



## THE EVOLUTION OF PRIVACY AND THE ‘RIGHT TO BE FORGOTTEN’ IN THE INDIAN LEGAL LANDSCAPE

By Aditi Singh

From Army Institute of Law, Mohali

### ABSTRACT

As the requirements for consideration snowball, several countries around the globe have introduced a multitudinous array of legal frameworks like DPA (Data Protection Act) 1998 in the UK, ECPA (Electronic Communications Privacy Act of 1986) in the USA, and such others. Some special privacy laws exist only to protect delicate data like student educational records, children’s online privacy, medical records of individuals, and other private financial information in the US. Much expectedly, in India, over time, there’s been a boom with respect to privacy and data protection-related judgements and discussions. It has been a controversial topic with satisfactory developments, albeit still entangled in a mesh of issues. One of the most crucial Privacy-related advancement in the 21st Century has been the *K.S. Puttaswamy judgement* of 2017. Therein the Supreme Court declared the “Right to Privacy” a fundamental right under the Indian Constitution. And even though this has been a landmark judgement, many other

neglected requirements have come to the forefront since the data privacy landscape is broad, ever-changing, and transformative. Needless to say, there is a need for a legislative instrument that is de règle so as to confer rights on the subjects and prescribe consequences for the entity responsible in case of breaches of those defined rights. This paper deals with the advancements of privacy-related laws in India and provides a distinct emphasis to the “Right to be Forgotten” in the context of India and the UK, and the US.

### I. INTRODUCTION

In the early 1970s, the use of computers started to be majorly incorporated for the processing of personal information<sup>1</sup>, albeit fewer individuals actually used the web. However, with the advent of the 21<sup>st</sup> Century and a rapid buildup of technology therein, a staggering proliferation of Internet users can be seen around the world. As of 2021, there are 4.66 billion active internet users worldwide i.e., 59.5 percent of the global population, and out of these, India has approximately 560 million online users<sup>2</sup> with a growth rate of 7-8%<sup>3</sup>. Therefore, it is safe to say that the digital revolution has permeated all over the world while India, with various technological advancements and explosive rise in internet users, is quickly transforming into a digital economy with a large market catering to global players. This digital environment is a relatively new landscape for a country that is not only one of

<sup>1</sup> Shatakshi Singh, *Data Protection - Protection of What, Protection from Whom & Protection for Whom - An Analysis of the Legal and Judicial Provisions in India and Abroad*, 7 NLIU LR 79, 81 (2018).

<sup>2</sup> Joseph Johnson, *Global digital population as of January 2021*, STATISTA (Sept. 10, 2021, 11: 00 AM),

<https://www.statista.com/statistics/617136/digital-population-worldwide/>.

<sup>3</sup> MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY (MEITY), DATA PROTECTION IN INDIA 2 (2018), <https://digitalindia.gov.in/writereaddata/files/6.Data%20Protection%20in%20India.pdf>.



the largest IT service providers in the world but also the biggest market for these services. Therefore, we need to understand the innate capabilities and impediments of such an atmosphere, especially considering that there is no legislation defining the same.

## **II. DATA PROTECTION AND PRIVACY ADVANCEMENTS IN INDIA**

Personal data is an important essential of the digital economy, which has the capability to ‘identify’ an individual. Labelled as the “currency” of the digital economy, protection of personal data has assumed great importance in this electronically interconnected globalised world<sup>4</sup> and, facilitated by an explosion of visual and electronic media, seeks the protection of privacy of individuals. Therefore, personal information is a valuable asset that needs to be protected against unauthorized access, use, and modification, as well as against flaws and unrestrained use. Privacy and data protection require that information about individuals should not be automatically made available to other individuals and organizations. It is pertinent for everyone to possess the capability of exercising a considerable degree of control over their data and its use. Data like names, addresses, phone numbers, family information, occupation, marital status, etc., if carelessly passed off or given unauthorised access to, can lead to intrusion in privacy<sup>5</sup>. Needless to

say, an impending need for legislative protection of privacy and personal data & identity arises simultaneously to the information revolution in such a situation. Although the distinction between data protection and privacy is fundamental to legislative enactments, the same has been conceptualised all over the world by lawmakers.

