ISSN PRINT 2319 1775 Online 2320 7876

Research paper

 UGC CARE Listed (Group -I) Journal Volume 8, Issue 4, 2019

DATA PROTECTION *vis-à-vis* PRIVACY

Doddapaneni Geethanjali Chowdary,

5/5 BB. A, LL.B, Department of Law, Koneru Lakshmaiah Education Foundation, Green Fields, Vaddeswaram, Guntur, Andhra Pradesh, 522502,

geethanjalidoddapaneni4380@gmail.com 7382493263

Dr. Sailaja Petikam,

Associate Professor, Department of Law, Koneru Lakshmaiah Education Foundation, Green Fields, Vaddeswaram, Guntur, Andhra Pradesh, 522502, sailaja.petikam@gmail.com

8500673169

ABSTRACT

Digital world continues to grow and expand, which makes it imperative to make data protection and privacy our top priorities. The rapid growth in data collection, storage, and sharing has resulted in a significant need for thorough legal protections. This article is aimed at examining the significance of data protection and privacy, as well as the necessity of such legislation at present.

The proliferation of advanced technology and the expansion of digital services has led to the creation of a complex network of interrelated personal data. Sharing confidential information online may lead to misuse and manipulation of that information. The recent occurrences of data breaches serve as empirical evidence of how vulnerable is personal data, hence highlighting the establishment of robust regulatory frameworks.

The article focus is on the several factors that highlight the necessity of data protection regulation. It places a strong emphasis on upholding personal liberties like the right to privacy and the ability to exercise control over personal data. One data leak is all it takes for users to lose faith in digital platforms and services. Thus, the article places significant emphasis on the establishment of consumer trust.

The article also discusses the recent enactment of a data protection bill, which serves as a significant milestone in the effort to safeguard privacy and data in India. Analysis of bill's fundamental provisions is done, which includes data minimization, process of consent, and severe repercussions for violations. The legislation demonstrates the Government's

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 4, 2019

awareness for finding an equilibrium between fostering innovation and safeguarding privacy.

FULL PAPER

Introduction

One of the primary issues in an era of technological advancement is the protection of individuals' personal information, which might become subject to data gathering, storage, and sharing without consent. This article places significant emphasis on elucidating the significance of legislation pertaining to data protection and privacy laws, and the rationale for its necessity in the contemporary era of digital technology. Technological progress and the increased use of digital services have given way for web of personal data, which exhibits convenience and better connectivity. Nevertheless, sharing vulnerable personal data online makes such information to become an easy target to be misused or manipulated. The recent occurrences of data breaches serve as empirical evidence of how vulnerable is personal data, hence highlighting the establishment of robust regulatory frameworks.

The article explores the crucial factors that emphasize the need for rigorous data protection regulations. A strong emphasis is made on protecting the fundamental rights to privacy and data control. One data leak is all it takes for users to lose faith in digital platforms and services. Thus, the article places significant emphasis on the establishment of consumer trust. It also discusses the recent enactment of a data protection bill, which serves as a significant milestone in the effort to safeguard privacy and data in India. The government has begun to focus on finding an equilibrium between promoting innovation and protecting the privacy of individuals by making an analysis of the fundamental provisions laid out in this legislation, which includes, data minimization, processes of consent, and the repercussions for violations.

Privacy

Being able to keep one’s identity and sensitive information hidden from others and get the desired seclusion is termed as privacy. Privacy is acknowledged as Human Rights under the international treaties, which state that an individual’s liberty cannot be violated by anyone, be it their correspondence, family, or strangers. Neither their information can be misused to defame their reputation in the society. Data protection laws come as rescue from such

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 4, 2019

breaches of privacy. Any personal data that discloses one's identity can neither be collected by entity or Government without the consent of the individual.[1]

What is data protection?

The users of digital technology require a means to protect their right to privacy and their personal information from being collected without their consent. The international and regional laws make the right to privacy, an individual's fundamental right.

