

Research Article

## Constitutional and Legal Landscape of the Right to Be Forgotten in India

Manoj Kumar Sharma \* 

*Rajiv Gandhi National University of Law, India*

Prabhjot Kaur 

*Rajiv Gandhi National University of Law, India*

**ABSTRACT:** The right to be forgotten has emerged as an important right in the internet era, where on one hand information multiplies almost every day and on the other hand, the information appears to be preserved eternally. The presence of huge amounts of information in the public domain, particularly personal information, raises concerns about privacy in the digital era where sensitive information is often retained in the public domain, at times without consent of the data holder. When examined from the perspective of criminology and penology, the availability of information in the public domain about the past behavior of people adversely affects the chances of rehabilitation and reformation due to societal taboos. This raises an important question as to why one should suffer because of their past acts, thus underscoring the importance of the right to be forgotten. This paper traces the evolution and contours of the right to be forgotten in the European Union, the UK, the USA, and India, highlighting challenges in its implementation and recognition. The constitutional and legislative measures to recognize and enforce this right have also been examined in the light of judicial decisions.

**KEYWORDS:** Right to Be Forgotten, Right to Privacy, Court, Constitution, Data.

\*Corresponding author, email: manojkumarsharma@rgnul.ac.in

Submitted: 17 July 2024 | Reviewed: 19 July 2025 | Revised: 23 August 2025 | Accepted: 29 August 2025

## I. INTRODUCTION

The right to be forgotten (RTF) has become much much-debated human right in the context of the ever-expanding reach of the internet and communication technology.<sup>1</sup> The internet has undoubtedly become a significant technological advancement, revamping how the world collects, communicates, and disseminates information.<sup>2</sup> However, the downside of the advent of the digital age is that information once published remains accessible forever until removed. In the early days of the internet, the major concerns were with reference to the technical aspects of sharing information. Today, however, there is a shift from sharing information to the concerns associated with its erasure.<sup>3</sup> With this backdrop, the right to privacy has come under serious challenge owing to the increasing accessibility to one's data, especially personal data. The eternal availability of personal data raises concerns regarding its use and misuse by third parties without the consent of the concerned individual. There are also concerns regarding the impact of past actions or writings that are available on the internet on an individual's present and future. This raises concerns as to why one should suffer because of past transactions or acts, thus underscoring the importance of the RTF.

The RTF is a crucial aspect of the right to privacy. The right to privacy has been recognized as a fundamental right in various countries, including India.<sup>4</sup> However, RTF as a facet of the right to privacy has not received much legislative or judicial attention. RTF is at a nascent stage, and therefore, the contours of the right are still unclear. Besides, there are various legal, institutional, and infrastructural challenges in the implementation of the RTF.

The effective implementation of RTF requires national and international cooperation, which further complicates the situation.<sup>5</sup> The murky scope of RTF

---

<sup>1</sup> John Dowdell, "An American Right to Be Forgotten" (2017) 52:2 Tulsa Law Review at 312.

<sup>2</sup> *Ibid.*

<sup>3</sup> J Tejasree, "The Need for the Right to be Forgotten in India" (2018) 5:1 RMLNLU Financial and Mercantile Law Review at 106.

<sup>4</sup> The Nine judge constitutional Bench in *Justice KS Puttaswamy v Union of India*, [2017] AIR 4161 declared right to privacy as a fundamental right under Article 21 of the Constitution of India.

<sup>5</sup> Naveen Thakur, "Right to Privacy — An Implicit Fundamental Right under Article 21" (1998) AIR Journal at 145.

and the implementation challenges, coupled with the lack of global recognition of RTF, necessitate a thorough examination of its contours in India vis-à-vis other countries, such as the USA, UK, and the European Union.

## II. RESEARCH METHODOLOGY

The primary aim of the present study is to conduct a holistic and comprehensive study of the constitutional and legal premise of the RTF. To achieve this end, a combination of descriptive and doctrinal methods of research has been employed.

A wide variety of sources, including legislation, rules, regulations, explanations, treaties, legal journals, rulings, and publications, have been systematically studied in the pursuit of a doctrinal perspective. These resources serve as the foundation for assessing the current state of RTF across various jurisdictions. Conceptual framework, issues, and challenges concerning RTF were analysed by studying the legal and scholarly material.

Concurrently, the descriptive method has been used to clarify the current situation of RTF. This approach makes use of qualitative analysis to give a rich and complex picture of the topic at hand.

## III. RIGHT TO PRIVACY AND RIGHT TO BE FORGOTTEN: CONCEPTUAL FRAMEWORK

RTF is an important aspect of the right to privacy. Therefore, before proceeding further, it is necessary to examine the concept of the right to privacy and the conceptual framework of RTF.

### *A. Right to Privacy*

The quest for privacy derives from the natural need of man,<sup>6</sup> to establish boundaries and to restrict the entry of others within that domain.<sup>7</sup> The right to privacy has been recognized since ancient times, albeit to a limited extent. In

---

<sup>6</sup> *Ibid.*

<sup>7</sup> G V Ramaiah, "Right to Conceive vis-à-vis Right to Birth" (1996) AIR Journal at 136.

matters related to family, marriage, procreation of children, etc., privacy has been recognized in almost all civilizations as a natural need of man.<sup>8</sup> According to Alan Westin, privacy is “the right of individuals, groups or institutions to decide for themselves when, how, and to what extent the information related to them is communicated to others.”<sup>9</sup>

Right to privacy has various dimensions. Daniel J. Solove has identified six aspects of privacy: “the right to be left alone; restricted access to one's person (physical person) or protection from unauthorised access; right to keep certain things hidden from others; control over personal information; protection of one's dignity, individuality, and persona and intimacy; the right to control and limit access to information related to intimate relationships and other private aspects of life.”<sup>10</sup>

Chief Justice Chandrachud in his concurring opinion in *Justice K.S. Puttawamy* referred to nine aspects of the right to privacy, viz. (i) privacy related to one's physical body, or *bodily privacy*.<sup>11</sup> Having the ability to stop other people from touching your body or limiting your movement is an inherent part of this freedom; (ii) *spatial privacy*, which manifests itself in the seclusion of one's physical spaces, particularly the home, and safeguarding personal and family life from unauthorized access; (iii) *communicational privacy*, the right to privacy in one's communications, including the ability to limit who can see one's messages and to control how they are used; (iv) the right to *privacy in one's property (proprietary privacy)*, including the ability to keep one's own ideas and theories secret (intellectual property); (v) the right to privacy in one's own mind, including the freedom to form one's own opinions and beliefs, which is labelled as *intellectual privacy*; (vi) the autonomy in one's intimate decisions, including those pertaining to one's sexual or procreative nature and intimate relations referred to as *decisional privacy*; (vii) *associational privacy*, which is seen in an individual's choice of which people to engage with; (viii) *behavioral privacy*, which takes into account an individual's need for privacy even when engaging in activities that are visible to the public; and (ix)

---

<sup>8</sup> *Ibid.*

<sup>9</sup> Alan F Westin, *Privacy and Freedom* (New York: Atheneum, 1967) at 167.

<sup>10</sup> Daniel J Solove, “Conceptualizing Privacy” (2002) 90 California Law Review at 1087.

<sup>11</sup> *Justice KS Puttaswamy v Union of India*, [2017] AIR 4161, *supra* note 4.

*informational privacy*, defined as the right to keep personal information private and limit who can see their possessions.