Kharak Singh v. State of UP<sup>6</sup> was a landmark judgement wherein the ‘right to privacy’ was denied the status of a fundamental right on vague ratiocination. On the other hand, the case of Gobind v. State of Madhya Pradesh<sup>7</sup> marked a watershed in providing constitutional recognition to the right to privacy. Furthermore, in X v. Hospital ‘Z’<sup>8</sup>, the Supreme Court recognised an individual’s right to privacy as a facet of Article 21 of the Constitution of India. Nevertheless, there has been a horde of other judgements in this regard<sup>9</sup>. Therefore, the Right to Privacy as a fundamental right has had an extensive and laborious journey insofar as India’s legal framework is concerned until the case of K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors.<sup>10</sup> in 2017 (“Puttaswamy Judgement”) recognising the Right to Privacy as a fundamental right. And this has had a significant impact on Data Protection in India. This judgment has laid down some broad rubrics for the data protection regime<sup>11</sup>. Even though this has been a step in the right

<sup>4</sup> Diane A. MacDonald & Christine M. Streatfield, *Personal Data Privacy and the WTO*, 36 Hous. J. INT'L L. 625, 626 (2014).

<sup>5</sup> Shiv Shankar Singh, *Privacy and Data Protection in India: A Critical Assessment*, 53 JILI 663, 672 (2011).

<sup>6</sup> Kharak Singh v. State of U.P., AIR 1963 SC 1295 (India).

<sup>7</sup> Gobind v. State of Madhya Pradesh, (1975) 2 SCC 148 (India).

<sup>8</sup> X v. Hospital ‘Z’, (1998) 8 SCC 296 (India).

<sup>9</sup> M.P. Sharma v. Satish Chandra, AIR 1954 SC 300; Unni Krishna, I.P. v. State of Andhra Pradesh, AIR 1993 SC 2178; R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632; Peoples Union of Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301.

<sup>10</sup> K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCC 1 (India).

<sup>11</sup> Singh, *supra* note 1, at 85.



direction for India, the Indian Government still shoulders the dual responsibility of framing appropriate legislation for the protection of individual privacy and managing economies oiled by data since the Information Technology Act, 2000 has failed to balance the rapid technological advancements along with the ramifications arising thereof.

Up till this point, India lacks proper legislation. However, the Personal Data Protection Bill, 2019 ("PDP Bill"), i.e., based on the Report of the Justice B.N. Srikrishna Committee is approaching the standpoint seeking to provide statutory recognition of the aforementioned rights to the general public. Unfortunately, this Bill still has major complications contrasting the European Charter of Fundamental Rights (or EU Charter) and the US privacy protection laws<sup>12</sup> on certain base levels, which is a cause of concern. It is conclusively pointed out that issues like unrestricted Government control and the absence of safeguards to guarantee the right of privacy of the individuals need to be broadly discussed instead of implementing ill-conceived legislations.

The Right to Privacy is a comprehensive concept. It is noteworthy that there are certain parts to this right that require definite protection as well. In the *Puttaswamy Judgement*, the Supreme Court, among everything else, observed that "the right of an individual to exercise control over his

personal data and to be able to control his/her own life would also encompass his **right to control his existence on the Internet**."<sup>13</sup> And that privacy includes "the preservation of personal intimacies, the sanctity of family life, marriage, procreation, the home and, sexual orientation. **Privacy also connotes a right to be left alone.**"<sup>14</sup>

Therefore, every individual has the ability to limit, delink, delete, or correct the disclosure of personal information on the internet that might be misleading, embarrassing, or irrelevant<sup>15</sup> under justified circumstances. This right is known as 'RIGHT TO BE FORGOTTEN' or 'RIGHT TO ERASURE'.

### III. RIGHT TO BE FORGOTTEN

The French Jurisprudence, "*droit à l'oubli*" (i.e., right to oblivion), is the place of origination of the Right to be Forgotten. This Right was historically exploited in exceptional cases wherein an individual who had completed a criminal sentence wished to be disentangled from their criminal actions<sup>16</sup>. In the 21<sup>st</sup> Century, this right aims to establish itself as a new form of Human Rights. For instance, in situations where individuals seek anonymity with regards to the internet specifically and prefer to get rid of detrimental information pertaining to them available digitally after a certain amount of time has passed, considering there's enough justification behind the same.

