Page 793 - 813 **DOI:** *https://doij.org/10.10000/IJLMH.115468*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 6 | Issue 4

2023

Data Protection Laws: A Contemporary Study of EU and Indian Laws

BHAVESH VASHISHT[1]

ABSTRACT

The current Article focuses on the various aspects relating to Data Protection Laws with special reference to Indian and European laws and it's contemporary development. The Article focuses on the various aspects relating to Data Privacy and starts with the very definition of what includes and is "Privacy", followed by the concept of "Right to be forgotten" in Indian as well as global Scenario with the help of relevant case laws. The article then illustrates the concept of Data protection and includes Data protection laws in EU encompassing various provisions of GDPR and the Indian context of Data Protection laws. The Article also includes the draft personal data protection bill of 2019 and the legislative history regarding the same. The Article ends with the newly issued Data protection bill of 2022 and the various advantages and shortcomings regarding the same too.

Keywords: *Cyber law , GDPR , Data Protection Bill , Right to be forgotten.*

I. INTRODUCTION

The development of technology and the overdependence of our day-to-day life activities for their social economic activities on Information and Communication Technology has in turn it's own pool of merits and demerits. The so called IT revolution has helped in transforming many ambits of both society as well as the economy. One of the Famous quote from Google; "we no longer surf online, we live online" describes the need and the demand for data driven society in today's time. Further, it also provides for sharing vital information of many kinds which occurs through this medium, which can be purposefully or unintentionally. The advanced technology transmits, saves, and processes secret information of a private nature of persons with or without their consent, inflicting them social and economic harm. The social and economic harm is often beyond repair for both states and subjects, leading to international efforts by states in their separate jurisdictions to govern privacy and data protection.

In simple terms, Data protection can be defined as act of safeguarding the critical data against loss, compromise, corruption, and also the capacity to restore the data to a state from where it

[1] Author is a LL.M. Student at Maharashtra National Law University, Aurangabad, India.

 [ISSN 2581-5369]

can be accessed if something goes wrong to turn the data which is deemed to be not of any use or is not accessible.

The concept of Data protection although further ensures that the said information hasn't been corrupted, that it is only accessible for authorised intended use, also ensuring further that it adheres to respective relevant statutory and managerial norms. The data which is protected then ought to be used and utilised for any appropriate purpose when needed.

Data privacy as well as the security are not revolutionary notions in the world of outsourcing. When sensitive and confidential information is sent, security worries regarding data loss or abuse occur. Data privacy and security issues are identified as one of the key causes for anti-outsourcing lobbying. Some believe that the security concerns are the same whether the data is handled offshore or onshore, whilst others are concerned about data privacy and security legislation in countries such as India and see it as a major barrier to their choice to outsource. Whether or whether not the security worries are valid, firms in both the US and the UK are under increasing pressure due to legislation requiring the protection of consumers' financial and medical data. Indian organisations recognise the need of increasing data privacy in order to solve security risks before they become a problem. Proactive initiatives are being done by individuals and organisations such as NASSCOM to guarantee that India's unique selling proposition is "trustworthy outsourcing."

(A) Concept of Privacy

The concept of data protection usually takes it's essence from the term "Privacy" is derived from the Latin word 'Privatus', which means 'separated or excluded from the rest'. It derives it's essence from the many philosophical debates and has been seen from the Aristotle's distinction between the two realms of the life , One of which is the realm which is related to the public life of the individual , which is associated with the Political life and the private one which is the life of the individual at his home i.e domestic one.[2] The notion of privacy varies from country to country. as it is depended upon various other reasons like historical background, cultural and religious beliefs and practices which are the basis for all societies in the world. Something which is considered private may be public for other one. However, even after considering all the above challenges, 'Privacy is defined as private information about an individual's life or circumstances which is not publicly available. As it applies to all of an individual's personal information, it is their right to determine how eager they are to share intelligence with others. The notion of

[2] Vioreanu, D. (2022) *The origins of privacy and how it became a human right, CyberGhost Privacy Hub*. Available at: https://www.cyberghostvpn.com/en_US/privacyhub/the-origins-of-privacy-and-how-it-became-a-human-right/ (Accessed: 17 July 2023).

 [ISSN 2581-5369]

privacy has indeed been recognized all over the world in a number of international treaties in form of human rights like Universal Deceleration of Human Rights[3], International Covenant on Civil and Political Rights[4] and European Human Rights Convention[5]. To sum up the concept of privacy includes the following:

1. Privacy of credit information, medical reports, government data, and so forth included in the ambit of *Informational Privacy*
2. *Bodily Privacy* including things like genetic mapping, DNA, drug testing, physical selves, and so on.
3. *Personal communication privacy*, such as telephone call information, email, SMS, and so on.
4. *Territory Privacy*, such as encroachment or trespassing at home or business, etc. without consent

II. INDIVIDUALS AND PERSONAL DATA COLLECTION

Personal data also make up the identity Although the idea of privacy is multifaceted, experts ranging around the globe have attempted to reduce this into a single definable phrase. Warren and Brandeis said in their landmark paper that the right of privacy was predicated on the concept of "inviolate individuality," that lays down the framework for a categorization of the concept of privacy which we today recognise as possession over the personal information of the individual. Personal data in it's philosophical meaning can be defined as an exclusive perception of life and can be understood as a subset of attributive properties of any person which sufficiently defines this person within any set of persons.

