

**|LAW AUDIENCE JOURNAL|**  
**|VOLUME 1|ISSUE 2|DECEMBER 2018|ISSN (O): 2581-6705|**

**|LAW AUDIENCE JOURNAL™|**

**|VOLUME 1 & ISSUE 2|**

**|DECEMBER 2018|**

**|ISSN (O): 2581-6705|**

**EDITED BY:**

**LAW AUDIENCE JOURNAL'S**

**EDITORIAL BOARD**

**COPYRIGHT © 2018 BY LAW AUDIENCE JOURNAL (ISSN (O): 2581-6705)**

All Copyrights are reserved with the Authors. But, however, the Authors have granted to the Journal (Law Audience Journal), an irrevocable, non-exclusive, royalty-free and transferable license to publish, reproduce, store, transmit, display and distribute it in the Journal or books or in any form and all other media, retrieval systems and other formats now or hereafter known.

No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other non-commercial uses permitted by copyright law.

For permission requests, write to the publisher, subject of the email or letter must be "Permission required," at the email or postal address given below.

Law Audience Journal,

Mr. Varun Kumar, V.P.O. Gagret, Ward No.5, Tehsil. Ghanari, District. Una, Himachal Pradesh, Pincode: 177201,

Phone: +91-8351033361,

Email: lawjournal@lawaudience.com, info@lawaudience.com,

Website: www.lawaudience.com,

Contact Timings: 10:00 AM to 9:00 PM.

**DISCLAIMER:**

Law Audience Journal (ISSN (O): 2581-6705) and Its Editorial Board Members do not guarantee that the material published in it is 100 percent reliable. You can rely upon it at your own risk. But, however the Journal and Its Editorial Board Members have taken the proper steps to provide the readers with relevant material. Proper footnotes & references have been given to avoid any copyright or plagiarism issue. Articles published in Volume 1 & Issue 2 are the original work of the authors.

Views or Opinions or Suggestions, expressed or published in the Journal are the personal point of views of the Author(s) or Contributor(s) and the Journal & Its Editorial Board Members are not liable for the same.

While every effort has been made to avoid any mistake or omission, this publication is published online on the condition and understanding that the publisher shall not be liable in any manner to any person by reason of any mistake or omission in this publication or for any action taken or omitted to be taken or advice rendered or accepted on the basis of this work. All disputes subject to the exclusive jurisdiction of Courts, Tribunals and Forums at Himachal Pradesh only.

**RIGHT TO BE FORGOTTEN: BALANCING THE FUNDAMENTAL RIGHTS IN  
THE DIGITAL ERA.**

AUTHORED BY: MR. NITESH JINDAL & CO-AUTHORED BY: MS. SHIPHALI  
PATEL, DR. RAM MANOHAR LOHIYA NATIONAL LAW UNIVERSITY.

*“Since the beginning of time, for us humans, forgetting has been the norm and remembering  
the exception.”<sup>1</sup>*

**ABSTRACT:**

*With the emergence of Digital Eternity, everybody deserves a second chance into our digital spaces as well as real lives. The Right to be Forgotten provides people with this second chance to move beyond the shackles of their past. The concept of Right to be forgotten has not gained much traction on Indian soil. Indian courts have also been devoid to delve into much with regard to its importance and challenges it may be capable of giving rise to. Recent landmark judgment on Right to privacy does not categorically talk about the Right to be Forgotten but it can be very well inferred from the wording of judgment of Justice Sanjay Kishan Kaul. As a consequence of it, provision of the Right to be Forgotten has been incorporated under the Data Protection Bill, 2018. This provision has called into question the enforcement of various other Fundamental Rights which will be at the loggerheads with each other when the cases will start to knock the doors of the courts. Jurisprudence of Right to be Forgotten has also not developed completely around the globe. European Union and various other countries like Canada, South Africa, United States of America, etc. have also been trying to resolve the altercation between Right to be Forgotten on one side and other fundamental rights on the other side. This paper would analysis the conflict that would emerge between the Right to be Forgotten and various other Fundamental Rights with the emergence of Right to be Forgotten and how these rights will be at loggerheads with each other. This paper argues that balancing statutory test given under section 27 of Data Protection Bill, 2018 goes on to create subjectivity which may result in different outcomes of same facts and situations. This paper would pose various questions which may be helpful in bringing out the objectivity in these criterions by discussing them individually.*

---

<sup>1</sup> VIKTOR MAYER-SCHOENBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE 1 (Princeton University Press 2009).

## **1. INTRODUCTION:**

The inherent human nature is to forget. Today, due to technological advancements, forgetting has become the exception, and remembering the default.<sup>2</sup> The advent of internet has made these mailboxes, social media and online archives serve as perpetual extensions to our fallible memories.<sup>3</sup> Contrary to the permanency of technology, people change and they grow. Privacy gives them ability to evolve, to reinvent themselves from the shackles of their past.<sup>4</sup> Vivian Reding, EU Justice Commissioner, said that:

*“The internet has an almost unlimited search and memory capacity. So even tiny scraps of personal information can have a huge impact, even years after they were shared or made public”.*<sup>5</sup>

Before delving further, one question needs to be answered: What is Right to be Forgotten (RTBF)?

A committee of European Parliament in January, 2013 released an Albrecht Report which described the Right to be Forgotten (RTBF) as “the right of the individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes.”<sup>6</sup> “The right to be forgotten in the digital sphere refers to the right of individuals to request data controllers to erase any data about them from their systems.”<sup>7</sup> The Right to be Forgotten (RTBF) gives a remedy to data principle against disclosure of one’s personal data whose disclosure is no longer useful or lawful.<sup>8</sup> It is right which allows the data principle to have a control on his sensitive or personal data available online or identifiable to him in the public domain. In the famous privacy article by Samuel Warren and Louis D. Brandeis<sup>9</sup> one aspect of right to privacy is an individual’s right to control dissemination of his personal information. Keeping in view the technological improvements, this aspect of Right to Privacy has gained significance. Individuals want to limit their accessibility on internet to protect

---

<sup>2</sup> Id.