During the process of collecting information, it may be processed and stored by automated means and used unethically. Data protection is designed to safeguard such information by enacting laws that impede and exercise control over the activities of companies and government. It has been observed in the past, that such institutions make unethical use of such information despite making individuals believe that their data is neither collected, mined, or kept. But in reality, our personal information is put to a show without our consent, emphasizing the negligent behaviour of institutions and the necessity of vigilant oversight to prevent them from overstepping boundaries.[2]

Recent Data Breaches: A Wake-Up Call

Yum! Brands (KFC, Taco Bell, & Pizza Hut): April 2023

In April of 2023, Yum! Brands, the parent company of popular fast food chains KFC, Taco Bell, and Pizza Hut, notified about a cyber-attack that took place in January. It was initially believed by them that the data affected was corporate in nature, but later they also notified their employees of their possible personal data breach, and requested them to stay vigilant.

According to a statement sent to Electric, a spokesperson from Yum! expresses, "*During the course of our forensic analysis and investigation, we discovered that the cybersecurity breach in January 2023 exposed certain employee personal data. Individual notifications*

[1] "Kohl U, 'The Right to Be Forgotten in Data Protection Law and Two Western Cultures of Privacy: International & Comparative Law Quarterly' (*Cambridge Core*, 31 July 2015) <https://www.cambridge.org/core/journals/international-and-comparative-law-quarterly/article/right-to-be-forgotten-in-data-protection-law-and-two-western-cultures-of-privacy/31D2EDDE753A64F40FAFBF4B76CEA89C> accessed 20 September 2015"

[2] "Quach S and others, 'Digital Technologies: Tensions in Privacy and Data - Journal of the Academy of Marketing Science' (*SpringerLink*, 5 March 2015) <https://link.springer.com/article/10.1007/s11747-022-00845-y> accessed 24 September 2015."

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 4, 2019

are now being sent, and we are also providing free monitoring and security services. No customer information appears to have been compromised, according to us."[3]

In January, almost 300 locations of the company were shut down in UK, and the company continues to suffer losses in erecting measures for tight security, making the customers aware and maintain the goodwill of the brand.

1. ChatGPT: March 2023

The revolutionary AI capabilities of ChatGPT made it the favourite topic of the public, but the March data breach announced by them let to their major setback. Representatives from OpenAI, the parent firm of ChatGPT, stated: "Before we pulled ChatGPT offline on Monday, some users were able to view the first and last name, email address, billing address, last four digits (only) of a credit card number, and expiration date of another current user. No time were full credit card numbers disclosed.".

In order to mitigate the issue, the organization ensured that affected users were promptly notified and implemented enhanced security measures. The level of trust in ChatGPT and AI may experience a further fall, as is evidenced by the skepticism expressed by Americans against ChatGPT.[4]

2. MailChimp: January 2023

In January, the customers of the email marketing platform, MailChimp, were notified of the data breach. A social engineering attack let to such breach that facilitated the unauthorized access of individuals into an internal customer support tool.

Information and credentials of the employees were accessed by the hackers. The company had to suspend such identified accounts to protect them from further misuse. MailChimp has issued a statement in response to the occurrence of a data breach, "According to Bleeping Computer, "Our investigation into the incident is ongoing and involves finding ways to better defend our platform.[5]

[3] Jovi Umawing 'KFC, Pizza Hut Owner Employee Data Stolen in Ransomware Attack' (*Malwarebytes*) <https://www.malwarebytes.com/blog/news/2016/04/kfc-pizza-hut-owner-employee-data-stolen-in-ransomware-attack> accessed 20 September 2016."

[4] "'Slashdot' (*OpenAI Admits ChatGPT Leaked Some Payment Data, Blames Open-Source Bug*) <https://news.slashdot.org/story/23/03/25/0353238/openai-admits-chatgpt-leaked-some-payment-data-blames-open-source-bug> accessed 26 September 2016."

[5] "Abrams L, 'Mailchimp Discloses New Breach after Employees Got Hacked' (*BleepingComputer*, 19 January 2023) <https://www.bleepingcomputer.com/news/security/mailchimp-discloses-new-breach-after-employees-got-hacked/> accessed 21 September 2016."