So far as recognition of the right to privacy is concerned, similar provisions are found in the *Universal Declaration of Human Rights* (UDHR).<sup>12</sup> Article 12 of UDHR protects the right to privacy and prohibits arbitrary interference with the privacy, home, family, correspondence, etc. of a human being. The provision prohibits attacks on one's honour and dignity.<sup>13</sup> Though the provision lacks a binding effect, it is a source of inspiration for jurists and activists. Similarly, Article 1,<sup>14</sup> the *International Covenant on Civil and Political Rights* (ICCPR) also enacts a provision protecting the right to privacy.<sup>15</sup>

The European Union has formally recognized privacy as a fundamental right in its legal systems since the Second World War. *The Lisbon Treaty*,<sup>16</sup> and the *European Union Charter of Fundamental Rights* (EUCFR) is instrumental in protecting privacy in the EU.<sup>17</sup> The *European Convention on Human Rights and Fundamental Freedoms* (ECHR) grants protection to the private life of an individual as a fundamental right.<sup>18</sup> The first paragraph of Article 8 states that "everyone has the right to respect for his private and family life, his home and his correspondence." Article 8 of the ECHR explicitly protects the private life of the individual as well as their family life. The provision is similar to that of the UDHR, except that the scope of the ECHR is wider since it also specifically protects 'family life' separately from the individual's private life.<sup>19</sup>

Does the American Constitution guarantee privacy? Justice Black in *Griswold v. Connecticut*,<sup>20</sup> answered this question in the negative, affirming that his perusal of the US Constitution could not trace any provision or provisions concerning the

---

<sup>12</sup> UDHR, adopted on 10<sup>th</sup> of December 1948, is a grund-norm which forms the basis of development of human rights regime across the globe.

<sup>13</sup> Article 12 of *Universal Declaration of Human Rights*, 1948.

<sup>14</sup> Article 17 of *International Covenant on Civil and Political Rights*, 1966.

<sup>15</sup> Andreea Elena Matic & Valentina Cornea, "The Right to Be Forgotten in the Online Environment" (2022) 18:2 *Acta Universitatis Danubius Juridica* at 109.

<sup>16</sup> The Lisbon Treaty was signed in 2007 and it came into force in 2009.

<sup>17</sup> It was proclaimed in 2000 and was entered into force by the Treaty of Lisbon in 2009.

<sup>18</sup> ECHR was signed by the member States on November 4, 1950 in Rome.

<sup>19</sup> Matic & Cornea, *supra* note 15.

<sup>20</sup> *Griswold v Connecticut*, [1965] 381 U.S. 479.

right of "privacy" for individuals.<sup>21</sup> However, the US Supreme Court held that the right to privacy is rooted in the US Constitution, even though it is not expressly mentioned. The US Supreme Court has, through a series of pronouncements, declared the right to privacy as a fundamental right through the interpretation of substantive due process.<sup>22</sup>

Despite judicial recognition of this right in the USA, there is no particular legislation dealing with the right to privacy alone. Instead, the US follows a sectoral approach by dealing with various aspects of privacy in different legislations, like laws dealing with healthcare information, financial records, credit cards, video rentals, information held by governmental agencies, etc.<sup>23</sup>

In the Indian context, the right to privacy or to be let alone is an integral part of personal liberty. It is essential to the autonomy, dignity, and freedom of individuals, forming a core component of liberty as guaranteed under the Constitution. Despite this, it has not been specifically provided for anywhere in the constitution, unlike in the ECHR.<sup>24</sup> Instead, it has come to the forefront as a fundamental right through judicial interpretation and construction.<sup>25</sup> The right to privacy is a component of personal liberty, devoid of which personal liberty is ineffective and incomplete in the real sense of the term. With this backdrop, the Supreme Court of India, through its series of judgments beginning with *Kharak Singh v. State of U.P. to Justice K.S. Puttaswamy*, declared that the right to privacy is an integral part of personal liberty as enshrined in the constitutional provisions.<sup>26</sup>

---

<sup>21</sup> William Beaney, "The Right to Privacy and American Law" (1966) 31:2 Law and Contemporary Problems at 253.

<sup>22</sup> *Katz v United States*, [1967]; *McIntyre v Ohio Elections Commission*, [1995]; *NAAACP v Alabama*, [1958] 357 US 449.

<sup>23</sup> Sheetal Asrani-Dann, "The Right to Privacy in the Era of Smart Governance: Concerns Raised by the Introduction of Biometric-Enabled National ID Cards in India" (2005) 47:1 Journal of the Indian Law Institute at 59.

<sup>24</sup> Komal Khare & Devershi Mishra, "Contextualising the Right to Be Forgotten in the Indian Constitution: Juxtaposing Right to Privacy and Right to Free Speech" (2017) 3:2 CALJ at 70.

<sup>25</sup> Gautam Bhatia, "State Surveillance and the Right to Privacy in India: A Constitutional Biography" (2014) 26:2 National Law School of India Review at 128.

<sup>26</sup> *Kharak Singh v State of UP*, 1963; *Govind v State of Madhya Pradesh*, [1975] AIR 1378; *State of Maharashtra v Marudhar Narayan Maidkar*, [1991] AIR 207; *Neera Mathur v Life Insurance Corporation of India*, [1992] AIR 392; *R Rajagopal v State of Tamil Nadu*, [1995] AIR 294.

### *B. Right to Be Forgotten*

The rapid expansion of the internet has created an environment where there is eternal preservation of information and where every person is believed to be the owner of his or her own personal data.<sup>27</sup> However, this seemingly permanent preservation of data has led to growing anxiety among individuals about their past behavior, and as a result, individuals are requesting the removal of data that, while factually accurate and correct when published, is now incompatible with their current personal identity. Essentially, this data may neither be false nor defamatory, yet its continued presence in the public domain can negatively affect an individual's professional and personal life, thus generating the need for the RTF. Indeed, this is the precise legal basis for the RTF, as a right related to the essential value of autonomous self-identification.<sup>28</sup> In layman's terms, RTF refers to people's ability to rectify or remove inaccurate, misleading, humiliating, irrelevant, or outdated personal information that is accessible online.<sup>29</sup>

The RTF can be understood as an individual's right to request the removal and blocking of personal information about unpleasant things that have happened in the past and which they no longer wish to be publicly accessible. This includes information that does not serve a compelling public interest and is no longer relevant. On the one hand, this privilege grants individuals the ability to shape their own history, to forget certain events and persons, and to influence what others remember about them. Conversely, it requires those to whom it is addressed to take precautions to ensure that third parties do not recall or use specific personal information about the individual.<sup>30</sup> People should have the right to demand the removal of outdated information about past penalties or photos that could cause negative scrutiny, whether uploaded by them or by third parties. This right requires measures to be taken for the removal or erasure of information regarding certain past aspects of the individual.

---

<sup>27</sup> Pew Research Center, *As AI Spreads, Experts Predict the Best and Worst Changes in Digital Life by 2035* (2023).

<sup>28</sup> Marco Rizzuti, “GDPR and the Right Be Forgotten” (2020) 2020 European Journal of Privacy Law & Technology at 107.

<sup>29</sup> Michael J Kelly & David Satola, “The Right to Be Forgotten” (2017) 1 UIII Law Review at 1.

<sup>30</sup> Ali Tasar & Melike Atas, “The Right to Be Forgotten under Protection of Personal Data Law” (2020) 23 GSI Articletter at 13.

RTF is premised on the ground that a person shall have control of the information about him and shall be able to control the content and extent of his personal data accessible to third parties.<sup>31</sup> RTF can also be defined as the right to remain silent on things that have already happened in one's life and are no longer relevant. A data subject has the right to ask a search engine to erase (de-reference) connections to websites that contain personal data about them if the data subject can provide reasonable grounds referring to their circumstances.