<sup>3</sup> Fred K. Nkusi, *Is The Right To Be Forgotten Important?*, THE NEW TIMES (Nov. 2, 2018, 3:39 PM), <https://www.newtimes.co.rw/section/read/196270>.

<sup>4</sup> *K.S. Puttuswamy v. U.O.I.*, (2017) 10 S.C.C. 1, 632.

<sup>5</sup> V. Reding, *The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age*, EUROPEAN COMMISSION (Nov. 18, 2018, 9:49 PM), <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26&format=PDF>.

<sup>6</sup> DAVID LINDSAY, *EMERGING CHALLENGES IN PRIVACY LAW* 290 (Cambridge University Press 2014).

<sup>7</sup> WHITE PAPER OF THE COMMITTEE OF EXPERTS, *DATA PROTECTION FRAMEWORK FOR INDIA* 137 (2018), *available at*

[http://meity.gov.in/writereaddata/files/white\\_paper\\_on\\_data\\_protection\\_in\\_india\\_18122017\\_final\\_v2.1.pdf](http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf).

<sup>8</sup> COMMITTEE OF EXPERTS UNDER THE CHAIRMANSHIP OF JUSTICE B.N. SRIKRISHNA, *FREE AND FAIR DIGITAL ECONOMY PROTECTING PRIVACY, EMPOWERING INDIANS* 78 (2018), *available at* <https://drive.google.com/file/d/1dxgNiWuyHs9eteLbOGfHquEKf-U5XZS4/view>.

<sup>9</sup> Samuel Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HAR. L. REV. 193, 199 (1890).

their personality, individuality and dignity.<sup>10</sup> As was pleaded in the Gujarat High Court case of *Dharamraj Dave v. St. of Gujarat*<sup>11</sup> where the petitioner wanted a criminal proceeding to be removed from his name search on Google as it was causing reputational damage to him, court denied his plea on the ground that people's Right to Know is greater than his Right to Privacy.

As the right is emerging all over the world, its dissent is getting louder and louder. Google's global privacy counsel, Peter Fleischer in his blogs vehemently poses this right as a movement to censor content in the name of privacy.<sup>12</sup> The trouble is that one's Right to Privacy is other's Right to Know. One's Right of be Forgotten is other's Freedom of Speech and Expression or Right to Information.

Therefore it becomes imperative to balance out these various rights which have come at loggerheads with each other with the emergence of RTBF in India. Section 27 (3) of the Data Protection Bill, 2018 provides the adjudicating authority five criteria to decide this conflict. This paper is an attempt to analyse as to how RTBF is at loggerhead with various other rights and how the adjudicating authority will try to shorten subjectivity and increase objectivity in these criteria.

## **2. HISTORICAL BACKGROUND:**

The Right to be Forgotten finds its roots under the French Law, *le droit à l'oubli*– "Right to Oblivion" a right that allows a convicted criminal who has served his time and been rehabilitated to object to the publication of the facts of his conviction and incarceration.<sup>13</sup> Right to be Forgotten finds its existence under the value of this right. The EU Data Protection Directive, 1995 acted as a legal base to the Right to be Forgotten which talks about it under Article 12(b)<sup>14</sup>. In January 2012, European Commission adopted proposals for the framework of new EU data protection laws which would repeal the Data Protection Directive (DPD) of

---

<sup>10</sup> *K.S. Puttaswamy v. U.O.I.*, (2017) 10 S.C.C. 1, 583.

<sup>11</sup> *Dharamraj Dave v. State of Gujarat*, 2015 S.C.C. Online Guj. 2019.

<sup>12</sup> Peter Fleischer, *Foggy Thinking About The Right To Oblivion*, PETER FLEISCHER: PRIVACY...? (Nov. 13, 2018, 2:28 PM), <http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html>.

<sup>13</sup> Jeffrey Rosen, *The Right To Be Forgotten*, 64 Stan. L. Rev. 88, 88 (2012).

<sup>14</sup> Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 art. 12(b) states that "as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;"

1995. The Right to be Forgotten was an important component of the proposed GDPR due to increased personal data processing and high exposure to social networking services.

This right got recognition from the landmark case of *Google Spain v. AEPD and Mario Costeja*<sup>15</sup>; in which the European Court of Justice (ECJ) held that inadequate, irrelevant or excessive data or information in relation to the purposes of the processing to be carried out by the operator of the search engine, such information and links concerned in the list of results must be erased.<sup>16</sup>

On 27<sup>th</sup> April, 2016 EU got their new data protection law; GDPR<sup>17</sup> which repealed the DPD of 1995. Article 17<sup>18</sup> of this GDPR talks about the Right to be Forgotten as ‘Right to Erasure’. Its clause (1) talks about the right and the grounds on which it can be exercised. It states that the ‘data subject’ can ask the ‘data controller’ to erase his personal data which the ‘data controller’ is obligated to erase, if a) the personal data is no longer necessary, b) the consent for its processing has been withdrawn, c) there are no legitimate grounds to continue the processing after objection, d) the data has been unlawfully processed, e) there is a legal obligation and f) if the data collected is in relation to the offer of informational society services which deals with child privacy.

As no right can be absolute, this right too has been provided with restrictions under Article 17(3)<sup>19</sup>. It says that the Right to be Forgotten won’t come in the way of exercising Freedom of Speech and Expression in complying with any legal obligation, public health, scientific or historical research purposes and establishment, exercise or defence of legal claims.

In India this right got recognition by the famous landmark privacy judgement of *K.S. Puttuswamy v. UOI*<sup>20</sup> which declared Right to Privacy as a fundamental right. This judgement linked Right to Privacy with the data processing of personal data of an individual. J. Kishan Kaul clearly explains that how knowledge about a person gives one an edge over that person. How it can influence behaviour, choice, preferences and opinion which no democracy can

---

<sup>15</sup> Case C-131/12, *Google Spain S.L. and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, [2014] E.C.R. I-317.

<sup>16</sup> Id at 94.

<sup>17</sup> Commission Regulation 2016/679, O.J. (L. 119).

<sup>18</sup> Id at art 17.

