INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 4 | Issue 2

2021

Right to Erasure and Whatsapp's Privacy Policy: An Analysis

ANU SINGH[1]

ABSTRACT

Right to erasure derives its roots from Europe and has grown worldwide. This right came to limelight from the Google Spain case paving its way through the GDPR (General Data Protection Regulation). Recognizing the importance of this right, the Personal Data Protection Bill, 2019 introduced the right to be forgotten in India. But when WhatsApp introduced its new privacy policy it seemed to be in paradox with the fundamental right of privacy as well as right to be forgotten. This research paper analyses:

(a) The contradiction between the privacy policy of WhatsApp and right to erasure;

(b) The role of intermediary in the protection of the right to erasure.

The findings of this research show that the weak and insufficient provisions of the Information Technology Act, 2000 and The Information Technology (Intermediaries Guidelines) Rules, 2011 with Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018 are the main reason that India remain to fail in protecting the Indian users of such applications. This research paper also suggests implementing Uncompromising and stringent policies for the intermediaries by the government to create a deterrent effect.

Keywords: *erasure, privacy, data protection, information, WhatsApp*

I. INTRODUCTION

The dawn of technology also gave birth to the intimidation allied with it. The European Union was aware of the upcoming threats which were associated with the advancement of technology; they prepared European Data protection Directive in the year 1995; it set the optimum criterion for the requirement of data protection. In 2016 the General Data Protection Regulation superseded the 1995 directive, and strengthens the privacy laws in the European Union. But in India the lack of such laws give opportunity to social media applications to access and use the user data without any trouble. With more than 1.5 million users in India, whatsapp puts itself in a dominant position. So when the company declared its new privacy policy they knew that

[1] Author is an Assistant Professor at Invertis Univrsity Bareilly, UP, India.

 [ISSN 2581-5369]

one day or other the users will have to agree with the terms and conditions as the application has become an essential part of people's life. The right to erasure which is a counterpart of the right to privacy was certainly affected by this privacy policy.

II. RIGHT TO ERASURE

Right to erasure was acknowledged by the European Union's Court of Justice in the case of Google Spain SL, Google Inc. v Mario Costeja González[2]. In March 2010, Spanish national Costeja González brought a complaint before the country's Data Protection Agency against *La Vanguardia* newspaper, Google Spain, and Google Inc[3]. González wanted the newspaper to remove or alter the record of his 1998 attachment and garnishment proceedings so that the information would no longer be available through Internet search engines[4].Mr. González demanded the data to be deleted as it was no longer vital or pertinent for anyone. The Data Protection Agency disregarded the complaint against the newspaper on the saying that the publication of the article was according to the government orders. It, however, upheld the complaint against Google, finding that Internet search engines are also subject to data protection laws and must take necessary steps to protect personal information.[5]

The European Court of Justice ruled that the European citizens have a right to request that commercial search engines, such as Google, that gather personal information for profit should remove links to private information when asked, provided the information is no longer relevant. [6]

The Court found that the fundamental right to privacy is greater than the economic interest of the commercial firm and, in some circumstances, the public interest in access to Information.[7]

III. RIGHT TO ERASURE IN THE GENERAL DATA PROTECTION REGULATION

Article 17 of the General Data Protection Regulation deals with right to erasure. It states that, the person to whom the data is concerned with, have the right to get his or her data deleted without any undue delay. One has to acquire this right from the controller and the controller is

[2]CURIA - Documents, http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text=&pageIndex=0&part=1&mode=DOC&docid=152065&occ=first&dir=&cid=667631 (last visited Mar 8, 2021).
[3] Global Freedom of Expression | Google Spain SL v. Agencia Española de Protección de Datos - Global Freedom of Expression, https://globalfreedomofexpression.columbia.edu/cases/google-spain-sl-v-agencia-espanola-de-proteccion-de-datos-aepd/ (last visited Feb 5, 2021).
[4] Ibid.
[5] Ibid.
[6] *The Right to Be Forgotten - Under The Personal Data Protection Bill 2018 - Privacy - India*, MONDAQ https://www.mondaq.com/india/privacy-protection/860598/the-right-to-be-forgotten--under-the-personal-data-protection-bill-2018 (last visited Mar 8, 2021).
[7] Ibid.

duty bound to delete the data in question.

