Research Article

Volume-8 | Issue-2| Apr-Jun-2022|

VEETHIKA-An International Interdisciplinary Research Journal

E-ISSN: **2454-342x**

Double Blind Peer Reviewed Journal

URL: https://veethika.qtanalytics.in

A Comparative Study of Data Protection Laws: Current Global Trends, Challenges and Need of Reforms in India

Shailendra Prasad Godiyal[1*], Kuldeep Singh[2]

[1]St. Thomas' College of Law, Greater Noida, Uttar Pradesh, INDIA

[2]D. A. V. P. G. College, Muzaffarnagar, Uttar Pradesh, INDIA

Corresponding Author*: godiyal4law@gmail.com

ABSTRACT: "The best way to get a bad law repealed is to enforce it strictly." Abraham Lincoln's legacy is still relevant in this decade. The 21st century is sometimes referred to as "the information age" because of the tremendous growth in the variety of ways we use information. India is rapidly transforming into digital economy. India has also been affected by the digital revolution. Recognizing its importance and the potential for significant disruption in practically every area of society, Indian government devised and implemented the "Digital India" plan. India is on track to develop into a digital economy with a substantial market for foreign businesses. In January 2022, there were 658.0 million internet users in India. Between 2021 and 2022, there were 47 million more internet users in India (+8.2 percent). Internet penetration in India stood at 47.0% in January 2022.

Data security and protection are crucial given the world's increasing digitization. Processing of personal data is increasingly widespread, despite the fact that the shift to a digital economy is still in progress. Today's digital environment makes it so that almost every action a person takes involves some sort of data transaction. New markets have emerged as a result of the Internet, particularly those whose business plans directly or indirectly involve the collection, organisation, and processing of personal data.

It is pertinent and strange to mention the fact here that, "the world's largest taxi company UBER owns no vehicles; Facebook, the world's most popular social media platform, creates no content; Alibaba, the most valuable retailer, has no inventory; similarly, Airbnb, the world's largest accommodation provider, owns no real estate". All of these are the "Data Driven" and not the "information driven" companies. It indicates that the company collects, analyses, and applies data to make important decisions. It is a serious matter of concern around the world when it comes with right to privacy of an individual. This study deals with current data protection laws, challenges and reforms in India.

KEYWORDS: Data Protection Law, GDPR, IT Act 2000, Cyber Law

1. INTRODUCTION

We are living in the virtual world. Technology has become so smart and sophisticated that it can do anything which is not possible to do by human beings. This is due to the advancement in the technology. Just like "soul" which is the incorporeal embodiment of a living being. Similarly "Data" is also the incorporeal embodiment of a living being which includes whole information virtually. Traditionally, the immediate basic needs were food, cloth and shelter, but now a day's "Data" becomes the fourth and the ultimate basic need.

Personal data is an "information that relates to an identified or identifiable individual". A name or a number can be used to identify someone, or other identifiers like an "IP address", a "cookie identifier", or other details may also be used. It may constitute personal data if it may be used to directly identify a person from the information you are processing.

DOI: https://doi.org/10.48001/veethika.2022.08.02.004

Consider if the individual is still identifiable if you are unable to immediately identify the person from the information. The information you are processing and all the strategies that you or anybody else may use to identify that person should be taken into consideration. Even if you can identify or locate a person by the data you are processing, either directly or indirectly, it is not personal information until it "relates to" that person.

We know that "Data" are of two types. First which we voluntarily shared and the second is that data which is generated from our day to day activities we performed in digital/cyber space. This data is paramount. Individual, corporation or State needs this data for various purposes; it may be for security or for commercial purposes. "Data" is becoming the "New Currency" in the Fourth Industrial Revolution age of universal and free access of internet.

