningful if the role and obligations of these entities are equated to those of other categories or classification of data fiduciaries. Second, the issue of differentiated age of consent used in India seems ineffective. Even more complicated is the unclear definition of harm as defined in this bill. Finally, the lack of sensitive personal data in the government database is even more critical issue that's should equally be addressed when handling the problem of data protection.

VII. International Perspective: Data Protection and Right to Privacy

The issue of data protection vis a vis right to privacy, especially for children has attracted the attention of many governments across the international market. In the United States, the right to privacy is high ensrished in the Fourth Amendment to the U.S Constitution. In overall, it talks about the right that people have to be secure in their persons, houses, homes, and places of work from unreasonable searches or exposures of their private information. The right tor privacy for children is rather more unique and critical under the U.S Constitution. Under the United Nation's Convection, the right to privacy for children is captured in Article 16 of N Convention on the Rights of the Child (UNCRC). It prevents interference with his or her private information related to his or her personal life, family, and correspondence. It also outlaw attacks on a child's honor or reputation. This international law is what guides each and every customized legislation that countries across the international framework develops as they try to protect children. Countries such as the United Kingdom have equally strict data protection laws that help safeguard children' privacy rights. For instance, under the UK's new Data Protection Act, the legal age of consent for children is 13 years. This was based on the notion that children tend to be confused between paid content and free information available online.

VIII. RECOMMENDATIONS

The following recommendations can be implemented not only by the Indian Data Protection Authority but by also other countries' agencies to enhance protection of personal data and right to privacy:

- Ensure strict enforcement of the law; not just creating laws without implementing hem.
- Educate children about cybersecurity so they do not fall victims
- Work with parents and guardians to set usage limits
- Block or bar sites that are not age appropriate for children through parental control software
- Provide support always for children who may require online services.

IX. CONCLUSION

Data protection has increasingly become a major sensitive issue with the increased application of information communication in different sectors across the economy ranging from transport to realm of education. Sophisticated technology has also become even more popular in the field of entertainment, thanks to the digital/video games among other applications that sue advanced digital technologies. However, the risk of misuse of personal data and deliberate exposure of other people's private information has pushed governments across the world to adopt new policies and laws in data protection. India, particularly has been at the forefront of protecting personal data of children and ensuring their safety only by implementing the Personal Data Protection (PDP) Bill of 2019. While it has been effective in addressing most of its roles, it also presents a few limitations as discussed. However, in overall, the government move to ensure data protection and enhance the right to privacy through different laws is commendable.

X. ACKNOWLEDGMENT

Thepreferredspellingoftheword "acknowledgment" inAmericaiswithoutan "e" afterthe "g".Avoidthestiltedexpression, "Oneofus(R.B.G.)thanks..."
Instead,try"R.B.G.thanks".Putapplicablesponsoracknowledgmentshere;DONOTplacethemonthefirstpageofyourpaperorasafootnote.

XI. REFERENCES

[1] Abdullah Alqahtani et al., Sensitivity Level-Based Citizen Personal Information Model for Privacy Protection, 10 Journal of Software , 42-55 (2015).

[2] Yeo-Min Hwang & Hyun-Ah Seo, Awareness of Personal Information for Preschool Teachers and Level for Protection Personal Information in Preschool, 19 Journal of Children's Literature and Education , 109-131 (2018).

[3] Agata Jaroszek, Online Behavioural Advertising and the Protection of Children's Personal Data on the Internet, 4 Wroclaw Review of Law, Administration & Economics , 56-69 (2014).

[4] Mariya Stoilova et al., Children's understanding of personal data and privacy online – a systematic evidence mapping, Information, Communication & Society, 1-19 (2019).

[5] P. J.G. Stokes, Young people as digital natives: protection, perpetration and regulation, 8 Children's Geographies , 319-323 (2010)li, A. 2001.Macroeconomic variables as common pervasive risk factors and the empirical content of the Arbitrage Pricing Theory. Journal of Empirical finance, 5(3): 221–240.