Himachal Pradesh National Law University, Shimla (India)

Journal Articles | ISSN:2582-1903 | *Shimla Law Review*

Volume-II (2019)

THE RIGHT TO BE FORGOTTEN IN DIGITAL AGE: A Comparative Study of the Indian Personal Data Protection Bill, 2018 & The GDPR

Ashwinee Kumar

DOI: https://doi.org/10.70556/hpnlu-slr-v2-I1-2019-03

This article can be downloaded from: https://www.hpnlu.ac.in/journal-level-3.aspx?ref-id=11

Recommended Citation:
Ashwinee Kumar, THE RIGHT TO BE FORGOTTEN IN DIGITAL AGE: A Comparative Study of the Indian Personal Data Protection Bill, 2018 & The GDPR, HPNLU SHIMLA, II SML. L. REV. 75 (2019). https://doi.org/10.70556/hpnlu-slr-v2-I1-2019-03

This Article is published and brought to you for free and open access by Himachal Pradesh National Law University, Shimla. For more information, please contact editorslr@hpnlu.ac.in

Contents

Volume II | *ISSN: 2582-1903* | April 2019 - March 2020

Special Articles ***Page***

1. Episteme of Justice: A Genealogy of Rationality
   Mritunjay Kumar 1

2. Apocryphal 'State': Fragments on Theoretical Foundations, Constitution, Law and their Mythical Unification
   Chanchal Kumar Singh 40

Articles

3. The Right to be Forgotten in Digital Age: A Comparative Study of the Indian Personal Data Protection Bill, 2018 & the GDPR
   Ashwinee Kumar 75

4. Senior Citizens in India: A Critical Analysis of the Maintenance and Welfare of Parents & Senior Citizens Act, 2007
   Santosh Kumar Sharma 101

5. Privacy Issues in the Age of Pandemic: A Critical Analysis
   Lakhvinder Singh & Vibhuti Jaswal 119

Notes and Comments

6. Regulating Tax Havens: An Imperative Under International Law
   Girjesh Shukla 135

7. Building Insolvency Jurisprudence: Limits of the Judicial Role in the Constitutional Adjudication Relating to the Provisions of the Insolvency and Bankruptcy Code 2016
   Jasper Vikas 150

8. 'Sale', in Taxation Laws with Special Reference to Work Contract: A Journey of Conceptual Aberration during Pre and Post 46th Constitutional Amendment
   Alok Kumar 164

9. Full Protection and Security Standard in International Investment Law and Practice: An Indian Perspective
Santosh Kumar 177

10. Human Rights Education in the Field of Engineering and Technology
Vinit Kumar Sharma 191

11. Administrative Adjudication and Dispensation of Justice through Armed Forces Tribunal in India: A Way forward and Challenges
Sanjay Kumar Tyagi 209

12. An Escape Pod to Acquittal: Assessing the Impact of *Mohan Lal* v. *State of Punjab*
Bharat Barowalia 225

THE RIGHT TO BE FORGOTTEN IN DIGITAL AGE: A Comparative Study of the Indian Personal Data Protection Bill, 2018 & the GDPR

Ashwinee Kumar[*]

[***Abstract***: *Data protection requires enormous care and caution not only because of the sensitive nature of personal data but also because of its economic values. Personal data is by far the most valuable aspect of the human right of privacy. High dependency on the internet and technology-driven devices have led Indian lawmakers to conceptualize data protection altogether distinct from privacy. Protectionism and the concept of data protection finds place in many well-known documents like Treaty on the functioning of European Union and Charter of the Fundamental Rights of the European Union. The European Union took a step forward and gave data protection a legal meaning under the Directive of 1995. Though India is not only one of the largest IT service providers in the world but also the biggest market for the service. Unfortunately, Indian citizens do not receive the same respect, as the European subjects does, from the lawmakers but it's the Indian Supreme Court which paved the way for data protection to be treated as a fundamental right. However, 'the Personal Data Protection Bill, 2018, is being seen as an extensive investigation into the concept of privacy and data protection, and, especially the 'right to be forgotten'. This article will point out the serious lacunas of this report and the Bill, in regard to the right, analyzes them and attempts a solution in relation to the 'right to erasure' or 'be forgotten'.*]

I

Introduction

Data protection requires enormous care and caution not only because of the sensitive nature of personal data but also because of its economic value. Personal data is by far the most valuable aspect of the right to privacy. High dependency on the internet with

[*] LL.M (Goettingen, Germany); Ph.D Research Scholar at 'Law, Science, Technology and Society' group, Faculty of Law, Vrije University of Brussels. The author would like to thank Prof. Dr. Andreas Wiebe and Prof. Dr. Zsolt George Balogh for mentoring and encouraging him in the field of Data Protection Law. A sincere thank is extended to the University of Goettingen's Klinikum Library for its vast digital and uninterrupted facility of academic research. This piece of paper would not have been possible without the comments and consultations with Chanchal Kumar Singh and Mritunjay Kumar Singh.

technology-driven devices have led the lawmakers to conceptualize data protection as distinct from privacy. The more the technology has advanced the more are they concerned about protectionism. The concept today finds place in well-known documents such as Treaties relating to functioning of European Union and Charter of the fundamental rights of the European Union.[1] European Union took a step forward and provided data protection a legal meaning under the Directive of 1995.[2] India is not only one of the largest IT service providers in the world, it is also the biggest market for these services. One of the reasons attributable to this is the large population and the fact that many social media platforms are banned in China.[3] Unfortunately, the Indian citizens have not received the same respect, as the European subjects have, from the legislature with respect to data protection. It is the Supreme Court of India, which has paved the way for data protection to be treated as a fundamental right in the case of *K.S. Puttaswamy* v. *Union of India*.[4] Initially, in an affidavit in the Supreme Court, the Indian Government refused to accept privacy as a fundamental right. However, recently, a Bill in this regard has been prepared and is on the verge of introduction in the parliament.[5]

The government appointed Srikrishna Committee on data protection, in 2018.[6] The Committee submitted a draft Bill in 2018.[7] Subsequently, The Personal Data Protection Bill, 2018 was drafted to be tabled before the Parliament of India. In this essay, the author will analyze the schema, objectives, and the impacts of the Bill with respect to right to protect data within the context of 'right to be erasure' or 'right to be forgotten'.

---

1 *See generally,* Giacomo Di Federico (ed.), THE EU CHARTER OF FUNDAMENTAL RIGHTS: FROM DECLARATION TO BINDING INSTRUMENT (2011).

2 *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data* L 280 OFFICIAL JOURNAL, 31-50 (1995).

3 *Social media and censorship in China: how is it different to the West?* BBC (Sept., 26, 2017). *Available at*: http://www.bbc.co.uk/newsbeat/article/41398423/social-media-and-censorship-in-china-how-is-it-different-to-the-west (last visited Jan., 10, 2020).

4 (*2017) S.C.C. 996*.

5 Anurag Vaishnav,*The Personal Data Protection Bill, 2019: All you need to know* PRS LEGISLATIVE RESEARCH (Dec., 23, 2019). Available at: https://www.prsindia.org/theprsblog/personal-data-protection-bill-2019-all-you-need-know (last visited 10 Jan., 2020).

6 Committee of Experts under the Chairmanship of Justice B.N. Srikishna, *Report on a Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018). *Available at*: https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf (last visited 15 Jul., 2019).

7 *Id*.

II

Salient Features of the Bill

As the draft Bill is still under the executive domain and the European Union General Data Protection Law (hereinafter, GDPR) has turned out to be the torchbearer of data protection initiatives, and thus it is better to analyze the former in the light of the latter. The investigation will comprise of two-fold narratives; anatomic or root level scrutiny of bare title and provision; and the scanning orientation of the powers that be.

Section 27 of the Bill, titled 'right to be forgotten', deals with the omnipotent 'right of data principal' and drags the data 'fiduciary' into the ultimate devoir of obligation at the same time. The reader should keep in mind that obligation is not the apogee of the data protection legislation, but its compliance is crucial. It is not a matter of concern what duties a data fiduciary has and how should it be proceeded with in order to fulfill the same but the important aspect is what is required is the fact of compliance. Thus, it is important to scrutinize the anatomic standards of bare title and provision of section 27 of the Bill. The bare title is 'right to be forgotten' and emphasis is on 'be forgotten'. Forgotten is the past participle of the verb 'to forget', and is cognitive to, and has roots in old high Germanic term *firgazzen,* or in low Germanic *Vergetten,* and in present German *Vergessen,* means 'lose remembrance of'. The word forgotten its genesis in old English as *forgieten* in the King Alfred's Anglo-Saxon version of Boethius' Consolation of Philosophy, and in Wessex Gospel, a complete English translation of Christ Bible without any Latin text in c. 990, where it had been used as *forgeaton*. Gradually, it took the shape of forgotten as a past participle of 'forget', meaning 'fail to remember', (according to Oxford and Chambers' English dictionary). One thing is clear from this analysis, forgotten, as an action, requires complete losing or failing to remember something in the future for all purposes. Here, it means the loss of information or data shared in the past for a specific use.

