SUPREMO AMICUS

VOLUME 36 | December, 2024 ISSN 2456-9704

AN ANALYSIS OF DATA PROTECTION LAWS IN INDIA: WITH SPECIAL REFERENCE TO RIGHT TO BE FORGOTTEN

By *Nuvita Kalra*
Research Scholar, *Rajiv Gandhi National University of Law, Punjab*

Abstract
With the recognition of right to privacy as a fundamental right in *K.S.Puttaswamy v. Union of India*[1] in 2017 began the efforts to legislate upon data protection laws in India. After approximately half a decade spent on introducing a law regulating data protection laws in India, the Parliament enacted the Digital Personal Data Protection Act, 2023. Data protection guarantees a bundle of rights, the most prominent being right to be forgotten. This right allows an individual to request deletion of their personal information on the internet. It allows the individual to be in control of their data guaranteeing autonomy over the information. However, the right which found its due recognition under the GDPR in European Union is yet to find a definitive place in Indian scenario. The 2023 Act has included right to erasure including the principles of right to be forgotten, however, the implementation of it is still in question. The current research explores the development of data protection laws in India, highlighting the importance of right to be forgotten under the umbrella of data protection.

Keywords: Right to be Forgotten, Right to Privacy, Data Protection, DPDPA, Consent

1. Introduction

The world has now been reduced to a global village with people from different parts of it being connected to each other through the innovation of internet, famously referred to as the 'world wide web'. The emergence of information technology has brought about a change not only in the way we communicate but has had an overall impact on the way we live our lives. Thus, a mobile application which was developed in United States with no relation whatsoever in Asia can have people using that application in Asia.

In India, there has been a huge growth of internet users, especially due to easy and cheap availability of mobile phones and also due to increased activities through Internet as a consequence of the Covid-19 pandemic. Realizing the importance of the internet and the digital world, the Government of India has been pushing towards digitization of services by launching various programmes, the most prominent one being 'Digital India' which was launched in the year 2015. The objective of the Government, with this initiative is to make technology accessible and affordable.[2]

There has been a surge of Internet users in India from 795.18 million in 2020 to 825.30 million in 2024, with a quarterly growth rate of 3.79%.[3] About 43 percent of the total population in India uses the Internet at least once a month at present and Maharashtra has the highest Internet penetration in India with 61 percent of the population using it.[4]
This revolution caused by information technology has led to the production of huge amount of data. Data are the building blocks of information of the modern world. Businesses now rely on the collection of this

[1] Justice K.S.Puttaswamy (Retd.) & Anr. V. Union of India & Ors 2019 (1) SCC 1
[2] Ministry of Electronics and Information Technology, *Report on India's Trillion Dollar Digital Opportunity* (Government of India, 2024) ch 1.
[3] Telecom Regulatory Authority of India, *Report on The Indian Telecom Services Performance Indicators* (New Delhi, 2024) ch 1.
[4] IAMAI and KANTAR, *Report on Internet Adoption in India (ICUBE 2020)* (June 2021) <https://images.assettype.com/afaqs/2021-06/b9a3220f-ae2f-43db-a0b4-36a372b243c4/KANTAR_ICUBE_2020_Report_C1.pdf> accessed 14 January 2025.

data for providing services to their consumers instead of the age old concept of money in exchange of the services provided. This has given rise to the concept of Big Data wherein a bulk of information is accumulated from different sources including social media, websites, company database etc. It is being used by for data-driven marketing and digging in customer data to create tailor-made products, services, offers, discounts, etc. With the influx of new technology, targeting connectivity between different sets of data, particularly Big Data analytics, data processing or mining has become the core aspect of most of the businesses.

The benefits of data are derived not only by the private corporations and businesses but also by government by employing them in different sectors such as banking, telecom, health etc.

Data is broadly classified as personal and non-personal, depending upon the nature of the data and its capacity of identifying the data subject. Personal data refers to the kind of data through which the data subject may easily be identified whereas non-personal data is that which is partially anonymised or pseudonymised, thus making it difficult to identify the data subject. Personal data includes information such as name, phone number, email, address etc. It also includes certain sensitive information about the data subject i.e. sexual orientation, health records, biometric details etc.