The online privacy information of any individual can be defined as the surfing as well as the brwosing habits of the concerned users as well as the time stamps regarding the date and time of their visit, queries on search engines, files uploaded and downloaded, Uniform resource Locator etc. The interested groups therefore track this information for their own advantage. In fact technology has introduced new means of storing and exploiting privacy related matters against the persons concerned and further causing them social humiliation and economic loss.

(A) Right to be Forgotten[6]

[3] Article 12 of the Universal deceleration of Human Rights,1948
[4] Article 17 of the International convention on Civil and Political Rights, 1966
[5] Article 8 of European Human Rights Convention, 1950
[6] Vavra, Ashley Nicole. "The Right to Be Forgotten: An Archival Perspective." *The American Archivist*, vol. 81, no. 1, 2018, pp. 100–11. *JSTOR*, https://www.jstor.org/stable/48618003.

 [ISSN 2581-5369]

The right to be forgotten (RTBF) refers to any individual's capacity to request that a search engine delete connections to personal information from search results. The concept of Right to be forgotten[7] is mentioned under the Article 17 of the GDPR[8] and it also allows the people to question the inclusion of data which is given under the Article 15[9] of the GDPR. The RTBF has been the law of the land in Europe since a 2014 judgement by the Court of Justice, and it has ardent advocates in many areas of the world, but it has been opposed globally by archivists, librarians, and others whose job it is to enable public access to information. The Right here derive it's root from the French jurisprudence upon the subject of 'Right to Oblivion' or Droit a loubli in 2010. This Right of Oblivion benefited convicted criminals who had served their time in jail by prohibiting the release of details about their crimes and criminal lives.

Mario Costeja Gonz'lez, a Spaniard, had come into financial troubles and was in need of urgent cash in 1998. Consequently, the individual Mr. Mario have advertised a house for the process of auctioning by the way of newspaper, which accidentally appeared on the internet. Consequentially, the internet didn't forget Mr. Gonz. Minor details about the transaction were made accessible on the Google even after he had fixed his problems and sold his house. Now any person who want to look him up on the internet assumed he was bankrupt as the details of selling his house are still available on the Internet. As a result of this , it had fairly harmed the reputation of Mr. Gonz and leading him to pursue a lawsuit in furtherance of this. Finally, this lawsuit inspired the concept of the "Right to Forget."

The issue of individual information manipulation is apparent in the matter of **Jorawer Singh Mundy vs. Union of India[10]**. The Supreme Court ruled in this case and ordered the respondents (Google, Lex.in, and Indian Kanoon) to delete the ruling until further order. The petitioner here who was an NRI living in US lost considerable job opportunities as information regarding his former case was not erased from the web. In the lack of a data protection policy that limits the basic Right to remove useless and defamatory private material from the internet environment, this 'Right to be Forgotten' [11]has gained it's share of success in India. As a result of this case, it is evident that it is urgent to consider the "right to be forgotten" as to be a basic right.

Organizations that hold sensitive personal data and fail to maintain proper measures to secure such data which further leads to the loss or gain of an individul, may be compelled to pay considerable compensation to the individual whose data has been compromised, according to

[7] *ibid*
[8] https://gdpr-info.eu/art-17-gdpr/
[9] https://gdpr-info.eu/art-15-gdpr/
[10] W.P. (C) 3918/ 2020 , Delhi High Court
[11] *Supra*

 [ISSN 2581-5369]

Section 43A of the Information Technology Act of 2000[12]. The 'Right to be Forgotten' is not directly included in the notification of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021[13] by the Government of India. It does, however, include processes for registering complaints with the appointed Grievance Officer in order to have content exposing the information which was personal about the complainant deleted from the internet without the complainant's consent.

III. JUDGEMENTS RELATING TO THE RIGHT TO BE FORGOTTEN

In **Prem Shankar Shukla v. Delhi Administration[14]**, J. Krishna Iyer, stated for a three-judge Bench of the Hon'ble Apex Court, ruled: "*the guarantee of human dignity, which forms part of our constitutional culture, and the positive provisions of Articles 14, 19, and 21 spring into action when we recognise that to manacle man is more than to mortify him; it is to incarcerate him and, thus, to violate his very personhood, too often using the mask of 'dangerousness' and security*"[15]

The Gujarat High Court refused to recognise the so-called "right to be forgotten" in the case of **Dharamraj Bhanushankar Dave v. State of Gujarat[16],** The petitioner in this case was charged with criminal conspiracy, culpable homicide amounting to murder as well as kidnapping, along with string of many other serious offences. Although, he was also acquitted by the court of Sessions and in furtherance of this it was supported by a Gujarat High Court's divisional bench. The petitioner here on valid grounds argued that since the judgement was non-reportable, the respondent should be prohibited from displaying it on the internet because doing so would jeopardise the petitioner's life both personally and professionally.

