Page 1281 - 1290 **DOI:** *https://doij.org/10.10000/IJLMH.118373*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 7 | Issue 5

2024

Advocacy For Youth Privacy Laws and Policies in India

HARSHIT GUPTA[1]

ABSTRACT

Real world existed before the invention of computers and internet, where people met other people in physical world, which is not the case anymore, the invention and advancement of internet, has divided the world is into two parts firstly, a real physical world and secondly the virtual world, which is becoming the only world for the youth now a days. The privacy of a person as defined by many come to one conclusion that one shall be allowed to do whatever he wants to do within the boundaries of law. Privacy is the right to be left alone or to be free from misuse or abuse of one's personality. Now hopping onto Youth Privacy, it can be defined in the contemporary world with high Technological advancements, as it relates more to online privacy and protection of data in the world of internet which is not limited to online modes but also stretches to the physical privacy. The privacy if internet was not existing would have concerned and limited to physical privacy and the ambit of the same would have been narrow but situation is not the same as earlier. Technological advancements in India started to peak during and post covid-19 period. Now in India there are almost 1.14 billion subscribers of network including the non-active ones. Assuming 10% non- active subscribers, this reduces to 1.03 billion active subscribers which means a very large population of India is now connected to the Internet. The Right to Access Internet was declared as the fundamental right under article 19(1)(a) of Part III of Indian Constitution in the case of Anuradha Bhasin & Anr v. Union of India and Ors. This clearly shows that person enjoying its one fundamental right might lead to breach of another right. The paper focuses on discussing the term "Youth Privacy" and analyse the importance of it in todays era Across the globe. The paper mainly focuses on the existing legislation on the digital privacy and privacy as a right. It further extends to suggest some advancement that can be made in the laws existing as well as any law which required to be legislated by the Parliament of India in near future. This paper aims to connects dots between Youth Privacy and the technological advancement and their safeguarding. The Youth need more and strong statutes for protecting themselves in both the world i.e., real and virtual world. The State need to make more laws to regulate the access of personal information available online on different platforms and segments.

Keywords: *Data Protection, India, Internet, Privacy, Youth.*

[1] Author is a student at Department of Law, Invertis University, Bareilly, India.

 [ISSN 2581-5369]

I. INTRODUCTION

The youth of any country play a crucial role in the advancement and prosperity of the nation. India currently has the greatest adolescent and young population in its history. India possesses the most substantial youth demographic globally, since 66% of its populace falls below the age of 35. Despite a decrease, India will continue to have a relatively youthful population in 2030, with 24% falling into the 15-29 age bracket. It is currently undergoing a demographic window of opportunity, sometimes referred to as a "youth bulge," which is projected to persist until 2025.[2] The future development trajectory of India will be contingent upon its ability to foster and support its young population, particularly while other nations such as Europe, the US, and China grapple with the difficulties posed by an ageing population and diminishing youth. After the COVID-19 epidemic, there has been a significant and widespread shift towards digitalization throughout all areas of society, even among the younger population.

There are both new opportunities and new dangers for young people online as digital technology permeate almost every part of their lives, including school. We must be vigilant that our well-intentioned but hastily implemented measures to safeguard young people from harm do not severely restrict their prospects for growth and development. Instead, these initiatives should safeguard youth while enabling them to gain independence and resilience.

Young adults are the most engaged internet users, curating and consuming content across global social media platforms. They are undoubtedly the most active online today, leading the digital space to curate and consume content on world-wide social media platforms. These platforms and other online services collect massive amounts of personal and behavioural data to provide the best possible user experiences, such as adverts and show suggestions. However, this may give rise to prejudice and malpractice in handling information, raising worries about young adults' online safety and privacy, especially in terms of personal and data protection on the internet. The growing utilisation of data via online platforms gives rise to apprehension regarding a fundamental entitlement of young individuals, amongst many one of the most important rights is the right to privacy. The concept of privacy encompasses varying interpretations and connotations within different contexts. The issue of the right to privacy in India has been a subject of extensive deliberation, culminating in the landmark ruling of *Puttuswamy vs. Union of India*[3] in 2018. This decision affirmed the constitutional protection of

[2] Adolescents and Youth, UNFPA INDIA (2016), https://india.unfpa.org/en/topics/adolescents-and-youth-8 (last visited Mar 21, 2024).
[3] Fundamental Right to Privacy, SUPREME COURT OBSERVER, https://www.scobserver.in/cases/puttaswamy-v-union-of-india-fundamental-right-to-privacy-case-background/ (last visited Mar 22, 2024).

