Webology (ISSN: 1735-188X)
Volume 18, Number 6, 2021

Children Online Privacy Law- (Lacks Rational Classification For Effective Use Of Internet By Children)

Ms. Sumedha Ganjoo [1*], Dr. Garima Tiwari [2]

[1,2] School of Law, Bennett University, Greater Noida

Abstract

Any individual under the age of 18 is classified as a child under the Personal Data Protection (PDP) Bill, 2019. His or her data cannot be handled without the approval of his or her parents or guardians. The Srikrishna Committee, which drafted the bill, indicated that the 18-year-old age was selected to be consistent with other domestic regulations. It was decided that the cut-off age was too high and that it should be altered to take into account a child's development. In contrast to India's approach, the Children's Online Privacy Protection Act in the United States has set the age of consent at 13, with verified parental approval required only for children under the age of 13. The General Data Protection Regulation in Europe specifies a range of 13 to 16 years.

There is no distinction between a 17-year-old and a 13-year-old under the PDP Bill, 2019. It has the same standards for all age groups, and no kid under the age of 18 has the right to provide their permission to their data being processed. Such broad limitations may prevent youngsters from making effective use of the internet. We live in an era where information literacy has accelerated the rate of mental development in youngsters, who are now capable of becoming stakeholders in society building and guiding legislation. "Greta Thunberg", a 17-year-old Swedish environmental activist who utilises social media to increase climate change awareness, is a good illustration. Because there is no grading system for permission, service providers may adopt a risk-averse stance and just exclude minors from using internet-based services. This paper examines the PDP Bill, focusing on the collecting and processing of personal data on minors. There is also a comparison study based on the processing of children's data under EU and US data protection legislation.

Keywords- Processing Children's data, Children's Internet right, Data protection laws, GDPR.

I. INTRODUCTION

Children in today's society are increasingly exposed to the internet as a result of different activities that have become an integral part of their lives. Children inadvertently leave their digital fingerprints everywhere, from gaming and web series platforms to online schooling and social

media contact. Artificial intelligence and internet portals enable youngsters to participate in a variety of services that help them with their academics and projects. However, youngsters are not developed enough to grasp the wide phrase "online privacy"[1] when it comes to the digital world. They see internet privacy as a concept that allows them to isolate themselves from their parents by not informing them of the websites and platforms they use and frequent. Legal challenges develop as a result of such situations. Because the youngsters are legally minors, they are psychologically prepared to provide their approval for their "digital identities" to be stored by big data players. For the storage of children's data, parental authorization is required. As a result of their lack of awareness and understanding about online data privacy, children are vulnerable to cyber risks such as data theft, cyberbullying, and so on[2]. It has become vital to preserve children's "right to privacy" in light of the rising digital world and their growing involvement. Today, the state must protect children's right to participate as well as their right to privacy from commercial actors and peers, without imposing any limits.

One in every three Internet users worldwide is a youngster or teenager under the age of 18. Adolescence is the era when children move from children to young people, and it is curing this time that they gain information, develop qualities and abilities, and, most importantly, learn to manage emotions and relationships[3]. This includes their online behaviour as well as their digital identity. The majority of children and teenagers use the Internet for amusement and information, and they feel they have a legal right to do so. In the majority of situations, kids are also aware of the dangers of accessing the Internet and are aware of their right to privacy. They seem to be more worried about their right to privacy being violated by their parents or peers than by the government or commercial entities.

For putting all these activities under a legal framework in December 2019, the government finally introduced its first Personal Data Protection Bill, 2019[4] in Parliament, following a protracted wait. After this the bill was submitted to the Joint Parliamentary Committee for recommendations. The Committee is expected to provide its findings at this Parliament's winter session.

The personal data protection law aims to secure an individual's personal data while also establishing a data protection body. The processing of personal data and sensitive personal data of minors is addressed in Chapter IV of the Personal Data Protection Bill[5].