Advancement in technology brought several challenges before us. While we profit from it, data protection is essential. These days, data is highly vulnerable. The data has been misused by the cyber criminals. The facet of crime has been changed. Hence many serious questions regarding the data protection and right to privacy has been continuously floating around the world, summarily which are as following:

- Is our data which we stored or shared to the virtual world is safe or not?
- When we share our data to the cyber space, then who own that data?
- Who can access these data stored and what are the restrictions of accessing such data?
- Who can collect this data?
- How and when consent can be taken for data processing?
- For what duration can the data be stored?
- What are the obligations and liabilities of the government or the private bodies in relation with data collection from the people?
- What is the parameter to check and balance the misuse of the data?
- Does national security override all concerns of privacy?
- Lastly what will be the remedy if there was breach of data?

As we all know that the law is the duty bound soldier of the society. Whenever the sense of insecurity arises, the law protects and provides safe guards to the people. Legal luminaries around the world are struggling hard to patch up the conventional legal principles and the modern cyber challenges. These challenges further added on when there was a massive violation of these personal data around the world and there was no such law which is so compatible to tackle these challenges. Due to the digitization and globalization there has been a consistent threat to personal information been misused as there has been an alarming rise in data theft and breach of privacy of an individual around the world. India is also developing its own space in digital world by adopting "*Aadhar*" based biometric system of information of the citizen. The dependency on internet world worries over digital security, information assurance and data protection are logical and justified.

Although data can be used for good, the arbitrary and uncontrolled use of data, particularly personal data, has raised questions about an individual's privacy and autonomy. Recently, the honorable Apex Court in the landmark judgment in the case *Justice K.S.Puttaswamy (Retd) vs Union of India and Ors*[i] held that that "privacy is a key right" ensured by Part III of the Constitution of India. Henceforth India needs an appropriate law to address the worries over digital security, information insurance and protection.

In his book "A Practical Guide to the General Data Protection Regulation (GDPR) - 2nd Edition" (2020), Keith Markham, explains that despite numerous recent developments involving compensation claims, enforcement actions, and Brexit concerns, the "GDPR" is still very much in the public eye. In the book "Data Protection: Law and Practice" (2020) by Rosemary Jay, also clearly set out and all exceptions are defined well, along with the key differences between the 1998 Act and the new "GDPR".

In the article "European Union: Comparative Analysis: General Data Protection Regulation, 2016 and the Personal Data Protection Bill, 2019" by Sreenidhi Srinivasan, categorically explains in a very lucid manner the comparison between EU's "GDPR" and Indian "PDP" Bill 2019.The author of the article "Privacy and Data Protection – India Wrap 2020" by Purushotham Kittane, Inika Serah Charles, had tried to explains the need of the data protection law in India.

"Tom Gaiety" said: "*right to privacy is bound to include body's inviolability and integrity and intimacy of personal identity including marital privacy*".[ii] According to Edward, "*privacy as zero relationship between two or more persons in the sense that there is no interaction or communication between them, if they so choose*".[iii] According to Warren, "*once a civilization has made distinction between the outer and inner man, between the life of the soul and the life the body…..the idea of a private sphere is in which man may become and remain himself*".[iv]

Governments all across the world are now more concerned with protecting citizens' rights than with regulating the internet. Though most developing countries, like India, are still in the early stages of drafting legislation, many established countries, such as the United Kingdom and the United States, have already set the bar in this area. John P Barlow asserted, "*Governments of the Industrial World you weary giants of flesh and steel, I come from Cyberspace…You have no*

DOI: https://doi.org/10.48001/veethika.2022.08.02.004

sovereignty where we gather…We have no elected government, nor are we likely to get one".[v] This viewpoint presupposes a rent anarchism in the Internet's architecture, which is inherently beyond of institutional control. Prof. Lawrence has argued against this conclusion, claiming that "code is law". The code, or rather the hardware and software that shape today's internet, imposes a set of constraints on how individuals should act. "We are all regulated by software now," it has been said clearly. It is now feasible to conceive software governing the most fundamental parts of democracy, society, and even life itself.