<sup>19</sup> Commission Regulation 2016/679, O.J. (L. 119).

<sup>20</sup> *K.S. Puttaswamy v. UOI*, (2017) 10 SCC 1.

afford.<sup>21</sup> This judgement led to the formation of the B.N. Srikrishna Committee to form a data protection law in India which in turn led to the formation of Data Protection Bill, 2018.

### **3. INTERNATIONAL PERSPECTIVE:**

#### **3.1 EUROPEAN UNION:**

This right was first time explicitly recognized by a court in the year 2014. European Court Justice (ECJ) in the case of *Google Spain SL v. AEPD*<sup>22</sup>, filed by Costeja, dealt with the problem regarding the two links which used to pop-up on Google on his name search. The links were of articles published by a newspaper a decade ago, which dealt with a property auction as Costeja was not able to pay off his debts.

The appearance of these links, even after years on his Google name search was causing reputational damage to him. Therefore, he asked the Spanish Data Protection Agency to order the newspaper to take the notices down and to order Google to remove links of the articles from the search pages.<sup>23</sup> The newspaper wasn't hit by the case because it falls under the exception 'media' which Google has explicitly opted out of. As the request against Google reached ECJ, the court held that though the information published by the Third Parties (here Google) is lawful and true but at the same time is irrelevant, inadequate and excessive and hence must be erased.<sup>24</sup>

It can be evidently seen how ECJ balances out the two rights, one Freedom of Speech and Expression of Google and other Right to Privacy of Costeja. Though the information gathered was lawful and true, it was causing serious reputational damages to Costeja and though people had a right to know, they need not to know about his years old catastrophe as the information has now become old and irrelevant. Hence, ECJ struck a balance between these rights and kept Costeja's Right to Privacy or Right to be Forgotten above people's Right to Know and Google's Freedom of Speech and Expression. This case was the reason as to why RTBF gained such importance in the framing of new EU data protection laws. The new EU

---

<sup>21</sup> Id 591.

<sup>22</sup> Case C-131/12, *Google Spain S.L. and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, [2014] E.C.R. I-317.

<sup>23</sup> Eric Posner, *We all have the Right to be Forgotten*, SLATE (Nov. 14, 2018, 2:23 AM), [http://www.slate.com/articles/news\\_and\\_politics/view\\_from\\_chicago/2014/05/the\\_european\\_right\\_to\\_be\\_forgotten\\_is\\_just\\_what\\_the\\_internet\\_needs.html](http://www.slate.com/articles/news_and_politics/view_from_chicago/2014/05/the_european_right_to_be_forgotten_is_just_what_the_internet_needs.html).

<sup>24</sup> Case C-131/12, *Google Spain S.L. and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, [2014] E.C.R. I-317.

GDPR released in 2016 has explicit provision of RTBF in its Article 17<sup>25</sup>, a right which would be granted to all EU countries.

### **3.2 SOUTH AFRICA:**

In South Africa Section 14 of Bill of Rights<sup>26</sup> explicitly talks about right to privacy and in line of it, Justice Harms in *National Media Ltd v Jooste*<sup>27</sup>, defined privacy in the following terms: “Privacy is an individual condition of life characterised by exclusion from the public and publicity. The condition embraces all those personal facts which a person concerned has determined him to be excluded from the knowledge of outsiders and in respect of which he has the will that they be kept private.” It is very evident from just bare reading of interpretation given by Justice Harms is that RTBF, although not explicitly talked about, is a part of Right to privacy and it is the right of the individual to decide the competency of destiny of private facts.

Section 24 of the Protection of Personal Information (POPI) Act provides the data subject to request data fiduciary to correct or delete personal information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully<sup>28</sup> and destroy or delete a record of personal information about the data subject that the responsible party is no longer authorised.<sup>29</sup>

Here also POPI Act does not explicitly talks about RTBF, it gives rights to data subject equivalent to RTBF.

### **3.3 UNITED KINGDOM:**

The emergence of this right has not been restricted only to European or civil law countries. Common law countries too seem upfront to accept the Right to be Forgotten. Recently, just 4 months back a High Court in London has granted this right to a businessman in the case of *NT1 v. Google LLC*<sup>30</sup>.

---

<sup>25</sup> Commission Regulation 2016/679, O.J. (L. 119).

<sup>26</sup> SOUTH AFRICAN CONSTITUTION, 1996 §14.

<sup>27</sup> *National Media Ltd. v. Jooste*, 1996 (3) S.A. (262) A.

<sup>28</sup> The Protection of Personal Information Act, No. 4 of 2013 §24(1)(a).

<sup>29</sup> Id at §24(1)(b).

<sup>30</sup> *NT1 v. Google L.L.C.*, [2018] E.W.H.C. 799 (Q.B.).

The case was filed two businessmen who were convicted 10 years ago, one for six months imprisonment for conspiring to intercept communications (NT 1) and other for 4 months for conspiring to account falsely (NT 2). They both wanted the links related to their conviction to be removed from Google. While deciding this case, a fair balance had to be managed between the claimant's right to data protection and privacy and the citizen's right to freedom of speech and expression and right to know.<sup>31</sup> NT1's claim was rejected by the court on the ground that he had "not accepted his guilt, had misled the public and, in the instant case, the court, and had shown no remorse over any of those matters."<sup>32</sup> He was still in business and held the capacity of misleading the public again.<sup>33</sup> Whereas, NT2's claim was accepted on the ground that he had accepted his guilt after conviction and there is no risk of any kind of repetition of his offence.<sup>34</sup>

Here we can see a fair balance has been struck between the rights of the claimant's and rights of the citizens. As NT 1 still posed threat to the society and could repeat his offence, people had a right to know about his past before dealing with him. Whereas, NT2 had shown some improvement in his behaviour, he was no longer any threat to the society hence, had a right to privacy so that he can rehabilitate and built his reputation again.