II. A SUMMARY OF THE PERSONAL DATA PROTECTION ACT (2019)

[1] Yolanda Reid Chassiakos et al., "Children and adolescents and digital media" *Pediatrics* (2016).
[2] Sonia Livingstone, Mariya Stoilova and Rishita Nandagiri, "Children's data and privacy online: Growing up in a digital age" *Media and Communications* (2019).
[3] Mariya Stoilova, Rishita Nandagiri and Sonia Livingstone, "Children's understanding of personal data and privacy online–a systematic evidence mapping" *Information Communication and Society* (2021).
[4] PRS Legislative Research, "The Personal Data Protection Bill, 2019 | PRSIndia" *PRS india* (2020).
[5] *Ibid.*

The Indian Personal Data Protection Bill, which was passed in 2019[6], has made significant contributions to India's personal data protection.

First, it recognises "personal sensitive data" as a valuable resource that must be safeguarded at all costs. Ravi Shankar Prasad, the Minister of Electronics and Information Technology, presented the bill on December 11, 2019[7]. It continues to alter the methods in which data is secured in India's many areas and industries. The major goal of the newly established Data Protection Authority was to improve the protection of personal data.

Applicability: Within the Indian jurisdiction, the law may be applied in a variety of ways. It regulates the processing of personal data by the government, incorporated organisations in India, and foreign organisations that deal with personal data of Indian citizens. It's worth noting that this regulation classifies and categorises some types of personal data as 'sensitive.' These are treated or handled in a different way than those who aren't. Financial information, biometric data, caste, and political convictions are only a few kinds of personal data that are covered by the legislation[8]. These personal data have varying degrees of sensitivity.

The Data Fiduciary's Obligation: A data fiduciary[9] is the entity or individual who has the responsibility to specify how personal data is treated under this act. They make these judgments in accordance with the structure outlined in this statute. They also have a mission to guarantee that while processing personal data, all transparency and accountability protocols are followed. Another major power given to the data fiduciary by this Act is the ability to set security precautions. This has to do with the network security measures in place to prevent hacking, such as phishing, which has been more widespread in recent years. The problem of parental permission, which is sought from parents of children under the age of majority, is also focused at these corporations. Finally, they are responsible for establishing methods for grievance resolution. The PDP Bill of 2019 clearly defines each of these powers.

Data Principle Rights: The rights of persons when they handle data and seek new methods to preserve and ensure their personal information have been explicitly stated in this Bill of 2019. Individuals' rights to receive information from the fiduciary, to have any incomplete or erroneous personal information corrected, and to have court proceedings halted if they cancel the permission, they had given in the change of mind are all clearly out in the legislation. Each of these rights is critical in ensuring that people are protected to the fullest extent feasible. The fiduciary is also pressed to ensure that the rights to privacy of personal data of persons inside the nation are protected to the best of their abilities.

---

[6] *Ibid.*
[7] Information Technology, Electronics Niketan and Lodhi Road, "Data Protection India Is Rapidly Transforming."
[8] Sheshadri Chatterjee, "Is data privacy a fundamental right in India?: An analysis and recommendations from policy and legal perspective" *International Journal of Law and Management* (2019).
[9] Julia M. Puaschunder, "Data Fiduciary in Order to Alleviate Principal-Agent Problems in the Artificial Big Data Age" *SSRN Electronic Journal* (2019).

The Basis for Personal Data Processing[10]: As previously stated, fiduciaries are required to treat personal data. This is possible under two circumstances. Personal data can be processed with or without consent, depending on the nature of the personal data. Personal data can be processed without consent under certain circumstances, such as when the government wants to offer services to the person if it involves legal proceedings, or when the case involves a medical emergency to which the government is trying to respond in the case of a pandemic.

Intermediaries in social media: This data law also regulates online activity and the methods in which data is exchanged across social media sites[11]. The necessity to govern how individuals exchange information online, as well as the amount to which personal data may be exposed, was discovered to be crucial at the dawn of the digital revolution. Because social media has an impact on political order, the Indian government has been particularly interested in regulating it. This law governs social media engagement to an incredible level. Most academics feel that this rule has restored sanity and order to the internet community, where many Indians engage in everyday activities.

The law formed the Data Protection Authority[12], which is a regulating entity. Its responsibilities include safeguarding persons when it comes to data processing and information consumption, preventing any exploitation of personal data, and enforcing the law to guarantee that all of its components are carefully followed. Most significantly, the agency's chief should have at least 10 years of expertise with data security concerns. Six members of the authority are also in charge, with almost equal knowledge and experience.