The right to erasure can be used only in particular circumstances, such as:

- The data is concerned is not required anymore and has lost the zeal for which it was collected;
- The person to whom the data is concerned with has retracted his/her consent for such data; and there are no legal premises for operating that data any further.
- The data in question have been illegally dispensed.
- Person to whom the data is concerned with, does not approve the course of action taken with his/ her data.
- The organization has to delete any individual's personal data in order to act accordance with the law.
- If particular data belongs to a child and the organization has used this data to the information society services which share the information among member states of the European Union.

But the Right to erasure is not an absolute right; because it may give power to people to rewrite history, as they hold the power to delete the information about themselves. So the GDPR specifies some circumstances in which a person will not be able to exercise their right to erasure.

Such as:

- If the data is used in accordance with the right to freedom of speech and expression or right to information.[8]
- The data concerned is used in obedience of the law.
- The data is utilized for the public interest.
- If the data is required for medicinal purposes, but it should not fall within the ambit of medical secrecy.
- The data concerned is pivotal for the armed forces.
- The data constitute prime information that succor research relating to science, history, and is in public interest

[8] Ibid.

 [ISSN 2581-5369]

IV. Right to be forgotten and right to erasure under Personal Data Protection Bill, 2019

After the declaration of right to privacy as a fundamental right in Justice K.S. Puttuswamy Case[9], by the Supreme Court, India seemed all prepared to recognize ancillary right as well. A draft bill was prepared on the recommendation of Justice B.N. Shrikrishna Report. One of the rights which emerged from the right to privacy was the right to erasure. But in India's Personal Data Protection Bill, distinction between right to erasure and right to be forgotten has been mentioned. Clause 18 of the 2019 Bill provides the following rights of correction and erasure, namely the right to[10]:

(i) The user can correct the erroneous data about himself,

(ii) accomplish any fragmented personal data,

(iii) upgrade the obsolete data, and

(iv) get erased personal data which is redundant for the purpose for which it was processed.

Clause 20 of the Personal Data Protection Bill deals with right to be forgotten. This pertains to the right to restrict or prevent the continuing disclosure of personal data where such disclosure:[11]

(a) has served the purpose for which it was collected or is no longer necessary for the purpose[12];

(b) was made with the consent of the data principal/user under the PDB Bill and such consent has since been withdrawn[13]; or

(c) was made contrary to the provisions of the PDB Bill or any other law for the time being in force.[14]

The underlying difference between right to erasure and right to be forgotten is that a user can only exercise his right to be forgotten if it is imposed by an Adjudicating officer.[15]

[9] Justice K.S.Puttaswamy(Retd) vs Union Of India on 26 September, 2018, https://indiankanoon.org/doc/127517806/ (last visited Mar 8, 2021).
[10] Right of Erasure - Under The Personal Data Protection Bill 2019 - Privacy - India, https://www.mondaq.com/india/data-protection/877732/right-of-erasure--under-the-personal-data-protection-bill-2019 (last visited Mar 8, 2021).
[11] The WhatsApp Privacy Policy Dilemma, https://www.livelaw.in/law-firms/articles/whatsapp-privacy-policy-dilemma-169584?infinitescroll=1 (last visited Mar 8, 2021).
[12] Ibid.
[13] Ibid.
[14] Ibid.
[15] Ibid.

 [ISSN 2581-5369]

V. AN ANALYSIS OF WHATSAPP'S NEW PRIVACY POLICY WITH EMPHASIS ON THE RIGHT TO ERASURE

When on 4th January 2021, WhatsApp declared that it is going to change its privacy policy; it created a lot of controversy. As with about 340 million users, India constitutes the biggest market for the social media app, it had to change the privacy policy as well as the date for commencement of the same. Although WhatsApp provide end to end encryption on the chats, still the policy or the user agreement has a lot of repercussions related to it. As the right to erasure constitutes an integral part of the right to privacy, it should be a paramount priority of any organization dealing with any individual's data. Even though WhatsApp allows a person to delete his/her account from their application but it does not delete the user information from their servers and can share this information with its sister companies like Facebook or instagram. To be precise WhatsApp owns the data of the user and if an individual agrees to the privacy policy of WhatsApp he/she is also bound to share its data with the other companies. As the result the user's information is not used for the objective for which he/she shared that information.