The Orissa High Court explored the 'Right to be Forgotten' as an effective tool for victims which are harassed sexually and other heinous crimes where their explicit recordings or images often broadcast on social media and further results in tormenting the victims in **Subranshu Raot @ Gugul v. State of Odisha[17].**

IV. CONCEPT OF DATA PROTECTION

The concept of data protection as well as privacy are not synonymous ideas, despite certain

[12] Section 43A- Compensation for Failure to protect data.
[13] *The Information Technology (intermediary guidelines and Digital Media Ethics Code) rules, 2021* (2023) *PRS Legislative Research*. Available at: https://prsindia.org/billtrack/the-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021 (Accessed: 17 July 2023).
[14] Prem Shankar Shukla vs Delhi Administration on 29 April, 1980 ; 1980 AIR 1535, 1980 SCR (3) 855
[15] *Ibid*, Paragraph 5 of the Judgement by J. Krishna Iyer
[16] C/SCA/1854/2015 , Special Civil Application 1854 of 2015, Gujrat High Court
[17] BLAPL No.4592 OF 2020 ; Application under Section 439 of CrPC,1973

 [ISSN 2581-5369]

similarities. They are similar to twins but not identical[18]. Data protection does not cause privacy concerns and is not prohibitive if it is treated lawfully while adhering to directions of the relevant authorities. The scope of data protection is both small and extensive in comparison to privacy, since both ideas strive to preserve some of the rights and interests of others. Though privacy is the starting point for identifying and determining data protection rules. Personal rights to privacy exist with proprietary rights to data protection. The English Dictionary of Cambridge defines 'data' as any information which is in the form of any facts or statistics that has been collected and scientifically reviewed for use in decision making.

In the age of computers, sophisticated software is utilised by the computer to store, analyse, and use information in electronic form in order to make decisions. The Information Technology Act of 2000 defines "Data" in the absence of particular law on the subject as;

"a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and maybe in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer."[19]

The IT Act in it's provisions failed to define the term "processed," which is used in the definition above. While personal information may be expressed verbally or nonverbally, it is properly collected, kept, and processed for use in commercial decision-making. The information that has been analysed as data has proprietary values because of its commercial utility. There have been allegations in the past of corporate houses selling or misusing data information without asking for consent from people, endangering the integrity and security of people.[20]

(A) Data Protection Laws in EU

Data protection provisions EU are primarily controlled by the EU General Data Protection Regulation (GDPR)[21], which went into effect on May 25, 2018 leading to governing the collecting and processing of personal data across all sectors of the EU economy[22], and imposes new data protection requirements on controllers and processors, as well as new rights on EU citizens.

---

[18] *Shaping Europe's digital future* (no date) *Language selection*. Available at: https://ec.europa.eu/digital-agenda/en/news/legal-analysis-single-market-information-society-smart-20070037 (Accessed: 17 July 2023).
[19] Information Technology Act, 2008, Section 2(O).
[20] The Economic Times, 'Toughen law enforcement: Indian BPOs need to be extra vigilant', http://articles.economictimes.indiatimes.com/2006-10-05/news/27466453_1_indian-bpo-data-theft-bpo-industry
[21] https://gdpr.eu/tag/gdpr/
[22] Article 4(1) of the GDPR Act ; any information which are related to an identified or identifiable natural person

The GDPR imposes specific responsibilities on enterprises that process personal information about people (data subjects). The GDPR also providing the data subjects with numerous rights relating to the handling of their personal information. Failure to comply with the rules of the Act and Member State data protection rules adopted to improve the data protection obligations is a criminal offence, punishable by harsh fines and legal claims from data subjects who have suffered as a consequence. Despite the fact that the GDPR creates uniform data protection norms and principles, it provides EU Member States the right to keep or adopt national laws to further define the GDPR's implementation under Member State legislation.

(B) Scope and Implementation of GDPR

The GDPR[23] extend it's applicability to the ambit of data which is personal to individuals and which is processed entirely or partially by automated methods, as well as to the personal data processing that is part of or intended to be part of a file system other than by automated means. The Act although doesn't really extend to an individual's processing of personal information in the course of a strictly personal or domestic activity. The GDPR only applies whenever the processing occurs in the presence of the controller's or processor's establishment in the EU, or where the controller or processor doesn't have a establishment in the EU and yet processes personal data in connection to the proposition of services or goods to citizens in the EU; or when the surveillance of the behaviour of an individual in the EU takes place within the EU. This implies that many non-EU enterprises that have EU based consumers will be required to comply with the GDPR's data protection rules.

(C) Principles of Data Protection

Article 5 of this European data protection act aims at establishing important principles which form the foundation of the Act[24]. The Important Principles are mentioned as below:

1. Legality, Fairness, and Transparency

This concept demonstrates the need of lawful and equitable handling of personal data. The procedure by which personal data concerning persons is gathered, utilised, examined, or processed otherwise for some any other means, and also the degree upto the mark that the personal data is and is to be treated, should be totally clear to individuals. It is also necessary that whatever information which is available for the processing of personal data be simply understood and accessible.

[23] Ibid 19
[24] https://gdpr-info.eu/art-5-gdpr/

2. Purpose Restrictions

Personal data about any individual should be gathered only for defined, described also the legal objectives and they must not be treated in a way which is incompatible with the mentioned goals. The exact reason for which personal data is handled must be starightforward and justified. However, the consequential subsequent processing of the data should be in accordance with Article 89(1)[25] and it is not deemed incompatible with the primary aims

3. Data Reduction

The processing of personal must be strictly based upon the minimal use and should be pertinent to the specific reason for purposely it was handled. The Personal data of the individual shall only be processed if the goal of the processing cannot be reasonably achieved through other means. It also intends to keep the data for a set amount of time and not to the discretion of data handlers.