The choices they make or the policies they establish, on the other hand, may be challenged in the Appeal Court. It means that, although having virtually absolute authority when it comes to the protection of personal data, their word is not final when it comes to data protection.

Issues Concerning Data Transfer Beyond Indian Borders: The Indian government takes data transmission very seriously, particularly when it crosses national boundaries[13]. First and foremost, this permits for the voluntary movement of personal data outside of India. However, there are a number of stipulations attached to this act that might make the procedure much more difficult. The government mandates, via this regulation, that a duplicate of such data be kept and preserved in India even when it is sent outside the nation.

Exemptions: While this act is intended to safeguard people from the exploitation of personal data and to provide full data protection, the Indian government has the authority to suspend the

[10] Tadas Limba and Aurimas Šidlauskas, "CONSENT AS A LAWFUL BASIS FOR PROCESSING PERSONAL DATA UNDER THE GDPR" *INTED2020 Proceedings*, 2020.
[11] Surajit Deb, "Social Protection Network Across Indian States" *Social Change* (2021).
[12] Michael Hintze, "Data Controllers, Data Processors, and the Growing Use of Connected Products in the Enterprise: Managing Risks, Understanding Benefits, and Complying with the GDPR" *SSRN Electronic Journal* (2018).
[13] Pavel Khorev and Andrey Chernetsov, "The Problem of Ensuring Cross-border Personal Data Transfer and Methods for Its Solving" *2020 5th International Conference on Information Technologies in Engineering Education, Inforino 2020 - Proceedings*, 2020.

execution of certain parts of the Act under specific circumstances. These circumstances include, among others, situations involving national security and India's relations with other nations in the regional and worldwide environment, as well as prohibiting incitement aimed towards the state or any other state entity. The state institutions or the central government may exercise these exemptions directly.

Offenses: The bill defines a number of crimes that may be prosecuted in a court of law. Here are a few examples:

• Processing and transmitting personal data in accordance with the act's processes and rules. The person or organisation is fined Rs 15 crore if convicted[14].

• Another major infraction under this legislation is the re-identification or processing of de-identified data, which is punished by a three-year prison sentence.

• It's also possible to be a fiend for failing to do a data audit.

Personal Data Sharing: The measure empowers the government to get access to non-personal or anonymous data via fiduciaries in order to deliver different services to people. However, this should be done in accordance with the bill's available procedures.

III. CHILDREN UNDER PERSONAL DATA PROTECTION BILL, 2019

"A person who has not completed eighteen years of age" is classified as a "child" under the Bill[15]. As a result, the Bill proposes to make Internet access by anybody under the age of 18 subject to rigorous parental approval and age gating systems. Under the Bill, valid consent is defined as free, informed, precise, unambiguous, and revocable assent. Persons under the age of 18 are not considered capable of providing such legitimate permission under the bill, which means that their parents will have to agree on their behalf when their children join up for social networking services[16].

Children and adolescents under the age of 18 are predicted to account for one out of every three Internet users worldwide. Adolescence is the era when children move from children to young people, and it is during this time that they gain information, develop qualities and abilities, and, most importantly, learn to manage emotions and relationships. This includes their online behaviour as well as their digital identity. The majority of children and teenagers use the Internet for amusement and information, and they feel they have a legal right to do so. In the majority of situations, kids are also aware of the dangers of accessing the Internet and are aware of their right to privacy.

[14] Balaji Raghunathan, "- Overview of Data Anonymization" *The Complete Book of Data Anonymization*, 2020.
[15] Graham Greenleaf, "India's Personal Data Protection Bill, 2019 Needs Closer Adherence to Global Standards (Submission to Joint Committee, Parliament of India)" *SSRN Electronic Journal* (2020).
[16] Sonia Livingstone, Mariya Stoilova and Rishita Nandagiri, "Children's data and privacy online: Growing up in a digital age" *Media and Communications* (2019).

Over 472 million children under the age of 18 live in India alone[17]. With an increasing number of people accessing the digital world, it's become even more critical to protect their right to privacy online. India must explore how to facilitate their right to involvement while also ensuring their privacy from both parents and friends, as well as the State and commercial organisations, without compromising their autonomy.