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 4, 2019

The occurrence of data breach incidents in April and August of 2022, as well as in January of 2023, underscores the imperative for organizations to establish a strategic response framework following such breaches, with the aim of mitigating the likelihood of future attacks.

Statutory provisions on data privacy

The right to privacy is enshrined in the Article 21 of Indian Constitution and the related constitutional provisions. It has been stated by the Article 21 of Indian Constitution that no individual can be deprived of his or her personal liberty. In many cases, it has been specified by the Supreme Court that right to life and personal liberty comprises of the right to privacy. Nevertheless, it is important to note that private individuals or organizations are not subject to constitutional rights claims. They can be claimed only against the state or state-owned enterprises.[6] The Information Technology Act of 2000 has sections 43(a)–(h) that talk about cyber offenses and sections 65–74 that talk about cyber offenses. Cyber contraventions include getting access to computer networks against the law and forcing people to give up their data. This can lead to legal punishments in India.

Any interference with source code of computer, intention of damaging the system through hacking, and privacy violation are a few cyber offences, which may lead to criminal prosecution under IT Act. In an event, third party information is misused, the network service provider is made accountable for such breach as well as for not erecting rigorous measures to safeguard information, under the provisions of IT Act. According to the IT Act, an entity that takes action on behalf of another entity and receives, collects, transmits or provides service regarding an electronic message is termed as an intermediary.[7] Therefore, any service provider that acts like an outsourcing company can be held accountable for data breach. The Information Technology Act also encompasses offenses and contraventions of a foreign origin. If the computer network in question is situated within the borders of India, it will be subject to the regulations outlined in the Information Technology Act.

[6] "Asthana S, 'Article 21: Meaning & Scope of Protection of Life and Personal Liberty' (*iPleaders*, 11 January 2014) <https://blog.ipleaders.in/article-21/> accessed 21 September 2014."

[7] "Joseph V, 'Cyber Crimes under the IPC and It Act - an Uneasy Co-Existence - It and Internet - India' (*Cyber Crimes Under The IPC And IT Act - An Uneasy Co-Existence - IT and Internet - India*, 10 February 2014) <https://www.mondaq.com/india/it-and-internet/891738/cyber-crimes-under-the-ipc-and-it-act---an-uneasy-co-existence> accessed 23 September 2015."

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 4, 2019

There is no such legislation that protects all forms of sharing or receiving of personal information, including speech, written, or in electronic form. Despite the presence of protections, they are dispersed over a multitude of laws, rules, and policies. The most significant clauses are covered in IT (Amendment Act of 2008) and IT (Sensitive Personal Data or Information) Rules of 2011. Because of their name, Only the electronic information is covered under SPDI Rules, leaving no scope for no-digital information.

The digitally shared personal information received no protection from the IT Act, 2000 due to lack of data protecting rules and regulations. Such absence of laws, resulted in the establishment of the Information Technology Bill, 2006. On Oct 27, 2009 it was followed by the IT (Amendment) Act, 2008. This Act brought Sec43A under the IT Act, according to which, if an organisation collects and stores sensitive personal information and fails to set up rigorous safeguard measures, which makes the data vulnerable and results in and loss or gain wrongful in nature, then such organisation is held accountable under these provisions and shall compensate by paying for the damages incurred by individual(s) due to attack.[8]

Through the initiation of another Section, Sec 72A, a punishment is decided for a breach of lawful contract. It states that any disclosure of information in such contract, may be lead to imprisonment for a term not exceeding three years, or with a fine not exceeding up to five lakh rupees, or with both.