Now, it is important to analyze Sub-section (1) of Section 27, which confers upon the data principal the right to restrict or prevent a data fiduciary the continuing disclosure of his/her personal information, already provided for a specific purpose and with valid consent. Sub-section (2), narrows down the scope of the right provided for in the previous sub-section. Section 27(1), deals with two distinct but conjunctive legal phrases, i.e., 'restrict or prevent' and 'continuing disclosure'. As this Bill, indeed, is going to be the fundamental legal conception on the data protection in India, we further need to skim, the practical meaning of these two expressions, off while keeping the bare title of Section 27 in mind. As far as the meaning of the word 'prevent' is concerned, both the Chambers & Oxford English dictionary defines it as 'to stop someone from doing something or stop the occurrence of something'. On similar line the meaning ascribed to the word 'restrict', is 'to keep something in certain limit'. The common meaning of these two words entails, 'stopping of something for future occurrence while limiting the same as it is'. Logically speaking, the status quo can be a good synonym for the duo. The next part, of the Section, or phrase is more technical in nature than legal. The Oxford English Dictionary adduces the word, 'disclosure', as 'the action of making new or secret

information known'. In the data protection world, this meaning has two distinct parts. For the first part, it concentrates on further processing or profiling of personal information and in the second part, it talks about the existing personal information with the data fiduciary. So, the provision applies here with double impact. The Sub-section (1) restraining the data fiduciary from continuous disclosure and he should refrain from doing the same after getting the request in this regard.

After examining the lexical and logical meaning of the phrases of Section 27 (1), one serious question needs answer: Does the latter chimes with the former or even related to each other? For the time being, let's not make it even technical by applying the law to the information society services based on block-chain or any other distributed ledger technology. It is the legal enthusiasts, who must deliberate how horribly, hastily, and off the cuff, this provision has been conceived and drafted in the Bill. At this point, and before making any remarks on this analysis, it is necessary to scrutinize the ideological background of the Bill, which is contained in the Committee's Report.

It should be kept in mind, at least at this stage, that we are not going to discuss the balancing interest of data principal's right to privacy and others' freedom of speech and expression. In its report to the government of India, the Committee, diverged from the actual meaning asserted by the EU lawmakers and the Court of Justice for the European Union. The Committee in its report[8] constrained itself by trying to relate the right to be forgotten with the ability of an individual, and this ability includes deletion as well (it simply means that 'be forgotten' should be made anonymous to the permanent deletion of a piece of information. However, when the Bill talks about the data fiduciary; it is inclusive of individuals and entities while defining data fiduciary under Section 3(13). As far as the report is concerned, the committee tried to understand the right to be forgotten only in two ways. It says, 'there is no principled reason as to why the data principal's assessment of unfairness would override that of the fiduciary',[9] though the committee forgot to opined about what this 'principled reason' is? Further, it says, '… in case of a direct or subsequent public disclosure of personal data, the spread of information may become very difficult to prevent… and the purpose for a publication may often involve matters of public interest and whether the publication is necessary 'may depend on the extent of such public interest'.[10] The committee heavily relied upon the criticism of *Google Spain case* judgment by the House of Lords', Justice Committee & European Union Committee of the UK, but forgot to discuss the *Google Spain Case*, which evolved the concept of 'be forgotten', as synonymous to 'erasure'. It is always better and easy to quote something in your defense on a point, which you do not want to either discuss or confer as a right.

---

8 *Supra* note 6 at 75.

9 *Id.*

10 *Id.*

It is, necessary to discuss the *Google Spain* case,[11] in order to understand the jurisprudence behind the right to 'be forgotten' and the scapegoat approach of the Committee in this regard. The fact of the case was that a Spanish national resident lodged a complaint with the Spanish Data Protection Authority (AEPD), against a Catalonian newspaper and Google Spain and Google Inc. He pointed out in the complaint that when a user types a name 'Mr. Costeza Gonzalez', he obtains a link of the two pages articles of the newspaper mentioning about the real-estate auction against him for recovery of social security debts. Interestingly, the news, first published in 1998, and the complaint was filed decades later. In his complaint, Mr. Gonzalez requested two instant remedies, one against the newspaper and another against Google Spain & Google Inc. The reader should keep in mind that Google Spain used to have an office in Spain as a subsidiary of Google Inc. In his complaint against '*La Vanguardia'*, the newspaper, he requested that, the newspaper must 'either remove or alter those pages, so that the personal data relating to him no longer appeared or are made available by a search engine, in order to protect his data.'[12] And, against the Google duo, his assertion was the same, *i.e.*, they were required to remove or conceal the personal data relating to him so that they ceased to be included in the search results and no longer appeared in the links to *La Vanguardia*...'[13]. The Spanish data protection authority rejected the claim as far it was related to the newspaper but accepted the claim against Google search engine. The Google Spain and Google Inc. brought separate actions before the National High Court, but the Court stopped the hearing and sent for the preliminary ruling, to the Court of Justice for the European Union.

In response to the surmises of the Sri Krishna Committee report, it would be appropriate to mention certain established facts regarding this case including the reasoning of the *Google Spain judgment*. The committee while developing its sneaking suspicion failed to understand any principled reason behind the overriding effect of data principal's own assessment of unfairness to that of the fiduciary. To smash out the incoherent legal thinking, with due respect, of 'principled reasoning', first line of thought would be, for example, the checks and balances of the economic gains along with means thereof by the fiduciary. (Indian Data Protection Bill terms "data fiduciary" as one who controls the personal data of a natural person or with whom the natural person shares his/her data. Generally, the data fiduciary will be corporations or companies or alike institutions who professionally or for trading purposes collect personal data.), followed by market stability, fostering respect to the competition law issues, purpose centric consent system, lawfulness and place of processing, respect for fundamental rights of the citizen etc. The Spanish National High Court observed that 'Google search' indexes websites throughout the world and the information indexed by its web crawlers or robots or

---

[11] *Google Spain SL and Google Inc*. v. *AEPD* (C-131/12, 13 May, 2014). *Available at*: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0131&from=EN (last visited May, 16, 2019).

[12] *Id.*

[13] *Id.*

computer program used to locate and sweep up the content of web pages methodically and automatically at an unknown location because of competition'[14]. The Court further said that, 'the Google search does not merely give access to content hosted on the indexed websites but also takes advantage of the user activity and includes, in return of good payment, advertising associated with the internet users' search items, for the undertakings which wish to use the tool in order to offer their goods or services to the internet user.'[15] Furthermore, a sensational hidden fact was found by the Court that Google Inc. has access to its subsidiary Google Spain in order to promote the online advertising space generated by a search on www.google.com. Alternatively, Google Spain was acting as a commercial agent for the Google Inc. and used to target the activities of undertakings based in Spain with the sole object; to promote, facilitate, and affect the sale of online advertising products. However, Google Spain was acting as a data controller, in Spain and all the activities regarding the data processing were carried out in the US.

These findings are of great consequences and require strong protection. Data mining, unfair processing, and stealing of data are few examples which need to be looked into in order to discuss 'principled reason'. Unfortunately, in the presence of such activities, the Committee deliberately ignored the above parameters. In its justification, the Committee[16] accepted the opinion of House of Lords', which looks more pessimistic than realistic, and therefore ignored the critical observations of the Court of Justice for the European Union.

III

Balance of Interest

The second line of thought of the Committee is the 'balance of interest test', to be applied while considering the restriction of disclosure of personal information, of data principal' and other rights. The Committee discussed only two dimensions. If we stress upon the line of thought, public interest or public disclosure and freedom of speech and expression are two indicators to be used, while acting under Section 27 of the Bill. The Spanish Court, in the same case, noted that, 'the removal of links from the list of results could, depending upon the information at issue, have effects upon the legitimate interest of the internet user potentially interested in having access to that information, whilst it is true that the data of a subject is protected by the Charter, also override, as a general rule, the interest of internet user.'[17] It should be kept in mind that we are dealing with personal information which has been shared with the data fiduciary under a relationship of trust. It is the data fiduciary who has to determine the purpose and

---

[14] *Id. at* 43.