Section 16 of Chapter IV of the law deals with children's personal and sensitive personal data[18]. Before processing a child's data, a data fiduciary must verify the child's age and acquire the approval of the child's parent or guardian. The bill categorises minors as those who have not yet reached the age of eighteen, as do most Indian legislation. According to the law, the way in which this verification procedure will be carried out will be determined by rules. It's worth noting that when validating a person's age, a data fiduciary may up collect information concerning youngsters. Measures should be made to guarantee that this data is not utilised for any other purpose when creating the rule that defines the method of verification.

The demand for parental permission must be considered in the light of the children's general sociocultural milieu. Because age alone does not tell the whole picture, we must also consider social, physiological, and other important elements when deciding how to handle children's privacy. The contemporary educational environment has included technology tools that have allowed pupils to develop and obtain a deeper grasp of the digital world. Adolescents, or youngsters between the ages of 16 and 18, frequently have an in-depth comprehension of their online actions that is equivalent to that of adults. Regulatory frameworks that fail to take this into account have a detrimental effect on the interests of persons in this age range. In 2016, India has around 44 million youngsters aged 16 to 18[19]. It's critical that our rules don't limit their capacity to utilise the digital resources at their disposal.

Different legal regimes across the globe give extra safeguards to protect the privacy of children of various ages in respective countries. A kid who is at least 16 years old may consent to their data being processed in regard to information society services that are directly given to them, according to the General Data Protection Regulation of the European Union. It does, however, need parental approval for any kid under the age of 16. In the United States, however, the Minors's Online Privacy Protection Act requires website or online service owners to notify children that personal information is being collected and to get verified parental permission. Even China's Cyberspace Administration only needs parental authorization to handle data from children under the age of 14[20].

[17] Nutal Kumari, "An Assessment of Birth Registration System and Factors Affecting in India and its States." *Online Journal of Public Health Informatics* (2019).
[18] Anirudh Burman and Suyash Rai, "What Is in India ' s Sweeping Personal Data Protection Bill ?" 7–10 (2020).
[19] Simon Kemp, "The State of digital in April 2019: all the numbers you need to know" *We are social*, 2019.
[20] Emmanuel Pernot-Leplay, "China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.?" *Penn State Journal of Law & International Affairs* (2020).

There is a clear need for laws and policy frameworks that strike a balance between children's privacy rights and the need to safeguard their internet activities. While the new Indian legislation aims to protect minors' rights, it should rethink its approach of demanding parental agreement for all teenage internet activities. Policymakers should consider their unique situations and demands, and consider treating them as a distinct group from both children and adults.

IV. THE AGE OF CONSENT IS SET AT 18 YEARS OLD AS A GENERAL RULE.

Given the number of possibilities for young people to explore themselves and find what they want to achieve later in life on the Internet, an age limit of eighteen seems unfair.

The notion for 18 as a blanket age of consent may have come from the Indian Contract Act[21]. However, there are obvious problems with this: "There is a difference between entering into a legitimate contract and the perspective of youngsters on the Internet." You could have a youngster who is 12 or 14 years old and wants to watch YouTube videos to learn a particular language etc.

Even parents or guardians of children may not always comprehend what they are committing to on behalf of their children. Allowing parents to make decisions on behalf of their children may also take away a child's autonomy — "many of the children are struggling with their sexual orientation, and have begun exploring it around the age of 15 or 16, and they may not want their parents to know about it right away".

Requiring permission vs maintaining privacy: This issue may exacerbate, particularly for girls who live in families with just one smartphone. "In such family, a female youngster may have less access to that phone." In a patriarchal country like India, relying on a parent's permission would have an influence on women's privacy. Just relying on parents' approval will not guarantee women's privacy, if a female kid wants to learn more about reproductive rights or takes lessons about it.

Is this leading to effectively disenfranchising Indian children from receiving information that is beneficial to them, allowing marketers or anyone is attempting to reach them to provide them with good information?" However there has to be a balance between the two under the guise of protection.

What does it mean to give children meaningful consent? Children, like everyone else, need to know what they're getting into while using the internet and signing up for a service. In addition, youngsters must be allowed to revoke permission given before.