It also states that if an individual, in possession of sensitive data, misuses or manipulates any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned, shall be liable to punishment along with imprisonment for a term which may extend to two years, or with fine which may extend to Rs 1,00,000, (approx. US$ 3,000) or with both.[9]

The Sec 75 states that irrespective of the location of the cyber-crime committed, an individual shall be liable to the same legal actions against him or her. The powers of IT Act and Rules are limited as they do not cover the data breach committed non-digitally. The consumers have only a few choices to put any curbs on the organisations' data collection activities. Moreover, only business organizations, by whom automated data processing are

[8] "(*Ministry of Law, justice and company - eprocure.gov.in*) <https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMjk4NzY=> accessed 19 September 2018."

[9] "(*Privacy and the information technology act - centre for internet and ...*) <https://cis-india.org/internet-governance/blog/privacy/safeguards-for-electronic-privacy> accessed 23 September 2016."

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 4, 2019

carried out, come under such provisions. The primary concern of the Indian Government was data localization, prevalent in Chinese apps, is still not covered. This highlights the necessity of data privacy legislation to put curbs on such organisations and overcome any future manipulations and breach.

The Judiciary on protection of data

Following are the instances of judiciary's take on data protection in several cases:

In the case of "*State of Tamil Nadu v. Suhas Katti"*[10], a complaint was filed by the victim under Sections 67 of the IT Act and 469 and 509 of the Indian Penal Code, 1860. A woman was attacked and humiliated online by pornographic remarks about her in several group chats. Moreover, her number was made public and a fake account was set up in her name by the accused, to harm her reputation. He was found guilty by the charges brought against him. This particular case garnered lot of public support and encouraged the silent victims of online abuse to come forward and share their plight with the world.

In this case of "*Amar Singh v. Union of India"*[11] it was alleged by the petitioner that his calls were recorded without his consent by his telecom service provider, which clearly means that his right to privacy under Article 21 was violated and he was monitored secretly. According to the accused, he was just following the commands of the authorities of NCT. The particular case, brings Sections 69, 69A, and 69B of the IT Act, 2000, to attention. It was noted by the court that it is the duty of the telecom service provider to behave in a sensible manner. In order to follow government's commands of tapping into an individual's calls, the telecom service provider must first give solid evidence of such directive given to him by the government. Since, recording calls, without one's consent is unlawful and unethical, the court suggested the establishment of specific directives and rules by the central government.

"Shreya Singhal v. Union of India"[12] is one such landmark case. Disrespectful and inappropriate remarks were made by two ladies on Facebook over the righteousness of declaring a Mumbai bandh due to a political leader's demise, which led to their arrest by the police.

[10] CC. No. 4680 of 2004
[11] 2011 (5) SCALE 606
[12] AIR 2015 SC 1523

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 4, 2019

The Section 66A of the Information Technology Act of 2000 (ITA) states that, any person who intends to create nuisance, annoyance, invoke hatred, insult, danger, or cause injury by sending an information digitally, can be put under arrest by the police.

The Court, announced that Section 66A is completely against the constitution. Their restrictions went beyond reasoning, thus making their protection against any nuisance, annoyance, insult, inconvenience, danger, and criminal intimidation invalid under Article 19(2) of the Indian Constitution.

In the case of "*Justice K.S. Puttaswamy (Retd) v. Union of India*"[13], a nine-judge bench established that the right to privacy should be protected by the Indian Constitution.

As per the particular case, retired Judge K.S. Puttaswamy contested against the government's plan for establishing a digital India through the advent of a standard biometric identity, which would be required as a procedure for getting into government services as well as to avail the government benefits. However, a claim was made by the government, that the right to privacy is not specifically guaranteed by the Constitution. The court stated, that Article 21 protects the basic right of privacy. It also concluded that "No person shall be deprived of his life or personal liberty except according to procedure established by law."

In *Praveen Arimbrathodiyil v. Union of India*[14] a set of regulations were published by the Union Government in 2021. The Information Technology (Intermediaries Guidelines) Rules, 2011 are replaced under the provision of Section 87 of the IT Act of 2000. The aim is to bring the online streaming services, digital news outlets, and social media intermediaries under government's control. The government has laid down internal grievance redressal process that bounds the social media intermediaries to abide by it. These intermediaries must also disclose the accused's details to the government for sending serious offensive messages online to the victim. In case of violation by the social media intermediaries, they are deprived of the protection granted to them by Section 79 of the IT Act.