4. Accuracy

The Personal data controllers must always ensure that the individual's data is always correct and that if there is any requirement than it should be maintained up to date. Further , the personal data which is erroneous and wrongful in linkages with the services for which it is processed is destroyed or rectified as soon as possible.

5. Storage Capacity

This means that the data which is personal data of the individuals should be only stored and accepted in a prescribed format which allows them to be identified and should only be kept for as long as required for the objectives for which their sensitive data have been collected. Further in guaranteeing that the data is not stored for time period longer than required, then here the controller must always establish time limitations for deletion or periodic review.

6. Discretion and Ethics

The data which is personal to the individual must always be processed in a format which will ensure adequate privacy and protection of the personal data, including protection against unauthorised or unauthorised access to or usage of personal data and processing equipment, as well as accidental loss, using appropriate technical or organisational measures.

7. Accountability

[25] Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject

 [ISSN 2581-5369]

The controllers of the data should take accountability about their management of personal data, as well as checking upon how these controllers are adhering with the rules laid down in the Act, after which they can show compliance with data protection legislation.

Furthermore, Articles 10 and 11 provide that the subject must be notified of the identity of the controller or his representatives, and of the intention of the data processing, if he submits the information or it is obtained elsewhere. Subjects have the right to request and oppose[26] to details about how their personal data is being processed. The subject shall have the right to request that the controller correct, erase, or cease data processing that violates the provisions of guidelines. In the case of Google.Spain SL. v. Agencia ,Espaola de Protección de 'Datos, the European Court of Justice ordered Google to erase information from its website (AEPD)[27].

The directive, however, may also enable data protection to be questioned in circumstances of

a) Security relating to both of the Nation and Public at national and international level

b) defence of the state, authority with the state to regulate laws if defence of state is in question

c) if it is linked with the criminal investigation, detection, and prosecution of any offence and there are no other ways of doing so then by the approval of proper authorities may bypass these data protection laws

d) activities which are relating to state monitoring or regulating responsibilities.

V. DATA PROTECTION: INDIAN CONTEXT

In India, cybersecurity and data protection are now governed by a woefully insufficient set of laws. Authorities established under the ambit of ITAct, 2000[28] and also the IT (Amendment) Act,2008[29] to regulate compliance and enforce penalties for noncompliance. Although they have now been inactive for years. Until late 2017, there has been relatively little important jurisprudential progress on the themes of cybersecurity, privacy of individuals as well as the data protection. In the year 2013, the government issued a National Cybersecurity Policy, which drew widespread attention both in India and throughout the world, particularly given India's status as an increasingly rising outsourcing of business processes. destination. Unfortunately, work on the policy has been delayed for unclear reasons, casting doubt upon the government's

[26] Id. Article 14
[27] C-131/12, http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text&page Index=0&part=1&mode=DOC&docid=152065&occ=first&dir&cid=437838
[28] The Information Technology Act, 2000.
[29] The Information Technology Act, 2008.

aim of producing clear, comprehensive, and fully vaccumed regulation on these issues.

Following the launch of the government's heavily publicised Digital India campaign in 2015, the Prime Minister's office had been involved in a very fast pacing attempt to compensate for lost time in terms of cybersecurity enhancement. The main agenda of the campaign was the creation of "digital infrastructure" to facilitate the actual digital delivery of services and in turn also lead to increasing digital literacy. Since the launch of The Aadhar Act, the piece of law intended at the targeted distribution of financial assistance to the underprivileged, was approved by Parliament in 2016. This Act also mandated that every Indian citizen be provided an unique Aadhar card comprising of a unique identifying number, comparable to the social security numbers as used in the US.

(A) Legislative aspect of Privacy and Data Protection

In the context of India it is found to be an absence of a specific act and rules for the specific purpose relating to data protection and for this reason the applicability of the data protection is governed by a patchwork of various legislations which have been enumerated below:

1. IT Act,2000 & IT (Amendment) Act 2008[30]

The IT Act, which is the most important Act, has several safeguards for protection and regulating data protection rules in India. The IT Act under Section 43(a) – 43(h), penalises "cyber contraventions" and establishes civil remedies for "cyber crimes" from Section 63 to Section74 including criminal action

The main purpose of the enactment of IT Act was to facilitate e-trade and commerce and data protection was not in the ambit at that time and it made no explicit precautions for data security. Anyone who hacked into the system may face punishment under Sections 43 and 66 of the IT Act[31], 2000 if data security is breached. Although, it does not contained provisions for taking actions against the organizations if any breach of data occurs by them. The IT (Amendment) Act, 2008 was passed, which included two new provisions in the IT Act, Sections 43A and 72A[32], to hold corporations accountable and give relief to those who have suffered or are expected to incur loss as a result of their personal data not being effectively safeguarded.