The concern about the business account is even more severe as the information a user might share with a business account can be shared with other third party application. WhatsApp's new privacy policy also says in case of any merger, or WhatsApp being sold to any other company the data of the user will also be shared with the other company.

Despite the encrypted chats WhatsApp will also be able to share the metadata of the user. Metadata is the overall data of a person's online activity. This means WhatsApp will be able to share that the time for which the user remains online and any other data except the chats, and once this data is shared the user will not be in a position to delete it. If a person is not provided his right to erasure his/ her data remains with the organization and they can use that data or sell that data to any other company. Since data is considered as fuel in the 21st century, the right to privacy and right to erasure will play an integral role in the upcoming years, the corporate organizations dealing with any persons personal data should deal the data with due diligence as it can harm a person more than any kind of financial loss.

A writ petition [16]has been filed in the Delhi High Court against the privacy policy of whatsapp. The petitioner has submitted before the court that whatsapp's privacy policy is ambiguous about how and up to what extent the user data will be shared. It has also been mentioned in the

[16] Chaitanya Rohilla vs Union of India Through Secretary, ... on 25 January, 2021, https://indiankanoon.org /doc/171200111/ (last visited Mar 8, 2021).

 [ISSN 2581-5369]

petition that there is no data authority in India which allows such companies to function arbitrarily in India and the fundamental right to privacy also embrace one's right to dispersal of the information about oneself and to be in charge of their data.

VI. THE ROLE OF INTERMEDIARY IN THE PROTECTION OF RIGHT TO ERASURE

According to Section 2(w) of the Information Technology Act, 2000, Intermediary is any person who receives, stores or transmits that record or provides services with respect to that record. The record mentioned in this section is only for the electronic records. According to this definition the social media sites or applications will also come under the purview of this definition. Section

79 of the Information Technology Act, exempts intermediary from the liability in certain cases, which is a considerable hidey hole in the IT Act for the intermediaries.

The case[17] which changed the construct of Section 79 was the arrest and prosecution of Mr. Avnish Bajaj, CEO of Bazee.com (the erstwhile subsidiary of auction portal Bazee.com (the erstwhile subsidiary of auction portal eBay.com)[18] Mr. Bajaj was arrested after a video clip containing objectionable matter was offered for sale on Bazee.com[19]. He was made liable as his website was allegedly publishing the obnoxious content. Mr. Bajaj cried foul for initiation of the action against himself and the intermediary when the hosting platform did not host the actual clip and had no control over the third party that posted the content.[20] The outrage caused by his arrest was voiced by eBay to the then Secretary of State of USA and NASSCOM.[21] This case brought forth issues and concerns relating to intermediaries and in particular discussed the onus of proof lying heavily with the intermediary.[22]To decrease the pressure on intermediary, Section 79 of the Act was amended in 2008 and shifted the burden of proof from the intermediary. The non-obstante clause with which the provision commences, lays an emphatic foundation to exonerate the intermediary from liability for third party information etc. albeit with riders provided under Section 79, sub-sections (2) and (3) of the Act.[23]

Section 79(2) essentially covers cases where the activity undertaken by the intermediary is of a technical, automatic and passive nature. Thus, for section 79(2) to be applicable,

[17] Avnish Bajaj vs State on 29 May, 2008, https://indiankanoon.org/doc/309722/ (last visited Mar 8, 2021).
[18] The Conundrum Of Intermediary Liability In The Last Decade - Intellectual Property - India, https://www.mondaq.com/india/trademark/921920/the-conundrum-of-intermediary-liability-in-the-last-decade (last visited Mar 8, 2021).
[19] Ibid.
[20] Ibid.
[21] Ibid.
[22] Ibid.
[23] Ibid.

intermediaries are to have neither knowledge nor control over the information which is transmitted or stored.[24]