[15] *Id.*

[16] *See Supra* note 6 at 76.

[17] *Id.* at Para 81.

means of processing. And, if the above-mentioned processing of personal data is carried out under the heading of 'lawfulness of processing', public disclosure would definitely not be necessary in all cases. Here, we will concentrate on the right to be forgotten in relation to the personal information shared with the data fiduciary.

The Committee emphasized on the balancing of the right to privacy and freedom of speech whilst ascertaining the appropriateness of the right to be forgotten. However, this issue should have been covered under 'lawfulness of processing' rather than under the right to be forgotten. Because once it is decided that the information shared by the data principal is purely personal in nature and has nothing to do with the public interest, a balance of convenience lies with the data subject than to the fiduciary. The Committee cites *Bodil Lindqvist judgment*[18] in order to apply the balance test. In this case, a lady, *Bodil Lindqvist*, was charged with a criminal proceeding under Swedish data protection legislation for publishing the personal data of her colleagues on her internet website. The colleagues were working with her on a voluntary basis in a parish of Swedish protestant church. The lady was charged with the breach of the said law-(Sweedish data protection Act or simply the Data Act) as then it was. on the grounds that she processed the personal data of her colleagues without giving prior written notification to the *Datainspectionen* (A sweedish word as provided by the author and perhaps mentioned in the judgment); the processing was also related with sensitive data without authorization and transferred the same to third countries.[19] In answer to an important question that, whether the member state can provide more protection for the personal data or widen the scope present of the Directive 95/46? The Court of Justice opined that a consistent measure can be taken, while maintaining the free movement of personal data and protection of private life. The court also was of the opinion that member state can provide more protection by legislation in the area, which is not covered under the existing Directive. Thus, it is clear from this judgment that the protection of personal data is of higher importance depending upon the circumstances. More recently the ECJ, (the European Court of Justice), stretched the balance of convenience test between the right of data protection and right of privacy a bit more in, *Rynes* v. *Urad pro ochranu osobnich udaju*[20] case. The fact established under this case was that Mr. Rynes installed a CCTV camera on the exterior of his house to protect his property from illegal vandalism, which, in reality, was attacked once again even after this installation. However, the said camera not only used to capture the movement on his house property, but also of the public footpath outside.[21]

---

[18] *Bodil Lindqvist* v. *Åklagarkammaren i Jönköping* (C-101/01, 6 Nov. 2003) *Available at*: http://curia.europa.eu/juris/document/document.jsf?docid=48382&doclang=en (last visited May, 17, 2019).

[19] Andrew Murray, THE LAW AND SOCIETY 548 (2016).

[20] *František Ryneš* v. *Úřad pro ochranu osobních údajů* (C-212/13, 11 December 2014). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62013CJ0212&from=EN (last visited May, 17, 2019).

[21] Andrew Murray, *Supra* note 19 at 549.

The highest Czech Court referred the case to the European Court of Justice for its opinion on the question concerning balance between 'the right to privacy and personal space of one person and right to data protection of the other person'. The issue framed was that, 'whether the installation of such camera on a family home for the protection of personal property, health, and life of the owner, would be deemed to be the processing of personal data', although, such camera also monitors public space. The ECJ was of the opinion that capturing of an identifiable image of a person through a CCTV would be qualified as personal data.[22] In its opinion, the ECJ observed that 'surveillance in the form of video recording of persons, which is continuously stored in a recording device - the hard disk drive – constitute further processing of personal data'.[23] The court further explained the principle that 'if the processing of personal data is capable to infringe the fundamental freedoms, in particular, the right to privacy, it must necessarily be interpreted in the light of fundamental rights set out in the Charter and the exception provided under the Directive must be narrowly construed'.[24] The European jurisprudence is prone to protect the personal data, as a constituent of the right to privacy, than to other rights.

Since we are doing comparative analysis of the provision regarding the right to be forgotten under new Indian data protection Bill and the European Union General Data Protection Law, it is important to examine the status and scope of the law in European Union. The GDPR is not the new development, however, it has been made to adhere the unified application of the data protection provision throughout the Union, of course, with new and greater protection of personal data in comparison to old Directive 96/46.

In the GDPR, right to be forgotten does not exist alone, but with the right to erasure. Article 17(1) of the Regulations says, 'the data subject shall have the right to obtain from the controller the erasure of his/her personal data without undue delay, and the controller, on the other hand, shall have to do the same without undue delay if a certain condition exists'.[25] We can see that the Union law left no scope for the controller in erasing the personal data of the data subject, of course, if all or any of the conditions are met out. The peculiarity of the above said law is that the personal data needs to be erased or be forgotten the moment the request has been tendered to the controller. It must be noted that the title of the provision is 'right to erasure or be forgotten', and the law enshrined under it speaks well about its title *i.e.*, erasure is the only option. However, if we analyze the present Indian Bill, we find that it speaks differently as the title says something else and the provision contained therein, drifts in a different direction. No

---

[22] *Id.*

[23] *František Ryneš* v. *Úřad pro ochranu osobních údajů* (C-212/13, 11 Dec., 2014). *Available at*: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62013CJ0212&from=EN (last visited May, 17, 2019); Para 25.

[24] *Id.* at Para 29.

[25] Art. 17(1) Regulations (EU) 2016/679 of The European Parliament and of The Council of 27 April 2016 on *the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulations).*

tuning can be established between the title of Section 27 and the proposed provision under Section 27(1) of the Bill. In the title, it says that the data principal shall have right to be forgotten, while under the provision, it talks only about the restriction or prevention of continuing disclosure of the personal data, which is something absurd. In contrast, the GDPR has a separate provision for restriction of processing, where, in a certain situation, the data subject can get his/her personal data restricted from further processing instead of erasure.[26] One interesting point can be noted by scrutinizing both the separate provisions of the GDPR that the right to erasure or be forgotten deals with the wish of permanent action of the data subject, while the right to restriction of processing is of temporary nature. A European subject finds itself lucky enough with regard to their enjoyment of temporary as well as permanent right.

How beautifully, the Union went through in defining the 'restriction of processing'. It could be understood by reading Article 4(3) as well as Recital, (In civil law tradition objective, the behind a statute and how that objective should be achieved by that statute is provided in the beginning of that statute. Generally, the interpretation of the law is guided by recitals provided for in the statute), 67 of the GDPR. Article 4(3) of the Regulations provides, 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future.'[27] Recital 67 has further broadened the scope of the provision by mentioning that 'in automated filing systems, the restriction of processing should, in principle, be ensured by technical means in such a manner that the personal data are not subject to further processing and operations and cannot be changed.

Now, it is clear that the Regulations try to confer upon its subject two clearly separate right depending upon the wishes and circumstances of the particular situation. Actually, these rights, *i.e.,* 'right to be forgotten, and, restriction of the processing' depends upon the happening of two distinct events. Out of these two, *first* can be the situation where the data subject can think about the furtherance of his contractual relationship in near future with his/her data controller, but the shared information must be eclipsed for the time being as there does not exist an event which can trigger the relationship forward. It would be very helpful, both for the subject and the controller, in taking the status forward when they want to and in contrast the subject will not be required to share his/her personal information again, of course, with the same controller and the controller will not need to gather the same again. How mutually beneficial this right is, which will save the time, efforts, and from any kind of potential risks associated with the personal data! The s*econd* can be the situation where the data subject finds his/her contractual relationship finished with the present controller and no law stops him/her in destroying the information stored with the latter. It is also a cooperative and co-existing principle where the controller would have no loss for erasing the personal data of the subject, which, in turn, would be beneficial for less requirement of database

[26] *Id.*, Art. 18.

[27] Art. 4(3), *Supra* note 25.

storage capacity and the subject will feel relaxed as no threat of illegal data stealing, transferring, and hacking, etc., continue to exist.

Interestingly, neither the right to be forgotten nor the restriction of processing is absolute for the purpose of the Regulations but, at least, the Union tried to confer greater protection and gives more choice to its subject that may be enjoyed at a moment in relation to his/her personal data. Article 18 (3) of the Regulations further obliges the controller to communicate to the data subject about the lifting of the restriction, on the mentioned ground, of processing before to do so. In case of failure in compliance of these provisions, the controller can be fined with a hefty amount of money. In an action against Google, the *Commission Nationale de L'informatique et des Libertes, the* French National Data Protection Commission, noted that 'if the right to be forgotten were limited to certain extensions, it could be easily circumvented. Indeed, it would be possible to retrieve a delisted result by simply using another extension thereby depriving the right to be forgotten of its effectiveness'.[28] The reader may find himself surprised by knowing the fact that the same French Authority, on January 21, 2019, imposed a fine of 50 million Euros on Google LL.C., for lack of transparency, inadequate information, and lack of valid consent regarding ads personalization.[29] One thing is clear that the European Authority should not be understood as a toothless tiger; alternatively, they enjoy the vast power in order to protect the personal data of its subject.