 [ISSN 2581-5369]

the right to privacy, as enshrined in Article 21 of the Indian Constitution. This constitutional provision grants individuals the right to solitude, tranquilly, and protection from intrusion, unless otherwise mandated by law.[4]

In the contemporary era characterized by significant technological progress, the right of individuals is being curtailed in several ways. When considering the age span of the victims, it encompasses those belonging to the "Youth" category within the entire human species. They possess the ability to adopt novel technology advancements, whether consciously or unconsciously, resulting in the encroachment upon their own rights. For instance, young individuals may engage in the sale of their personal data without being aware that it may be exploited against them in the foreseeable future. The term "selling data" refers to the act of completing unfamiliar forms by clicking on different links or URLs that are accompanied with enticing captions such as "*click on this link and receive Rupees* ***." The Internet era is characterized by its transformative impact on the modes of life that are both private and public.

The Internet expands the public domain by providing online amenities and an infrastructure that allows for the recording, tracking, and sharing of life and habits. Privacy, when defined as the state of being left undisturbed, is an inherent component of personal space. The right to privacy extends beyond physical boundaries and encompasses the virtual realm as well. The right to access the internet is a fundamental entitlement that guarantees universal access to the internet for anyone who desires it. The state does not impose any limitations on the denial of an individual's fundamental rights. It may be deduced from the aforementioned rights that individuals possess both the right to privacy and the right to use the internet. Given that the internet serves as a platform for data collecting, it is plausible to argue that the right to access the internet may potentially encroach onto the right to privacy.

II. THE JOURNEY OF RIGHT TO PRIVACY

The concept of privacy has not undergone rapid development. The debate over privacy concerns is said to have existed since the dawn of human civilization. In order to fully experience being alive, rights are unavoidable. As a result, numerous liberties have been acknowledged gradually as inevitable consequences of the political, social, and economic reforms. Initially, only some rights were recognised by the law, such as the right to life and property. However, over time, the law began to recognise human emotions, intellects, sentiments, and more. Over time, the concept of the "right to life" has been expanded to encompass not only "the right to enjoy life,"

[4] RIGHT TO PRIVACY: AN INDIAN CONTEXT, THE TIMES OF INDIA, https://timesofindia.indiatimes.com/readersblog/the-daily-roam/right-to-privacy-an-indian-context-55047/ (last visited Mar 22, 2024).

 [ISSN 2581-5369]

but also "the right to be left alone," which is also referred to as "the right to privacy." [5] Article 12 of the Universal Declaration of Human Rights (United Nations, 1948)[6], Article 17 of the International Covenant on Civil and Political Rights (United Nations, 1966)[7], Article 16 of the Convention on the Rights of the Child, (United Nations,1989)[8] and several international and regional human rights accords and conventions all establish the right to privacy. In the year 2018, the United Nations officially recognised the "Personal Data Protection and Privacy Principles, 2018" as a comprehensive set of guidelines for the management of personal data by all UN entities. These principles were officially endorsed during the 36th Meeting of the UN High-Level Committee on Management. They establish the essential structure for the oversight of personal data, in accordance with the United Nations' commitment to protecting privacy and guaranteeing data security. Contemporaneously, in India, the ongoing debate regarding the right to privacy, which originated in the year of 1963 from the *Kharak Singh vs State of Uttar Pradesh*[9] case, was resolved in the *K.S. Puttaswamy and Anr vs Union of India*[10] case in 2017. This ruling confirmed that the Constitution of India ensures every individual a fundamental right to privacy explaining that the fundamental principle of privacy safeguards the personal integrity of an individual, encompassing their residence, family, and communication. Access control is a shared characteristic throughout various domains of privacy, encompassing the ability to regulate one's knowledge about others, exercise control over personal choices and behaviours, and maintain control over physical environments.

(A) What is Youth Privacy?

Westin was one of the pioneers in defining privacy as "the assertion of individuals, groups, or institutions to independently decide when, how, and to what degree information about them is shared with others." His ideas were based on a strong sociological background. Westin positioned privacy within a framework of dialectical social practices that governed both disengagement (through isolation, anonymity, and solitude) and social engagement.[11] The

[5] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARVARD LAW REVIEW 193 (1890), https://www.jstor.org/stable/1321160 (last visited Mar 24, 2024).

[6] Article 12: "*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."*

[7] *Article 17:* "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks."