The Information Technology Rules (IT rules)

The government periodically publishes sets of Information Technology Rules under various parts of the IT Act in order to widen its reach. The IT rules are statutory laws and it includes 4

[30] *Ibid*
[31] Penalty and compensation for damage to computer, computer system, etc ; Computer related offences
[32] *Supra ;* Punishment for disclosure of information in breach of lawful contract

sets of guidelines or rules framework within its ambit and is included under Section 43A[33] of the IT Act. These IT Rules focus on and govern certain areas of data collection, transfer, and processing, and most recently include the following:

(a) the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules[34],

(b) the Information Technology (Intermediaries Guidelines) Rules,[35]

(c) the Information Technology (Guidelines for Cyber Cafe) Rules[36],

Compliance Regulators : CERT-In

The government established CERT-In under Section 70B of the IT (Amendment) Act 2008[37], which is referred to as the 'Indian Computer Emergency Response Team'[38] on the Ministry of Electronics and Information ,Technology's website. CERT-In is a nationwide node that investigates into incidents regarding computer security as they occur. The following are the functions of the Department of Electronics and Information Technology:

i) Information concerning cybersecurity incidents is gathered, analysed, and shared.

ii) Cybersecurity event forecasting and alerting;

iii) cybersecurity emergency procedures

iv) Synchronization of cyber incident response activities

v) Issuing guidance, recommendations, advisories, security vulnerabilities notes, and white papers on data security policies, practises, cyber incident prevention, response, and reporting as needed.

Facebook and CERT-In

- After it was discovered that the personally identifiable data of 533 million Active social media worldwide, which include 6.1 million in India, was supposedly made public on the web and freely distributed on cyber-attack forums, the administration's premier cyber defence organisation, CERT-In, urged Facebook users to protect their profile

[33] *Ibid*
[34] *Supra*
[35] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, https://prsindia.org/billtrack/the-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021
[36] The Information Technology (Guidelines for Cyber Cafe) Rules, 2011 - Process of Registration, http://bareactslive.com/ACA/ACT2081.HTM
[37] Section 70B :- Indian Computer Emergency Response Team to serve as national agency for incident response.-
[38] *Ibid , note 34*

 [ISSN 2581-5369]

information.

- The Computer Emergency Response Team issued a statement indicating that there has been a global breach of Facebook profile information.
- Email addresses, profile IDs, full names, job titles, phone numbers, and birth dates are all made public.
- The scraped data, according to Facebook, does not include any financial, health, or password information.

The Indian Computer Emergency Response Team (CERT-In)[39] has collaborated on cyber security with counterparts in Malaysia, Singapore, and Japan. The Memorandums of Understanding (MoUs) would encourage greater coordination among India and the three nations in the detection, resolution, and prevention of surveillance events. CERT-In seeks to improve the country's cyber security by detecting and response to cyber threats.

(B) Judicial developments on right to privacy

In ***M.P Sharma versus Satish Chandra***[40], the Apex Court considered whether the search and confiscation of papers pursuant to filing of an FIR violated the constitutional right to privacy. The right to privacy is not a basic right under the Constitution, according to a majority ruling of the Constitution Bench's eight judges.

Following that, in ***Kharak Singh vs. State of Uttar Pradesh***[41], the question was if routine police monitoring amounted to a violation of constitutionally granted basic rights. A constitutional division bench of six judges examined the very question in the context of the legality of the Uttar Pradesh Police rules which were followed at that time,it authorized the police to do secret entering in the homes, house visits at night, and frequent monitoring. The Apex Court here ruled that Article 21 of the Indian Constitution is the treasurer of all the residuary personal rights whatsoever existing, and it also took cognizance of the right to privacy existing by the common law standards. However, The Court did, however, point out that privacy is not a guaranteed basic right. However, Justice Subba Rao, the dissent judge in this case, stated that "even if the right to privacy is not enshrined as a basic right, it was an integral component of personal liberty under Article 21 and hence is fundamental.[42]"

This approach of J. Subba Rao was adopted by the Supreme Court's, nine.-judge panel in the

[39] https://www.cert-in.org.in/
[40] M.P Sharma and Ors. Vs Satish Chandra and Ors. 1954, (1954) 1 SCR 1077
[41] 1963 AIR 1295, 1964 SCR (1) 332
[42] *Ibid ;* J. Subba Rao, para 15 of judgement

case of ***Justice K.S Puttuswamy(Retd.) and Anr. Vs Union of India and Ors.***[43]**,** which identified the right to privacy as an integral component of the fundamental existence and human liberty. Article 21 of the Indian, Constitution, in particular, guarantees liberty. The Bench further stated in this judgement that the Indian Constitution must grow over time in order to address the problems provided by a democratic system guided by the rule of law, and that the definition of the constitution cannot be frozen on the viewpoints common at the time it was formed.

The right to privacy was built on freedom rights under Indian Constitution Articles 21 and 19, which embraced both physical and mental freedom. "Privacy promotes freedom and is essential to the exercise of liberty," the court decided.

Although the Court acknowledged that the Right to Privacy is not an absolute right, it may be limited by reasonable constraints if judged such. To limit the state's discretion in such matters, the court established a test to restrict the possibility of the state clamping down on the right, which are:

1. the conduct should be authorized by law, it must be essential to fulfil a legitimate aim of the state
2. The government's intervention should be "equivalent to the requirement for such interference."
3. Procedural measures should be in place to avoid the State from exploiting its power.