The researchers has debated "whether lextechnologica, has a *sui generis* character that requires a new set of legal rules". The "First School of thought, promoted by jurists like *David Johnson* and *David Post*, states that, *cyberspace has its own inherent jurisdiction and is capable of self-regulation".*

Whereas the "Second School of thought, professed by jurists like P*rofessor Jack Goldsmith,* propounds that, *cyberspace doesn't have a sui generis character and current technological and legal tools, are sufficient to resolve claims, as those that arise in physical environment. The later school of thought of inherent regulation appears to be more apt in this century"*.[vi]

The "personal data protection Bill" (PDP), which was put forth in 2019 to completely restructure The "GDPR" served as a model for the existing data protection rules in India, which are presently governed by the "IT Act, 2000" and its implementing laws. The present version of the "PDP" Bill establishes data localization requirements for some types of sensitive data as well as compliance standards for all types of personal data. It also expands the range of individual rights and establishes a central data protection regulator. If specific nexus requirements are met, the "PDP" Bill extends extra territorial protection to non-Indian organisations and imposes severe financial penalties for non-compliance.

The "PDP" Bill was referred to a Joint Parliamentary Committee ("JPC") on December 12, 2019 for recommendations.

The GOI had constituted a "Committee of experts to study various issues relating to data protection in India and suggest a draft Data Protection Bill". The objective is to "*ensure growth of the digital economy while keeping personal data of citizens secure and protected*"[vii] headed by former Justice of honorable Supreme Court of India *Justice B N Srikrishna*, to think about the difficulties encompassing privacy assurance in India and give their important proposals and recommendations and standards on which to base the information security authoritative structure. The committee took less than 6 months as compared to the European Union's "GDPR" to create a complex legal framework for data protection. This creates many weaknesses and shortcomings in the "Report".

The "JPC" has held a number of meetings with government agencies, business associations, and other stakeholders. It has also held meetings to discuss the "PDP" Bill clause by clause. Importantly, according to recent reports, the "JPC" is reportedly considering broadening the Bill's application to include non-personal data as well as personal data in addition to only personal data. According to additional reports, the "JPC" is still divided and undecided over these crucial issues, including "Data Localization" and government access to data held in particular by social media platforms. The Bill was withdrawn from the Lok Sabha on August 5, 2022. The government promised to introduce a "set of new legislation" that would fit into a "complete legal framework."

2. "EUROPEAN UNION'S GENERAL DATA PROTECTION REGULATION" (GDPR)

Other than India, several countries treat data protection as a distinct discipline. They have well-crafted and well-established data protection legislation.The European Community saw the need to harmonize data protection policies among member states in order to facilitate internal and cross-border data transfers inside the European Union. The issue was that there were considerable disparities in degrees of protection, which failed to provide legal confidence for both data subjects and data controllers and processors. As a result, the European Union issued Directive 95/46/EC of the "European Parliament" and of the Council on October 24, 1995[viii] on the protection and free movement of "Personal Data" in order to harmonize individual data protection and transfer rights across "EU" member States. Another point to consider is that in order for "European Directives" to be enforceable, they must be incorporated into domestic legislation. As a result, each member State's implementation will be more difficult. Within the "EU", the data protection directive did not have the expected effect. The member State's attempted to enact the order resulted in a legal battle. Practices that were permitted in one member State but illegal in another, producing confusion among controllers. "GDPR" replaced the "Data Protection Directive" (DPD) in the "EU" in 2016. The "GDPR" that was finally implemented is the result of four years of talks and countless revisions. The fragmented data practices across the "EU", which produced legal uncertainty among the member states, were blamed for distorted competitiveness and stagnating economic activity in the "EU". This issue of distinct legal regimes was addressed by regulation since it applied directly to the addressees and did not require any additional steps for implementation or enforcement. With ongoing checks in place across the "EU", the potential barrier to unrestricted data transfer has been greatly reduced.The goal of "GDPR" implementation is to restore trust in the "EU Internal Market". In order to do so, businesses must now comply with the "GDPR New Data Protection" duties as well as come transparent about pre-existing "GDPR" mandates. The framers took into account the

DOI: https://doi.org/10.48001/veethika.2022.08.02.004

challenges of a global economy, as well as emerging technology and business models, and so crafted a law that would take into account a variety of similar variables in order to bring as many businesses as possible within the "GDPR" umbrella.