[8] Article 16: "*No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation. The child has the right to the protection of the law against such interference or attacks*."

[9] 1963 AIR 1295

[10] (2017) 10 SCC 1

[11] Alan Westin, *Privacy And Freedom*, 25 WASHINGTON AND LEE LAW REVIEW 166 (1968), https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20.

concept of privacy is fundamental to society; it influences social life in profound and nuanced ways and shapes our perception of the social world. Privacy functions as a social category, encompassing both normative and descriptive aspects, which are mutually influential. Privacy is a fundamental concept that governs societal and individual life, as well as organisations, customs, and activities. It regulates individuals' perceptions of their legitimate access to resources, thereby promoting both opportunities and constraints.[12]The concept of "youth" is frequently employed in policy formulation, media coverage, and commercial advancement as symbolic elements representing the forthcoming generation of students, consumers, employees, and citizens. Additionally, it is influential in shaping social and organizational norms within the context of the Internet era. Privacy holds significant importance for young adults, although it is a complex issue that encompasses several perspectives. The privacy measures implemented by these young individuals to regulate the content accessible to their parents are entirely circumvented when parents explicitly ask family members to supervise their children's accounts. Studies indicate that young individuals hold the belief that the mere presence of information on the internet does not necessarily imply that it is intended for widespread consumption, and it still constitutes a violation of their privacy. They appreciate the convenience of openly sharing information through anonymous or alternative accounts. Nevertheless, all data is uploaded with specific limitations in consideration, and any violation of these boundaries results in a violation of privacy. One argument is that there's a cultural loss in the importance of privacy, especially among young persons who are growing up in a setting characterised by open networks. Many of these individuals actively engage in online sharing and deliberately construct their daily routines inside inherently public social networks. Therefore, privacy is no longer considered a societal norm. Terms such as Generation Y, Millennials, the Net generation, or Digital Natives are utilized to delineate a disparity between an older cohort of business developers, policy-makers, educators, and parents, and a generation that is maturing alongside digital media as an inherent component of their daily existence and behaviours. Likewise, the portrayal of a cohort of technologically adept adolescents has been a subject of debate about the safeguarding of online privacy and the security of personal data.

III. YOUTH, ONLINE PRIVACY AND SOCIAL MEDIA: A TRILOGY

Privacy is a fundamental principle that protects an individual's personal integrity, including their residence, family, and communication. The right to privacy assumes that having a personal space is crucial for individual freedom and self-governance. Maintaining a general belief in

[12] PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY, (Ferdinand David Schoeman ed., 1984).

 [ISSN 2581-5369]

privacy prevents observation, eavesdropping, deception, and the presence of others and their knowledge of personal information. According to Fried (1984), the significance of privacy lies in its ability to facilitate crucial interpersonal connections. Privacy is essential for establishing and maintaining connections, such as love, friendship, and trust, without which we would not be considered human. The principle of privacy is equally applicable to both offline and online domains.[13] Nevertheless, the right to privacy of individuals has undergone a corresponding evolution in conjunction with the institutional restructuring of the public domain. As a result, the phrase "online privacy" is frequently employed to describe the difficulties and ramifications that the Internet presents concerning the right to privacy. Internet users may have become more cognizant of the need to manage their online privacy because of the increasing amount of media coverage on privacy-related issues and the exponential growth in the diversity of social networking site (SNS) users.[14] Around 93 percent of the world's population is linked to the internet, with almost 60 percent - 4.8 billion people - being active users of social media. Social media has become an essential aspect of people's life, particularly among the younger demographic. Nevertheless, the increasing prevalence of digital platforms is concurrently leading to adverse encounters. A report by "*the Institute for Governance, Policies & Politics, Social Media Matters*" and "*Youth Online Learning Organisation*" shows that over 85% of young Indians own a smartphone, enabling them to access the internet or web and social media at any given point of time. The primary source of internet usage is mobile phones, followed by computers/laptops. Among 18-25-year-olds, 86% use mobile phones for internet and social media.[15] Due to the vast volume of personal data exchanged on the internet, a significant portion of studies on informational privacy naturally focuses on the Internet. Nevertheless, the ramifications of youth privacy breaches beyond the digital realm when data is mistreated in the online realm. Essentially, infringements on online privacy pose a threat to offline privacy of youth, since it is impossible to safeguard one's offline privacy without safeguarding their online privacy. Youth face several online hazards, such as exposure to age-inappropriate information, instances of cyberbullying, predatory individuals, and cyber harassment and online data leakage. Less conspicuous hazards include business exploitation and social transformations such as the normalisation of monitoring. Privacy is further violated by the unauthorised collection of information only for the purpose of creating personalised adverts to target specific consumers, in addition to the risk of data leakage. Cookies also facilitate the acquisition of