Digital news media are directed to set up internal grievance redressal system and maintain the ethics and code of conduct mandated by the regulations. However, these regulations have been contested by a number of organisations, which include, Quint, LiveLaw, WhatsApp and the foundation for independent journalists. The future trajectory of Indian information

[13] (2017) 10 SCC 1.
[14] WP (C) No. 9647 of 2019

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 4, 2019

technology legislation will be influenced by the consequences of the judgment, which is presently awaiting listing before the Supreme Court.

Importance of the right to data privacy

Following are the importance of the right to data privacy:

1. Restricts the government from putting its people on surveillance

Th protection of a nation's citizens is in the hands of the government, but there are times when the protection actually becomes sheer surveillance. In 2013, Edward Snowden brought NSA's surveillance plan to notice, which highlighted the privacy issues under the government's control. There is a very thin line between national security and surveillance, which often violates the freedom of speech and expression. This highlights the need for government's explanation behind putting an individual to such surveillance.[15]

2. Mitigating the possibility of personal data being misused for another individual's benefits.

Miscreants are everywhere, specially over the online platforms, which make personal information even more sensitive. For instance, it was noted, that Cambridge Analytica was found guilty of violating the Facebook users'' privacy by collecting their personal information secretly. Such information was utilized as advertisement for political propagandas. Hence, the onus falls on the social media owners and technology organisations to protect the personal information of their consumers.[16]

3. Right to privacy ensures the punishment of the accused.

Constitution has mandated the right to privacy as fundamental to every citizen, and any breach of such privacy may lead to repercussions. By implementing the right to privacy, the government is put under restriction from directing the authorities to collect personal information of individuals without their consent.

4. The need for social limits

In the digital age, the meaning of social boundaries has changed. It no longer means not disturbing the other individual and remain in our limits, but now it stands for keeping one's personal information in control and under protection from being utilized for misuse. A goo d social boundary is a healthy boundary that nurture the relationships as well as career.

[15] "'Edward Snowden: The Whistleblower behind the NSA Surveillance Revelations' (*The Guardian*, 11 June 2013) <https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance> accessed 27 September 2005."

[16] "Confessore N, 'Cambridge Analytica and Facebook: The Scandal and the Fallout so Far' (*The New York Times*, 4 April 2018) <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html> accessed 23 September 2004"

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 4, 2019

Therefore, keeping a healthy boundary on social media ensures the peace of mind and safety.[17]

5. The right to privacy builds faith

The advent of the right to privacy has given relief to the individuals that they are under protection and any nuisance with their personal information by a miscreant, will have repercussions.

6. The data under user's control

The right to privacy assures an individual that their data is only accessible to them and no one can have control over it without their consent. Such right to control our own information online, gives a sense of satisfaction that their data is safe.[18]

7. The right to freedom, speech and thought

What is the point of the right to freedom being granted, if there's no provision of protection in exercising it? The privacy rights come to rescue, which enables an individual to speak their mind and express their opinions in the world, without the fear of being caught and prosecuted by the all-powerful government.

8. The freedom of political engagement

The health of a society is determined by the politics and the elected leader voted by the citizens. To exercise one's freedom of choice, the voting system keeps the identity of individuals hidden, which protects them from any attacks from political tactics. The right to privacy is imperative in our day to day lives and offers us the right to expression.[19]

9. The protection of one's esteem

There are times when we post something online, but realise it later that it needs to be removed. The right to privacy comes to our rescue. It has been addressed as the "right to be forgotten" by the European Union. One such example is, the revenge porn, which ruins an individual's image in the society.