When it comes to the legal side of the legislation, "GDPR" replaces 28 diverse judicial and legal frameworks with a single, classic legal framework. This would create a fair playing field for all businesses (current and potential), resulting in a favourable influence on the economy and business in general. "GDPR" emphasises the notion of accountability to reduce the superfluous and somewhat lengthy process of previous notifications. It doesn't stop there; "GDPR" included a number of rules aimed at ensuring transparency and customer-friendly regulations, giving the term "consent of consumer" new meaning. The "GDPR" has introduced weapons such as the "Right to Data Portability", "Data protection by design and default", and standard privacy icons in order to sow the seeds of fair competition in the direction of stronger data protection services and goods. To prevent violation of notification and assess the impact of data protection, the deterrent approach has been adopted. "Data Protection Officers" (DPO) have been appointed to protect the fundamental right to data protection in a similar manner. The "GDPR" bestows 8 major rights on its subjects which are as; "Right to be informed" (Article 14), "Right of Access" (Article 15), "Right to Rectification" (Article 16), "Right to Erasure" (Article 17), "Right to Restrict Processing" (Article 18), "Right to Data Portability (Article 20), "Right to Object" (Article 21), and "Rights in relation to automated decision making and profiling" (Article 22).

Now, consent is treated with the deference it deserves. The "GDPR" assures that companies don't exploit customers by using jargon-filled, difficult-to-understand terms and conditions. Enterprises are now required to write the form in straightforward English and to state that consent can be revoked as easily as it was granted. Furthermore, if a data breach is likely to "result in a risk for the rights and liberties of individuals", member states are required by the "GDPR" to issue a breach notification within 72 hours of the incident. In addition to the notification, the controllers must also notify the customer "without excessive delay." Another significant achievement of "GDPR" is that it provides consumers with the right to inquire of the controller about whether and for what purpose personal data is being processed. To boost openness even more, the controller is required to provide a free electronic copy of the data to the consumer.

The "Right to be Forgotten" was also strengthened by "GDPR". Also known as "Data Erasure" the consumer has the right to ask the processor to stop further data processing and erase his or her personal data at any time. The conditions for exercising the right are outlined in Article 17, such as when consent is revoked or when the data is no longer necessary for the processing for which it was originally intended. When deciding how to respond to these requests, the controller must weigh the consumer's right against "the public interest in the Data availability". In terms of data portability, the subject has the right to have their personal data transferred from one controller to another in a "commonly used and machine readable format." Furthermore, while privacy by design has been present for a long, it was only following the implementation of "GDPR" that it became a legal necessity. Essentially, it means that data security should be a priority from the start of the system's architecture rather than being added later. Article 23 lays the groundwork for this by saying expressly that the controllers must handle data that is *sine-qua-non* for the system to function (Data minimization).There is a significant change in data processing activities under the "GDPR".

Even the "Court of Justice of the European Union" (CJEU) made it very apparent that following "GDPR", there will be no way to avoid the EU's high degree of personal data protection. The rule would be based on the concepts established in historic judgments such as *Google Spain*[ix] case ("Right to be Forgotten") and "*Facebook v. Ireland* Case" *i.e* ("Safe Harbour"). In response to the difficulties posed by the digital ecosphere, the judiciary made clear decisions in favour of market principles and imposed stringent regulations on cross-border data transfers. The "GDPR" has upped the standard for data protection by clearly identifying the "EU" as the largest digital market in the world. In order to secure access to "EU" markets, businesses from all over the world must comply with "GDPR" rules.