#### **4. EMERGENCE OF THE RIGHT TO BE FORGOTTEN IN INDIA:**

##### **4.1 EMERGENCE:**

The Right to be Forgotten was not originated in India but emerged by two High Court cases. The first Indian case which ever went close to talking about this right was the Gujarat High Court case of *Dharamraj Dave v. St. of Gujarat*<sup>35</sup>. In this case the petitioner was involved in charges like culpable homicide not amounting to murder. Although he was acquitted, the easily accessible judgement on the internet by his name search was causing reputational harm to him. The petitioner prayed "permanent restrain of free public exhibition of the judgement and order"<sup>36</sup>. The court rejected this plea saying that High Court is a court of record and all

---

<sup>31</sup> Id 1.

<sup>32</sup> Id 2(VII)(g).

<sup>33</sup> Id.

<sup>34</sup> Id 4V(c).

<sup>35</sup> *Dharamraj Dave v. State of Gujarat*, 2015 S.C.C. Online Guj. 2019.

<sup>36</sup> Id.

the judgements are available on the High Court website uploaded every day<sup>37</sup>. The High Court of Gujarat kept people's Right to Know<sup>38</sup> about the judgement above the petitioner's Right to Privacy<sup>39</sup>.

The next case which talked about the Right to be Forgotten is a Karnataka High Court case, ***Sri Vasunathan v. Registrar***<sup>40</sup>. In this case, for the first time this right was recognised by Indian judiciary. A woman X had filed an annulment against her husband. Later she decided to continue with her marriage and quash the charges. The order contained her name and address. Her father came before the honourable High Court of Karnataka with the request to mask his daughter's name from the order. It was apprehended that a lot of damage would be caused to her reputation and marital life due to the public accessibility of this order.

Though the court decided to make no such changes to the certified copy of the order, but assured that no internet search in the public domain regarding the order would carry her name on it. J. Byrareddy progressively stated:

*“This would be in line with the trend in the Western countries where they follow this as a matter of rule “Right to be forgotten” in sensitive cases involving women in general and highly sensitive cases involving rape or affecting the modesty and reputation of the person concerned.”*<sup>41</sup>

This case upheld a women's Right to Privacy over people's Right to Know. There can be seen a recognition of Right of be Forgotten as the information masked, though was true and lawful, was irrelevant to the public and was causing serious damages to the petitioner. Therefore, petitioner's name was allowed to be forgotten from the judgment.

## **4.2 RECOGNITION:**

This right was recognized in the ***K.S. Puttuswamy v. UOI***<sup>42</sup>, the judgement which declared Right to Privacy as a fundamental right. This judgement discussed the Right to be Forgotten in the realm of personal data processing and digital privacy for the first time in India. J. Kishan Kaul in his opinion talked about the devils of internet:

---

<sup>37</sup> Id 4.

<sup>38</sup> *Reliance Petrochemicals Ltd. v. V. Proprietors of Indian Express Newspapers*, (1998) 4 S.C.C. 592.

<sup>39</sup> INDIAN CONSTITUTION, 1950 art 21.

<sup>40</sup> *Sri Vasunathan v. Registrar*, 2017 S.C.C. Online 424.

<sup>41</sup> Id. 9.

<sup>42</sup> *K.S. Puttuswamy v. UOI*, (2017) 10 S.C.C. 1.

*“Humans forget, but the internet does not forget and  
does not let humans forget.”<sup>43</sup>*

He talks about the importance of having a control over existence on internet. He brings in the concept of second chance for whoever is *“bound by the shackles of unadvisable things which may have been done in the past.”<sup>44</sup>*

The judgement talks about how privacy is a fundamental right and leads to personal autonomy. Personal autonomy has been declared a part of Right to Privacy in the **Anuj Garg v. Hotel Assn. of India**<sup>45</sup> where the court includes the positive right of individuals to make decisions about their life and its expression under personal autonomy.<sup>46</sup> Hence, it can be said that personal autonomy of a person is control of that person on his life, his information and its public accessibility.

In this age of information it is absolutely necessary for individuals to limit their accessibility.<sup>47</sup>

J. Kishan Kaul very clearly states:

*“The information explosion has manifold advantages but also some disadvantages. The access to information, which an individual may not want to give, needs the protection of privacy.”<sup>48</sup>*

This is a call to the legislation to bring in India data protection laws. In other words, the accessibility of the personal information of a person also falls under the ambit of Right to Privacy, hence giving validity to RTBF. This judgement led to the formation of B.N. Srikrishna Committee which in turn led to the release of Data Protection Bill on 27<sup>th</sup> July, 2018.

### **4.3 DATA PROTECTION BILL, 2018:**

Data Protection Bill is a huge step for the patrons of data privacy in India. The proposed law is on lines of EU GDPR but has its own inhibitions. The bill has given a broader aspect to

---

<sup>43</sup> Id. 64.

<sup>44</sup> Id. 65.

<sup>45</sup> *AnujGarg v. Hotel Assn. of India*, (2008) 3 S.C.C. 1.

<sup>46</sup> Id. 34-35.

<sup>47</sup> *K.S. Puttuswamy v. UOI*, (2017) 10 S.C.C. 1, 584.

<sup>48</sup> Id.

**[LAW AUDIENCE JOURNAL]**  
**[VOLUME 1|ISSUE 2|DECEMBER 2018|ISSN (O): 2581-6705]**

sensitive personal data under section 3(35)<sup>49</sup> including passwords, sexual orientation, biometrics etc., trying to give complete autonomy to data subject on his own data. The proposed bill has made the grounds for processing ‘sensitive personal data’ consent-centric. They have talked about ‘explicit’ consent in section 11 of the proposed law as opposed to the general consent which we often give unknowingly by just checking a box.