10. The right to protect our finances

[17] "Barrett-Maitland N and Lynch J, 'Social Media, Ethics and the Privacy Paradox' (*IntechOpen*, 5 February 2002) <https://www.intechopen.com/chapters/70973> accessed 27 September 2002"

[18] "'Chapter 5: Technology and Privacy Policy' (*National Telecommunications and Information Administration*) <https://www.ntia.gov/page/chapter-5-technology-and-privacy-policy> accessed 20 September 2002"

[19] "Anderson J, '3. Concerns about Democracy in the Digital Age' (*Pew Research Center: Internet,Science & Tech*, 21 February 2002) <https://www.pewresearch.org/internet/2000/02/21/concerns-about-democracy-in-the-digital-age/> accessed 27 September 2002."

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 4, 2019

It is the responsibility of the corporations to ensure the protection of an individual's personal financial details. It is also important for an individual to understand, that they must be cautious while sharing their debit or credit card information. Severe cautions must be taken to safeguard such information and refrain from sharing it carelessly online, without comprehending the consequences.

Analyzing India's Data Protection Act

On 3 August, 2023, the Digital Personal Data Protection Bill was released by the Ministry of Electronics & Information Technology introduced in the Lok Sabha. A framework was designed and proposed by the Bill, which recognises that personal data should be protected and processed in case required by the law. In November, 2022, the Ministry of Electronics & Information Technology (MEITY) introduced the Draft Digital Personal Data Protection.

The Data Protection Board's constitution was given a proposal by the Bill to set up a digital office that runs independently and works as an adjudicatory authority.[20]

Data Fiduciaries and data processors come under the applicability of the Bill, which determines what data was processed by the entities and what must have been their means of access and purposes. The Bill is applicable to the data processed in India as well as outside India, which may involve the goods and services activities relating to the Data Principles.

Key changes in the 2022 Draft

Exclusion of profiling: This omission is significant, especially considering that the concept of "profiling" is neither mentioned nor referenced within the stipulations of the legislation. It is important to acknowledge that although the 2022 Draft and previous drafts suggested the inclusion of provisions regarding the application of the Bill to the processing of personal data outside of India in relation to the profiling of Data Principals within India, this particular aspect is not explicitly addressed in the Bill. However, the current scope of the Bill is limited to processing activities conducted outside of India that are associated with the provision of goods or services to individuals within India. This provision was also included in the 2022 Draft of the Bill. One could argue that profiling could be considered as a kind of processing within the scope of the Bill. However, it is important to note that if such profiling is conducted outside of India, there would be no additional protections or constraints

[20] "Nandi EBT, 'Lok Sabha Clears Digital Personal Data Protection Bill amid Disruptions by Oppn' (*mint*, 7 August 200) <https://www.livemint.com/politics/policy/lok-sabha-clears-digital-personal-data-protection-bill-amid-disruptions-by-opposition-over-manipur-issue-11691401081428.html> accessed 22 September 2000"

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 4, 2019

imposed on it. Nevertheless, the Bill imposes limitations on the monitoring of children's behavior, particularly where it pertains to profiling, unless there are specific exemptions.[21]

Enhanced notice requirements: The Bill demonstrates a modest enhancement over the 2022 Draft's proposition, which mandates the disclosure of personal data collection details and processing objectives. This improvement is achieved by stipulating that the notice must also include information regarding the Board's complaint procedure, as well as the rights of Data Principals to withdraw consent and seek remedies for grievances.

Substitution of deemed consent with legitimate uses: The implemented the concept of 'deemed permission', wherein Data Principals willingly disclosed personal data in circumstances where such sharing was anticipated. The Bill currently includes the concept of 'legitimate uses' as one of the criteria for processing personal data. The act of willingly disclosing personal information is encompassed within the circumstances in which it can be utilized for the purpose of processing personal data. Nevertheless, the Bill explicitly stipulates that in order for voluntary sharing to be considered reliable, it must be done for a designated purpose and may still require adherence to notification requirements.

Grandfathering provisions: The Bill exhibits a moderate improvement compared to the proposal in the 2022 Draft, which requires the revelation of specific information regarding the gathering of personal data and the objectives of its processing. This enhancement is attained by mandating that the notification must additionally encompass details concerning the complaint system established by the Board, in addition to the entitlements of Data Principals to revoke consent and pursue redress for grievances.