However, RTF is not an absolute right, despite its importance. A request to remove search results that might harm other people's rights must be carefully considered. It should be mentioned that RTF naturally lies at the intersection between the rights to privacy and reputation and the freedom of speech and expression.<sup>32</sup> Since RTF entails erasing data after usage, the question arises as to what criteria should be utilized to decide if data should be erased after its retention is no longer necessary.<sup>33</sup> The key test to be applied in RTF cases is whether the personal information in question is "inadequate, irrelevant or no longer relevant."<sup>34</sup>

RTF comprises varied aspects of privacy as it enables individuals to be left alone and have their personal information protected from public scrutiny.<sup>35</sup> It must be noted that RTF is "not an absolute right but is more than that an impossible right."<sup>36</sup> Right to privacy can be better effectuated by conferring a right enabling erasure of data that might be harmful.<sup>37</sup>

---

<sup>31</sup> Jasmine E McNealy, "The Emerging Conflict between Newsworthiness and the Right to Be Forgotten" (2012) Rochester, NY at 119 & 121.

<sup>32</sup> Shaniqua Singleton, "Balancing A Right to be Forgotten with Freedom of Expression in the Wake of Google Spain v. AEPD" (2015) 44 Georgia Journal of International & Comparative Law at 165 & 179.

<sup>33</sup> Matic & Cornea, *supra* note 15.

<sup>34</sup> Akriti Gupta & Mahima Sharma, "Data Privacy in Digital World: Right to Be Forgotten" (2018) 8:1 Nirma U LJ at 98.

<sup>35</sup> Niloy Ghosh, "Right to Be Forgotten: Balancing between Privacy and Freedom of Expression" (2022) 4:2 Indian Journal of Law and Legal Research at 1.

<sup>36</sup> Jessica Friesen, "The Impossible Right to Be Forgotten" (2021) 47:1 Rutgers Computer & Tech LJ at 173 & 176.

<sup>37</sup> Shreya Bansal & Deboleena Dutta, "Right to Be Forgotten: A Critical and Comparative Analysis" (2018) 5:1 RGNUL Financial and Mercantile Law Review at 81-82.

Therefore, RTF has been acknowledged on the premise of privacy. However, the current legislative framework is found to be insufficient due to the extraordinary development of technology and the interconnections between humans and technology, leading to the call for the establishment of a new regulatory framework.<sup>38</sup>

The idea of the RTF or the right to erasure is still in its infancy. Because of the difficulty in implementing RTF and the room for interpretation, it is a topic of controversy on a worldwide scale. With the ever-growing reach and influence of search engines and the vast reach of digital platforms, it is evident that people need stricter safeguards to keep their private information safe, which is why RTF must be acknowledged and put into practice.<sup>39</sup>

### *C. Evolution of the RTF*

The earliest conception of the RTF can be traced to the 'right to oblivion',<sup>40</sup> or *Droit à l'oubli* in French jurisprudence,<sup>41</sup> which allowed the accused to ask for the removal of the information concerning their past crime after serving their sentence, aiming to facilitate their reintegration into society.<sup>42</sup> RTF has been acknowledged by the Court of Justice of the European Union since 2014.<sup>43</sup> The inception of RTF in the EU can be traced back to the judgment in the case of *Google Spain SL & Google Inc. v Agencia Espanola de Proteccion de Datos (AEPD) & Mario Costeja Gonzalez*.<sup>44</sup>

The case of Mr. Costeja Gonzalez played a crucial role in the recognition of RTF in Europe. Mr. Costeja filed a complaint before the Spanish Data Protection Authority, raising concerns that whenever anyone enters his name in the Google search engine, the search engine takes the users to newspaper links from 1998, which covered the attachment of his property for the recovery of social security

---

<sup>38</sup> *Ibid.*

<sup>39</sup> Norbert Bernsdorff, "Search Engine Operators and the 'Right to Be Forgotten'" (2023) 1 *Journal of Personal Data Protection Law* at 37.

<sup>40</sup> Robert Bolton, "The Right to Be Forgotten: Forced Amnesia in a Technological Age" (2014), Rochester, NY at 133.

<sup>41</sup> Jeffrey Rosen, "The Right to Be Forgotten" (2012) 64 *Stanford Law Review* at 88.

<sup>42</sup> Ghosh, *supra* note 35.

<sup>43</sup> *Google Spain SL & Google Inc v Agencia Espanola de Protección de Datos (AEPD) & Mario Costeja Gonzalez*, [2014] 317 ECLI.

<sup>44</sup> *Ibid.*

debts. Although the matter had already been closed, the persistent online availability of this information was causing ongoing harm to his privacy and reputation. He claimed that his personal data should not be publicly disclosed since it is no longer relevant. The complainant wanted Google to remove the reference to attachment proceedings under the RTF. Accordingly, Google was directed to remove the personal data.

The matter was taken before the Spanish National High Court, which ruled that search engines do control the data processing and therefore play a very important role in the overall dissemination of the data. The Court ruled that data controllers like Google should resolve requests for removal of personal data and examine direct requests keeping in view the genuineness of the requests. The Court went on to hold that when data controllers like Google do not accede to the requests of the complainant, the matter may be brought before the supervisory body or the courts.

According to the court, RTF is a legitimate tool that may be used to challenge search engine companies. After deciding that data subjects had a right to be forgotten under Directive 95/46, the Court further ruled that Google must assess each request on a case-by-case basis, determining whether to grant the RTF. The main point of criticism leveled against the verdict was the Court's lack of regard for the right to freedom of expression. Additionally, some have raised concerns with the fact that Google, as a search engine provider with commercial interests, has been entrusted by the court to carry out the evaluation process rather than an independent entity. This ruling spread like wildfire over the globe. Though the Costeja case brought RTF to the limelight and is a landmark ruling on RTF, the widespread reporting of the ruling had an adverse impact so far as Mr. Costeja was concerned.<sup>45</sup> The ruling had a *Streisand effect*—when the attempt to censor or protect private information results in it becoming much more widely publicized. Accordingly, the search for Mr. Costeja's name now leads to multiple links, including a reference to his case involving his personal data regarding the attachment of properties, etc. Thus, the case brought the RTF into the limelight,

---

<sup>45</sup> *Ibid.*

but it also led to a ‘debatable’ violation of the RTF of the complainant, Mr. Costeja.<sup>46</sup>

#### IV. RTF IN OTHER JURISDICTIONS

RTF has received mixed responses in various jurisdictions across the globe.<sup>47</sup> In this section, the status of RTF in EU, USA and UK shall be traced, and in the succeeding section, the status of RTF in India shall be analyzed.

##### *A. RTF in the EU*

After the 2014 judgment of the European Union Court of Justice in the Costeja matter, the EU adopted General Data Protection Regulation 2016/679 (GDPR), which replaced Directive 95/46/EC. The GDPR rules were adopted in 2016 and implemented in 2018 to strengthen the data protection regime and to protect data privacy.<sup>48</sup>

The EU enacted GDPR to increase individual privacy in the digital age.<sup>49</sup> Article 17 of the GDPR establishes the RTF.<sup>50</sup> According to Article 17 of GDPR, a person can request data erasure and the removal of the data instantaneously in any of the six circumstances which are detailed in the Article, viz., when the purpose for the personal data was collected has been accomplished and the need for retaining data is over; when the processing of data has been objected to by the data principal; when the concerned individual has withdrawn consent; when the processing of data is unlawful as per the law of the land; where the data pertains to the services provided for remuneration to a child and a request is made for removal of the data to protect the interest of the child; and when erasure of personal data is mandated by the law of the land.