In the case of Shreya Singhal vs. Union of India[25], the Supreme Court examined Section 79(3)(b) of the Information Technology Act, 2000.[26] This provision abides intermediaries to eliminate or out of action data to certain types of content if the user requests. The Supreme Court stated that it would be difficult for intermediaries to judge the legitimacy of each item render given high volumes of content. It read down the provision to say that content needs to be removed or disabled only if[27]:

(i) it is done on the basis of the order of a court or government[28], and

(ii) The order relates to one of the restrictions under Article 19(2) of the Constitution (such as national security and public order).[29]

Therefore, we see that the Supreme Court undermined the right to erasure and put limitation on it, as the right can only be used by any government agency or if it comes under the purview of Article 19(2). The user has given no right to request for deletion under this Section. Complementary to this Section the guidelines for the intermediaries' were introduced as the Information Technology (Intermediary Guidelines) Rules, 2011.

The Ministry of Electronics and IT has prepared the Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018 (hereinafter referred to as "2018 Rules") in order to prevent spreading of fake news, curb obscene information on the internet, prevent misuse of social-media platforms and to provide security to the users[30]. The Information Technology (Intermediaries Guidelines) Rules, 2011(hereinafter referred to as " 2011 Rules)created a lot of heat waves in the digital world with regard to the duties and liabilities of the intermediaries even after safe harbor protection provided under Section 79 of the Information Technology Act,2000(hereinafter referred to as "the Act"). Section 79 of the Act provided that the Intermediaries or any person providing services as a network service provider are exempted

[24] Intermediary Liability under the IT Act: Time for an Amendment?, https://www.barandbench.com/columns/intermediary-liability-under-the-information-technology-act-time-for-an-amendment (last visited Mar 8, 2021).
[25] Shreya Singhal vs U.O.I on 24 March, 2015, https://indiankanoon.org/doc/110813550/ (last visited Mar 8, 2021).
[26] Draft Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018, *supra* note 1.
[27] Ibid.
[28] Ibid.
[29] Ibid.
[30] Analysis of the Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018 - Media, Telecoms, IT, Entertainment - India, https://www.mondaq.com/india/social-media/794624/analysis-of-the-information-technology-intermediaries-guidelines-amendment-rules-2018 (last visited Feb 19, 2021).

from the liabilities in certain instances[31]. In 2018, the government has come out with certain changes in the 2011 Rules and has elaborately explained the liabilities and functions of the Intermediaries and to oversee that the social media platform is not misused.[32]

In order to make the internet a more secure place, the intermediaries have to comply as par the 2018 guidelines and have to inform the user monthly if they have not complied with the restrictions applied by the government then the intermediary will hold the right to cease and stop the access to such account. The government has made it compulsory for the intermediaries to follow such Rules within the time limit prescribed whereas, no such time limit was provided for in 2011 Rules; it will Act as a constant reminder for the users about such policies and regulations and prevent them from committing breach, which can lead to bad repercussions.[33]

The highlights of the Draft Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018 are as follows:

- The Intermediary Guidelines Rules, 2011 require intermediaries to prohibit users from hosting certain content on its platform (e.g. obscene content). The Draft Rules prohibit a new category of information, i.e., content which threatens 'public health or safety'[34].
- Intermediaries are obliged to, accommodate any government organization, within 72 hours. Further, they have to facilitate uncovering the originator of the information on their platform.
- Intermediaries must deploy technology-based automated tools to identify and remove public access to unlawful information. Further, intermediaries with more than fifty lakh users must incorporate a company in India.[35]

All these features seem to give the power to the government of what content should be made available on the social media or on any other platform and if it is to be made accessible by the people or not. In this situation it seems to be violation of Article 19(1) (a) which provides the right to freedom of Speech and expression to the citizen of India and violating the right to privacy as well.

But if the content comes under the purview of Article 19(2) which provides the restriction on

[31] Ibid.
[32] Ibid.
[33] Ibid.
[34] Draft Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018, *supra* note 1.
[35] Chapter At A Glance, PRSINDIA , https://www.prsindia.org/node/840397/chapters-at-a-glance (last visited Mar 8, 2021).