The case of **Karmanya Singh Sareen & Anr vs UOI & Ors**[44] is among the most recent cases that has highlighted the need of data privacy. This complaint was launched in the interest of the general public by two university students against large social media firms such as Facebook and WhatsApp, as well as the Union of India (through the Ministry of Transport and communications and TRAI)[45]. The major source of worry was that, following Facebook's acquisition of WhatsApp, WhatsApp change it's policy regarding privacy of users in the month August in 2016, stating they will share user information which although is quite limited with their parent firm Facebook , for optimization in marketing and suggestions. On September 23, 2016, the same court issued an injunction forcing WhatsApp to "clean" any data of users which they have received prior to September 25, 2016 which means the data of those users that

[43] (2017) 10 SCC 1, AIR 2017 SC 4161
[44] W.P.(C) 7663/2016 & C.M.No.31553/2016 (directions) at High Court of Delhi at New Delhi
[45] *Ibid , note 43*

withdrew away from the service prior to this date. If users continue to utilise the service, the court ordered that any data obtained after the date of September. 25 be handled only with Facebook and also its relating organisations.

This case is noteworthy because it is the sole explicit declaration of the right to privacy for persons that our law has seen in recent years, except from the momentous Supreme Court decision in 2015 that struck down Section 66A of the IT Act.

(C) Legislative Developments

The *Puttuswamy* judgement being a landmark legal judgement in the discourse of privacy especially informational privacy and steps have been taken by the Legislature. These include various attempts and some of them are discussed below :

a) The Information Technology (Reasonable Security Practices and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules)[46]

The SPDI Rules were promulgated under Section 43A of the Information Technology Act[47] of 2000. This refers to *"Compensation for Data Failure"* and allows for the implementation of "reasonable security methods and procedures" for the protection of sensitive personal data. To a limited extent, the SPDI Rules contain the OECD Guidelines on gathering limitation, purpose specificity, use limitation, and individual engagement.

Certain standards, such as a clear privacy policy, are mandated by the SPDI guidelines. It also specifies the time period for which information can be maintained and gives the individual the opportunity to rectify their information. Without the approval of the supplier, or unless contractually authorised or necessary for legal compliance, information distribution is not permitted.

These SPDI laws although only applies to the business entities, leaving out other organisations such as governments. The laws laid down in the SPDI act only applies to the 'Sensitive Personal Data,'[48] which includes characteristics such as sexual orientation, medical record history, personally identifiable information, and so on, and not to the broader category of personal data.

b) The Aadhar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016 [Aadhaar Act][49]

[46] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 Annex 3, https://cis-india.org/internet-governance/files/it-reasonable-security-practices-and-procedures-and-sensitive-personal-data-or-information-rules-2011.pdf
[47] *Supra*
[48] *Supra*
[49] The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016,

 [ISSN 2581-5369]

The Aadhar Act was one of the most revolutionary steps taken by the government. This Act although authorised the authorities in collecting identifying information from individuals, which may include their biometric data but in turn provided them with an individual identification number or an Aadhar Number based on such biometric information given by them.

This Aadhar Act also resulted in establishing a new authority to be called as UIDAI i.e Unique Identification Authority of India whose main agenda was to oversee the correct implementation of the Act. It also helped in the establishment of a Central Identities Data Repository (CIDR)[50], which in turn is a huge database which contains all the information of the individuals including Aadhar numbers as well as their biometric and demographic information. This Act although restricted the sharing and also using of the core biometric information of the individuals for any purposes other than the production of Aadhar Numbers and authentication. Under some situations although by the consent of the individuals their information other than their own core biometric information may be shared by the concerned authorities.

The Personal Data Protection Bill, 2019

In its historic judgement in the landmark decision of ***Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India And Ors.***[51] on August 24, 2017, the Hon'ble Apex Court of India declared the right to privacy in India to be a fundamental right ("Right to Privacy Case"). Leading to this case, it was determined that tougher regulations must be implemented to protect the people's personal data and privacy. As a response, in August 2017, the Central Government constituted a committee for the very purpose of data protection chaired by former Supreme Court judge Justice Srikrishna[52], and on July 27, 2018, the group produced a detailed white paper on the importance of data security. Following that, in July 2018, the committee released a draught of the 2018 Personal Data Protection Bill (PDP Bill)

Key Provisions of the Data Protection Bill

1. **Change in name and scope to "Data Protection Bill"**

The PDP Bill solely attempted to govern people' personal data as stated in the bill. However, based on the Report's suggestions, the JPC has advised changing the name of the draught bill to "Data Protection Bill," which would encompass non-personal data as well. It should be emphasised that the current draught of the PDP Bill permits the Central Government to get

https://uidai.gov.in/images/Aadhaar_Act_2016_as_amended.pdf

[50] *Shaping Europe's digital future* (no date) *Language selection*. Available at: https://ec.europa.eu/digital-agenda/en/news/legal-analysis-single-market-information-society-smart-20070037 (Accessed: 17 July 2023).

[51] *Supra*

[52] *Srikrishna Committee* (2023) *Wikipedia*. Available at: https://en.wikipedia.org/wiki/Srikrishna_Committee (Accessed: 17 July 2023).

 [ISSN 2581-5369]

anonymized or non-personal data from any data fiduciary in order to more focused service delivery or formulating evidence-based policies.

2. Appointment of a Data Protection Authority (DPA)

The measure requires just a fraction of entities to designate DPOs, but how the Indian government would differentiate such businesses isa bit unclear and the bill must be passed in order for businesses to understand their data fiduciary status and if they must comply with the DPO standards[53]. However, the Report recommends that, in additional to administrative officers on the selection panel, the selection committee regarding the appointment of DPA which include skills like technical expertise, legal, and academic professionals, and any other people as may be prescribed under the ambit of the bill.