There are a lot of ways through which data is collected and one such mechanism is through 'cookies'. The cookies allow a website to collect information from a user who visits a website in order to remember the user's actions or preferences over a period of time. As far as laws with respect to cookies in India are concerned, it is observed that there is no law that compels websites in India to provide for a cookie policy or take consent of the user prior to collecting information through cookies as it is not considered within the purview of personal data, which is quite commonly found in European websites.

Research Methodology

The researcher has conducted an analytical study of the legal framework dealing with data protection using primary data consisting of primary documents such as Draft Bills, Committee Reports, GDPR, DPDA, Information Technology Act 2000, etc. as well as secondary data including books, article, case comments etc.

2. Right to Privacy

The basic idea behind privacy has been to provide freedom to a person to be left alone. Therefore, privacy allows a person to prevent others from intruding in one's physical space. Right to privacy implies that a person has the right to enjoy his life without any kind of interference from others.

In the virtual world, the concept of privacy has undergone a slight change and it has assumed importance now more than ever. Here, it relates to the ability to control the dissemination and use of one's personal information. Since the data relates to natural persons, they should have the right over what happens with that data and not private corporations.

In India, it was only recently in the year 2017 that right to privacy was elevated to be a fundamental right and read as a part of right to life and personal liberty under Article 21 of the Constitution of India.[5] However, as any other right, even right to privacy is not absolute in nature and can be curtailed in certain exceptional circumstances if the same is required in public interest. The Supreme Court was of the opinion that if the following three conditions are satisfied, the taking away of right to privacy of an individual or a group may be justified:

1. Legality
2. Legitimacy
3. Proportionality

[5] *Justice K.S.Puttaswamy (Retd.) v Union of India* [2017] 10 SCC 1 (SC).

The Court, through this judgment, took note of the emerging concept of information privacy. An individual has the freedom to choose any medium, as per his preference to express his views and opinions and the State cannot interfere with an individual's choice. There is a duty upon the State to ensure that whatever information is generated while an individual exercises such choice, should become the property of the individual unless provided by law.

Applying the principles of the above judgment, the Supreme Court had in the case of *Indian Hotel and Restaurant Association v. State of Maharashtra*[6], held that data which is stored through CCTV cameras comes under the purview of personal information of an individual as it is quite easy to identify the individual through the CCTV footage.

Even though the Supreme Court had taken a step in the right direction in guaranteeing right to privacy as a fundamental right and also recognizing the growing need of informational privacy, it is observed that the Government of India has not been too keen on the implementation of the said right.

4. Development of Data Protection in India

4.1. Information Technology Act, 2000 and SPDI Rules, 2011

The legislators in India have always played catch up when it comes to introducing laws with respect to technological advancements. The core law dealing with Internet and cyberspace in India called the *Information Technology Act*, 2000 (hereinafter referred to as the IT Act, 2000) has only been amended a few times as opposed to vast technological changes that have taken place in the last decade. This lack of initiative by the government to regulate cyberspace has given a head start and an unfair advantage to the stakeholders involved.

It was only in the year 2011 that the government recognized the importance of placing some kind of regulation on the collection and use of personal data. Thus, the *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules* (hereinafter referred to as the Rules) were introduced. The Rules defined as to what constitutes as sensitive personal information[7] and also imposes an obligation on body corporates collecting, processing and storing personal information to comply with certain procedural requirements provided under the Rules. However, the application of the Rules had been restricted to body corporates and the same had not been made applicable to government or its entities while dealing with the data of its citizens. This shows reluctance on behalf of the government to regulate its own affairs when it comes to dealing with the data of its citizens.

The *IT Act*, 2000 has also provided for certain civil as well as criminal liabilities against service providers, in case of disclosure of an individual's personal information. However, there is no dedicated authority which deals with the compliance of the said rules, making its implementation haphazard and weak.