3. LEGISLATIONS IN UNITED STATES OF AMERICA TO PROTECT PERSONAL DATA

The US Constitution doesn't speak much about "law enforcement in the context of data protection law". The 4th Amendment to the constitution is the only option that offers a modicum of protection against intrusive law enforcement action; under the phrase "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures", certain information is secured, including phone and financial records. The same is true, though, only in cases where there is a "legitimate expectation of privacy". Although every legislation has an exception, and this is true for this particular right as well, the exception is that when a person freely gives their data to a third party, such data is not entitled to protection. It is known as the "third party doctrine". If we interpret this right, we will see that the fourth amendment does not apply to a significant portion of personal information, including information on websites visited, phone numbers called, email addresses, and financial and educational records. Furthermore, foreign citizens are not protected by the 4th Amendment. Furthermore, the government has occasionally used "reasonable" government interests to defend the Fourth Amendment's application. If the right is still upheld in such circumstances, the government's

DOI: https://doi.org/10.48001/veethika.2022.08.02.004

final option is to suppress evidence in the criminal prosecution and award damages in the civil case. Despite the limitations on its use, the judiciary recently turned to the fourth amendment to provide a landmark decision that might be read broadly to establish a "right to deletion" of the old data that the agencies are holding. There is a huge vacuum in the laws defending privacy and data security, notwithstanding the widespread panic around these issues. Despite being one of the largest IT centres in the world, the United States lacks clear and comprehensive data protection regulations.

The "Privacy Act of 1974" left a gap that is being filled by this legislation. By granting foreign nationals of the so-called "Covered Countries" (also known as "covered persons") a status similar to that of US residents under the "Privacy Measure", this act fixes the flaw in the "Privacy Act". In other words, international nationals covered by this law will have access to the same legal options as US citizens in the event of data misuse. Only "covered records", which broadly speaking encompasses the records kept by US agencies, are subject to these protections. All such terms are defined in the "Privacy Act" itself: "transferred (A) by a public authority of, or private entity within, a country or regional economic organization, or member country of such organization, which at the time the record is transferred is a covered country; and (B) to a designated Federal agency or component for purposes of preventing, investigating, detecting, or prosecuting criminal offenses." There are other cases like these that make it abundantly evident that the data supplied to sources that are not designated will be exempt from this act. Additionally, a more thorough study would reveal that the protection does not apply to data transferred before the nation was designated as a "covered country". The right to file a lawsuit under this act is also lost by a citizen of a designated country if the Attorney General has withdrawn that country's designation as a "covered country". This once more demonstrates how limited the United States' view of the protection of personal data handled by federal institutions is. The fact that only three of the four remedies outlined in the Privacy Act are available to foreigners under this Act is another significant finding. The "right to recover damages, costs, and attorney fees if it is determined that the agency is at fault for failing to keep records about individuals with the accuracy, relevance, timeliness, and completeness" required to ensure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to, the individual that may be made on the basis of such records. The major paradox of the act is that "the data under its ambit is restricted to for purposes of preventing, investigating, detecting or prosecuting criminal offence", while affirmatively stating that "the covered person shall be subjected to the same limitations, including exemptions and exceptions", applicable on the individual under the "Privacy Act,1964", which in "turn leads to the conclusion that given the encyclopedic exemptions stated in the Privacy Act", the already sectarian scope of application of rules would be further "comprehensively diminished", if the same exemption are imposed.

4. A BIRD'S EYE VIEW OF INDIA'S DATA PROTECTION LAWS

Under the Article 19 (1)(a) *i.e* "Right to freedom of speech and expression" is enshrined in the Part III of the Constitution of India, which can be translated as the freedom to express one's thoughts on various issues. Furthermore, under Article 21 of the constitution " person's life and liberty" are protected and can only be taken by the "procedure established by law." These articles can be seen as torchbearers for the "right to privacy" and "data security". "Personal information" is said to be the incarnation of a person's personality, which is why Indian courts have repeatedly stated that the "right to privacy" is a basic right. Articles 19 and 21 of the Constitution have been interpreted by judicial activism to include the right to privacy in the scope of fundamental rights. In the case "*Govind v. State of M.P"*[x], Justice Mathew delivered the majority judgment asserting that the "right to privacy is a fundamental right" and can be interfered with on the grounds of pressing public interest only. In numerous occasions, the "concept of privacy" has been tinkered with, and it has been understood differently in various situations. For some, privacy meant "*desire to be left alone*," but for others, it meant "*desire to be paid for data and the ability to act freely."*