Literacy in the digital age- Internet literacy varies by country, making the concept of a universal age of consent for children even more challenging. Access to telecommunication services is vital, and that a 13-year-old may grasp consent better than an 18-year-old in many circumstances.

[21] Shivprasad Swaminathan and Ragini Surana, "Minors' Contracts: A Major Problem with the Indian Contract Act, 1872" *Statute Law Review* (2021).

Children's empowerment: A blanket age of consent places children in a bubble. Rather than entirely enclosing children in a cocoon, it is more necessary to empower them to shield themselves against potentially dangerous material or when they believe they are being unjustly targeted. Age of permission for sites such as YouTube is less than 18 years old. The EU's GDPR[22] sets the age of consent at 16 years, the UKs[23] at 13 years, and Australia has no such idea[24]. So essentially it means that a 12-year-old kid has the same capacity as a four-year-old child, or a 16-year-old child, or an 18-year-old child.

Young people use the internet for their own social mobility, growth, and engagement with topics they may not otherwise have access to. For example, students from tier-three cities are very eager to engage in online learning activities since they may not have the same exposure in their home cities. These youngsters want to go online and be a part of groups to understand and connect with individuals who are going through similar things.

Many social media stars are really kids who wind up earning endorsement agreements. "Imagine if they had to get parental permission for that." These are restriction on access. Age in India is not the sole element that decides whether a kid would grant permission or not. There are a number of additional considerations. Access can influence behaviour: a 15-year-old who spends more time online than a seventeen-year-old may be able to recognise that targeted ads are targeting them based on their online activity, and thus be better positioned to give informed consent, or at the very least instinctively avoid risky services that might compromise their privacy. Access is also heavily favoured by boys, who have more unlimited access. Given India's socioeconomic circumstances, certain families, who may not have a comprehensive grasp of the hazards, may be at a disadvantage.

V. THE EFFECTIVENESS OF GUARDIAN DATA FIDUCIARY

The bill's fourth chapter covers the function of a guardian data fiduciary in improving the entire process of data protection and online service provision for children. First and foremost, they are not responsible for tracking and monitoring children's internet activity[25]. In particular, their position must not include participating in any action that may endanger the children. This section of the clause is intended to prohibit Google and You Tube from being penalised for participating in child-endangering advertising. Only data fiduciaries who provide critical services such as counselling and child protection may be permitted to handle such personal data. This raises the issue of whether guardian data fiduciaries are making a major contribution to children's online

[22] Chris Jay Hoofnagle, Bart van der Sloot and Frederik Zuiderveen Borgesius, "The European Union general data protection regulation: What it is and what it means" *Information and Communications Technology Law* (2019).
[23] Simon Jay, Colin Pearson and Natalie Farmer, "Some Reflections on Brexit and the U.K. Data Protection Regime" *Intellectual Property & Technology Law Journal* (2016).
[24] Robert Walters and Matthew Coghlan, "Data Protection and Artificial Intelligence Law: Europe Australia Singapore - An Actual or Perceived Dichotomy" *American Journal of Science, Engineering and Technology* (2019).
[25] Anirudh Burman, "Will India's Proposed Data Protection Law Protect Privacy and Promote Growth?" 39 (2020).

safety. When guardian data fiduciaries fail to execute or extend their obligations beyond what is stipulated, the PDP bill of 2019 is quite clear about the punishment that should be enforced. They might face a fine of INR 15 crore, for example.

VI. DOES CHAPTER IV OF THE PDP BILL PROVIDE ADEQUATE PROTECTION FOR CHILDREN?

When discussing children's data protection, one of the most important topics to consider is whether the fourth chapter is sufficient. Many academicians believe that far more protection is needed to properly secure children's personal data and guarantee that they are safe while utilising internet services. Their data should be processed with even more effective procedures and rules that are more focused on their predicament and hazards. Chapter Four of this legislation serves two broad aims, according to the debate.

The primary function of this section is to ensure that age verification is carried out in a manner that benefits the kid in question. Age verification is undeniably a crucial topic in this debate that must not be overlooked. Second, it aims to safeguard children from unwanted or needless monitoring and tracking of young children for the sake of advertising and other commercial objectives, as was recently shown in the case of YouTube and Google. While these duties are admirable, there are a few more pressing concerns that must be addressed.