The Justice Srikrishna Committee quoted and was apparently guided by the criticism made by the UK's House of Lords' European Union Committee, while scrutinizing the *Google Spain Judgment* of the Grand Chamber of the Court of Justice for the European Union. The House of Lords' Committee observed that 'once information is lawfully in the public domain, it is impossible to compel its removal, and very little can be done to prevent it spreading'.[30] It (House of Lords' Committee) finally opined, in its recommendation that, right to be forgotten principle in the European commission's proposal is misguided in principle and unworkable in practice'.[31] This House of Lords Committee somehow tried to speak on behalf of the tech business entities without even testifying the responses and evaluating the actions done in regard to the request for getting the right to be forgotten complied with and, perhaps, was in its sixes and sevens on account of 'unworkability of this right in tech world'.

Google itself in a response to the EU's Article 29, accepted that till July 2015, it got a request for the removal of more than one million URLs and successfully removed

---

[28] *Supra* note 19 at 578.

[29] *Available at*: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc (last visited Jun., 12, 2019).

[30] European Union Committee, House of Lords, *2nd Report of the Session 2014-15 on EU Data Protection Law: a 'right to be forgotten?*, HL PAPER 40 (30 July, 2014). *Available at*: https://publications.parliament.uk/pa/ld201415/ldselect/ldeucom/40/40.pdf (last visited Jun., 23, 2019).

[31] *Id.* at Para 62.

around 41% of the same.[32] The process was, even then, continuous and Google did comply with the delisting requests. The Google went with a sense of reluctance towards doing the same from its non-EU websites. However, that was not the end of the game. The UK's Ministry of Justice responded to the recommendations made by the House of Lords Committee that, 'it is clear that individuals do have the right to request deletion of their personal data where it is irrelevant, outdated or inappropriate. The judgment does not change that right but rather extends that obligation of the search engines.[33] The Committee itself noted, while taking shreds of evidence from the stockholders, that Information Commissioners' Office 'supported the concept behind the right to be forgotten and agreed that it was possible for the ruling to operate in practice'.[34] After examining the report and the responses, it is clear that on the right to be forgotten even the UK's democratic institutions did not speak the same language.

It would be pertinent to mention, for clearing the air surrounding the conscience of Justice Srikrishna Committee, the emphasis on the necessity to have this right as a fair provision and devising a balance with that of freedom of speech and expression. The House of Lords Committee further wrote a letter to the European Commission and enclosed the same report. The response from the Commission, by a member Martine Reicherts, was revealing. The European Commission stated that the findings of the *Google Spain* judgment apply 'when information is inaccurate, inadequate, irrelevant, outdated, or excessive for the purpose of data processing. The Court explicitly stated that the right to be forgotten is not absolute, but that it will always need to be balanced against other fundamental rights, such as the freedom of expression and the freedom of media – which, by the way, are not absolute rights either'.[35] The Commission, further, vehemently disagreed by the findings of the House of Lords' European Union Committee, in which the latter said that, 'right to be forgotten is misguided in principle and unworkable in practice or left the law in a precarious situation'.[36] The Commission positively suggested that 'the removal of such links is technically possible, as demonstrated by Google themselves, since they have started complying with the request. Essentially, nothing changes for the way the search engine works as they

---

[32] Ruslan Nurullaev, *Right to be forgotten in the European Union and Russia: comparison and criticism* HIGHER SCHOOL OF ECONOMICS RESEARCH, 187 (2015).

[33] *Government response to the House of Lords' European Union Committee's enhanced scrutiny of the European Court of Justice judgment in the Google Spain case and its implications for the ongoing negotiations for a new data protection framework* (3 Oct., 2014). *Available at*: <https://www.parliament.uk/documents/lords-committees/eu-sub-com f/righttobeforgotten/government-response-right-to-be-forgotten.pdf. (last visited Jun., 15, 2019).

[34] *Supra* note 30.

[35] *Available at*: https://www.parliament.uk/documents/lords-committees/eu-sub-com-f/ righttobeforgotten/311014-Right-to-be-forgotten-Commission.pdf. (last visited Jan., 10, 2020).

[36] *Id.*

already filter out some links from the search result. For example, each day Google handles around one million take-down requests for copyright violations.[37]

The Srikrishna Committee report makes us ponder over that some commentators were against the incorporation of this right, as such, in the law on the ground of 'guarantee of non-additional benefit'. However, owing to the vitality of the report, it should have mentioned the class, the interest shared, nature attributed, and the logic and reasoning of the commentators which opposed this right to be incorporated. The class, here, may to the business or economic or technological services or MSMEs or NGOs or International Organizations like UN or Intelligence or Diplomatic services, artificial-intelligence driven processors, cloud-computing agencies, medical services, think tanks, admission counselors, the ringleader of fake news, etc. The interest may include commercial interest, data mining, espionage, advertisement, political or electoral benefit, to name a few. The nature attributable to the particular class can be determined by way of commencement or mode of business operation. Whether the entity is providing free digital services to the data principal and, in turn, gets salary or finical support from the government or an equally trusted organization or has a hidden agenda in their mind or is a Janus-faced entity, is a matter of serious concern. It is pertinent to mention a note from Sir Tim Berners-Lee, the creator of the World Wide Web that, 'the changes we have managed to bring have created a better and more connected world. But for all the good we have achieved; the web has evolved into an engine of inequity and division; swayed by powerful forces who use it for their own agenda'.[38]

It will not be a baptism of fire, how 'fake-news', found a place in India, especially political one, in recent years in order to gain sympathy from the electorates. It is an issue which needs explanation, in the context of fake news, whether the 'commentators' referred in the Report, are the political parties, information society service providers of these parties, or the social media websites, that have commented against the incorporation of the right of erasure? The Committee is silent on this point. We must know what interest these commentators represented because recognizing 'this right' would have made the data fiduciary liable under the law.

The issue of fake-news not only disturbs the equilibrium of the society, but also distorts the conscience of common man, and India, indeed, is not alone here. The 'disinformation and fake news' are mushrooming and have spellbound effect on many democratic well-wishers to think upon. An 'International Grand Committee', comprising of representatives of eight democratically elected countries met in the UK to discuss cross-border co-operation for tackling the distortive, disruptive, and destabilizing tendency of 'disinformation and fake news' and its discrete spread. The Grand Inquiry of this Grand Committee spanned over almost eighteen months and covered aspects such as

---

[37] *Id.*

[38] Select Committee on Communications, House of Lords, *2nd Report on Regulating in a digital world* HL PAPER 7 (Mar., 9, 2019). *Available at*: https://publications.parliament.uk/pa/ld201719/ldselect/ldcomuni/299/299.pdf. (last visited Jan., 12, 2020).

individuals' privacy rights, how their political choices might be affected and influenced by online information, and interference in political elections both in this country and across the world—carried out by forces with destructive intent on causing disruption and confusion'.[39] The committee also 'experienced propaganda and politically-aligned bias, which purports to be news, but this activity has taken on new forms and has been hugely magnified by information technology and the ubiquity of social media'.[40] Suspicion even continues with the Srikrishna Committee's non-disclosure of the class, interest, and nature of the opposites who succeeded in convincing the Committee to put the 'right to be forgotten', in its report almost as a toothless tiger. Moreover, we must see the beauty of the UK's House of Commons' Digital, Culture, Media, and Sport Committee report which, with utmost trust to the people, found that, even, the UK's electoral law needs amendment to make it suitable for the purpose of coping with modern technology.