[13] PHILOSOPHICAL DIMENSIONS OF PRIVACY, *supra* note 12.
[14] Yabing Liu et al., *Analyzing Facebook Privacy Settings: User Expectations vs. Reality*, PROCEEDINGS OF THE ACM SIGCOMM INTERNET MEASUREMENT CONFERENCE, IMC (2011).
[15] Social Media Matters, *Patterns of Internet Usage Among Youth in India*, SOCIAL MEDIA MATTERS, https://www.socialmediamatters.in/internet-usage-among-youth-in-india (last visited Mar 25, 2024).

 [ISSN 2581-5369]

information. The acceptance of these cookies by users may give rise to unidentified consequences, such as user profiling and the formation of echo chambers. Therefore, it is important for young people to possess awareness and engage in practical thinking to mitigate these privacy dangers. It is essential for businesses to prioritise the establishment of a certain degree of trust and effectively communicate the risk profile to users prior to engaging in any interactions. It is recommended that predetermined boundaries be established for the collection of data and enhancements be made to customer privacy rules in order to guarantee the collection of only essential data.

IV. EXISTING LAWS ON PRIVACY IN INDIA

Policymakers may establish fundamental legislative safeguards to ensure the proper acquisition and use of data by governments, enterprises, organisations, and other entities involved in the collecting, processing, and sharing of personal data pertaining to young people. The main topics being debated are establishing the suitable age for digital consent, granting consent rights to either the parent or the kid, advocating for a framework that is based on consent or rights, and depending on legislation that is broad or sector-specific.

Digital Data Protection Act, 2023: After getting Presidential approval, the Digital Personal Data Protection Act, 2023 has been successfully passed before both houses of Parliament and then published in the official Gazette. The primary objective of the Act is to provide a legal framework that aligns with the principles of the right to privacy, as delineated by the Supreme Court of India in the Puttaswamy Judgements, and subsequently by subsequent constitutional Courts. The notion, which has become more established, posits that an individual's autonomy is intrinsically connected to their autonomy in managing their personal data. Hence, within a system that remains firmly grounded in consent, the inquiries about the identification of children, their capacity to provide permission for the collection of their personal data, and the permissible and impermissible actions pertaining to it, have significant importance in determining their future role as 'Digital Nagariks'. It applies to situations where personal data is collected in digital or non-digitized form and converted into digital form. The Act defines 'personal data' broadly, including any identifiable data about an individual. It also defines 'digital personal data' as digital data. It is applicable to Indian entities including processing personal data and has extra-territorial applicability to foreign entities offering goods and services to Data Principals within India. However, it does not apply to personal or domestic data used for personal or domestic purposes or to publicly accessible data made by the Data Principal or other law-mandated individuals or entities. By situating India in a global

 [ISSN 2581-5369]

framework, the DPDP Act draws lessons from the European Union's General Data Protection Regulation (GDPR) which governs the acquisition and utilisation of personal data. This document outlines the legislation pertaining to safety, privacy, and the necessary precautions for safeguarding data. Regarding minors, the General Data Protection Regulation (GDPR) stipulates that the lawful processing of a child's data is contingent upon the kid reaching the age of 16 or above. In situations involving a kid who is below the age of 16, it is essential to get agreement or approval from the one who has responsibility as a parent for the child. Given the anticipated valuation of India's digital market at $1 trillion by 2025, the establishment of a resilient cybersecurity framework becomes imperative in order to foster investor confidence and ensure the sustained viability of digital advancements. It is instrumental that public and private entities collaborate to ensure a seamless implementation during the current phase of our digital transformation. If the suitable course of action is implemented, India has the potential to overcome its cybersecurity challenges and position itself as a global leader in safeguarding data. The DPDP Act goes beyond its legal significance and declares India's dedication to safeguarding the digital independence of its citizens while fostering a secure environment that encourages progress and growth. Currently, India boasts an exceptionally vibrant reservoir of cybersecurity experts, which serves as a valuable resource not only for the country but for the global community as a whole. India is presented with a substantial opportunity to attain a position among the most secure nations worldwide in terms of conducting digital commerce through the DPDP Act.