The *IT Act*, 2000 deals with only a small sphere of data protection as a plethora of other legislations provide for data protection either directly or indirectly. Thus, there was no specific or comprehensive law dealing exclusively with data protection in India, and each sector has its own set of laws regulating data processing. This led to overlapping in certain circumstances. The other legislations include the *Indian Contract Act*, 1872; *Credit Information Companies (Regulation) Act*, 2005; *Indian Copyright Act*, 1957 etc.

The various gaps in Indian legislations with respect to data protection have been taken advantage by various groups, specially the private corporations. One such incident that highlighted this issue was an attempt to update the social media messaging application WhatsApp's privacy policy in the year 2021. The application had sought to collect data from business accounts and share the same with Facebook and other businesses. The data to be collected included

[6] *Indian Hotel and Restaurant Association v. State of Maharashtra* [2019] 1 SCC 45 (SC).

[7] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, r 3.

information such as phone number, IP address, transaction details etc. The Ministry of Information and Technology had directed WhatsApp to withdraw the said policy as it was against the principles of data privacy and also it was discriminatory of the company to impose the policy compulsorily as opposed to the freedom given to users in Europe to opt out of the said policy without any consequences.[8] The application was also alleged to have misused its dominant position in the Indian market. The issue is presently sub judice and the application of the policy for users who did not consent to the same has been put on hold.[9]

As noted earlier, it is not only the private corporations that are taking an advantage of the lacunas in legal framework with respect to data protection but the government itself has not been willing to put restrictions on its power and usage of data of the citizens which becomes apparent through the ever expanding surveillance powers of the government. *The Indian Telegraph Act*, 1885, passed during the colonial period and also the *Indian Telegraph Rules*, 1951 have given wide powers to the government as well as law enforcement agencies to intercept information on the condition that they have received authorization for the same from the Ministry of Home Affairs. Theoretically, there is a comprehensive review mechanism to ensure that this provision is not misused. However, as far as practical application is concerned, it is often seen that the provisions are not applied strictly. [10]

The Snowden controversy in United States of America highlighted how States can misuse the data of its own citizens under the garb of national security or public interest and carry out mass surveillance and profiling without any valid justifications or reasons. These are the features of a surveillance State which tries to be non-transparent on it and at the same time keeps a constant watch over its citizens.

A National Intelligence Grid (hereinafter referred to as NATGRID), NETRA (Network Traffic Analysis) and CMS (Centralized Monitoring System) are some of surveillance projects that are to be established by the Ministry of Home Affairs under anti-terrorism measures. The objective of the NATGRID project is to collect information such as travel details, financial information, income tax details etc. and become a centralized database for different intelligence agencies. The solutions provided by NATGRID would be technology sensitive, i.e. they would involve use of Big Data and analytics. However, the said projects are currently being challenged before the Delhi High Court[11] as an infringement of Right to privacy of citizens as it would involve interception of communications of citizens involving telephonic as well as internet communication in bulk without any reasonable basis.[12]

Such data driven surveillance projects pose a risk to the security of the personal information being gathered belonging to the citizens, which has

[8] PTI, 'IT ministry directs WhatsApp to Withdraw New Privacy Policy: Government Sources' (*The Times of India*, 19 May 2021) <https://timesofindia.indiatimes.com/business/india-business/centre-reiterates-demand-for-withdrawal-of-whatsapps-new-privacy-policy/articleshow/82764544.cms> accessed 10 January 2025.

[9] Sofi Ahsan, 'WhatsApp to Delhi High Court: Will not compel Users to accept Privacy Policy' (The *Indian Express,* 10 July 2021) <https://indianexpress.com/article/cities/delhi/whatsapp-privacy-policy-delhi-high-court-7396439/ > accessed 10 January 2025.

[10] EPW Engage, 'What Enables the State to Disregard the Right to Privacy?' (*Economic & Political Weekly,* 16 January 2019) < https://www.epw.in.rgnul.remotexs.in/engage/article/what-enables-state-disregard-right> accessed 13 January 2025.

[11] *CPIL v Union of India* <https://sflc.in/legal-challenge-cpil-and-sflcin-surveillance-projects-cms-natgrid-and-netra> accessed on 12 December 2024.