Processing of Children's Personal Data:

The amended version of the bill upholds obligations pertaining to the handling of personal data of minors, including obtaining parental consent and safeguarding children against tracking, behavioral monitoring, and targeted advertising. Furthermore, the proposed Bill broadens the scope of a limitation outlined in the 2022 Draft, which pertains to engaging in processing activities that are likely to cause harm, to encompass a wider range of restrictions on processing activities that have a negative impact on the well-being of a child. This represents a deviation from a previous framework of injury that was confined to a narrower

[21] "'Analysing the Digital Personal Data Protection Bill, 2023' (*Lakshmikumaran & Sridharan: Top Law Firm in India*) <https://lakshmisri.com/insights/articles/analysing-the-digital-personal-data-protection-bill-2000/> accessed 24 September 2000"

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 4, 2019

scope, encompassing physical harm, harm to one's identity, harassment, or the obstruction of legal benefits or substantial losses. The reason for this is that the Bill broadens the scope of the limitation outlined in the 2022 Draft.

The proposed legislation also establishes a framework for exemptions from the aforementioned standards in the following manner:

It is suggested that the Government preserve the power to offer exemptions to particular types of fiduciaries or to specify particular objectives for which exemptions may be granted, subject to defined requirements, in a manner reminiscent of the 2022 Draft.

Furthermore, the Government may offer exemptions (and prolong an age advantage) to Fiduciaries who are involved in processing activities that it has determined to be "verifiably safe" based on an assessment of pertinent criteria. The evaluation procedure's goals and standards are not made clear. It has been mentioned that this examination may potentially involve the Ministry of Women & Child Development.

Data Subject Rights: Similar to the 2022 Draft, the proposed Bill grants Data Principals a range of entitlements that include the ability to access information, rectify inaccuracies, erase and update data, seek redress for grievances, and nominate individuals. The Bill incorporates various substantial modifications pertaining to the rights of data subjects.

The extent of the entitlement to access information is restricted to personal data that is being handled by the Fiduciary and does not comprise personal data that has been processed and furnished in accordance with the 2022 Draft.

The right of access to information only applies to the personal data that the trustee is responsible for managing. It does not include personal data that has been processed and given according to the 2022 Draft.

The right to access has been changed so that information about data processors with whom personal data has been shared can also be given out.

To limit the number of times the right of access can be used, exceptions have been made that allow personal information to be sent from one data guardian to another.

Cross-border transfers: In accordance with the study, the proposed legislation employs a "black-list" strategy, granting the Government the authority to limit the transmission of personal data to nations or territories that have been officially notified by the Government on an ongoing basis. It should be noted that this clause does not impose limitations on regulations that may establish a more stringent level of protection or impose further

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 4, 2019

restrictions on the transmission of personal data concerning any individual or fiduciary. This pertains to law that is specific to particular sectors, such as payment system data and insurance records, which would still be subject to applicable limits.

Moreover, there have been extensions made to exclusions that exempt some rules, such as cross-border transfers, from being applicable. These extensions specifically apply to the processing of data that is essential for business restructuring operations, provided that they have been allowed by a court, tribunal, or other authority. It is important to note that these exemptions do not apply to data processing for debt recovery purposes.

Exemptions for Startups: Apart from exemptions related to the State and its instrumentalities, as well as exemptions for research and statistical purposes, the Bill also proposes some clauses to be exempted for startups. In addition, the Government possesses the authority to grant exemptions to specific categories of Fiduciaries from particular rules for a limited duration, not exceeding five years.

Data Protection Board: The Board would become a legal entity with everlasting succession under the proposed statute. The headquarters of the Board's "digital office" are anticipated to be selected by the government. There is at least one legal specialist on the Board, according to additional information. The qualifications, terms of appointment, processes for the chairperson and members' removal and resignation, as well as the powers, responsibilities, and practices of the Board, have also been covered.