3. Exemptions to government

In order to protect national interests, the PDP Bill absolved the government from complying with the said legislation of data protection. Section 18(2)[54] of the draft bill absolved the government from the provisions of the Act and allows them to process user data without their consent.

4. Data breaches

The Companies are now obligated under the Bill under which they are obligated in notifying of the personal data breaches whenever they lead to causing harm to the data subject. It also imposes a 72-hour reporting timeframe for such breaches. Strict Punishments ranging to a massive amount of Rs. 250 crs. can be imposed if the said ‘data processor’ or ‘data fiduciary’ fails to take reasonable safeguards regarding security in protecting personal data breach.

5. Social Media regulation

The proposed data protection bill in it’s various clauses advises that the accounts of the users present on the social media intermediaries should be vetted to prevent the threat of misleading news and phoney accounts. The Bill proposes that the Information Technology Act of 2000's intermediary structure failed to fulfil its purposes, and so suggests that social media intermediaries be recognised as "publishers" in certain specified instances, notably in regards

[53] Adams, S. (2022) *An examination of the DPO requirements in India’s proposed Data Protection bill*, *An examination of the DPO requirements in India’s proposed Data Protection Bill*. Available at: https://iapp.org/news/a/an-examination-of-the-dpo-requirements-in-indias-proposed-data-protection-bill/ (Accessed: 17 July 2023).

[54] Kashyap, H. (2022) *Data protection bill: From deemed consent to exemptions, lack of clarity may hurt the cause*, *Inc42 Media*. Available at: https://inc42.com/buzz/data-protection-bill-deemed-consent-exemptions-lack-clarity-hurt-cause/?login=1 (Accessed: 17 July 2023).

 [ISSN 2581-5369]

to information from unverified accounts.

Comparison of Personal Data Protection Bill of India with GDPR

1. **Permission**: In order to opt in or out, users must provide informed consent about how their data is processed.
2. **Breach**: Within 72 hours after the release, a breach must be notified to authorities.
3. **Transition term**: GDPR laws will be applied over a two-year transition period.
4. **Data Fiduciary**: Under EU regulation, a data fiduciary is any actual or legal person, governmental body, organization or group that decides on the purpose and techniques of data processing . Non-governmental organisations (NGOs) are also included in India (NGOs).

Criticism of the Bill

1. The Concerns were raised by technology businesses about a potential provision in the said proposed bill regarding the concept of data localization which has been finally addressed in the 2022 draft amendment of the bill and has allowed sharing of data to some selected countries. Firms were directed now in maintaining a copy of prescribed [55]sensitive personal data in India under this provision, and also of the export of undefined "important" personal data beyond the country would have been prohibited.
2. The activists questioned passages that exempted the Union government and its agencies from all of the Bill's responsibilities.

Loopholes in the Data Protection Bill,2019

1. Data protection legislation must ensure that, while respecting the rights of the data principal, the compliance requirements for data fiduciaries are not so onerous that even authorised processing becomes unworkable.
2. The challenge is to achieve a proper balance between data privacy requirements and justifiable exceptions, especially when it comes to government management of personal data.
3. Given the rapid advancement of technology, an ideal data protection legislation design must be future-proof. It should not be unduly complicated and should focus on providing solutions to current problems while avoiding potential future problems.
4. Given their unequal bargaining position with respect to data fiduciaries, laws must be

[55] *Supra, Section 43A contains provisions regarding safeguarding of sensitive personal data*

 [ISSN 2581-5369]

designed to offer a framework of rights and remedies that data principals may readily exercise.

Controversy regarding Data Protection Bill Draft,2022

- **Weakning of RTI Act,2000**

Clause 30(2) of the proposed Data Protection Bill intends to change Section 8(j) of the RTI Act, thus excluding personal data from being disclosed. Section 8(j) of the RTI Act stipulates that personal information is excluded from the RTI Act if its publication has no relevance to any public interaction or interest and creates any unjustified breach of an individuals personal privacy. However, if the authorities are satisfied, the Public Information Officer can direct the publication of such personal information such that "the broader public interest justifies the revelation of such information."

Furthermore, a provision in Section 8(j) states that personal information that can't be refused to the State Legislature or Parliament cannot be refused to an RTI request.

Now, the proposed Digital Personal Data Protection Bill intends to remove all restrictions on the disclosure of people' personal data, as well as the authority of Public Information Officers to enable any type of publication of such information. It also seeks to eliminate the proviso in Section 8. (j).

The insertion of Clause 30(2) of the Data Protection Bill will "seriously impair the RTI Act," according to the primary concerns. Notable RTI activists and groups raised their opposition to the aforementioned section, stating that "it will transform the RTI Act into the Right to Denial of Information Act" . Prior to this rule, many personal details were already refused, and the law that was previously *de facto* has now been changed into *de jure*, leading to an increase in corruption and wrongdoing.