As a result, the "right to privacy" has received much-deserved attention and cannot be violated unless there are compelling grounds, such as national security or public interest. There is currently no specific regulation governing the subject of data protection or privacy. Nonetheless, there are a number of laws that provide certain safeguards for privacy and data protection.The "IT Act of 2000", together with amendments in 2008 and associated guidelines, is the torchbearer for India's IT laws. It covers the majority of data protection law. The "IT Act, 2000" enables legal recourse in the event of a data breach from computer systems, regardless of the perpetrator's location, as long as the crime is committed on an Indian system. Furthermore, this act prohibits the unauthorised use of a computer, computer systems, and data stored on them. It also makes you personally liable for the same. The internet or network service provider, as well as companies that handle data, are not explicitly covered by this section. As a result, any businesses entrusted with the safe distribution and processing of data, such as suppliers and outsourcing service providers, are exempt from the Act's reach. Section 79 of the IT Act, which applies to two conditions of "knowing" and "Best Efforts" in determining the quantum of punishment, further weakens these liabilities. In other words "a service or network provider could escape the liability under the provisions of this act if they successfully prove that the offense was commissioned without their knowledge, or that they had exercised due

DOI: https://doi.org/10.48001/veethika.2022.08.02.004

diligence to prevent the commission of the offense". However, it is important to highlight that if an employee violates the Act's restrictions, the company's main persons (managers and directors) would be held personally liable for the infringement.

"The IT legislation primarily addresses issues such as legal recognition of digital signatures and electronic documents, offences and violations, and cybercrime adjudication mechanisms. In 2008, the act was amended to include key features such as a focus on data privacy and information security, the definition of terms such as cybercafe, the neutralisation of digital signature technology, the definition of intermediaries, inspectors, and the Indian computer emergency response team, and the inclusion of crimes such as child pornography and cyber terrorism".

The Indian Penal Code can also be used to seek remedy in cases of cybercrime. Because the criminal code was written in 1860, it would be useless to expect it to include a data protection provision. However, with the implementation of the IT Act, the IPC was revised to include "electronic records" in its record-keeping obligations, thereby putting them on par with traditional documents.Furthermore, the associated offences can be used to infer responsibility for cybercrime. For instance, section 463 deals with forging and false documents; if the accused attempts or fabricates the documents with the intent to injure another person, they will be penalised under section 465, which, if given a broad interpretation, might include instances of email spoofing. Similar to how section 416 of the IPC, which deals with impersonation fraud, may apply to identity theft, section 420 of the IPC may apply to other computer scams. The protection of individual rights has traditionally been given top priority by Indian courts. In this regard, it is reasonable to assume that they will employ a liberal reading of the law to make up for any legislative shortcomings, such as when interpreting Section 43A of the Act where the IT Act lacks to specify what constitutes unfair loss or unlawful gain.

Similarly, "personal information collected under the Credit Information Companies (Regulation) Act, 2005" (CICRA) must be processed in accordance with the CICRA regulation's privacy criteria. Any data leak or manipulation is the responsibility of the entities responsible for collecting the data. The "Fair Credit Reporting Act" and the "Graham Leach Biley Act" are the cornerstones of the strict structure that governs a person's credit and money. The Reserve Bank of India establishes the fundamental concept that controls data privacy. As a result of globalisation and increased rivalry among market competitors, software businesses have been forced to take steps to protect data in order to gain the trust of overseas investors. The largest technology trade association, the "National Association of Service and Software Companies", wants to improve data security and privacy.

5. LATEST UPDATES ON PERSONAL DATA PROTECTION BILL 2019

On August 5, 2022, the government announced that it was withdrawing the "Personal Data Protection Bill" from the Lok Sabha in favour of a "set of new legislation" that would be compatible with a "complete legal framework".

Limitations on the use of personal data without the citizens' express consent were included in the abandoned Bill. It had also controversially tried to grant the government the authority to exempt its investigation agencies from the Act's requirements. Opposition who had filed dissent notes vehemently opposed this proposal. The government will introduce a new set of bills during the winter session of Parliament to replace the current bill with others that deal with cyber security and privacy.