Changes in Adjudication of Disputes: Some major changes to the Adjudication of disputes process were proposed under this. Following are some changes:

The board may now imply monetary penalties specified in the schedule according to this bill. However, the earlier law of a penalty amount being a maximum of 500 crores have been dropped under this bill. Within 60 days after receiving the Board's judgment, appeals from the Board may be made to the Telecom Disputes Settlement and Appellate Tribunal ('TDSAT').

Under this measure, the government has been given some authority. However, as is shown below, some aspects of this measure also frequently interact with the Information Technology Act of 2000 (IT Act), the Intermediaries Guidelines, and the Blocking Rules.:

Information solicitation: The bill tells us right away that any Board, Fiduciary or Intermediary are liable to any questions asked by the central government to them. They are

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 4, 2019

always answerable to them. This section, purportedly taken from the Personal Data Protection Bill, 2019, is still uncertain.

Blocking of Information: The government may also tie the bill to the information blocking regulations after the information is blocked. Since the Board lacks the jurisdiction to prohibit access to information or its resources, it may request the involvement of the central government in any Given that Data Fiduciary is being taken into consideration and has already been penalized financially more than twice, they must recommend to the government that access to the computer resources be blocked so that they can continue to provide goods and services to our citizens. Everything done here is done with the "general public's interest" in mind.

According to the aforementioned proverb, the government may decide to order agencies or intermediaries to ban any such information after providing all parties with an opportunity to be heard on the topic.

The method by which the Board may recommend or the Government may accept such reference to blocking is not described in great detail.

This remedy aims to resolve all risks that come with conducting business as normal and pose a substantial threat to the personal data kept by the Data Fiduciary who committed the infringement. In any case, any reference to the government is subject to the Blocking Rules and the right to a hearing.

The Bill proposes a novel method for regulating the “processing of personal data by fiduciaries and, by extension, processors. It includes identified grounds for processing personal data, specific consent requirements, recognition of additional obligations for processing children's data, classification of significant data fiduciaries, provision of the data for subject rights, and specific transfer provisions.”[22]

While a flexible structure could be perfect for the Act to remain responsive to changes in technology and processing, while other components of the Bill, such as the right to request information and the right to exercise blocking powers, may require a complete check again. It is still unknown that if this bill would be able to make its way in to the legislation or not.

[22] “(*Confidentiality and privacy of personal data - health data in the ...*) <https://www.ncbi.nlm.nih.gov/books/NBK236546/> accessed 27 September 2000”

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 4, 2019

Conclusion

In this world of rapid increase of data protection and privacy laws, one thing we have noticed is the important role these regulations have in safeguarding the private information of the individuals in this digital age. Technological advancements have completely modified the way we live, work and interact by launching the civilization into an age of unique connection and convenience. However, this digital transition has brought a different set of difficulties, specifically in regard to the security and privacy of personal data. Governments and all the regulatory organizations have been forced to act quickly in response to the changing data handling picture, realizing the urgency to strike an equilibrium between innovation and privacy protection.

A very recent Act, that was India's data protection Act. It had provisions for everything like Data protection, strict penalties for violations, consent processes, etc. All of it reflects a nuanced knowledge of the necessity to balance the protection of individual freedoms with technological growth. Importantly, this balancing act includes much more than just the legal frameworks, it is a societal undertaking that calls for cooperation between governmental regulatory bodies, tech corporations and people. It is everyone's responsibility to uphold the values of responsible data handling and develop a respect for personal privacy as technology develops. By doing this, we can promote a climate that would encourage innovation without compromising any of the people's rights and security. It will be a complete win-win situation.

The data protection and privacy laws state the continuous evolving nature of our technology and tells the need to adapt accordingly. As we advance, it is very necessary for us to welcome innovation while acting as watchful stewards of individual privacy—a long lasting commitment that will influence how our increasingly interconnected world develops in the future. Our successful route to a more secure and innovative future will be defined by how well we manage the equilibrium between innovation and privacy protection, which is both a legal and societal necessity.