---

<sup>46</sup> Hannah Carnegy-Arbuthnott, “Privacy, Publicity, and the Right to Be Forgotten” (2023) 31:4 *Journal of Political Philosophy* at 496.

<sup>47</sup> Ajay Pal Singh & Rahul Setia, “Right to Be Forgotten: Recognition, Legislation and Acceptance in International and Domestic Domain” (2018) 6:2 *Nirma University Law Journal* at 39.

<sup>48</sup> *Ibid.*

<sup>49</sup> Henry Nunn, “Consumer Data Privacy and the First Amendment: The Right to Be Forgotten in a Room of Your Own” (2023) 56:4 *Creighton Law Review* at 541.

<sup>50</sup> Ghosh, *supra* note 35.

GDPR provides that where personal data has been made public by the data controller and as per Article 17 or other provisions, there is an obligation to erase the personal data. Considering the technology available and the cost of implementation, it is the duty of controller to take such reasonable steps, including required technical measures to ensure the erasure so requested. However, right to erasure is not absolute and is not available in certain situations.<sup>51</sup>

### B. RTF in the USA

As stated in Section III of this paper, there is no explicit guarantee of privacy in the United States Constitution; rather, the right to privacy is a product of case laws. Among other things, the United States Supreme Court interpreted the Fourth Amendment to protect an individual's right to privacy. As a result, the current state of privacy rights in the United States lacks the same textual justification as the right to freely express oneself.

This framework stands in stark contrast to the European norm of personal data protection and privacy guaranteed by the ECHR. The United States is a country where free expression often triumphs when right to privacy and freedom of speech and expression clash. For instance, if a narrative is factual, the right to free expression will allow it to be published even if the subject of the publication may be embarrassed.<sup>52</sup>

Distribution of text, images, and videos on the internet is regulated under the *Digital Millennium Copyright Act* (DMCA), which was enacted by Congress in 1998. In Section 512(c)(1)(A) of the DMCA, there is a safe harbor provision that exempts service providers from responsibility for copyright-infringing works,

---

<sup>51</sup> Right to erasure is not available when data is required:

- a) to make sure availability of the right of freedom of expression and information; or
- b) to ensure compliance with a legal obligation which calls for processing of data by Union or Member State law to which the controller is subjected to or for the performance of a task which is to be carried out in the public interest or in exercising official authority vested in the controller; or
- c) for reasons of public interest or public health; or
- d) to archive purposes in the public interest, or scientific or historical research purposes or statistical purposes; or
- e) to establish, exercise, or defend legal claims.

<sup>52</sup> *Florida Star v BJF*, [1998] 491 US at 524 & 532.

although such materials must be deleted upon notification or in response to an order.<sup>53</sup> For instance, when the service provider has the authority and capability to control the infringing behavior, the safe harbor provision can be applied if the provider does not benefit financially from the data.

To combat child pornography, another piece of legislation, *Communications Decency Act* of 1996 (CDA), was enacted, which makes it a crime to send sexually explicit or otherwise obviously inappropriate messages or images to children.<sup>54</sup> US courts have, accordingly, held the internet service provider liable in *Stratton Oakmont, Inc. v. Prodigy Services Co.* because the internet service provider had established commentator standards, utilized screening tools, and was responsible for overseeing the guidelines.<sup>55</sup> The decision led to the amendment of CDA, which provided "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."<sup>56</sup> Section 230(c) of the CDA further provides that "the interactive computer service will not be liable for any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected."<sup>57</sup>

Although right to privacy has been constitutionally recognized in the US through judicial interpretation, the RTF has often been viewed to conflict with freedom of speech and expression. The US Supreme Court was of the view that right to freedom of speech and expression is superior and there is a social value in published facts.<sup>58</sup> Accordingly, the Court ruled that contours of RTF were limited primarily because RTF does restrict the right to freedom of speech and expression.

---

<sup>53</sup> *Omnibus Consolidated and Emergency Supplemental Appropriations Act*, [1999] 112 Stat 2860.

<sup>54</sup> *Communications Decency Act*, [1996] USC 47 at 223.

<sup>55</sup> *Stratton Oakmont Inc v Prodigy Services Co*, [1995] Westlaw 323710.

<sup>56</sup> *Communications Decency Act*, USC 47, 230(c)(1), *supra* note 54.

<sup>57</sup> *Ibid*, USC 47 230 (c)(2).

<sup>58</sup> *Sidis vs F-R Publishing Corporation*, [1940] 311 US 711 61 S. Ct. 393 85 L. Ed. 462.

In the US, there is no provision for RTF as such.<sup>59</sup> In *Garcia v. Google Inc.*, the U.S. Court of Appeals for the Ninth Circuit declared that the right to be forgotten does not exist under the US law.<sup>60</sup> In this case, an actress had a brief cameo appearance in a film. When the filmmaker used that clip in another movie without her consent, Garcia received death threats. The film was broadcast on YouTube. She sought to have the content removed, arguing her control over her appearance, however, the court rejected her case because a right to be forgotten does not exist under the US framework. As stated earlier, RTF is viewed as a contradiction to free speech and expression in the US.

The first state to introduce a law on RTF in the US was New York, when it introduced *Right to Protection Bill A05323* in the State Assembly in March 2017. Under this legislation, people would have the right to request that internet resources and search engines delete content that is no longer relevant to public conversation or discussion due to being incorrect, irrelevant, insufficient, or excessive. Data that is clearly harmful to the subject and falls under one or more of these categories can be requested to be removed under the New York law.<sup>61</sup>

In the US, there is another dimension of the implementation of RTF in the online context. In most States in the US, companies can do whatever they want with someone's data without informing them.<sup>62</sup> Courts in the United States have been hesitant to place onerous legal requirements on internet intermediaries just because they operate as a conduit and temporarily store material. Courts tend to rule that service providers do not have control over third-party data when interpreting these regulations, unless a certain action is explicitly authorized by a legal requirement.<sup>63</sup> Though the law in US does not specifically provide for RTF, there is a growing number of judges and journalists who believe that information about one's criminal past or present should be protected. There is also growing

---

<sup>59</sup> Ankita Aseri, "Juxtaposing Right to be Forgotten and Copyright Law" (2020) 25:3 Journal of Intellectual Property Rights at 101.

<sup>60</sup> *Garcia v Google, Inc.*, [2015] 786 F3D 733.

<sup>61</sup> Srishti Jain, "Right to Be Forgotten and Article 19" (2022) 4:1 Indian Journal of Law and Legal Research at 3.

<sup>62</sup> Amy Beloume, "The Problems of Internet Privacy and Big Tech Companies" (2023), online: *The Science Survey* <<https://thesciencesurvey.com/news/2023/02/28/the-problems-of-internet-privacy-and-big-tech-companies/>>.

<sup>63</sup> Kelly & Satola, *supra* note 29.

public sentiment regarding the protection of RTF. Based on polling data from a 2020 study conducted by Brooke Auxier titled “Most Americans Support Right to Have Some Personal Info Removed from Online Searches,” it has been found that 85% of Americans supported some aspect of RTF and more than half (56%) were of the view that all Americans should have the right to remove negative media coverage about themselves from public search results. Additionally, 39% think that RTF should apply to data collected by law enforcement, such as criminal records.<sup>64</sup>

### C. RTF in the UK

Reference to RTF in the UK can be found in the *Rehabilitation of Offenders Act*, 1974. The Act was passed by the UK Parliament to establish that once the convict has undergone a rehabilitation period and he has not been convicted further, then the previous conviction shall be deemed as ‘spent’ and shall be ignored in future in insurance, civil matters, or employment matters. Though there are certain exceptions to this rule, the essence of the Act, being the protection of a person’s future reputation from the lifelong stigma associated with past acts, aligns with the RTF. The rationale behind the RTF is the same as that behind the Act of 1974.<sup>65</sup>

In addition, the *Data Protection Act* (DPA) of 1998 was passed to execute the Data Protection Directive 95/46/EC.<sup>66</sup> The primary focus of the 1998 DPA was on data processing regulations and protecting individuals' private information.<sup>67</sup> Until 2018, RTF, as such, did not exist in UK law, though the same protections could be deciphered from the right of privacy and data protection laws. The UK's legal environment, however, saw a dramatic shift as a result of changes in both national and international law and conditions. The government passed the *Data Protection Act* (DPA) 2018 in response to the UK's planned exit from the European Union. During the time leading up to the departure, this law transposed the GDPR exceptions into national law; after Brexit, the regulation

---

<sup>64</sup> Amy Gajda, “Privacy Rights, Internet Mug Shots, and a Right to Be Forgotten” (2023) 3:1 Journal of Free Speech Law at 109.