[12] PTI, 'National Intelligence Grid to finally see Light of Day' (*The Hindu,* 12 September 2021) < https://www.thehindu.com/news/national/national-intelligence-grid-to-finally-see-light-of-day/article36414741.ece> accessed on 12 December 2024.

particularly come to light through another controversy. Pegasus is the name of a malware categorized as a spyware, developed by an Israeli firm called NSO Group. The spyware gained access to the mobile phones of the targeted user through "zero click attacks" which means that the malware was able to gain access of the device even without any action allowing the same by the user. Thus, through the spyware, the firm gained access to the emails, texts, social media messages, camera, video etc. of the targeted user. The website of the firm disclosed that it sells the software only to "certain undisclosed Governments" and that their end users are intelligence and law enforcement agencies. This software was used against people all over the world, including India where about 300 people were found to be its victims. The Supreme Court[13] while constituting a Committee to investigate the allegations of involvement of the Government of India in using Pegasus for spying on private citizens drew a link between surveillance and self-censorship. The knowledge that one is under the threat of being spied on leads to self-censorship and potential chilling effect. The chilling effect surveillance can produce is an assault on the vital public-watchdog role of the press, which may undermine the ability of the press to provide accurate and reliable information.

In an earlier incident in 2019, it was alleged that NSO's software was used by Government to exploit a vulnerability in WhatsApp to illegally spy on 24 citizens, and hack as many as accounts of 121 Indians.[14]

In recent years, the State has realized the importance of data protection and has made attempts to introduce certain measures for providing the same. This includes introducing a legislation specifically dealing with data protection.

This was mainly triggered as a consequence of the *Facebook-Cambridge Analytica* case in the USA wherein it was found that the data of around 87 million Facebook users was used for influencing elections by the political consulting firm Cambridge Anlaytica.[15] The aspect that left everyone surprised was that this was done without the permissions of the users. A pseudo application was created on Facebook which ended up collecting the data of not only the people that were using the application but also of friends of those users. This incident particularly brought to light how data processing can be used for manipulating the opinions and preferences of the people and they have no idea that they are being manipulated.

The government in India has been making attempts for legislating since the year 2017, however it was only in 2023 that the Digital Personal Data Protection Act (hereinafter referred to as DPDPA) was enacted. Prior to this, the Government had made efforts in the form of certain draft bills for data protection which could not materialize due to various reasons.

4.2. Draft Bills of 2018, 2019 and 2021

In 2017, an expert committee was set up by the Ministry of Information and Technology to assess data protection and regulation in India, headed by retired Justice B.N.Krishna. The Committee submitted a report along with a draft bill on data protection in the year 2018 called the *Personal Data Protection Bill*, 2018 (hereinafter referred to as the 2018 Bill). The Union Government introduced a Bill to the Parliament in the year 2019 (hereinafter referred to as the 2019 Bill), which was referred to a Joint Parliamentary Committee. The Committee tabled its report in 2021 making policy recommendations along with a Draft

[13] *Manohar Lal Sharma v Union of India* <https://main.sci.gov.in/pdf/LU/27102021_082008.pdf> accessed on 20 December 2024.

[14] Mishi Choudhary, 'Pegasus scandal points to the making of a surveillance state in India. Our freedoms are at stake' (*The Indian Express*, 10 August 2021) <https://indianexpress.com/article/opinion/columns/pegasus-spyware-surveillance-state-indian-govt-freedom-7446179/ > accessed on 14 January 2025.

[15] Becky Hogge, Travel Guide to the Digital World: Data Protection for Human Rights Defenders' (Global Partners Digital, 11 July 2018) < https://www.gp-digital.org/publication/travel-guide-to-data-protection/> accessed on 25 December 2024.

Data Protection Bill, 2021 (hereinafter referred to as the 2021 Bill).