Information Technology Act, 2008 : The primary purpose of the Act was to provide legal acknowledgment for electronic commerce and impose penalties for the improper use of computers. Nevertheless, the document lacked explicit rules pertaining to the safeguarding of data. Violations of data security may lead to legal action against persons who gained unauthorised access to the system, as outlined in Sections 43 and 66 of the IT Act. However, the Act does not provide other solutions, such as pursuing legal action against the entity responsible for the data. The IT (Amendment) Act 2008 was enacted to include two additional provisions, Section 43A and Section 72A, into the IT Act. These sections aim to provide a solution to individuals who have experienced or are expected to experience a loss due to insufficient protection of their personal data.

The government subsequently enacted the "*Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011*" in response to the amendment. As per the provisions stated in Section 43A of the IT Act, the "IT Rules" defines "personal information" as any data concerning an individual that, when combined with

 [ISSN 2581-5369]

other data, can be used to directly or indirectly identify that individual; this is referred to as "Personally Identifiable Information." Additionally, a subcategory known as "Sensitive personal data or information" is established to encompass the aforementioned items, including but not limited to user names and passwords, financial information, health conditions and biometrics, and sexual orientation. According to the IT Rules, body corporates are required to furnish a privacy policy that includes the following: a description of the practices that are transparent and simple to understand; the rationale behind the collection and utilisation of such information; and the nature of the data collected, including whether it is sensitive personal information or personal data. Additional regulations stipulate that prior to gathering such data, written or electronic mail consent must be obtained from the provider specifying the intended use. Before gathering any information, including sensitive or personal data, the provider of that data must provide a choice to opt out of disclosing that information. Additionally, the user must retain the option to revoke their consent at any time while using the service or otherwise. Body corporate disclosure of sensitive personal data or personal information to a third party shall be subject to the provider's prior consent. It is required that the body corporate appoint a Grievance Officer and make his name and contact information available on its website. The rules provide for obtaining written or electronic consent that is explicit. (To provide consent, look for a "tick box" or "pop-up" containing the terms and conditions and privacy statement.) A choice to refrain from disclosing personal information and the ability to withdraw consent or information that has already been provided. It is necessary to obtain the information provider's permission before disclosing any collected data to third parties. As an exception to the general norm regarding the maintenance of privacy and seclusion of information, Section 69[16] of the Act states that the Government may, in the following circumstances, deem it necessary:

[16] "*[69. Power to issue directions for interception or monitoring or decryption of any information through any computer resource.–(1) Where the Central Government or a State Government or any of its officers specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient so to do, in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.*
(2) The procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.
(3) The subscriber or intermediary or any person in-charge of the computer resource shall, when called upon by any agency referred to in sub-section (1), extend all facilities and technical assistance to–
(a) provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or
(b) intercept, monitor, or decrypt the information, as the case may be; or
(c) provide information stored in computer resource.
(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with imprisonment for a term which may extend to seven years and shall also be liable to fine."

 [ISSN 2581-5369]

safeguarding the sovereignty or integrity of India; ensuring the security of the State; maintaining amicable relations with foreign nations; maintaining public order; preventing incitement to commit a cognizable offence pertaining to the aforementioned matters, or conducting investigations into such offences. Section 72[17] of the Information Technology Act, 2000 addresses privacy breaches by data processors. If someone gains access to electronic records or materials without their consent, and discloses them to another person, they may face imprisonment for up to two years, a fine of Rs 1,00,000, or both.

V. CONCLUSION

In conclusion, it is widely acknowledged that young adults must increase their online vigilance and practise greater caution. One of the initial steps towards significantly ameliorating this situation is for the government to enact a robust and all-encompassing legislation aimed at safeguarding citizens' data. Young adults, particularly in the wake of a global pandemic, spend the majority of their lives online and utilise social media for a variety of interactions. We delved deeper into the social media platforms WhatsApp and Instagram, which have both instituted numerous security and privacy features. Nonetheless, considerable scope exists for enhancement. Additionally, there is a belief that young individuals ought to have authority over their personal information, as opposed to being obligated to reach the age of majority in order to determine what they wish to disclose. However, mere awareness is insufficient; immediate action is required to enhance the safeguarding of data privacy for young adults on the internet. This can solely be accomplished via advocacy, with collaboration among businesses, citizens, civil society organisations, the government, and social media platforms in order to establish a harmonious equilibrium that serves the collective welfare.

*****

[17] *72A. "Punishment for disclosure of information in breach of lawful contract.–Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both.]"*

 [ISSN 2581-5369]