<sup>12</sup> For instance, the Privacy Act, the Electronic Communications Privacy Act, The Federal Trade Commission Act (FTCA) and such else.

<sup>13</sup> See K.S. Puttaswamy, at 631 ¶ 629.

<sup>14</sup> See K.S. Puttaswamy, at 504 ¶ 307.

<sup>15</sup> Devika Sharma, *High Court emphasised the need of 'Right to be Forgotten' in cases of objectionable photos and videos of victims on social media*, SCC ONLINE BLOG (Dec. 7, 2020, 04: 30 AM),

<https://www.scconline.com/blog/post/2020/12/07/oris-sa-hc-read-how-high-court-emphasised-the-need-of-right-to-be-forgotten-in-cases-of-objectionable-photos-and-videos-of-victims-on-social-media/>

<sup>16</sup> Sowjanya S, *Right to be Forgotten: A Forgotten Part of Right to Privacy*, THE LAW BLOG (Nov. 7, 2018, 08: 00 PM), <https://thelawblog.in/2018/11/07/right-to-be-forgotten-a-forgotten-part-of-right-to-privacy/>.



The right to be forgotten enables an individual to “determine the development of his life in an autonomous way, without being perpetually or periodically stigmatized as a consequence of a specific action performed in the past.”<sup>17</sup> In simpler terms, the right to be forgotten aims to enable individuals to move past their past actions and live freely in the context of data retention, online portals, and general digital memory on the internet<sup>18</sup>. This right is extensively debated and controversial. It has been expressed as a hindrance to the right of free speech and sometimes denominated as a human right.

The General Data Protection Regulation specifies the limitations of the Right to be Forgotten, i.e., in certain areas, the Right to be Forgotten is not applicable because of the importance of the data to the public. The areas include: “the protection of the freedom of expression, interests in public health, research for historical, statistical and scientific purposes, for compliance with a legal obligation, and in cases where restriction instead of erasure should follow.”<sup>19</sup>

#### (1) Right to be Forgotten in the US and UK

It is well-known that India’s legislative framework has borrowed attributes from around the globe, specifically from the UK and the US. Therefore, its notable that the

right to be forgotten has already been recognised as a part of the right to privacy in both these countries. The European Union (EU) developed this concept and sanctioned it in the General Data Protection Regulation<sup>20</sup>. However, it is not regarded as an absolute right and necessitates to be adjusted as per the right to freedom of speech information. For instance, the England and Wales High Court, considering the “right to be forgotten,” ordered Google to delist search results referring to the spent conviction of a businessman (NT2) but rejected a similar request made by a second businessman (NT1)<sup>21</sup>. On the other hand, under the Rehabilitation of Offenders Act (UK), one’s criminal convictions become immaterial while seeking employment opportunities or during civil proceedings after a certain period of time<sup>22</sup>. In the US case of *Melvin v. Reid*, the Court opined that every person possesses “a freedom from unnecessary attacks on his character, social standing or reputation” and therein recognised the right to be forgotten as a part of the right to privacy. In yet another case, the US Supreme Court held that “there is a limit to the right to control one’s life and facts about oneself, and there is social value in published facts, and that a person cannot ignore their celebrity status merely because they want to.”<sup>23</sup>

<sup>17</sup> Alessandro Mantelero, *The EU Proposal for a General Data Protection Regulation and the Roots of the “Right to be Forgotten”*, 29 COMPUTER L. & SEC. REV. 229, 231 (2013).

<sup>18</sup> Kunika Khera, *Case Commentary: Right To Be Forgotten*, 3 JAMIA LJ 219, 219 (2018), [http://docs.manupatra.in/newsline/articles/Upload/E755F76D-D287-430F-B17E-F805666A7D33.%20Case%20Commentary-Right%20to%20be%20Forgotten%20\\_%20Civil.pdf](http://docs.manupatra.in/newsline/articles/Upload/E755F76D-D287-430F-B17E-F805666A7D33.%20Case%20Commentary-Right%20to%20be%20Forgotten%20_%20Civil.pdf).