<sup>65</sup> Vedant Tapadia & Mridushi Damani, “The Right to Be Forgotten: An Aspect of Data Privacy” (2019) 1:4 LexForti Legal Journal at 10.

<sup>66</sup> *Data Protection Act*, (c.29), 1998.

<sup>67</sup> Dowdell, *supra* note 1.

remained in domestic law.<sup>68</sup> It is worth noting that the primary objective of the EU regulation (GDPR) was to establish a single law for data protection; however, the UK voted to leave the EU.<sup>69</sup> Therefore, in order to have smooth relations with the EU as a single market, UK data protection standards had to be equivalent to GDPR, thus leading to the enactment of the 2018 DPA.<sup>70</sup> Recently, the UK has come up with a new data protection bill, the *Data Protection and Digital Information Bill*, which is pending in the UK Parliament.<sup>71</sup>

From the foregoing discussion, it is clear that the UK has laws to ensure the RTF and regulate its implementation. The foregoing account shows that though RTF did not exist in the UK before 2018 yet the same can be inferred from the *Rehabilitation of Offenders Act*, 1974; right to privacy and data protection laws. The enactment of the *Data Protection Act*, 2018, has clearly recognized this right.<sup>72</sup>

#### *D. RTF in India*

As stated in section III, the Constitution of India and laws enacted thereunder do not specifically provide for the right to privacy. Right to privacy is the outcome of judicial interpretation of the constitutionally guaranteed fundamental rights, in particular right to life and personal liberty. Right to privacy has been conferred the status of a fundamental right by the pronouncement of a nine-judge bench decision of the Supreme Court in *Justice K.S. Puttaswamy*. Despite this, it is important to note that the Constitution of India has not explicitly recognized RTF.

---

<sup>68</sup> Franz Werro, *The Right to Be Forgotten: A Comparative Study of the Emergent Right's Evolution and Application in Europe, the Americas, and Asia* (Cham: Springer International Publishing, 2020) Ius Comparatum – Global Studies in Comparative Law.

<sup>69</sup> Judith Townend, "Data Protection and the 'Right to Be Forgotten' in Practice: A UK Perspective" (2017) 45:1 International Journal of Legal Information at 28.

<sup>70</sup> Gupta & Sharma, "Data Privacy in Digital World", *supra* note 34.

<sup>71</sup> The Data Protection and Digital Information Bill aims to update and simplify the UK's data protection framework. It contains provisions to require social media companies to retain information in connection with an investigation into the death of a child who was suspected to have died by suicide. The bill will also legislate to increase fines for nuisance calls as well as reduce 'user consent' pop-ups and banners. The bill was introduced in the 2023-2024 session of Parliament. The session ended (prorogued) on 24 May 2024 ahead of the General Election on 4 July, 2024 and so this bill was discussed but is pending till date.

<sup>72</sup> *Data Protection Act*, Section 47, *supra* note 66.

## 1. Statutory Provisions

Before proceeding to the discussion of judicial pronouncements of the Indian Constitutional Courts, it is necessary to briefly refer to some of the legislations that have a direct impact on the RTF, including the Information Technology Act, 2000; the *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules*, 2021, and the *Digital Personal Data Act*, 2023.

The *Information Technology Act* and the rules thereunder do not recognize the RTF directly. However, under Section 43A of the Act, compensation may be required for the victims of information leaks if a business, under any situation, fails to secure the information entrusted to them by the victims of the leak.

While the Government of India's *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules*, 2021, do not directly mention the RTF, it outlines the steps to be taken by an authorized Grievance Officer when a grievance is submitted regarding online material that discloses the complainant's personal information without their consent.<sup>73</sup>

Section 66(E) of the *Information Technology Act*, 2000, recognizes the right to privacy and lays down punishments for violation of privacy. Section specifies that a person can face a fine of up to 200,000 Indian Rupees, three years in jail, or both for wilfully or negligently violating someone's privacy by photographing, publishing, or transmitting an image of their private area without their consent. Furthermore, the *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules*, 2021, provide due diligence requirements for intermediaries. Rule 3 clause (1) lays down certain measures to be adopted by intermediaries while providing services to their users, including the timely removal of certain types of information.

A grievance redressal mechanism has also been provided in the intermediary rules. The names and contact details of the Grievance Officer and the mechanism for lodging complaints are required to be published on the intermediary's website. The complaint must be acknowledged within 24 hours and be resolved within fifteen days. Furthermore, if the complaint relates to the removal of any kind of

---

<sup>73</sup> Shabnam Ahmed Zaman, Saptarishi Prasad Sharma & Modhu Chanda Dey, "Right to Be Forgottwn: Socio-Legal Study" (2022) 4:1 Indian Journal of Law and Legal Research at 4.

information, it shall be acted upon within 72 hours of receipt. If the complaint is regarding the removal of content that exposes the private area of any person, it must be addressed within 24 hours of receipt.

Another important development concerning data protection in the Indian legal landscape is the enactment of the *Digital Personal Data Protection Act, 2023* (DPDP). DPDP improves on various aspects as compared to the previous versions of the draft bill.<sup>74</sup> Statutory recognition is given to RTF under DPDP. The DPDP Act applies to data processing within the territory of India and also to personal data processing outside India if it relates to the provision of goods or services in India. The decision to give such recognition is mainly influenced by Article 17 of the GDPR. Section 12 of the DPDP explains the right to correction and erasure of personal data.<sup>75</sup> It lays down that the Data Principal shall have the right to correction, completion, updating, and erasure of the personal data for the processing of which consent has been given previously.<sup>76</sup> The Data Principal has been conferred the right to make a request to the Data Fiduciary for erasure of personal data.<sup>77</sup> The Data Fiduciary has been made liable to erase the personal data unless retention is mandated under the DPDP. Thus, the DPDP Act has recognized RTF, though to a limited extent.

However, the Act has several exemptions, viz., the DPDP does not apply to state instrumentalities in the performance of functions bestowed upon them by law or in the interest of sovereignty and integrity of India or security of the State.<sup>78</sup>

---

<sup>74</sup> Siddharth Chaturvedi, “Digital Personal Data Protection Bill, 2023: An Incomplete Development” (2023), online: *The Contemporary Law Forum* <<https://tclf.in/2023/08/15/digital-personal-data-protection-bill-2023-an-incomplete-development/>>.

<sup>75</sup> Section 12 of the DPDP Act lays the statutory framework for the right to correction and erasure of personal data, giving data subjects the right to request erasure of personal data, including the right to inaccurate and misleading data.

<sup>76</sup> Data Principal is defined in the DPDP act to mean “the individual to whom the personal data relates and where such individual is (i) a child, includes the parents or lawful guardian of such a child; (ii) a person with disability, includes her lawful guardian, acting on her behalf.”