It is important to digress, for the time being, from the current topic and concentrate on the factual and objective analysis of the 'Law & Technology Academics' on the hidden agendas of a few data fiduciaries in relation to personal data. Dr. Jennifer Cobbe and Prof. John Naughton, of the University of Cambridge, propounded a concept known as '*surveillance capitalism'*. This concept, according to them, has been developed by Google to provide free search service for users, on the one hand, and on the other hand, it is used to analyze phrases, which were entered by the user in the search box. This analysis was carried on for two interdependent purposes, *i.e.*, '(a) to make inferences to predict the user's wants; and (b) to sell to other companies 'the opportunity to target those users with advertising based on this prediction,'[41] and they asserted that, this model is the real driving force behind Google's entry as the richest tech giant. They, further, describe this model as an outcome of the *applied psychology*. The biggest setback for the opponents (one who either does not believe in the 'surveillance capitalism' model or deliberately opposed it) would be to consider a testimony given by Mr. Margot James MP, the Minister for Digital and Creative Industries, 'that some airlines' websites use an algorithm which identifies passengers with the same surname and deliberately allocates them seats. The airlines can then charge passengers to change their seat to be with their

---

[39] House of Commons, *Final Report Digital, Culture, Media, and Sport Committee, Disinformation and 'Fake news* HC 1791 (Feb., 18, 2019). *Available at*: https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf. (last visited Jan., 10, 2020). Political and democratic enthusiasts are highly requested and recommended to go through this report. As this report raised, worked upon, and summarized very serious issues regarding malfunctioning in the electoral festival of number of countries including India. On para 275 of this report, the committee highlighted that the Strategic Communications Laboratories group of companies, including Cambridge Analytica, have been involved in Indian election campaigns. The same stressed on para 277 that these entities had not been financed transparently and in doing so they overstepped legal and ethical boundaries.

[40] *Id.* at Para 3.

[41] *Supra* note 38.

family'.[42] According to Prof. Naughton, 'most datasets are not clean; they are colored in one way or another with all kinds of unconscious and other biases'.[43]

Facebook, for example, has been seen to be the biggest culprit in influencing the political elections across the Europe; Germany, France, and the UK, which legislated against illegal content.[44] Ashkan Soltani, a former chief technologist at the US Federal Trade Commission, disclosed to the 'International Grand Committee', that in Public the Facebook supported the newly framed California Consumer Privacy Act, but lobbied against it behind the scenes.[45] The Committee also got testimony on how Facebook app collects users' data from android phones' apps. Enlarging these issues make us highly concerned about the fate of our personal data which is not only a piece of data but also our digital money. This aspect is discussed below.

Balancing Freedom of Speech and Right to be Forgotten

The next point of consideration is Srikrishna Committee's concern about the balancing of interests of right to be forgotten (or erasure) of data principal and the others' freedom of speech and expression and right to information. Interestingly, we should not forget that like the latter right, which in itself is not a single, but a bunch of rights, the former is also not an absolute right. The latter is, in a way, merely a tool for furthering the freedom of data protection and privacy. It must not be seen as the counterpart of the latter, because it is one of the mechanisms, to secure the freedom of privacy. *Stricto sensu*, the freedom of protection of one's personal data, as a fundamental right, is definitely a European approach, where, the freedom of expression, too, has the same revered place as the former. Nothing has been said which will override the other.

In this digital age, where personal data is not just a piece of information but more in the nature of digital money, which actually are traded in the manner in which slave trade used to happen generations back. In themselves, slaves had no value, but they had been traded because the same had, actually, certain hidden values in the trade or business of their master. Ashoka, the great, is credited with abolishing the slave trade, first of its kind in the historical account, but not slavery.[46] Lord Mansfield, in 1772, held slavery to be illegal, in the celebrated case of *Somerset* v. *Stewart*,[47] which was followed by enactment of the Slave Trade Act, 1807, by the British parliament. Individuals were owned, bought and sold under property law, which suggests that, there was an economic value of an individual depending upon his/her color, sturdiness, sexual and sensual orientation, languages known, and ability to bear healthy child, etc. Inference

---

[42] *Id.* at Para 94.

[43] *Id.* at Para 93.

[44] *Supra* note 39.

[45] *Id.*

[46] William G. Clarence-Smith, 'Religions and the abolition of slavery – a comparative approach', http://www.lse.ac.uk/Economic-History/Assets/Documents/Research/GEHN/GEHNConferences/conf10/Conf10-ClarenceSmith.pdf>, p.2, (last visited on Sep., 8, 2019).

[47] *Somersets* v. *Stewart* (1772) 98 ER 499

can be drawn that apart from the physical presence their trading would have required additional information, too, in order to enhance the monetary value of the slave by letting the buyer know about their behavior, workability, likes and dislikes, demand for food and cloth variety, the mode of happiness, scientific or mathematical skills, the lists may be countless. It shows that personal information was present and not only needed to watch closely, but also would have recorded somewhere and profiled accordingly. But the slaves would have either no-knowledge, or misinformed in many cases, or compelled to share the information related to them, which must not only be true but also capable of being verified.

It may, also, not be disputed that the information apparent, by physical appearance, and recorded on a register or ledger or with other instruments would have been targeted, either jointly or independently, by any market operator, who, on the other hand, used to spread the information to the market players in order to gain benefits. Qualities about a slave or an individual could not be gathered solely by one's bodily mien but require plenty of related exercises. More the qualities a slave would have, more would be the marketability. Moreover, the number of slaves would have been directly proportional to the volume of information, so increase in former would have required not only vast seat of information register or ledger but also their profiling in order to make them up to date in the easiest possible way, for the buyer. It can also mean that individual's information, now data in the digital age, played a vital role in decision making about the haves and have nots of a particular chattel or slave. Alternatively, it was also not necessary that slaves needed to share the information to every buyer in a 'one to one interview'. Before a slave was subjected to the market, his/her information would have been shared with a particular buyer. This routine slave trade would have also resulted into a mammoth information register or ledger in which each and every kind of qualities, which could be expressed by way of information, about countless number of slaves might have been available or supplied from one organizer to the other and so on and so forth.

It was not allowed, in most of the cases, that a slave could even speak or express himself, but there would have always existed a chance that his/her noticed behavior or likes or dislikes or other information would have spoken or expressed everything.

This analysis poses two serious questions: whether it is only the mouth that speaks or bodily frame and actions can also express vital attributes? Furthermore, whether or not the personal information is sufficient to speak and express, about the individuality of the person? To understand this theme properly, it is important that it must not be treated in a 'rights' framework. For example, the personal information, or personal data in the digital age, not to be merely analyzed as a fundamental right and explored independently and then draw circles of rights, in order to reach any conclusion whether the right of personal data protection falls under what heading?

Srikrishna Committee report tried to pose a balancing test between the right to privacy of one with the freedom of speech and expression of the other(s). This is, certainly and absolutely, not the case. With due respect, there should be no hesitation to say that they failed to understand the logic and reasoning behind the protection of personal data.

And, then, on that basis, they proposed this balancing test. However, in our opinion, they left a serious lacuna which such a high level Committee cannot and must not afford.

We must first understand that we claim the protection of personal data or the right to be forgotten only when we will have personal data. No one can claim this right without having certain personal information known to somebody else. Right to be forgotten, indeed, under the heading of right to privacy, falls somewhere in the middle of the fundamental rights table because there must be a genesis of information, and for that, we either need to speak or express first, then, there would be simultaneous recording keeping to make it non-volatile, at least until we want. Destruction of any of these or all information comes at the end, such as at death, that follows life which starts after birth. Therefore, the demand for erasure or the right to be forgotten of information is just a momentary upshot of behavior on a certain point of time by keeping facts and circumstances of the situation in mind which requires its existence, first, somewhere on the *axes*. Axes, here, means coordinate axes by plotting time as *X-axis* and situation as *Y-axis*. It means when we draw the coordinate axes, by keeping both the factors, to locate a piece of information in a given point of time and with the actual situation, a multitude of indicators come into the picture to decide upon the prevalence of a particular right or class of rights. This multiplicity of indicators can be freedom of speech and expression, property and economic freedom, equal legal protection, right to privacy and data protection, informational self-determination, and protection from disgraceful informational trespass, etc., Prof. Sartor divides these factors, in two different tables, *i.e.,* 'pro-processing interest' and 'con-processing interest'.[48] Nonetheless, this tabular analysis falls and works only after the existence of information at a point of time. So, the crux is information, not only after having a good economic value, *i.e.,* profiled or 'de-anonymized' or processed in a particular way.