First, the job of the guardian data fiduciary is underutilised. This legislation seems to be oblivious to what appears to be a serious problem. The task they have been given seems to be perplexing, and many of them may face charges of incompetence. Some argue that equating the roles and responsibilities of these organisations to those of other categories or classifications of data fiduciaries would be more relevant. Second, the problem of India's varied age of consent seems to be ineffectual. The bill's ambiguous definition of injury makes things much more confusing. Finally, the absence of sensitive personal data in government databases is an even more pressing issue that must be addressed alongside data privacy concerns.

VII. ALTERNATIVES TO A BLANKET CONSENT AGE

As an alternative to having a blanket age of consent, the United Kingdom recently released an age-appropriate code, which includes roughly 15 principles that businesses must follow. For example, under the code, privacy must be enabled by default; platforms must clearly explain to children why their data is being gathered in a manner that they understand; and corporations cannot use nudge methods to persuade children to change their privacy settings.

In India's instance, the Data Protection Authority may provide age-appropriate regulations and standards that different platforms must follow. A graduated approach to permission is also a viable option. Children under the age of 14 will need parental approval, while those between the ages of 14 and 16 will not. Different ages, different needs: Data fiduciaries may grade age of consent to

recognise that varying age groups have varied degrees of development and different levels of issue recognition. Evolving US and UK regulations, such as COPPA, suggest the necessity for parallel initiatives.

VIII. DATA PROTECTION AND THE RIGHT TO PRIVACY FROM AN INTERNATIONAL PERSPECTIVE

The problem of data protection in relation to the right to privacy, particularly for minors, has piqued the interest of many governments throughout the world. The right to privacy is protected in the United States by the Fourth Amendment to the United States Constitution[26]. Overall, it discusses people's right to privacy in their persons, residences, and places of employment, as well as their right to be free from unjustified searches and disclosures of their personal information. Under the United States Constitution, children's right to privacy is even more distinctive and important.

The right to privacy for children is protected under Article 16 of the United Nations Convention on the Rights of the Child (UNCRC)[27]. It protects his or her private information about his or her personal life, family, and communication from prying eyes. It also makes it illegal to insult a child's honour or reputation. This international law serves as the foundation for all specific laws developed by governments across the world in order to safeguard children. Data protection rules in countries like the United Kingdom are similarly strong, ensuring that children's privacy rights are protected. The legal age of consent for minors in the United Kingdom, for example, is 13 years old under the new Data Protection Act. This was predicated on the idea that kids can't tell the difference between sponsored material and free information on the internet.

IX. RECOMMENDATIONS AND CONCLUSION

To improve the security of personal data and the right to privacy, the Indian Data Protection Authority, as well as other nations' authorities, may adopt the following recommendations:

• Ensure that the law is strictly enforced, rather than just passing legislation without putting them into effect.

• Teach kids about cybersecurity so they don't become victims.

• Set use limitations with parents and guardians.

• Use parental control software to block or restrict access to sites that are inappropriate for children's age.

• Always be available to help youngsters who may need internet services.

[26] David Schultz and John R. Vile, "United States Constitution" *The Encyclopedia of Civil Liberties in America*, 2019.
[27] Jörg M. Fegert, "United nations convention on the rights of the child" *Zeitschrift fur Kinder- und Jugendpsychiatrie und Psychotherapie*, 2019.

With the expanding use of information communication in several areas throughout the economy, ranging from transportation to education, data privacy has become a key sensitive problem. Thanks to digital/video games and other applications that use advanced digital technologies, sophisticated technology has grown even more popular in the realm of entertainment. However, the threat of personal data abuse and intentional disclosure of other people's private information has prompted governments throughout the globe to enact new data protection rules and legislation. Only by enacting the Personal Data Protection (PDP) Bill of 2019 has India been in the forefront of protecting children's personal data and ensuring their safety. While it has performed well in most of its functions, it does have a few drawbacks, as noted. Overall, the government's efforts to safeguard data and strengthen the right to privacy via various legislation are praiseworthy.