- **Need for Unblemished Law on Data Protection in India**

As per the reports of UN, India is set to be the most populous country of the world in the coming years. This growing population therefore means increased interference with the digital devices and the internet, consequently resulting in a humongous amount of generated digital data by the users or the "data principals." This data, which is largely available on the internet, can be effectively accessed and used by the mega-companies or organizations which are referred to as "data fiduciaries" sometimes even without intimidating the data privacy and infringing their Right to Privacy which is a fundamental right under Article 21 of the constitution. India, for long, has struggled to table a nearly flawless and not-so-controversial law on privacy. The

 [ISSN 2581-5369]

present legal framework which primarily governs privacy nearly fails to keep up with the technological advancements and the growing exigency to have a proper data protection law, especially after the aforementioned 2017 judgement of privacy. Thus, the need to enact an unblemished law on privacy and data protection in India is undisputed.

- **Deviation of the Latest Bill from The Personal Data Protection Bill,2019**

As opposed to 90 in the previous version, the Digital Data Protection Bill, 2022 has only 30 clauses. It means that a big but crucial fragment of subsequent rulemaking has been delegated, which raises concerns about excessive delegation. The 2022 version of the bill only covers the automated or digital data and not manual data. Also, some provisions of the 2022 bill are deemed imprecise or vague in certain aspects. For instance, the definition and degree of public interest "in public interest" can be subject to misinterpretation. The phrase "as may be prescribed" has been used around 18 times in the bill. The bill indirectly gives excess powers to the Center.

Another and one of the most crucial changes which have been made in this version of the bill for the good is in the matter of cross-border data flow. The present bill allows for the free movement of data across borders or the cross-border flow of data. It allows for the data transfer to countries and territories which would be notified by the Central government.

- **The Unbriddled Powers Vested With The Center**

Leaving a huge chunk of the critical operative part of the bill for subsequent rule-making for the Central government and a few provisions of the bill is evidence of the excess power that has been vested with the Center.

For instance, clause 19 of the bill talks about the Data Protection Board of India. According to the provisions of the bill, the board, which will have the powers equivalent to that of a civil court, would entirely be constructed by the Central government. The strength, functioning, appointment, and removal of its officials must be "as may be prescribed" by the provisions of Central government. Instead, the board should function independently of the government and should be able to adequately implement the rights which are fundamental to the citizens ensuring justice.

Furthermore, the bill authorizes the Central government to exempt any State body, which it deems fit, to be exempted from it. This authority will not only grossly violate the principles of natural justice but also aid those who are corrupt. Empowering the government to this extent is unacceptable in a democratic country.

 [ISSN 2581-5369]

VI. CONCLUSION

The Privacy rights of an individual are quite an integral part for the growth of their personality also the concept of privacy should always be applied uniformly and properly. Due to the rapid growth of technology and the overburdening emphasis over technology has lead to a huge threat upon the concept of privacy for individuals. The concept of Privacy and Data Protection being related to each other can be defined as twins but not identical to each other. Further new means of Cyber violations such as spamming , cookies theft as well as identity theft have been skyrocketed and there is a need for a comprehensive regulation as regard to privacy.

In the Indian context it is observed that the legislature while protecting the rights of the data principal, the data protection laws must ensure that the necessary compliances for the data fiduciaries are not so onerous as to further making even the legitimate processing impractical. The big challenge which should be addressed is finding an proper balance as to the right to privacy of data principals and also the reasonable exceptions especially where the processing of personal data is concerned with the government. The rate at which the technology is evolving must lead to the optimum data protection law design that needs to be future proof according to needs of future. It should not be focused on giving solutions to the concerns of the present are prioritised over those that may arise in the future.

*****

 [ISSN 2581-5369]

VII. REFERENCES

(A) Books

- Rodney Ryder, "'Guide to Cyber Laws", Wadhwa Nagpur, 2nd Edition, 2003
- Vakul Sharma, "Information Technology: Law and Practice", Universal Law Publishers, 2nd edition, 2007.
- Vakul Sharma, "Handbook of Cyberlaws", Universal Law Publication, Reprint Edition 2010

(B) Articles and papers

- Veale, Michael, et al. "Algorithms That Remember: Model Inversion Attacks and Data Protection Law." *Philosophical Transactions: Mathematical, Physical and Engineering Sciences*, vol. 376, no. 2133, 2018, pp. 1–15. *JSTOR*, https://www.jstor.org/stable/26601843.
- Duraiswami, Dhiraj R. "Privacy and Data Protection in India." *Journal of Law & Cyber Warfare*, vol. 6, no. 1, 2017, pp. 166–86. *JSTOR*, http://www.jstor.org/stable/26441284.
- Voss, W. Gregory. "European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting." *The Business Lawyer*, vol. 72, no. 1, 2016, pp. 221–34. *JSTOR*, https://www.jstor.org/stable/26419118.
- Kulhari, Shraddha. "Data Protection, Privacy and Identity: A Complex Triad." *Building-Blocks of a Data Protection Revolution: The Uneasy Case for Blockchain Technology to Secure Privacy and Identity*, 1st ed., Nomos Verlagsgesellschaft mbH, 2018, pp. 23–37. *JSTOR*, http://www.jstor.org/stable/j.ctv941qz6.7.
- http://www.sciencedirect.com/science/article/pii/S1449403505700643
- https://www.insightsonindia.com/2022/03/05/data-protection-bill-2/
- https://www.medianama.com/2022/03/223-deep-dive-data-protection-bill-impact-social-media-platforms/

*****

 [ISSN 2581-5369]