There had been a plethora of changes in the proposed legislation of 2021 as compared to what was initially recommended under the 2018 Bill.[16] There was lesser focus on rights of the user and more on carving out exceptions from applicability of the law to the State. A few of the differences in the draft legislations over the years have been listed below:

1. Following its previous trend of imposing lesser regulation on government and its agencies, the 2019 Bill as well as the 2021 Bill have empowered the government i.e. the executive to exempt itself from the application of provisions of the law, as opposed to the conditions provided in *Puttaswamy*[17] judgment wherein privacy could be taken away only through a law made by Parliament and the same was necessary and proportionate.

2. The 2018 Bill had proposed for an independent Data Protection Authority which would be responsible for implementation of the law. In contrast, the Draft Data Protection Bill, 2021 made the Union Government the sole authority to determine the composition of the Authority despite the fact that the Authority will also regulate government agencies.

3. The 2018 Bill provided for personal data to be processed on the basis of consent of the data principal which had to be free, informed and clear and capable of being withdrawn at a later stage. Under the 2019 Bill, the provision on consent was made non applicable for the performance of any function of the State authorized by law for the provision of any service or benefit to the data principal from the State or for issuance of any certification, license or permit for any action of the data principal.

4. The 2018 Bill recognised the right to be forgotten for the first time in India and had provided that the data principal shall have the right to restrict or prevent continuing disclosure of personal data by a data fiduciary related to the data principal on the grounds of fulfilment of purpose for which data was collected or the disclosure no longer being necessary. However, the right may only be enforced if an application to be forgotten is approved by an Adjudicating Officer appointed by the Union Government. The 2019 Bill had accepted the provisions of the previous Bill but the right would be available on the condition that the data principal would have to demonstrate to the Adjudicating Officer that their right in preventing disclosure of personal data overrides the right to speech/receive information of any other citizen. The 2021 Bill has recommended to expand the right to be forgotten for processing as well which was previously limited to only disclosure.

5. The Bill of 2019 removed 'passwords' from the definition of sensitive personal data which was included in the 2018 Bill. Moreover, it provided power to the Central Government after consultation with the Data Protection Authority to classify any data as sensitive personal data whereas under the 2018 Bill the power was given exclusively to the Data Protection Authority.

6. A very peculiar alteration has been proposed in the 2021 Bill as the Joint Parliamentary Committee has recommended applying the same legislation to processing of both personal as well as non-personal data thus,

[16] Internet Freedom Foundation, 'Comparing the Draft Data Protection Bill, 2021 with its Predecessors' (*Internet Freedom Foundation,* 2021) <https://internetfreedom.in/comparing-pdpb/> accessed on 12 January 2025.

[17] *Justice K.S.Puttaswamy (Retd.) v Union of India* [2017] 10 SCC 1 (SC).

removing the word 'Personal' from the said Bill. However, there has not been any such legislation in other jurisdictions which may have combined the regulation of both personal as well as non-personal data under a single framework.

All these frequent changes in the draft legislations bring out the uncertainty of the legislators with respect to data protection and regulation. Even the bill proposed by the Joint Parliamentary Committee, submitted after two years of deliberations appears to be flawed in many aspects. The bill fails to make the government accountable for the surveillance activities carried out and has in fact, expanded this power in certain aspects. It appears as if the legislators have forgotten the objective behind the legislation of providing protection to the data of the users in order to ensure their data privacy and are now more concerned with providing unfettered powers as well as protection to the Government.

4.3. Digital Personal Data Protection Act, 2023

The law has been enacted after more than half a decade of efforts and deliberations on the law related to Data Protection in India. The objective of the DPDPA is to protect the rights of the individual as far as their personal data is concerned and also to regulate processing of personal data for lawful purposes. The processing can take place either with the consent of the user or for lawful purpose which has been defined under the law. Individuals also have the right to correction, completion, updating, and erasure of their data.

The Act has also added another category of data fiduciaries known as Significant Data fiduciaries. Additional responsibilities have been imposed on them considering that they deal with high volume of sensitivity of data.

As far as the regulatory under the Act is concerned, it has made a departure from the structure of authority as proposed under the 2019 Bill. The earlier Bill had proposed establishment of Data Protection Agency, conferring powers on the authority akin to those exercised by such authorities in European countries. It was also supposed to be an independent body, and not working under the influence of the Government. However, the Act has scrapped off the Authority and has instead established the Data Protection Board. In comparison to the Authority, the Board has lesser powers as far as remedial action, conduct of inquiries and issue of penalties for non-compliance is concerned. The Board has not been given the power to frame code of conduct or any regulations.