<sup>77</sup> Data Fiduciary is defined in the DPDP act to mean “any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.”

<sup>78</sup> Exemption from applicability is available to the State and any of its instrumentalities in connection with provision of subsidy, benefit, service, certificate, licence or permit etc; to comply with a court order, decree, or judgment from any law; in response to a medical emergency that poses an immediate danger to the Data Principal's or another person's life or health; to administer medical treatment to anyone in need during a public health crisis; to safeguard the safety of people or

Furthermore, the government has been conferred with the power to exempt personal data processing in certain cases.<sup>79</sup>

It is important to note that in the previous versions of the data protection bills, i.e., the 2018 and 2019 versions, as well as in the 2022 and 2023 versions, one aspect of the approach has been strikingly consistent—the exemptions granted for official tasks. The Indian data protection regulations do not apply to state surveillance agencies. The 2019 bill watered down the 2018 draft's efforts to limit exclusions and provide some checks and balances. The 2019 bill also granted the executive branch the authority to exclude any national security agency from the proposed law in whole or in part. Under the DPDP Act, the government will continue to be able to utilize data for purposes unrelated to security. Finally, it has already been mentioned that the DPDP Act grants the government an excessive amount of discretion in certain instances.<sup>80</sup>

Analysis of the previous versions of law and the DPDP Act shows that RTF in India has been diluted and has simply been recast as the right to erasure. In light of various exemptions, the scope of RTF in India is much lesser than the contours of the right under GDPR.

## 2. Judicial Decisions

After having discussed the legal provisions in India, it is important to investigate the judicial landscape of the RTF in India. In this section, the decisions of the constitutional courts regarding RTF shall be discussed.

In *Justice KS Puttaswamy vs. Union of India*, the Supreme Court of India expressed that RTF was a part of the more extensive right to privacy.<sup>81</sup> The Court ruled that RTF is recognized in the fundamental rights, primarily Article 21's right to privacy.

---

provide them with assistance or services in the event of a natural disaster or a collapse of public order; for reasons related to employment or protecting the employer from loss or liability, like preventing corporate espionage, keeping trade secrets, intellectual property, and classified information confidential etc.

<sup>79</sup> *The Digital Personal Data Protection Act*, Act 22, c III, IV, IX s 7,9,17 and 40, 2023.

<sup>80</sup> Anirudh Burman, *Understanding India's New Data Protection Law* (Washington DC: Carnegie Endowment for International Peace, 2023) at 12.

<sup>81</sup> *Justice KS Puttaswamy v Union of India*, 10 SCC 1, *supra* note 4.

In 2019, in the case of *Zulfiqar Ahman Khan v. Quintillion Business Media Pvt. Ltd.*, the court again highlighted and affirmed the petitioner's "right to be left alone" and their RTF.<sup>82</sup> The case involved two articles published against the petitioner during the 'MeToo movement.' The petitioner contended for the removal of these articles from the public domain as they affected his reputation. The court decided in favour of the petitioner and opined that the petitioner has the RTF.

In another case, *Sri Vasunathan v. Registrar General*, the Court allowed RTF to a married woman on the request of her father to remove her name from the previous litigation about the annulment of her marriage.<sup>83</sup> However, in this case, the Court recognized RTF due to the sensitivity of the matter and to protect the modesty of women, not under the ambit of the right to privacy.

In *Subbranshu Rout v. State of Odisha*, the court was dealing with a rape case wherein the perpetrator had taken a video of the incident and had uploaded it on social media.<sup>84</sup> The Court observed that, although there are strict laws to deal with such heinous crimes and to address the questions of privacy of victims, the RTF has not been recognized in India despite growing demand. The Court held that the victim had the right to seek appropriate orders to remove objectionable content from the internet.

In *Jorawer Singh Mundy v. Union of India*, the Delhi High Court gave an Indian American citizen the right to request that a judgment be taken down from Google, Indian Kanoon, vLex.in, and other law websites when the accused was found not guilty.<sup>85</sup>

In *X v. https://www.youtube.com/watch?v=iq6k5z3zys0*, the plaintiff asked the court to grant an interim stay against the publication, etc., of several videos on the ground that the content violated her right to privacy.<sup>86</sup> The Court ruled that the right to privacy includes the RTF and the right to be left alone as intrinsic aspects of privacy. As a result, the court ruled that the plaintiff had a right to privacy, particularly when her person is being seen in a public forum against her will.

---

<sup>82</sup> *Zulfiqar Ahman Khan v Quintillion Business Media Pvt Ltd and Ors*, [2019] 175 DRJ 660.

<sup>83</sup> *Sri Vasunathan v Registrar General*, [2017] SCC Online 424.

<sup>84</sup> *Subbranshu Rout v State of Odisha*, [2020] SCC Online 878.

<sup>85</sup> *Jorawer Singh Mundy v Union of India*, [2021] WP(C) 3918.

<sup>86</sup> *X v https://www.youtube.com/watch?v=iq6k5z3zys0*, [2021] SCC Online 4193, 4 RCR (Cri) 19.

Recognizing RTF, the Court directed the removal of the content and also prohibited the uploading, publication, dissemination, etc. of the content.

In *SJ v. Union of India*, the petition sought directions for the removal of online publications and articles against the petitioner by the respondents.<sup>87</sup> The court reiterated that RTF and the right to be left alone are important facets of the right to privacy. Taking note of the same, the court allowed the removal of publications and articles against the petitioner.

In *Vysakh K.G. v. Union of India*, numerous petitions were clubbed together to finally determine the questions involved.<sup>88</sup> The party to the proceedings requested the removal of names and addresses from the cause title and body of the judgment to protect his or her right to privacy. The Kerala High Court ruled that the RTF and the right to be delisted are important aspects in a digital setting. The Court concluded that RTF can be used to legally wipe memories, allowing people to move forward with dignity. The Court opined that when an individual or entity is ultimately determined to be innocent of any wrongdoing in a criminal prosecution, they should be able to swiftly remove any internet references to their name by utilizing their right to erasure. In a claim based on RTF, the primary consideration is the party's desire to put the past in the past and focus on the present and future in an honest and good-hearted way so that they may move on with their lives.

*X v. Union of India* again presented an opportunity to the High Court of Delhi to consider the contours of RTF.<sup>89</sup> The High Court of Delhi, after considering the previous precedents, ruled that search engines may not feign helplessness in disabling links containing illegal content. The Court ruled that search engines undoubtedly have the responsibility to disable access to the content that is offensive in nature. The search engines cannot brush aside their responsibility in such circumstances.

---

<sup>87</sup> *SJ v Union of India*, [2023] SCC Online 3309, 2 HCC 520.

<sup>88</sup> *Vysakh KG v Union of India*, [2023] SCC Onlone 7337, 1 KLJ 227, 1 KLT 83.

<sup>89</sup> *X v Union of India*, [2023] SCC Online 2361.

## V. ISSUES AND CHALLENGES IN IMPLEMENTATION OF RTF

Although there are many developments with respect to RTF, this right is in an infant stage, and there are many issues and challenges associated with its implementation. Evolution of RTF in many jurisdictions has been viewed as an inhibition of freedom of expression, and these two rights are often viewed as conflicting. In the absence of RTF being explicitly guaranteed in the constitutions, the right to freedom of expression is generally given higher priority, especially in countries like the USA. However, as pointed out by Professor Luciano Floridi, who served on Google's Advisory Council, it is best not to rank these rights in a hierarchical order but instead, "one is better off saying that it depends on specific instances, contexts and practices, and there is no useful, general way of establishing a *priori* what comes first and what comes later, but only intelligence and wise discernment."<sup>90</sup>

In this section, the discussion shall be focused on the issues and challenges in the recognition and implementation of RTF.