How can we protect life if one cannot have a life *i.e.*, without birth? Life begins with birth. Information can be and would definitely be protected under the right to life but this protection will be subservient to the right to speech and expression. If we cannot speak and express, digitally, no information will come out and hence no further right can be enforced. We can only protect a thing, at a certain point of time, which does exist. So, the real root of informational protectionism lies not, primarily, in right to life or even right to personal data or privacy protection, but in the fundamental right of speech and expression. Interestingly, we can only have information when we speak or express with the help of keys and mouse of a computer keyboard, or by commanding or touching the pad of mobile phones or alike devices. If we do not get protected, first, under freedom of speech and expression we cannot deliver information, in the digital age, as a command of our emotional and material wishes. Enjoyment of this freedom, actually, results as a launching pad of information and communication technology satellites. Until a piece of information survives, this freedom will nanny them as each time an already existing information will need additional digital expression to command a wish,

---

[48] Giovanni Sartor, *The Right to be forgotten: Balancing Interest in the Flux of Time* INTERNATIONAL JOURNAL OF LAW AND INFORMATION TECHNOLOGY, 24, 72–98 (2016).

irrespective of the fact that whether the data principal wants to modify or restrict or finally erase his/her already shared information with the data-banker. So, it would be a grave injustice to the common people and dereliction of jural thought to surmise informational self-determination, independent of freedom of speech and expression.

Answer to the question, whether only physical presence of a human being can alone be capable of speech and express, would be in the negative because in digital world one does not need the mouth to speak or senses to express. However, the information, result of one's thought can be given speech and expression through technologically advance devices. So, it can be observed that protection of personal information may be a distinct kind of protection, but can never exist devoid of freedom of speech and expression. Freedom of right to life, equal protection of the law, right to privacy and data protection can be the additional protection, or sometimes special, but can never let this birthright bypassed.

The question that follows is, whether the proposed balance test of Srikrishna Committee, really deserves applause or legal mayhem by 'proffering that data principal's right to be forgotten', should be checked on the anvil of speech and expression, and right to information of others. It is certainly, not the same, but the real balance test should be that of 'individual right' versus 'collective interest'. All the related fundamental rights should be tested one on one by keeping 'informational self-determination', of, first, on one hand and 'collective interest' of the rest on the other. Here, 'collective interest' does not mean the society as whole, but concentrates on the digital service providers. The real fight is between the tech moguls and a common man. A war must be fought between equals having almost analogous weapons. We must keep in mind that algorithms and computer programs or software are protected not only under intellectual property rights, but also their roots lie in the freedom of speech and expression. Request of erasure of information or be forgotten is nothing but an ultimate expression, spoken by way of tech-twisting, for a purpose, in an immediate contractual relationship. That contractual relationship began, when an online search engine or information society service provider expresses, on the mobile or computer screen, the service available, spoken through well-developed computer programs or smart apps, as an offer, and we, as a data principal, in return, accept the same by expressing our intention through keyboard or touch pad or mouse or sometime replying through our voice. Therefore, in this digital age, data is very crucial factor, which says everything on behalf of both the parties. And, if one's offer making or offer expressing a thing, is protected under freedom of speech and expression, then why not mine? Indeed, in the 'Digital Age', 'information, alone, speaks louder than humans', and can have a better price tag than the person to whom it actually and legally belongs. Who cares, of course in this age, where we live, how much we earn, how we are treated, how far we are, whether one is corrupt or ingenuous etc. The litmus test is, 'are we capable enough to give business and is our data worth of profiling or processing in order to share with different market players'? From Silicon Valley to Shenzhen, and from Bengaluru to London, it is 'information' which propels the ICT industry.

One thing is clear, for now, that the balancing test is not the same which has been proposed by the Committee, but it is really, what we have established here. The next question is, how are we proceeding with or taking care of 'individual's informational right' and 'collective interest' of another? The Committee tried to subdue the data principal's right to be forgotten, overwhelmed by a few hidden commentators- great soul, so to say so- who thought that it cannot provide an additional measure or will be detrimental to another's right to information. The Committee sometimes felt that permanent deletion of personal information must not be part of the right to be forgotten but on the in next moment, it changed its mind.

We must keep in mind that worldwide Internet of Things (IoT) marketability is increasing exponentially from 2.99 trillion dollar in 2014 to 8.9 trillion dollar by 2020.[49] Internet market, as a media platform, is almost dominated by 'Gang of Four', *i.e.*, Google, Amazon, Facebook, and Apple, followed by Microsoft and IBM. Professors Phil Simon and Scott Galloway describe that, 'these tech giants as driving force of the consumer evolution on the internet, which, in turn, avoid taxes, invade privacy, and destroy jobs'.[50] The catalog of consequences in the observation is final, but also includes repercussions in the form of anti-competitive attitude, illegal surveillance, non-transparency, data mining, etc.[51] Facebook, for example, has been in a series of controversies ranging from privacy breach, Cambridge Analytica data scandal, political manipulation, fake news, and web trafficking, etc. Recently Facebook claimed its monthly user list crossed 2.3 billion with overall revenue of about 55 billion dollars, that mostly comes from advertising. But also, significantly, from bulk data access sold to the other companies or entities. One thing is clear that it is not the internet or mobile or computer that speaks but our personal data does. These companies and social media are not making money just by giving free services to us and, in return, one day the Almighty came in their dream and asked for a boon (for such a constant and uninterrupted access to personal data). No, it is definitely not the case and, indeed, our personal data makes them a billionaire. The impulse from these trustees of 'collective

---

[49] Louis Columbus, *2017 Roundup of Internet of Things Forecasts*. *Available at*: https://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/#7f0b8e5e1480 (last visited Jan., 11, 2020).

[50] *Available at*: https://www.cnbc.com/2017/10/02/scott-galloway-the-four-amazon-apple-google-facebook.html (last visited Jan., 15, 2020).

[51] In a personal meeting with the Chief Information Officer of a Company, it was a matter of surprise to know that there are exist only a few tech corporations which provides cloud services; and, when a company needs this service from any one of them, they just give an already prepared seats of agreement paper and demand, in return, only signature and seal of the authorized person of beneficiary company without any addition or subtraction of provision. His meaning of the whole discussion was that the other companies have no negotiation power as there are only a few players which provide the same and if you need it just sign and seal on the already agreed terms and conditions. If such a kind of companies around the world does not have negotiating power in these cases, then we should assume that what will have for us?

interest' would be unbearable for a common man without having formidable 'individual rights'.

Ronald Dworkin argued that 'individual rights are political trumps, held by individuals. Individuals have rights when, for some reason, a collective goal is not a sufficient justification for denying them what they wish,'[52] whereas, Warren & Brandies endorsed right of protection of one's self from pen portraiture in 1890, and, just after 126 years, Dr. Miyashita reiterates for protection of one's self from internet portraiture.[53] Justice Sir James Yates in his dissenting opinion in *Millar* v. *Taylor*[54], penned that 'it is certain that every man has right to keep his own sentiments, if he pleases. He certainly has right to judge to whether he will make them public, or commit them only to the sight of his friends'. Warren and Brandies, keeping their findings as a central theme of analysis, advocated that, 'it is always secured in our common law system that up to what extent an individual wants to share his thoughts, sentiments, and emotions with others.[55] It is the 'forgetfulness', which is eternal bliss of information spread over the internet. If a debate on privacy starts from the words of Warren & Brandies, 'forgotten' can be the only resort of internet-driven speech and expression. This is why, where the list of IoT is growing endlessly, Dr. Miyashita sees, 'the right to be forgotten' as a 'worldwide right' in the 'global village'.[56]

If we consider the rights proposed under Indian Personal Data Protection Bill, 2018, it is clear that either the corrective or additional measures must have been taken into consideration for the protection of the right. The Bill recognizes the right to 'confirmation and access', 'correction', 'data portability', and 'be forgotten'. Out of all these available rights, a protective step can only be taken under 'right to be forgotten', as a permanent and ultimate desire of the data principal in a contractual relationship wherein either the object has been fulfilled or the data fiduciary lost the trust of the data principal. Right to restriction or prevention from continuing disclosure of personal information, cannot even bear permanent relief as this right is temporary in nature wherein the data principal either wants to continue with the same data fiduciary in future or letting the stopgap of personal information from trepidation.

However, the trust still lies, with the data fiduciary and continuance of a contractual relationship can be assumed in the near future. The latter right would be limited in nature for the purpose of protection but adequate for the purpose of additional measure yet, certainly, cannot be corrective. Data portability, on the other hand, is completely an

---

[52] Ronald Dworkin, TAKING RIGHTS SERIOUSLY 563 (1977).

[53] Hiroshi Miyashita, *The 'Right to Be Forgotten' and Search Engine Liability* 2(8) BRUSSELS PRIVACY HUB (2016). *Available at*: https: //brusselsprivacyhub.eu/BPH-Working-Paper-VOL2-N8.pdf. (last visited Jan., 18, 2020).

[54] *Millar* v. *Taylor* (1769) 4 Burr. 2303, 98 ER 201.

[55] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy* 4(5) Har. L. Rev., 193-220 (1890). *Available at*: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf. (last visited Jan., 16, 2020).