5. Consent based Approach to Data Protection

The data protection laws in India tend to work on the pretext that the data subject is responsible for their own data and thus, if they have given their consent for the processing of their data, then the processors would not be bound for any kind of liability. This 'consent' is obtained through terms of service or privacy policies that are displayed prior to using of the services and only if the consent has been given, the user would be able to avail the services.

There are a lot of complications that are involved with this consent based approach. The approach has been based on the assumption that such consent shall be informed and free. The problem arises because these privacy notices are often in the form of long legal documents which is difficult to understand by a common man. They are often lengthy with complicated and ambiguous words.[18] It becomes a challenge for the users to comprehend as to how their data is going to be processed and ultimately used.

Moreover, with the kind of dependency that has evolved with respect to the internet and information technology services, data is collected continuously making it humanly impossible to exercise meaningful consent. If a person is expected to go through the

[18] Amber Sinha and Arindrajit Basu, 'The Politics of India's Data Protection Ecosystem' (*Economic and Political Weekly Engage,* 27 December 2019) < https://www.epw.in.rgnul.remotexs.in/engage/article/politics-indias-data-protection-ecosystem> accessed on 12 January 2025.

privacy notices of all the applications and websites that he or she utilizes in a day, the entire day would be spent going through the policies and still they might not be able to go through them all!

To expect that in a country like India, where most of the citizens are affected by poverty and illiteracy, should have to constantly keep a check with respect to the collection and usage of their data, even from their own government is a gross violation of their rights and thus, not much care and attention has been given to this particular issue. Even the most educated people often do not comprehend the privacy notices and are not aware of what rights they are giving up when they tick the "I accept" box at the bottom of the terms and conditions of service.[19]

6. Right to be Forgotten: An Emerging Right in the Digital Era

With every type of information being only a click away, a lot of personal information that is found on the internet could invade the privacy of an individual. This has given rise to the concept of right to be forgotten and right to erasure wherein the person to whom the information belongs to, has the right of getting that piece of information or data removed from the internet. The right came into limelight with the decision of the European Court of Justice in the case of *Google Spain v. AEPD and Mario Costeja Gonzalez*[20]. The Court included internet search engines within the purview of data processors and held that they must consider requests from individuals to remove links to information available online that results from a search of the person's name. Thus, this right is considered as an extension of right to privacy wherein the person with respect to whom the information is stored, has the right to remove that information. Consequently, the said right was incorporated under the General Data Protection Regulation. The Regulations do not differentiate between right to be forgotten and right to erasure. There appears to be conflicting opinions with respect to necessity of right to erasure. There are some who view the right as a necessary subset of right to privacy and data protection as it allows people to truly have control over their data. On the other hand, there are others who believe that conferring such a right to the people is in direct conflict with the freedom of expression and/or right to information of all the other people.

Right to be forgotten is basically an individual's right to have personal information removed from the publicly available sources, such as the internet, search engines, databases, websites etc. once the information is no longer necessary or relevant.[21]

Presently, in India, there is no legislation that guarantees this right to its citizens. However, the *Data Protection Bill* of 2019 as well as 2021 has provided provisions referring to right to be forgotten as well as right of erasure.

Clause 18 of the 2019 and 2021 Bill provides the following rights of correction and erasure, namely the right to

"(i) get corrected inaccurate or misleading personal data,
(ii) get completed any incomplete personal data,
(iii) get updated personal data that is out-of-date, and
(iv) get erased personal data which is no longer necessary for the purpose for which it was processed."