Article 19(2) then it is another kind of dilemma for the interpreter of the Constitution as it will have to choose between the rights of the citizen and the reasonable restriction to put a boundary on those rights, because public health and safety may not come under the purview of Article 19(2).

Moreover the rules are not about that how the counting of users will be done for any social media platform as they may have less than fifty lakh active users but the downloading of that application might be more than fifty lakh, what would happen in that situation, will the intermediary still have to register itself under the Companies Act, 2013? Such questions are still unanswerable in the guidelines.

VII. CONCLUSION AND SUGGESTIONS

The threats relating to the privacy of a person are increasing gradually, and if the law of a country is unable to protect the data privacy of a person, it surely wouldn't be able to call itself as 'Good Government'. As the welfare of the state is of the utmost importance for the government, the data privacy and the ancillary rights will also come under this purview for the purpose of 'Good Governance'. Even though the right to erasure is a complicated one, as if given the power to delete the data about himself or herself everyone will delete the ghastly data about themselves. So the lawmakers need to find exquisite balance between the restrictions and powers given to individuals. But there is a dire need of restrictions to be applied on the intermediaries. As the data of the citizen might be misused by these intermediaries, the users of these apps are mostly those citizens of India which are unaware of such privacy policy and ignorant of the importance of their data privacy, in such circumstances stringent regulation on the intermediaries should be pivotal for the government. We should use General Data Protection Regulation of Europe as a guiding light, because of their stern laws regarding privacy; whatsapp's privacy policy was not applicable on the countries of the European Union. Some Suggestions for the improvement the data protection policy of India are hereby given below:

- All the intermediaries should inform about their privacy policy in all 22 official languages of India, specified in the eighth schedule of the Constitution of India; so the person who is not able to understand English will be able to understand the privacy policy in their native language and can decide if he / she wants to agree with that policy or not.
- In the circumstances where intermediaries misuse data of a person a colossal amount of fine should be imposed on that company and shall be banned to function in India;

 [ISSN 2581-5369]

- There should be awareness camps about the data privacy and how a person's data can be misused, so how it abuses their right to privacy;
- The users of an application should be well aware about how they can exercise their right to erasure or forgotten, and the terms and conditions of the data deletion should be crystalline
- The Personal Data Protection Bill, should be passed promptly, with necessary changes;
- The Bill has expanded the scope of exemptions for the government, and additionally provided that the government may direct data fiduciaries to provide it with any non-personal or anonymised data for better targeting of services.[36]
- In an interdependent and data-abundant world, government access to data is a necessary but insufficient condition to ensure optimal national security outcomes[37]. The digital economy is influenced by a multi-layered ecosystem of domestic laws, commercial choices, bilateral arrangements, and international norms and institutions. In this ecosystem, access to data is *one tool* to secure our increasingly digital societies. This tool must be complemented by others, such as transparency and accountability frameworks for technology platforms, new bilateral data-sharing agreements, and cooperation with international security organizations[38]. Where access to data is necessary, it would be in the government's interest to tailor access norms as narrowly as possible, including by providing clear stipulations on the conditions under which data can be accessed, the precise nature of data that can be sought, and the purpose for which it can be accessed.[39]

The Government of India has introduced The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (the "Intermediary Rules") which has been under criticism because it takes the digital freedom of a person and gives government power of censorship in 'incognito mode'. Here the responsibility of Government is of paramount nature as they need to give citizens the rights while using social media platforms as well as put limitations on the right and should not use their power to control the digital rights of a person.

[36] The Personal Data Protection Bill, 2019: All you need to know, PRSINDIA (2019), https://www.prsindia.org/theprsblog/personal-data-protection-bill-2019-all-you-need-know (last visited Mar 8, 2021).
[37] Akhil Deo and Arjun Jayakumar and Samir Saran and Trisha Ray and Akhil Deo, *The personal data protection bill 2019: Recommendations to the Joint Parliamentary Committee*, ORF, https://www.orfonline.org/research/the-personal-data-protection-bill-2019-61915/ (last visited Mar 8, 2021).
[38] Ibid.
[39] Ibid.

 [ISSN 2581-5369]