### *A. Sharenting and RTF*

Parents across the world love to share pictures, content, videos etc. of their children out of natural love and affection and the keenness to share their joy with the world. The sharing of images, posts, and videos on social media containing personal information by parents of their wards is referred to as 'sharenting'. Sharenting has its own set of issues and challenges. On the one hand, parents want to share the lovely and funny moments of their children on social media. On the other hand, the process leads to sharing of the child's personal information with the world at large. Some parents resort to oversharing about the lives of their children, which can lead to disclosure of huge amount of personal information regarding the children. If this information is allowed to stay permanently on the internet, it may cause embarrassment to the child in future and may lead to identity theft, bullying, loss of employment etc. The content relating to the child is shared by the parents without the consent of the children and even otherwise, children are not capable of giving a valid consent due to their

---

<sup>90</sup> Kelly & Satola, *supra* note 29, at 39.

age.<sup>91</sup> Therefore, the child's future may be affected adversely by sharenting, necessitating the need for regulation.

RTF in the context of children is very important, but recognition of the RTF of the child can lead to conflicts between the parental interest in sharenting and the child's interest in privacy. Thus, the issue of the regulation of sharenting is complex.

As far as the EU is concerned, RTF for children can be effectuated through Article 17 of GDPR. Under Article 17, GDPR, data subject and in case of children less than 16, the parents or guardians can request for the removal of data. In case of children above 16, GDPR empowers them to directly request the removal of personal data affecting their reputation from search engine results.<sup>92</sup> Additionally, individuals can also exercise RTF once they reach the age of majority.<sup>93</sup> However, Article 17 also contains certain exceptions. These include that the data controller is not bound to erase the personal data where such data processing is essential for the exercise of a right to freedom of speech or information.

The French National Assembly has passed a bill regulating sharenting.<sup>94</sup> Under the new law, children can exercise their RTF once they attain majority. Further, the bill gives children control over their images and mandates parents to involve children, keeping in view their age and maturity level, before sharing their images online. Thus, the consent of the children will have to be obtained before uploading images and sharing information, thereby preventing future privacy violations. The parents can also be banned by the court from posting pictures of their children online.

In India, the *Information Technology Act*, 2000, does not regulate sharenting. Section 67B of the IT Act does make a provision criminalizing the publication of obscene

---

<sup>91</sup> Julia Anna Joseph, “‘Sharenting Problem’ in the Backdrop of Indian Legislation” (2023) 7:3 NUJS Journal of Regulatory Studies at 43.

<sup>92</sup> Keltie Haley, “Sharenting and the (Potential) Right to Be Forgotten” (2020) 95:3 Indiana Law Journal.

<sup>93</sup> *Ibid.*

<sup>94</sup> Laura Kayali, “France Aims to Protect Kids from Parents Oversharing Pics Online” (2023), online: *Politico* <<https://www.politico.eu/article/emmanuel-macron-france-law-aims-to-protect-kids-against-oversharing-parents/>>.

material concerning children. DPDP also does not regulate sharenting. Furthermore, DPDP does not regulate personal data shared for domestic or personal purposes.<sup>95</sup> Section 9(1) of DPDP makes a provision for obtaining the verifiable consent of the parent or the lawful guardian of the children if they wish to process the personal data of the children.<sup>96</sup>

Unlike various other jurisdictions, sharenting is not legally regulated as such in India. Recognition of the RTF of the child and regulation of sharenting as part of the RTF of the child is a grey area which will need consideration from the regulators and policy makers in the near future, who may have to take some inputs from the French experiment.

### *B. Contours of RTF*

RTF is a relatively new concept for legal jurisprudence and is in its infant stage. Despite the availability of references to this right in various judicial systems, this right has not been defined precisely. The scope and contours of this right vary across jurisdictions wherever RTF has been recognized. In some countries, including the EU, RTF has been given an expansive meaning, whereas in India and US, RTF has a rather narrow scope. There is a dire need to have conceptual clarity regarding the boundaries of the RTF if people are really to be enabled to have their digital footprints forgotten and to free themselves from persistent data shadows.<sup>97</sup>

What is right to erasure, what is included in RTF, and when can information be deleted? For example, Lisa Owings has suggested a three-fold test for a person requesting removal of data. Owings is of the opinion that these folds may stand alone. Owings feels that it is enough to require a website to delete the data if the data meets any one-fold. Furthermore, the websites might also gain if the users are allowed to delete their own data, albeit this feature would not always be available. One way to look at the criteria is as follows: if the information is personal or would offend a reasonable person but is not newsworthy, the person may decide not to publish it. Second, if a person has the right to publish data, he

---

<sup>95</sup> *The Digital Personal Data Protection Act*, Act 22, C I, s 3 (c), *supra* note 79.

<sup>96</sup> *Ibid*, Act 22, c II, s 9(1).

<sup>97</sup> Bert-Jaap Koops, “Forgetting Footprints, Shunning Shadows. A Critical Analysis Of The “Right To Be Forgotten” In Big Data Practice” (2011) 8:3 Scripted at 229.

may also be able to withdraw or have removed any material that is either personally identifiable or an expression of his opinion that he has posted. Any data that the individual chooses to share should be subject to this rule and this rule should not be limited to only sensitive information like financial or medical records. The third way is that someone may ask for the removal of material if it is irrelevant, has gone out of date, and there is no good reason for the data to be kept online.<sup>98</sup> Be that as it may, the contours of the right are still debatable and the scope of the right is still murky.

So far as India is concerned, there are many exemptions regarding the applicability of RTF, narrowing the scope of the right. Furthermore, in India, legislature has recognized RTF only in the latter half of 2023 and the implementation mechanism is yet to be put in place. Therefore, the contours of the right are still at a nascent stage and will develop over a period of time.

### *C. Issue of Jurisdiction*

The implementation of RTF is tedious due to the borderless nature of the internet. The information on the internet can be uploaded anywhere in the world and can be accessed almost everywhere. However, states cannot implement their laws outside their jurisdiction. This raises the issue of the efficacious implementation of RTF when the nation states cannot erase data controlled from outside their jurisdiction.

The deletion of data from the public domain involves complex considerations which are required to be taken into account to identify the data, determine its relevance, and ensure erasure of the data from the internet space.<sup>99</sup> If the data controller is out of the jurisdiction of the state where the erasure request is made, such a nation-state would not be in a position to help the individual. Furthermore, as RTF is not a universally accepted right and only a few countries have recognized RTF, there is hardly any platform for coordination among nations for the erasure of personal data. Therefore, the implementation of RTF is marred by jurisdictional issues.

---

<sup>98</sup> Lisa Owings, “The Right To Be Forgotten” (2016) 9:1 Akron Intellectual Property Journal at 76.

<sup>99</sup> Prashant Mali, “Privacy Law: Right to Be Forgotten in India” (2018) 7:1 NLIU Law Review at 1.

#### *D. RTF and Freedom of Speech and Expression*

Freedom of speech and expression is a fundamental right in many jurisdictions, including India and the US. In the present information age, freedom of speech and expression has received greater focus from citizens as well as the judiciary. RTF may collide with freedom of speech and expression. On the one hand, citizens want control over their personal data, while on the other, the information society wants greater information to enable them to express.<sup>100</sup> The judicial precedents in India and the US have shown that the constitutional courts generally lean in favour of protecting freedom of speech and expression (which is a constitutional right) when it comes into conflict with RTF.