If a data principal wishes to exercise his/her right to erasure, they will have to put a request for the same to the respective data fiduciary. However, the data fiduciary may reject the request, if it is of the opinion that that such erasure or correction etc. is not required and shall provide the reasons for doing so to the data

[19] Ibid.
[20] Case C-131/12 *Google Spain SL and Google Inc*. v. *AEPD* [2014] ECR< https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0131&from=EN > accessed on 2 December 2021.
[21] General Data Protection Regulation (EU) 2016/679 [2018] OJ L 127, art 17.

principal. If the data principal is not satisfied with the justification provided by the data fiduciary for rejecting the data principal's request, the data principal may require that the data fiduciary take reasonable steps to indicate, alongside the relevant personal data, that the same is disputed.

The right to erasure provided for in Clause 18 of the 2019 Bill needs to be distinguished from the right to be forgotten, provided for in Clause 20 of the 2019 Bill. As per the aforementioned Clause 20, every data principal shall have the right to restrict or prevent continuing disclosure of personal data (relating to such data principal) by any data fiduciary if such disclosure meets any one of the following three conditions, namely the disclosure of personal data:

"(i) has served the purpose for which it was collected or is no longer necessary; or

(ii) was made on the basis of the data principal's consent and such consent has since been withdrawn; or

(iii) was made contrary to the provisions of the personal data protection act or any other law in force."

Thus, unlike the right to erasure, a data principal's right to be forgotten can only be enforced by an order of the Adjudicating Officer. Despite the usage of the word 'forgotten', there is no right of erasure under Clause 20. Instead, it merely restricts or prevents continuing disclosure of personal data.

Under the DPDPA, the right to be forgotten, which was expressly mentioned as a separate right has now been recast as a right to erasure. Section 12 of the Act has allowed individuals to request deletion of their personal data under the following conditions:

1. The purpose for which the data was collected is no longer valid.
2. The consent for processing of data has been withdrawn.
3. Retention of data is no longer required under the applicable law.

Even though the Act has recognised the Right to be forgotten in some form, however, its implementation will be dependent on rules and guidelines, which are yet to be introduced. Thus, the procedure for requesting deletion of information is yet to be established. Another lacuna in the provision is that it does not recognise automatic deletion of data, a practice recognised under the GDPR. Instead, even though the intended purpose for which the data was collected or processed is complete, the data principal would have to request the deletion of even that data.

Though, no law yet has been enacted which recognizes right to be forgotten in India, the courts, especially High Courts, have stepped up to implement the said right. The courts have expressed the opinion that even though the right has not been formally recognized under a specific statute, but the same may be inferred from other legislations and thus people may seek relief from the courts to remove certain contents from the internet under other legal provisions such as defamation, indecency and obscenity, intellectual property law violations etc. till *Personal Data Protection Bill*, 2019 comes into effect.

In the case of *Dharmaraj Bhanushankar Dave v State of Gujarat*[22], a petition was filed seeking removal of a judgment in which the petitioner was an accused. He was acquitted in the said case and even though the judgment was non-reportable, the petitioner said that the copy of the judgment was available online for all to see. However, the court refused any kind of relief to the petitioner and thus 'right to be forgotten' was not recognized by the Gujarat High Court.

An opposite view was taken by the Karnataka High Court wherein the court recognized right to be forgotten as a right which was in trend in western countries and therefore, is necessary to be incorporated in the country as well.[23]

The Orissa High Court for the first time discussed the provisions of the Personal Data Protection Bill, 2019 during proceedings, in the case of *Subhranshu Rout @*

[22] *Dharmaraj Bhanushankar Dave v State of Gujarat* [2015] SCA No. 1854 of 2015.

[23] *(Name Redacted)* v. *The Registrar, Karnataka High Court* [2017] SCC OnLine Kar 424.

Gugul v. *State of Odisha*[24] and remarked that "*information in the public domain is like toothpaste, once it is out of the tube one can't get it back in and once the information is in public domain it will never go away*".

The Madras High Court also observed that, "*an accused person who is acquitted of all charges is entitled to have his name redacted from all court orders in relation to the offence he was accused of in order to uphold his fundamental right to privacy.*"[25]
Recently, the Delhi High Court[26] had made passed an interim order protecting the rights of an American citizen. The court directed Google and IndiaKanoon to remove access to a judgment from their portals which relates to acquittal of the petitioner. The court remarked that a balance has to be created between right to be forgotten and the right of the public to access court records.
Thus, there have been conflicting views of different High Courts as far as the recognition of right to be forgotten in India is concerned.