The Bill in its section 27 has listed out three conditions on which an individual can exercise his “right to restrict or prevent continuing disclosure of personal data” or the Right to be Forgotten. This will be applicable if data disclosure is no longer necessary, the consent to use data has been withdrawn or if data is being used contrary to the provisions of the law. An adjudicating officer will have to determine the applicability of one of the three scenarios. The officer will also have to determine that the right of the individual to restrict use of her data over-rides the right to freedom of speech or right to information of any other citizen.<sup>50</sup> Although the bill proposed by the government has given a narrow meaning to the Right to be Forgotten. The proposed bill grants “the right to be forgotten” but deceptively defines it as disallowing further disclosure of data. It seems like an attempt to revamp the globally accepted meaning of “forgotten” to “limited recollection”. It shows as if the government is merely posing as an upholder of privacy.<sup>51</sup>

The bill has been widely criticised for various reasons. Firstly, on one hand this bill has provisions for explicit consent of the data principle before processing and on the other hand there are provisions like section 17 and 22 which provide wide discretionary powers to the Data Protection Authority under the Act.<sup>52</sup> Secondly, J. Kishan Kaul in his concurring opinion in *Puttuswamy*<sup>53</sup> clearly explains how information in the form of data can be used by state against people and how it can influence people’s opinion which can be extremely harmful for any democracy.<sup>54</sup> Yet, the bill doesn’t talk about surveillance. India was hoping that this bill would bring a comprehensive framework on surveillance - in consonance with

---

<sup>49</sup> Data Protection Bill, 2018.

<sup>50</sup> Sheikh Zoaib Saleem, *What is the Right to be Forgotten in India*, LIVEMINT (Nov. 16, 2018, 12:24 AM), <https://www.livemint.com/Money/yO3nlG7Xj4vo2VJsmo8bIL/What-is-the-right-to-be-forgotten-in-India.html>.

<sup>51</sup> Shashi Tharoor, *To Plug the Data Spill*, THE INDIAN EXPRESS (Oct. 29, 2018, 7:16 PM), <https://indianexpress.com/article/opinion/to-plug-the-data-spill-5323759/>.

<sup>52</sup> Sheikh Zoaib Saleem, *3 Things To Know About The New Draft Law On The Data Privacy*, LIVEMINT (Aug. 29, 2018, 7:37 PM), <https://www.livemint.com/Money/DiBBSI9e4ybGBI5Me0bWEI/3-things-to-know-about-the-new-draft-law-on-privacy.htm>.

<sup>53</sup> *K.S. Puttuswamy v. UOI*, (2017) 10 S.C.C. 1.

<sup>54</sup> *Id.* 591.

the international standards. However, the bill doesn't provide any substantive changes in the surveillance regime in India.<sup>55</sup> Though RTBF has not been originated in India, it is the most upcoming and dynamic fundamental right. It is a new beacon for the upholders of privacy in India. It would be interesting to see in what direction this right would turn after being discussed in the Indian Parliament.

## **5. RIGHT TO BE FORGOTTEN AT LOGGERHEADS WITH VARIOUS OTHER FUNDAMENTAL RIGHTS:**

This paper will analyse the conflict of RTBF with other various rights where both of them are fundamental rights. Firstly, this paper will highlight the conflict between individuals who want to exercise RTBF and individuals who want to exercise Freedom of Speech and Expression under Article 19(1)(a) of the Indian Constitution and secondly the conflict between RTBF and Right to know.

### **5.1 FREEDOM OF SPEECH AND EXPRESSION:**

Freedom of press, in the present era, is the heart of social and political intercourse.<sup>56</sup> Freedom of press got its constitutional sanctity not for the benefit of press but for the benefit of public good.<sup>57</sup> The primary purpose of press is to advance public interest without which a democratic institution like India would not be able to function.<sup>58</sup>

Privacy is the new black in censorship fashions. Previously people used to file cases of libel or defamation whose invoking requires speech not to be true to justify censorship. But now privacy claim will be invoked on the speech which is true.<sup>59</sup> In other words, RTBF would be emerged as a new justification for censorship, a threat to freedom of press, wherein people will bring cases of libel or defamation even when news disseminated is true in nature. Peter Fleischer, Google's global privacy counsel in his blog titled "*Foggy thinking about right to*

---

<sup>55</sup> Save our privacy team, *Initial Statement on Justice Srikrishna Committee Report* (Oct. 31, 2018, 6:44 PM), <https://saveourprivacy.in/blog/initial-statement-on-justice-srikrishna-committee-report>.

<sup>56</sup> *Indian Express Newspaper v. Union of India* para 32 (1985) 1 S.C.C. 641.

<sup>57</sup> *Time Inc. v. Hill*, SCC OnLine U.S. S.C 1, 20.

<sup>58</sup> Indian, *supra* note 56, 32.

<sup>59</sup> Peter Fleischer, *Foggy Thinking About Right to Oblivion*, PETER FLEISCHER: PRIVACY...? (Nov. 13, 2018, 8:21 PM), <http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html>.

*oblivion*<sup>60</sup> made a simple effort to remember rather difficult concept by covering three categories, each of which proposes greater threats to freedom of speech.<sup>61</sup>

First and least controversial one is “if I post something online, should I have the right to delete it again?” If I post a photo, I should be able to delete it or take it down at later point of time after having second-thought over it. Since many social networking sites like Facebook already permits me to do so, mostly it is unobjectionable. However, there is one issue i.e. whether deletion of content from his/her site would amount to deletion of content from the internet?

Moving on to the second and classical category i.e. “If I post something, and someone else copies it and re-posts it on their own site, do I have the right to delete it?” For example, I regret posting a photo having a bottle of beer in my one hand, now I want to delete it and after deleting it, I found that several of friends have downloaded or copied it and reposted it on their sites. What remedy am I left with? Should I ask my friends to delete it but what if they are refusing to do so? Should I ask the platform (e.g. Facebook) hosting the content to delete it? Here comes my privacy claim versus album owner’s freedom of expression. Should such platforms be allowed to arbitrate such entangled dilemmas where they will decide whether to uphold my privacy rights or not? i.e. Either my RTBF or album’s owner Freedom of expression.

Third category mostly relates to the freedom of press which is “If someone else posts something about me, should I have a right to delete it?” This also raises the controversial issue between Right to be forgotten emanating from Right to Privacy versus Freedom of speech and expression.

Suits will be filed against press in the courts even if the information published is true. Karnataka High court in Vasunathancase<sup>62</sup> mentioned about safeguarding the identity of rape victim or women involved in highly sensitive cases like rape where the reputation of the person is at stake.<sup>63</sup> The practical problem would arise in determining the fact that when right

---

<sup>60</sup> Id.