<sup>19</sup> General Data Protection Regulation 2016/679, art. 17, 2016 O.J. (L 119) 43, 44.

<sup>20</sup> Khera, *supra* note 16, at 220.

<sup>21</sup> *NT1 & NT2 v. Google LLC*, [2018] EWHC 799 (QB).

<sup>22</sup> Charles Arthur, *Explaining the ‘right to be forgotten’ - the newest cultural shibboleth*, THE GUARDIAN (May 14, 2014, 6: 42 PM), <https://www.theguardian.com/technology/2014/may/14/explainer-right-to-be-forgotten-the-newest-cultural-shibboleth>.

<sup>23</sup> *Sidis v. F-R Pub. Corp.*, U.S. LEXIS 26, 311 U.S. 711, 61 S. Ct. 393, 85 L. Ed. 462 (1940).



Presently, the “right to be forgotten” in the UK and US has become a little more evolved. And this is conspicuous from the case of Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González<sup>24</sup>, wherein the European Court of Justice examined the counterbalancing of right to privacy and data protection with the right to information. The Court placed precedence on an individual’s right to privacy over the interest of the search engine and the public, which seems to be a categorical step regarding the advancement of the right to be forgotten and the direction it is proceeding in. It was further held that the “internet search engine operator is responsible for the processing it carries out of personal data, which appear on web pages published by third parties.”<sup>25</sup> Another approach pertaining to the erasure of data has been dealt with in Europe versus Facebook conflict, wherein even though the right to be forgotten hasn’t been used — the case illustrates the concept of data erasure by not displaying it to anybody to whom it was displayed before. Considering the fact that Facebook is a tech giant with billions of dollars and exceptional lawyers at its disposal, predictably, the case dragged on for ages. Thus, despite filing 22 complaints, over years of legal battle, in 2014, the Petitioner withdrew the complaints. Since then, multiple other lawsuits have been filed, and at the moment, the case is in front of a higher bench, and the lawsuit is still ongoing. However, after all this, it has been brought to

light that in various social networking sites, data doesn’t get deleted even though the user clicks on ‘delete’<sup>26</sup>. Needless to say, this kind of progression has proven to be beneficial for India as well.

## (2) India’s approach towards Right to be Forgotten

Currently, no statute in India provides for the Right to be forgotten or getting data erased permanently. However, the Ministry of Law and Justice, on recommendations of Justice B.N. Srikrishna Committee has included the Right to be forgotten as a statutory right in the Personal Data Protection Bill, 2019 — albeit vague by definition, Section 10 of the Bill envisages the “Right to be forgotten.”

The PDP Bill provides for right to be forgotten that “enables a data principal to restrict or prevent the continuing disclosure of his personal data by a data fiduciary where such disclosure (a) has served the purpose for which it was collected or is no longer necessary for the purpose; (b) was made with the consent of the data principal and such consent has since been withdrawn, or (c) was made contrary to the provisions of this Act or any other law for the time being in force.”

In addition to the “right to be forgotten,” the PDP Bill also recognises the “right of erasure” under Section 18. And Section 20 of the PDP Bill allows a data principal (or the natural person to whom the personal data

<sup>24</sup> Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, C-131/12 [2014] QB 1022.

<sup>25</sup> Judgment in Case C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, *Court of Justice of the European Union*, PRESS RELEASE NO. 70/14 (May 13, 2014)

<https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf>.