7. Conclusion

There is no denial of the fact that data is evolving to be the currency of the new world. It has great economic as well as social value. However, since the data relates to a natural person and often consists of sensitive information related to them, it becomes important to protect it. From information shared on social media sites, to cookies collecting user browser history, to individuals transacting online, to mobile phones registering location data – information about an individual is generated through each use of the internet. In some cases the individual is aware that they are generating information and that it is being collected, but in many cases, the individual is unaware of the information trail that they are leaving online, do not know who is accessing the information, and do not have control over how their information is being handled, and for what purposes it is being used.[27]
Thus, if the data is not protected, such information may easily be misused by any person or organization for their own benefit. Therefore, there is a responsibility to not only protect the data from any kind of security breaches so that the data of the data subjects are protected but the same is necessary to enforce their right to privacy.

Even though the efforts made to introduce the DPDPA are commendable, however, the Act still suffers from various defects. There still persists a looming uncertainty regarding the implementation of the law and the procedure to be adopted for various enforcement mechanisms.

Right to be forgotten is an important aspect of right to privacy and data protection shall be incomplete without the recognition of right to be forgotten. Despite the fact that through various decisions of the High Courts the right is being applied but the scope of the same remains to be uncertain in India. Under the DPDPA, the right has not been given a separate recognition and has been brought under the right to erasure. Moreover, the enforcement of the right is dependent on future guidelines and rules, yet to be introduced. Thus, there is a need to provide clear guidelines regarding the procedure to be followed for requesting deletion of data.

*****

[24] *Subhranshu Rout @ Gugul* v. *State of Odisha* [2020] BLAPL No. 4592 / 2020.
[25] *Karthick Theodore v. Madras High Court* [2021] SCC OnLine Mad 2755.
[26] *Jorawar Singh Mundy v Union of India* [2021] W.P.(C) 3918/2021 & CM APPL. 11767/2021.
[27] Centre for Internet and Society, 'Internet Privacy in India' (*The Centre for Internet and Society)* < https://cis-india.org/telecom/knowledge-repository-on-internet-access/internet-privacy-in-india> accessed on 14 January 2025.

8. References

Duraiswami DR, *Privacy and Data Protection in India*, Journal of Law and Cyber Warfare, Vol. 6(1) (2016).

Floridi L, *Right to be Forgotten: A Philosophical View*, Annual Review of Law and Ethics, Vol. 23 (2015).

Joshi AS, *Leave me Alone! Europe's Right to be Forgotten*, Litigation, Vol. 41(2) (2015).

Kemp K and Buckley RP, *Protecting Financial Consumer Data in Developing Countries: An Alternative to the Flawed Consent Model*, Georgetown Journal of International Affairs, Vol. 18(3) (2017).

Kumar A, *The Right to be Forgotten in Digital Age: A Comparative Study of the Indian Data Protection Bill, 2018 & the GDPR*, Shimla Law Review, Vol. 2 (2020).

Lozano GMT, *Fundamental Rights in the Digital Society*, Revista Chilena de Derecho, Vol. 46(1) (2019).

Newman AL, *What the right to be forgotten means for privacy in a digital age*, Science, New Series, Vol. 347 (2015).

Richterich A, *The Big Data Agenda*, University of Westminster Press (2018).

Singh SS, *Privacy and Data Protection in India: A Critical Assessment*, Journal of the Indian Law Institute, Vol.53(4) (2011).

Singh A, *Data Protection: India in the Information Age*, Journal of the Indian Law Institute, Vol. 59(1), pp. 78-101 (2017).

Linscott M and Raghuraman A, *Aligning Data Governance Frameworks*, Atlantic Council (2020).

Mahapatra S, *Digital Surveillance and the Threat to Civil Liberties in India*, German Institute of Global and Area Studies (2021).

Kothari CR, *Research Methodology: Methods and Techniques* (4th edn New Age International Limited 2019).