<sup>61</sup> Jeffery Rosen, *Right to be Forgotten*, SLR (Nov. 15, 2018, 8:25 AM), <https://www.stanfordlawreview.org/online/privacy-paradox-the-right-to-be-forgotten/>.

<sup>62</sup> *Sri Vasunathan v. The Registrar General*, 2017 S.C.C. OnLine Kar. 424.

<sup>63</sup> Id.

to privacy would override Freedom of speech and expression and wouldn't. A balancing test should be applied for this which authors would be dealing with in the next part.

The issue at hand is that as to what extent the RTBF can be compatible with the right to freedom of speech and expression – whether it will cover one category or two categories or all the categories mentioned by Peter Fleischer.<sup>64</sup> In other words, what should be the parameters where data principal would be able to exercise RTBF over the other person's freedom of expression? Another issue that will become very evident is whether laws would obligate the third parties (platform hosting the content) to delete information on request of data subjects.<sup>65</sup>

## **5.2 RIGHT TO KNOW:**

Individual desire to forget is an expression of autonomy<sup>66</sup> but it is very imperative to mention that this may impact other individual freedoms like Right to Know. Report of the committee of experts under the chairmanship of Justice B.N. Srikrishna noted that “removing publicly available information takes away from an individual's right to know at the same time” and this would bring the nature of information with regard to public realm in question.

Hon'ble Supreme Court in the case of *Advocates on Record Association v. Union of India*<sup>67</sup> while dealing with right to know of the general public on one hand and right to privacy of the individuals on the other hand noted that “the balance between transparency and confidentiality is very delicate and if some sensitive information about a particular person is made public, it can have a far reaching impact on his/her reputation and dignity.”<sup>68</sup>

Human dignity is an integral part of the constitution.<sup>69</sup> RTBF (or privacy) may help an individual to lead a life of dignity by securing the inner recesses of the human personality

---

<sup>64</sup> WHITE PAPER OF THE COMMITTEE OF EXPERTS, DATA PROTECTION FRAMEWORK FOR INDIA 137 (2018), available at

[http://meity.gov.in/writereaddata/files/white\\_paper\\_on\\_data\\_protection\\_in\\_india\\_18122017\\_final\\_v2.1.pdf](http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf).

<sup>65</sup> Peter Fleischer, *Right to be Forgotten or How to Edit*, PETER FLEISCHER: PRIVACY...? (Nov. 13, 2018, 8:20 AM), <http://peterfleischer.blogspot.com/2012/01/right-to-be-forgotten-or-how-to-edit.html>.

<sup>66</sup> COMMITTEE OF EXPERTS UNDER THE CHAIRMANSHIP OF JUSTICE B.N. SRIKRISHNA, FREE AND FAIR DIGITAL ECONOMY PROTECTING PRIVACY, EMPOWERING INDIANS 78 (2018), available at <https://drive.google.com/file/d/1dxgNiWuyHs9eteLbOGfHquEKf-U5XZS4/view>.

<sup>67</sup> *Advocates on Record Association v. Union of India*, (2016) 5 SCC 1.

<sup>68</sup> Id. 953.

<sup>69</sup> *K.S. Puttuswamy v. UOI*, (2017) 10 S.C.C. 1, 108.

**[LAW AUDIENCE JOURNAL]**  
**[VOLUME 1|ISSUE 2|DECEMBER 2018|ISSN (O): 2581-6705]**

from unwanted intrusion.<sup>70</sup> When talking about privacy, personal autonomy and liberty need to be taken into consideration. Personal autonomy<sup>71</sup> and liberty<sup>72</sup> being fundamental rights are the responsibility of the state to protect them. Personal autonomy includes both negative right and positive right. In the former sense it means “not to be subject of interference by others” and in the latter sense it means “to make decisions about their life, to express themselves and choose which activities to take part in.”<sup>73</sup>

RTBF linked to the positive autonomy refers to “the ability of individuals to limit, de-link, delete, or correct the disclosure of personal information on the internet that is misleading, embarrassing, irrelevant, or anachronistic.”<sup>74</sup> At the same time it may infringe upon the implicit<sup>75</sup> fundamental right “Right to Know” by restricting the general public from acquiring or knowing truthful and rightful information about an individual which would otherwise may prove important or relevant for them.

In light of making people aware about their “right to know”, Right to Information Act, 2005 was passed, arousing a sense of feeling of to be informed. Right to Information is a constitutional right protected under Article 19(1) (a) of the Indian constitution.<sup>76</sup>

Clash between Right to privacy and Right to information was highlighted by Hon’ble Supreme Court in the case of **Bihar Public Service Commission v. Saiyed Hussain Abbas Rizwi**<sup>77</sup> by noting that “there may be cases where the disclosure has no relationship to any public activity or interest or it may even cause unwarranted invasion of privacy of the individual.”<sup>78</sup>

The real questions are that how the court will resolve this conflict? What factors would be needed to balance out this conflict? Who would be the final authority on definition of the terms ‘misleading’, ‘embarrassing’, ‘irrelevant’ and ‘anachronistic’, despite knowing the inherent and limitless subjectivity present in them?

---

<sup>70</sup> Id. 127.

<sup>71</sup> *NALSA v. UOI*, (2014) 5 S.C.C. 438, 72.

<sup>72</sup> INDIAN CONST. Art 21.

<sup>73</sup> *NALSA v. UOI* (2014) 5 S.C.C. 438, 75.

<sup>74</sup> Michael J. Kelly and David Satola, *The Right to be Forgotten*, UNL OF ILLI. L. REV. 1, 1 (2017).

<sup>75</sup> *Advocates on Record Association v. Union of India* Page (2016) 5 SCC 1 953.

<sup>76</sup> *Secretary General, Supreme Court of India v. Subhash Chandra Agarwal*, 2010 (2011) 1 S.C.C. 496, 11.

<sup>77</sup> *Bihar Public Service Commission v. Saiyed Hussain Abbas Rizwi* (2012) 13 S.C.C. 61.