<sup>26</sup> M. M. Vijfinkel, *Technology and the Right to be Forgotten*, RADBOUD UNIVERSITY 15-16 (July, 2016), [https://www.ru.nl/publish/pages/769526/z\\_thesis\\_mrkvijfinkel.pdf](https://www.ru.nl/publish/pages/769526/z_thesis_mrkvijfinkel.pdf).



relates<sup>27)</sup> to “prevent or restrict the continuing disclosure of personal data, in three situations, i.e., when (a) *the data has served its purpose; or (b) the data principal withdraws his consent for collecting his personal data; or (c) when the disclosure of personal data is in violation of any existing legislation.”*

Before the introduction of the PDP Bill, several courts in India had encroached on the subject regarding the Right to be forgotten. Even though the decisions were inconsistent in interpretation, several judgements were in favour. For instance, the Delhi High Court, in the decision of Zulfiqar Ahman Khan v. Quintillion Business Media (P) Ltd.,<sup>28</sup> recognised the “Right to be forgotten” and “Right to be left alone” as an integral part of an individual’s existence. Similarly, the Karnataka High Court, in Sri Vasunathan v. The Registrar General & Ors.,<sup>29</sup> granted the Petitioner’s prayer for the removal of his daughter’s name from the cause title of cases based on searches for the case conducted on the internet. The Court further held that “it was acting in line with the trend in the western countries where they follow this as a matter of rule in sensitive cases involving women in general and highly sensitive cases involving rape or affecting the modesty and reputation of the person concerned.”<sup>30</sup>

Recently, the Orissa High Court, in the case of Subhranshu Rout v. State of Odisha,<sup>31</sup> stated in reference to the Personal Data Protection Bill that, “Section 27 of the draft Bill, 2018 contains the right to be forgotten. Under Section 27, a data principal (an

individual) has the right to prevent continuing disclosure of personal data by a data fiduciary. Court points out that the said Bill carves out the *right to be forgotten*”.

Therefore, although the absence of proper legislation pertaining to data protection, or more specifically, Right to be Forgotten, still exists, the silver lining exists in the fact that the Indian judiciary is warming up to the concept as highlighted by the aforementioned decisions of various Indian Courts. With a bit of luck, the law that will be enacted for the above-mentioned cause will safeguard and enforce the rights of individuals to be ‘left alone’ and ‘erase data’ and will not circumvent the issue instead.

#### **IV. CONCLUSION**

Privacy is a basic human right in a world where computer systems contain large amounts of sensitive and personal data. Unfortunately, nowadays, anyone can access any information related to anyone from anywhere at any time. Even though this might seem convenient, it also poses a newfound threat to private and confidential information. Consequently, this threat needs to be navigated around appropriately everywhere. India is a country with a population of billions, and out of them, millions are accessing plenitude of private data — storing, using, and processing it — which is why there’s a requirement of explicit protections against the aforementioned terrorisation. Currently, the Information Technology Act, 2000 is the only legislation for data protection, and it’s just not enough. There is an immediate requirement of distinct

<sup>27</sup> The Personal Data Protection Bill, 2019, Bill No. 373 of 2019, §3(14) (India).

<sup>28</sup> Zulfiqar Ahman Khan v. Quintillion Business Media (P) Ltd., 2019 (175) DRJ 660 (India).

<sup>29</sup> Sri Vasunathan v. The Registrar General & Ors., 2017 SCC OnLine Kar 424 (India).

<sup>30</sup> *Id.*, ¶ 9.

<sup>31</sup> Subhranshu Rout v. State of Odisha, BLAPL No. 4592 / 2020 (India).



legislation for data protection that will strike an effective balance between personal liberties and privacy. Despite the 2017 *Puttaswamy Judgement*, the PDP Bill, and its considerable recommendations, there's a long way to go even so, as far as digital protection is concerned. Under these conditions, it is exigent that the agencies involved in collecting, using, and processing private, individual data are positioned within a formal framework of accountability.

Additionally, individuals whose information is at stake must be conferred with a bundle of rights and adequate forms of legal remedy in case of infringement of their right to privacy concerning such information. Furthermore, even though the PDP Bill is a positive step towards securing data privacy and protection in India — it is riddled with loopholes that curtail the right to be forgotten. The Bill needs to incorporate uniform terms, lay down expeditious procedures to respond to requests for the removal of personal data, streamline the manner in which data is removed, and it must also be compatible with the global data security climate, among other things.

All in all, the Data Privacy landscape in India is rapidly evolving and transforming — turning more performative and protective with time. Hopefully, the same resonates with individuals as well as remain third parties and government-friendly so as to maintain a peaceful digital ecosystem.

\*\*\*\*\*