[56] *See* Hiroshi Miyashita, *Supra* note 51.

additional step by requiring the data fiduciary to transfer his/her personal data either to the data principal or another data fiduciary. This right does not give any meaning which can support either the corrective or protective measure. Confirmation and access to one's personal data also do not qualify the test. The only quintessential and durable protective measure would be 'erasure' or 'deletion' or 'be forgotten', when there is a complete loss of trust in a particular contractual relationship. There exists little room for the fulfillment of object between the duo and no further relationship on the same issues for now exist.

Learning from a Hypothetical Case

Let us take a hypothetical example in which A, as a frequent visitor of an online E-commerce website XYZ Inc., visits the website to order underpants having letter 'P', inscribed on the front and a de-bossed rose on the back. The fascination arises with respect to its design. A has never ordered even a single piece of this undergarment, which does not fulfill this requirement. The point should be taken into consideration that A is the richest guy in this area, where young ones portray him as a fashion model and follow continuously. In the course of time, A gets notified by the XYZ Inc. that he has won a competition by way of an online survey in which the participants were asked to choose a name, whom they match their preferences the most about color, design, and company. He is surprised to know that this XYZ Inc. will give me an offer, in which, he will get an extra garment for free for the whole year, if he orders from this online platform. After one week of this announcement, he wants to buy a complete set of fabrics from different companies, other than from XYZ Inc. What he has found now that each and every company advertises and tries to allure him by availing a particular dress in the same design, and with a special facility that the 'letter 'P' and the picture of the 'rose' in different colors, which he opts the most for underpants. It is not crucial whether the thing is swatter, cap, shirt, or jeans. Is it not shocking that how all other companies know this, why they want to manufacture a cloth in this way just because people follow him and order the thing alike him? He feels cheated and under fear that whether these brands consider him as a psycho, he will only like this design irrespective of the nature of a dress. He wants an immediate and permanent remedy under Indian Personal Data Protection Bill, 2018, and has started searching for an adequate provision to do the same. Would it be sufficient to know, under Section 24 of the Bill, from the XYZ Inc. that whether it processes his personal data and, if yes, he needs a summary of all these events? However, he will not be happy with this glossy summary, and will inquire for something more. Now, he will have right to correction, under Section 25 of the Bill, which provides for the correction of personal information, if he finds the same inaccurate or misleading or incomplete or not up to date with time. But, here, these factors are just redundant for him, because everything is correct, accurate, complete, and of course up to date. This frustrates him and he concentrates on the next provision with a wish to find a solution. Now he has the right to data portability, under Section 26 of the Bill, under which he can transfer his whole bunch of personal data to another online E-commerce platform in machine-readable, structured, and commonly used format the order and format thereof he does not know. It is infuriating, now, that does he really

have something, which can protect not only the exploitation of his psychic abilities, but also his right to express his feelings? Yes, why not, the legislature put forward 'right to be forgotten', under section 27 of the Bill, which will get his personal data deleted, so that, nobody can process or profile, in future and, eventually, he saves himself from being insane. But here lies the dichotomy. The title refers to 'be forgotten' while the operative provision deals, only, with 'prevention or restriction of continuing disclosure of the personal data' from XYZ Inc. This provision can only prevent or restrict XYZ Inc., for disclosure in future, but what about the disclosure which has already taken place? He can find no answer here. Perhaps, he needs to search for another legal instrument for this. That, therefore, raises questions about the utility and the very object of this proposed law!

Personal Data and the Sovereign

The final exploration of the 'right to be forgotten', as mentioned previously, under the present Bill, would be the 'scanning of the procedural stratagem of the sovereign'. It is explicit, at this stage, that neither the Committee's opinion nor the present Bill is coherent and cohesive enough and so, in reality, a bit iffy to understand what this provision is all about. Moreover, the Bill tries to subject the data principal into litigation, against whom, even a government can sometimes be easily outweighed. The provision, Section 27(4) of the Bill, requires filing of an application in a prescribed manner and in a special form. [57] The Bill further holds the right in check by using expressions such as 'shall have' in Sub-section (2). In every case, it will be the Adjudicative Authority, who will decide whether an order of the right to 'prevention or restriction of disclosure' should be issued. Notwithstanding the order passed after the punctilious tutelage of the essentials of law, 'any person' can request for review and may get the same passed in his/her favor. Even though, it is a legal conundrum that what this provision wants to confer upon the data principal, the latter may feel jolted by the double impact of litigation and *locus standi* of any person. Moreover, the Bill is silent over the time frame within which an Indian common man will get his personal data, not deleted at all, but possibly restricted from future disclosure. Keeping the pendency of the cases at various adjudicating authorities in mind, we should be ready to fight endlessly just to get our personal data prevented from disclosure. Alternatively, it can also be deemed that we must hire an expert of legal or technical field and invest a hefty sum of money and time. We cannot consult or directly ask our data fiduciary to do the same as the Bill deliberately provides a scapegoat for them.

On the other hand, we can see the fact of convenience and effectiveness in the approach of European Union lawmakers, in relation to strengthening its subjects' right to be forgotten in a time-saving fashion and with a formidable warrant of punitive measures against data companies. Article 17 of the GDPR confers upon its subjects the right to erasure of his/her personal data without any undue delay from the controller (data

[57] Indian Personal Data Protection Bill, 2018.

fiduciary in the Indian context) in a case when even a single ground exists to do so.[58] There is no use of terms such as, 'shall only', kind of provision, in the Regulations and the controller is under obligation to do the same without undue delay. *The data controller is not only under obligation to inform the outcome of the request of the data subject, but is also necessitated to notify other controllers, if a situation so warrants, about the request of erasure*.[59] The outcome of the latter request also needs to be reverted to the data subject. There is no requirement, fortunately, at first instance, to file an application in an appropriate fashion before an authority paid from the tax-payers pocket. It should also be noted with great care that 'restriction of further processing' is altogether different and distinct right in the European Union, and has a separate way to exercise the right thereof. Moreover, two genuine questions directly come to our mind, first, what will happen when, at first instance, the controller will defy the data subject's request or has failed to oblige; and second, is there a precise meaning of 'without undue delay' in the Regulations?

The answer to the first query is more candid than the latter under the GDPR. Under Article 77(1), the data subject can, at the second stage, and after getting his/her wish unfulfilled, lodge a complainant with a supervisory authority irrespective of the place of residence, work, or where the infringement occurred. Another mesmerizing power which the data subject enjoys is the communication from the supervisory authority. Under Articles 77(2) and 57(1)(h), the supervisory authority is duty bound to inform, from time to time, the outcome of the complaints with regard to the investigation done or will be done in near future or about the coordination with another supervisory authority. Mercifully, the data subject only requires lodging a complaint with the same and the duty interchanges thereafter.

This is not the only remedy available to the data subject but, he/she can opt for other administrative or judicial decisions. Furthermore, any person or organization or non-profit body active in the data protection, can file a complaint, either on behalf of a data subject or independently, without having any defense against *locus standi*.[60] As far as the phraseology of 'without undue delay' is concerned, a general approach has been taken as '72 hours', and if not possible to do the same then the controller must notify the nature and extent of the violation of rights and freedoms to the concerned supervisory authority, if it failed, and detailed reasons must be accompanied to the authority.[61] Overall, we can say that the Union does not want its citizen to move here and there for a thing which strictly belongs to them. The data subject need not file any proper application written in such and such manner and in a special form. How lucky they are?

---

[58] Regulations (EU) 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulations).

[59] *Id.*, Art. 19.

[60] *Id.*, Art. 80.

[61] *Id.*, Recital 85 & Art. 33(1).

We will be overwhelmed or might feel humiliated by the approach taken under our Bill. A member of the European Commission replied to the chairperson of the UK's House of Lords' European Union Committee by stating that 'currently, the trust of European citizens in digital services is low! It is precisely because global access to detailed personal information has become part of the way of life that we therefore need to put our citizens in control of their personal data. We should not be afraid of empowering our citizens'.[62] These marvelous words were communicated, by the Commission when it was trying to conceive the 'right to be forgotten' having a distinct place in the Regulations, as an acute necessity.