The Bill, which was introduced on December 11 and referred to the Joint Committee of the Houses for consideration, has been withdrawn, according to what is known. The administration distributed a statement to MP's describing its reasons for doing so. In December 2021, the Joint Parliamentary Committee's (JCP) report was delivered to Lok Sabha. The 2019 Bill was thoroughly discussed by the JCP, which recommended 81 modifications and 12 recommendations for a comprehensive legislative framework for the digital ecosystem, according to the statement distributed to Lok Sabha members on August 3. "A complete legal framework is being developed taking the JCP's report into consideration. Hence, in the circumstances, it is proposed to withdraw "The Personal Data Protection Bill, 2019" and present a new "Bill" that fits into the comprehensive legal framework".

6. CONCLUSION

In conclusion, this made an attempt on the comparative analysis of global data protection legislation with the India's Personal Data Protection Bill. There are some of the improvements should be taken into considerations. First, the measure establishes important restrictions on data processing and mandates notice and consent for data acquisition. Since they are founded on concepts for the control of data (fair information practices) developed prior to the creation of the current market framework, these collectively may not actually effectively protect privacy. Additionally, they do not shield consumers from the negative effects of a privacy infringement. Instead, these duties can boost moral hazard and cause consumers to overestimate the advantages of privacy protection. Second, there is no empirical understanding of the trade-offs users make when disclosing their information, hence the law has no basis in reality. The Srikrishna committee, which created the initial draught of the bill, did not do any research to determine the particular situations in which users are willing to trade personal information for advantages. Evidence from different jurisdictions suggests that these

DOI: https://doi.org/10.48001/veethika.2022.08.02.004

trade-offs vary depending on the transaction's environment. If the bill efficiently safeguards personal data without demonstrating its relevance to consumers, it may have a negative impact on the advantages of data-led innovation. Third, the law suggests charging data processing companies hefty compliance fees. Small firms are excluded from a lot of requirements, however these exemptions only apply to companies who process data by hand. As a result, putting the measure into effect would be quite expensive for a wide range of economic actors. The regulations that force companies to give non-personal data to the government are especially onerous and significantly erode property rights. Long-term consequences for innovation and economic growth may result from this.

These problems point to the need for a more realistic and restrained approach to data privacy and the harms caused by improper use of personal information. The proposed structure is preventive, all-encompassing, and heavily regulated since the measure views privacy as a goal. By doing this, it considerably expands the state's ability to control organisations that gather data and offers it more tools for conducting surveillance. The effectiveness of safeguarding privacy through this regulatory structure obviously has its limits. The framework should instead concentrate intently and narrowly on issues that can be meaningfully resolved by legislation.

REFERENCES

i AIR 2017 10 SCC 1

ii Tom Gaiety, "Right to Privacy", Harvard Civil Rights Civil Liberties Law Review, 233.

iii Edward Shils, "Privacy: Its Constitution and Vicissitudes", Law & Contempt Problems 281 (1966).

iv Samuel Warren & Louis D. Brandeis, "The Right to Privacy", Harvard Law Review 193 (1980).

v Aimée Hope Morrison, An impossible future: John Perry Barlow's "Declaration of the Independence of Cyberspace", 11 New Media & Society 53-71 (2009).

vi Anisha Agarwal, "Sanctity of personal data: A comparative study of data privacy laws in EU, US and India", International Journal of Legal Developments and Allied Issues, Volume 6, Issue 3, May 2020.

vii "White Paper of the Committee of Experts on Data Protection Framework for India 2018".

viii Alan Calder, EU GDPR (2016)

ix Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. 2014.

x AIR 1975 SC 1378.

xii Gupta, A., Mittal, P., Gupta, P. K., & Bansal, S. (2022). Implication of Privacy Laws and Importance of ICTs to Government Vision of the Future (pp. 383–391). https://doi.org/10.1007/978-981-16-3071-2_32

xiii Mittal, P., Kaur, A., & Gupta, P. (2021). The mediating role of big data to influence practitioners to use forensic accounting for fraud detection. European Journal of Business Science and Technology, 7(1), 47–58.

DOI: https://doi.org/10.48001/veethika.2022.08.02.004