<sup>78</sup> Id. 23.

## **6. CRITERIONS FOR BALANCING OUT THE CONFLICT OF RIGHT TO BE FORGOTTEN WITH OTHER RIGHTS:**

As discussed earlier, RTBF while protecting rights and interest of data subject can override freedom of speech and expression and right of information of other individuals. In that case, Section 27(3) of the Data Protection Bill, 2018 provides adjudicating authority with five criterions to decide the applicability of RTBF. These criterions are sensitivity of personal data<sup>79</sup>, scale of disclosure of data and how much accessibility to be restricted<sup>80</sup>, role of data principle in public life<sup>81</sup>, relevance of data to public<sup>82</sup> and nature of disclosure.<sup>83</sup>

Authors are of the opinion that these criterions possess great subjectivity which may result, while adjudicating, in having different decisions under same facts and situations. This paper poses various questions which an adjudicatory authority may encounter while adjudicating a case. This paper also tries to define contours of otherwise limitless subjective criterions of section 27(3).

### **6.1 SENSITIVITY OF PERSONAL DATA:**

Publication of sensitive information can have far reaching effects and implications. However, answers to questions like what is sensitive and to what extent it will affect the data principle once publication of sensitive data is made are not clear. Who will provide the definition of “what is private”, where its context differs from person to person? There can be two types of information: first, private sensitive and second, public sensitive. Private and confidential medical information is highly sensitive to an individual.<sup>84</sup> In such cases, disclosure of even true information may affect the mental peace of an individual. For instance, court in the case of *Mr X v. Hospital Z*<sup>85</sup> dealing with the conflict between privacy and medical information noted that “disclosure of even true facts has the tendency to disturb a person’s tranquillity. It may generate many complexities in him and may even lead to the psychological problems.”<sup>86</sup> Therefore, there must be a reasonable basis for disclosure, which must serve a greater public interest as privacy of an individual is at stake here.

---

<sup>79</sup> Data Protection Bill, 2018 §27(3)(a).

<sup>80</sup> Data Protection Bill, 2018 §27(3)(b).

<sup>81</sup> Data Protection Bill, 2018 §27(3)(c).

<sup>82</sup> Data Protection Bill, 2018 §27(3)(d).

<sup>83</sup> Data Protection Bill, 2018 §27(3)(e).

<sup>84</sup> *NM and others v. Smith*, 2007 S.C.C. OnLine ZACC 6, 40.

<sup>85</sup> *Mr X v. Hospital Z*, (1998) 8 S.C.C. 296.

<sup>86</sup> *Id.* 28.

Various other examples of “private sensitive information” are intimate sex relationship, extra marital affairs, bank account numbers, Aadhar card number, financial information, health information, information received through interception of cell phones by private and public entities apart from the information received in the “public interest” and other information which will come in limelight with the passage of time as more and more cases will approach the doors of the courts.

Public sensitive information is generally in public interest which often indulges in public discourses. Report of the advisory council of Google on the RTBF<sup>87</sup> highly recommended that information towards a public interest be rarely delisted and should not be subject to much disclosure. Information related to criminal activity, opinions of the public figures (which is in itself highly controversial), public health etc. are in public interest.

Data Protection Bill, 2018 does not talk about surveillance power of the State. The bill provides certain broad exceptions in its Chapter IX. These exceptions are security of the state<sup>88</sup>, prevention, detection, investigation, prosecution of contravention of law<sup>89</sup>, data processing for the purpose of legal proceedings<sup>90</sup>, research purpose<sup>91</sup> and journalistic purpose<sup>92</sup>. Under the garb of these exceptions, the bill has given wide power to the State to keep a watch on the privacy of individuals in ways like interception of cell phones, access to virtually all kind of personal information on social media and internet, etcetera.

Hon’ble Supreme Court in the case of *Amar Singh v. Union of India*<sup>93</sup> noted that interception of telephonic conversation is invading of the privacy right of person which is a fundamental right protected under the constitution.<sup>94</sup> Therefore, interception must be carried out with sanctity. Absence of any such provision in the Data protection Bill leaves a big gaping loophole which demands immediate attention. Authors are of the opinion that processing of data may go in the wrong hands which will be a huge setback for RTBF for

---

<sup>87</sup> LUCIANO FLORIDI, REPORT OF THE ADVISORY COUNCIL TO GOOGLE ON THE RIGHT TO BE FORGOTTEN 7-14 (2018), *available at* <https://static.googleusercontent.com/media/archive.google.com/en//advisorycouncil/advisement/advisoryreport.pdf>.

<sup>88</sup> Data Protection Bill, 2018 §42.

<sup>89</sup> Data Protection Bill, 2018 §43.

<sup>90</sup> Data Protection Bill, 2018 §44.

<sup>91</sup> Data Protection Bill, 2018 §45.

<sup>92</sup> Data Protection Bill, 2018 §47.

<sup>93</sup> *Amar Singh v. Union of India*, (2011) 7 S.C.C. 69.

<sup>94</sup> *Id.* 39

keeping a strong foothold in the Indian jurisdiction. Even Justice Sanjay Kishan Kaul in *Puttaswamy*<sup>95</sup> noted that knowledge in the hands of “Big Brother” State can be used as tool to exercise control over us.<sup>96</sup>

## **6.2 SCALE OF DISCLOSURE OF DATA:**

Liberty of press must not be misunderstood to mean that press could publish what it wanted. Hon’ble SC in the case of *Sanjoy Narayan v. High Court of Allahabad*<sup>97</sup> noted that “The unbridled power of the media can become dangerous if check and balance is not inherent in it.”<sup>98</sup> Therefore, authors are of the opinion that only such information must be put to disclosure which is in public interest and serves some public good, rather than all the information in relation to data principle.