The Court of Justice for the European Union and the European Court of Human Rights applauded the concept of the 'right to be forgotten' or 'erasure'. The latter Court held that the restriction on the freedom of expression of an online news portal is justified when its prior automatic filtering and take-down notice system fails to protect the rights of third parties.[63] In this case, the applicant company appealed the findings of an Estonian court before the ECHR, under Article 10 of the ECHR, in which the former Court imposed fine 320 Euro for letting the defamatory content continued on its online news portal for six weeks. Louis Brandies, in 1928 (the year in which Olmstead judgment was pronounced), had something to say on the right to privacy while acting as a puisne judge in one of the landmark cases on 'privacy', *i.e.*, *Olmstead* v. *United States*.[64] The privacy doyen gave his dissenting judgment, observing that even 'tapping of a man's telephone line may make possible 'every unjustifiable intrusion by the Government upon the privacy of the individual'[65] and the US Federal Supreme Court took 90 long years to rectify the error made in this case. The Court in an historic case of *Carpenter* v. *USA*[66] held that even the government is under requirement to obtain a prior warrant in order to access past cellphone records. The majority found that, the seismic shifts in digital technology made possible the tracking of not only carpenter's location but also everyone else's, not for a short period but for years and years.

IV

Conclusion

As a concluding remark, it is found that the Committee's attitude towards the 'right to be forgotten' has been dubious on the grounds that; a) it totally fails to understand that it has been constituted to look upon the citizen's right to protection of personal information and not the information which already has been made public either by the

---

[62] *Available at*: https://www.parliament.uk/documents/lords-committees/eu-sub-com-f/righttobeforgotten/311014-Right-to-be-forgotten-Commission.pdf. (last visited Feb., 10, 2020).

[63] European Court of Human Rights, *Delfi AS* v. *Estonia* (64569/09, Oct., 10, 2013).

[64] *Olmstead* v. *United State* 277 U.S. 438 (1928).

[65] *See* Hiroshi Miyashita, *Supra* note 51.

[66] *Carpenter* v. *United States* (585 U.S., 2018).

data principal himself or under a requirement of the law; b) it also erred in analyzing the right to be forgotten in relation to the public disclosure or public interest only, however, such a disclosure or interest again falls outside the scope of personal information or can be one of the aspect of personal information but the usage of such information is even much broader; c) by doing so the committee diminished the economic value of data by understanding only the normal and natural interaction of citizen with the social media platforms where plenty of human beings conjoin to share their interdependent feelings; d) the committee, while stressing the public and civil image of the one's information, turned it aside from amplifying the tremendous market of internet of things where tens of thousands of people participate in buying or selling or advertising goods or services and the 'personal data', in return, plays vital role in smooth functioning of internet driven market; e) the committee is seriously mistaken by completely abandoning the importance of trillion dollar business of E-commerce which almost requires no publicizing of personal information; f) the committee instead of understanding the modes of operation of the online or digital market players, good or bad intention of the same about the citizen's personal data and the data's economic value, tried to question the understanding of the data principle in relation to fairness of processing; g) it totally misunderstood the intention of the UK's House of Lords' European Union Committee and guided itself mostly by the former's approach about the 'right to be forgotten', however, in the UK there exists a 'right to erasure' which confers the same power as 'be forgotten' does; h) the committee indeed tried to surround itself by proposing 'balance of interest test' when data principal's privacy right comes in front of freedom of speech of expression of others but did not understand that the genesis of the right to be forgotten lies in the freedom of speech and expression of data subject; i) it also proposed a balance test of the 'right to be forgotten' and 'right to information' but again misguided itself as one can only have a right to information upon lawful and public information and cannot be allowed to trespass the informational personality of others acting legally; j) the committee took into its consideration the US position while working on such an important issue, actually the most important personality right of 21st century, where the right to data protection is just a baby step not even at the federal level but only in two-three states; k) the committee let itself be influenced by some hidden commentators who opposed this right to be included in the Bill, but ignored the fact that they can be social media players or free online search engine providers or an E-commerce platform which feeds their industry by processing of personal data, and in return neither wants to have any constructive liability to the data principal nor want any share in their monetary gain as they know that in the digital world data speaks aloud; l) the same also feared that the data principal may misuse this right but failed to grasp that one can only ask to erase its own data validly shared with the data fiduciary where the object of the mutual relationship came to an end. How can this can be termed as misuse is difficult to understand; m) the committee sympathized with a few companies that the same got plenty of requests to de-list the personal data and, and therefore, termed the GDPR, a legal instrument which privatized the responsibilities. Nonetheless, it seems that the committee was working not for the Indians but for the tech moguls which lobbied against this right everywhere in order to

escape from any obligation. The Regulations, however, not only obliges the controller but also makes them compliant with the same and the failure of compliance leads to a huge penalty. The committee termed it privatization but the situation is not what it felt. The rule is simply that if X makes money from my data it is X who has to take the course.

On the other hand, the present Bill is even more disturbing and inadequate than the report of the committee. It just dilutes, what has already been distorted by the committee, the right of the data principal by alluring through the bare title as a heading but actually confers restriction of processing right which is a limited and temporary protective right. The Bill further subjects the citizen to the discretion of the adjudication authority, technical mayhems, and odious form of litigation. It means that may be due to the anxiety of such a complex procedure, the data principal could not approach against the threat of the right to be forgotten.

So, the gist of the overall findings is such that the Hon'ble Committee could not understand this modern and interdisciplinary approach of law, science, technology, and society. It also lacked juristic faculty in analyzing the things ethically. It looks like a newcomers' research paper submitted in order to pass a subject in which the tutor already dictated in the class that this right has no significance, and the committee's report must reflect the same. Perhaps, someone can even say that the committee acted as a puppet of hidden players who do not want to raise their voice in public in lieu of severe distrust but ordered this committee to propose what they desired. It would be shameful and hilarious if the present Bill will be tabled before the Houses of the Parliament as the title says something else and the operative provisions something different. It is our duty as a law enthusiast to oppose this Bill not only because of breach of public trust but also because of the foolishness of the legislators because the physical meaning of the words were not considered. We must raise our concern in favor of the presence of 'right to erasure or be forgotten' in the upcoming Personal Data Protection Act. Otherwise, this future law will become a toothless tiger which cannot even afford to let its citizens' data protected in a manner it is protected in the European Union.

In the light of the above analysis, the following conclusion could be drawn:

1) The bare title of section 27, 'Right to Be Forgotten', of the proposed Bill must be replaced by 'Right to Restrict the Processing of Personal Data' because the present title is misleading.
2) A separate section on 'Right to Be Forgotten or Erasure' must be provided for in the Bill to trade off the interests of data principal and fiduciary.
3) In the 'Right to Be Forgotten' provision data principal must be equipped to compel the data fiduciary to erase or remove or delete or make inaccessible the complete or partial set of personal data that are not only under the control of the latter but also from its subsidiaries and third party data processors. It must be kept in mind that the legal provision on Forgotten right must be simple and clear in its outcome. The provision should not hassle itself among its words and phrases. The gist of this right should be removal of personal data, and, that too, up to an extent the data principal wants from the latter, of course, as feasible.

4) The 'Right to Be Forgotten' principle should not be subjected to a particular design of communication technology. This right should adhere with the principle of technological neutrality. It means that the complexity of a design network should not be pleaded as a defense against the fructification of this right. We must be aware of the fact that Tech-moguls can plead for impossibility of deletion of a piece of information when shared with third parties either on the ground of being out of their control once it is shared with others or due to the inability of their communication system to delete the data because of technical problems.
5) The present provision of Section 27 (4) & (5) and Section 28 of the Bill required for procedural and monetary burden on the data principle and the same has to first request to the data fiduciary about their exercise of the right with a reason and only then the latter will decide whether to proceed with the request so made by the former or not. Then only can the former reach to the adjudication authority. Such restriction should be removed from the way of 'Right to Be Forgotten'. There must be a supporting provision, with this right, that once a request is made by the data principle to the data fiduciary about the erasure of his/her personal data, it would be the obligation of the latter to inform and update the outcome of such request from time to time in not more than 3 days. Thereafter, the former will be free to complain with the concerning adjudicating authority if situation so warrants. Once a complaint in this regard is made, it would be the data fiduciary and the adjudication officer who can communicate with each other on such compliant. Now, the data principle should get the update on their complaint from the adjudicating authority and not from the data fiduciary.
6) Readers should understand that techies have mighty hand with a focused section of it for and on litigation. Unfortunately, it is not easy for a common man to fight them legally because of the retinue of legal professionals the former employ. A separate sub-section should be attached where adjudicating authority should be vested with the power to inquire the situation on behalf of the complainant.
7) By keeping the present days scenarios of Distributed Ledger Technology like Block-chain in mind, a data fiduciary should only be allowed to switch their current ecosystem of technology on to DLTs only if they assure the state about their ability to delete the data from the chain in which it is operating.