## **6.3 ROLE OF DATA PRINCIPLE IN PUBLIC LIFE:**

In this scenario, virtually all individual will fall under three categories provided by the Google’s advisory committee report. First category would comprise individuals with “clear roles in public life” like politicians, sports and celebrity stars, religious leaders, artists, etc.<sup>99</sup> Second category would comprise those individuals which have not any substantial role in public life. Third and final category would include those individuals with “limited or context specific role in public life.”<sup>100</sup> For instance, individuals who have been thrust into public eye because of some event or leading role they play within their specific community would be a perfect example of the third category.

Authors are of the opinion that disclosure of information of first category individuals would serve greater public interest since public will have an overriding interest.<sup>101</sup> However, wholesale invasion into the lives of prominent public people will be an invasion on their

---

<sup>95</sup> *K.S. Puttaswamy v. U.O.I.*, (2017) 10 S.C.C. 1.

<sup>96</sup> *Id* ¶591.

<sup>97</sup> *Sanjoy Narayan v. High Court of Allahabad*, (2011) 13 S.C.C. 155.

<sup>98</sup> *Id.* ¶6.

<sup>99</sup> LUCIANO FLORIDI, REPORT OF THE ADVISORY COUNCIL TO GOOGLE ON THE RIGHT TO BE FORGOTTEN 7-14 (2018), available at <https://static.googleusercontent.com/media/archive.google.com/en//advisorycouncil/advisement/advisoryreport.pdf>.

<sup>100</sup> LUCIANO FLORIDI, REPORT OF THE ADVISORY COUNCIL TO GOOGLE ON THE RIGHT TO BE FORGOTTEN 7-14 (2018), available at <https://static.googleusercontent.com/media/archive.google.com/en//advisorycouncil/advisement/advisoryreport.pdf>.

<sup>101</sup> *Id.*

privacy.<sup>102</sup> The real questions that would emerge will be evident from third category. It will be highly controversial as the numbers of individuals in this category will be huge and what will be line where one can say that he or she has become a public figure? News on individuals who are not considered public figures, but they did something in the past that had public importance<sup>103</sup> would pose various challenges before the adjudicating authority.

#### **6.4 RELEVANCE OF PERSONAL DATA TO THE PUBLIC:**

Passage of time and change in circumstances of data subject will be some of the criteria to determine the relevancy of the personal data for the public. Information at one point of time may be relevant but with the passage of time, its relevancy may fade away.<sup>104</sup> This relevancy of personal data would play an important role in the criminal matters. Pennsylvania court in a case<sup>105</sup> of 2015 noted that long ago crime did not make the plaintiff a present public figure and “the details about his past likely not newsworthy twenty five years after the fact”<sup>106</sup> Court further noted that his past had “no relation to any public concern.”<sup>107</sup> Time would be of much essence here especially for individuals indulged in minor crime. If their past is published after a period of time, when they are not anymore what they used to be, it may cause serious harm to their reputation and psychological conditions. However there would always be cases which would not lose their relevancy with passage of time like crimes against humanity.<sup>108</sup>

#### **6.5 NATURE OF DISCLOSURE OF PERSONAL DATA AND ACTIVITIES OF DATA FIDUCIARY:**

Here adjudicatory authority would take into account various factors like whether data fiduciary is a credible source or not, whether disclosure is a matter of public record, whether information received by the data fiduciary regarding data subject is through lawful means or unlawful means and if by latter then whether data fiduciary remains a credible source or not

---

<sup>102</sup> Samuel Warren and Louis D. Brandeis, *The Right to Privacy*, 4 H.L.R. 193, 216 (1890).

<sup>103</sup> Pere Simón Castellano, *The Right to be Forgotten under European Law: a Constitutional debate*, 16.1 LEX ELECTRONICA, 13 (2011).

<sup>104</sup> Case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, 94 (2014).

<sup>105</sup> *Hartzell v. Cummings*, 2015 P.A. D & C., 1.

<sup>106</sup> *Id.* 4.

<sup>107</sup> *Id.* 7.

<sup>108</sup> LUCIANO FLORIDI, REPORT OF THE ADVISORY COUNCIL TO GOOGLE ON THE RIGHT TO BE FORGOTTEN 7-14 (2018), available at <https://static.googleusercontent.com/media/archive.google.com/en//advisorycouncil/advisement/advisoryreport.pdf>.

or whether the information published has good motives and justifiable ends. Where publication is proved to be false and actuated by malice or personal animosity, publisher or data fiduciary in the present context would be liable for damages.<sup>109</sup>

## **7. CONCLUSION:**

This article has conceptualise the conflict between the Right to be Forgotten (RTBF) and other Fundamental Rights like Freedom of speech and expression and Right to Know which have come at crossroads not only in civil law but also in common law countries. RTBF as a concept has not evolved much in the Indian milieu and even Indian courts did not get much opportunity to ponder upon this topic barring few cases. In lieu of this, jurisprudence of RTBF is in its nascent stage around the globe. Some countries like European Union member states generally place RTBF over speech and expression and others like USA generally give impetus to its first amendment rights. In India, after Puttaswamy judgment and Section 27 of Data Protection Bill, RTBF has started to keep foothold on the Indian soil with the possibility of overriding other rights. Statutory balance test given under section 27 to balance out this conflict is very subjective in nature which will give wide powers to adjudicating authorities, so as to whether to entertain RTBF request or not, without keeping checks and balances on it. Exceptions given under chapter IX of the bill has provided “Big Brother” state the power to exercise control on virtually each and every aspect of citizens. It has created a gaping loophole which may result in the infringement of privacy of ordinary citizens. Consent of the data principal for exercising RTBF has been given weightage in the data protection bill. However, regarding the “unfairness” of data the data principle and the Adjudicating Authority may not be on the same page. What may be unfair for data subject may or may not be unfair for adjudicating authority. Where India is adamant on creating the “the new oil of 21st century”, “the world’s largest biometric database” in the form of Aadhaar, seeing data leaks in such system shows the nonchalant attitude of government towards data protection. We need a robust Data Protection system and if we couldn’t manage it then “we Indians are all sitting ducks in the world of data fraud and misuse.”<sup>110</sup>

---

<sup>109</sup> *Rajgopal v. State of Tamil Nadu*, (1994) 6 S.C.C. 632, 26.

<sup>110</sup> *Id.*