#### *E. Implementation Mechanism*

The implementation mechanism for RTF is a serious challenge. The intermediaries will be inundated with requests to delete private information from the public domain. To deal with such a situation, there will be a need for separate machinery to address such requests, specifically to investigate the genuine claims and to adjudicate which one needs to be agreed upon. There is a need to have data protection institutions dealing with personal data of the data principals, but also there is a need to have a monitoring mechanism and a grievance redressal mechanism. The institutional mechanism would be required to deal with requests received from within and outside the country, requiring additional technical resources and expertise. The aggrieved person may also approach the judicial system, leading to the burdening of the already overburdened judicial system.

Apart, recognition of RTF will pose a challenge for journalism. Deleting information from public access will lead to the permanent disappearance of stories. There will be no measures for their revival in the future. People will lack references to past incidents, which may lead to unconnected and incomplete information.

---

<sup>100</sup> Information society is 'a society in which the creation, distribution and treatment of information, based on the use of ICT, have become the most significant economic and cultural activities. See United Nations Unniversity, *Knowledge Societies Policy Handbook* (2016) at 8.

## VI. CONCLUSION

RTF is a new dimension of human rights. RTF, also known as right to oblivion or right to erasure, is a new, distinct, and independent right but it has not been recognized as a constitutional right in many jurisdictions. It is further important to underscore that even fundamental rights, such as the right to privacy, are not absolute. There may be reasonable restriction on their exercise. In addition, these rights are required to be harmonised in case of conflict, for example, the right to information and the right to free speech and expression can be viewed as conflicting with RTF. But it must be noted that though RTF and free speech are perceived as mutually exclusive, in reality they are interdependent. RTF would strengthen the right to free expression since people will not inhibit while expressing themselves due to fear that their expression would cause future problems. If we guarantee RTF, people will lose the fear that their expression would be detrimental to them in future, and hence RTF would indeed promote freedom of speech and expression. Not only will this right help safeguard biometric and personally identifiable information, but it will also strengthen free expression, broaden the reach of the right to privacy, and apply it more broadly to digital information.

Thus, there is a need to have a system to safeguard everyone's privacy in light of the proliferation of easily accessible information through search engines and other technological advancements. Data insecurity and exploitation of any type of personal information can be put to rest with the implementation of the RTF in relation to search engines in India and elsewhere. But RTF should not be confined to the right to erasure or the right to have one's identity erased from criminal records or from crimes committed as a minor; it should cover the digital footprint of all citizens, taking into account the right to privacy and, more specifically, the right to oblivion.<sup>101</sup>

Further, it must be noted that when it comes to digital immortality, RTF at the domestic level is not the only solution. This is because it is fundamentally a domestic reaction to a global problem.<sup>102</sup> Thus, in theory, RTF may appear to be

---

<sup>101</sup> Dowdell, *supra* note 1.

<sup>102</sup> Michael Douglas, "Questioning the Right to be Forgotten" (13 July 2016) Rochester, NY at 109.

an all-important right expanding the domain of rights available to citizens, yet in practice, this is a very complicated domain.<sup>103</sup>

## ACKNOWLEDGMENTS

None.

## REFERENCES

*Communications Decency Act*, 1996.

*Data Protection Act*, 1998.

*International Covenant on Civil and Political Rights*, 1966.

*Omnibus Consolidated and Emergency Supplemental Appropriations Act*, 1999.

*The Digital Personal Data Protection Act*, 2023.

*Universal Declaration of Human Rights*, 1948.

*Florida Star v BJR*, 1998.

*Garcia v Google, Inc*, 2015.

*Google Spain SL & Google Inc v Agencia Española de Protección de Datos (AEPD) & Mario Costeja González* [2014] 317 ECLI .

*Govind v State of Madhya Pradesh*, [1975] AIR 1378.

*Griswold v Connecticut*, 1965.

*Jorawer Singh Mundy v Union of India*, 2021.

*Justice KS Puttaswamy v Union of India*, [2017] AIR 4161.

*Katz v United States*, 1967.

*Kharak Singh v State of UP*, 1963.

*McIntyre v Ohio Elections Commission*, 1995.

*NAAACP v Alabama*, 1958.

---

<sup>103</sup> Harikartik Ramesh & Kali Srikari Kancherla, “Unattainable Balances: The Right to be Forgotten” (2020), online: *NLIU Law Review* at 422.

*Neera Mathur v Life Insurance Corporation of India*, [1992] AIR 392.

*R Rajagopal v State of Tamil Nadu*, [1995] AIR 294.

*Sidis vs F-R Publishing Corporation*, 1940.

*SJ v Union of India*, 2023.

*Sri Vasunathan v Registrar General*, 2017.

*State of Maharashtra v Marudhar Narayan Maidkar*, [1991] AIR 207.

*Stratton Oakmont Inc v Prodigy Services Co*, [1995] Westlaw 323710 .

*Subhranshu Rout v State of Odisha*, 2020.

*Vysakh KG v Union of India*, 2023.

*X v https://www.youtube.com/watch?v=iq6k5z3zys0*, 2021.

*X v Union of India*, 2023.

*Zulfiqar Ahman Khan v Quintillion Business Media Pvt Ltd and Ors*, 2019.

Burman, Anirudh, *Understanding India's New Data Protection Law* (Washington DC: Carnegie Endowment for International Peace, 2023).

Pew Research Center, *As AI Spreads, Experts Predict the Best and Worst Changes in Digital Life by 2035* (2023).

United Nations Unniversity, *Knowledge Societies Policy Handbook* (2016).

Werro, Franz, *The Right to Be Forgotten: A Comparative Study of the Emergent Right's Evolution and Application in Europe, the Americas, and Asia* (Cham: Springer International Publishing, 2020) Ius Comparatum – Global Studies in Comparative Law.

Westin, Alan F, *Privacy and Freedom* (New York: Atheneum, 1967).

Aseri, Ankita, “Juxtaposing Right to be Forgotten and Copyright Law” (2020) 25:3 Journal of Intellectual Property Rights.

Asrani-Dann, Sheetal, “The Right to Privacy in the Era of Smart Governance: Concerns Raised by the Introduction of Biometric-Enabled National Id Cards in India” (2005) 47:1 Journal of the Indian Law Institute.

Bansal, Shreya & Deboleena Dutta, “Right to Be Forgotten: A Critical and Comparative Analysis” (2018) 5:1 RGNUL Financial and Mercantile Law Review.

Beaney, William, “The Right to Privacy and American Law” (1966) 31:2 Law and Contemporary Problems.

Bernsdorff, Norbert, “Search Engine Operators and the ‘Right to Be Forgotten’” (2023) 1 Journal of Personal Data Protection Law.

Bhatia, Gautam, “State Surveillance and the Right to Privacy in India: A Constitutional Biography” (2014) 26:2 National Law School of India Review.

Carnegy-Arbuthnott, Hannah, “Privacy, Publicity, and the Right to Be Forgotten” (2023) 31:4 Journal of Political Philosophy.

Dowdell, John, “An American Right to Be Forgotten” (2017) 52:2 Tulsa Law Review.

Friesen, Jessica, “The Impossible Right to Be Forgotten” (2021) 47:1 Rutgers Computer & Tech LJ.

Gajda, Amy, “Privacy Rights, Internet Mug Shots, and a Right to Be Forgotten” (2023) 3:1 Journal of Free Speech Law.

Ghosh, Niloy, “Right to Be Forgotten: Balancing between Privacy and Freedom of Expression” (2022) 4:2 Indian Journal of Law and Legal Research.

Gupta, Akriti & Mahima Sharma, “Data Privacy in Digital World: Right to Be Forgotten” (2018) 8:1 Nirma U LJ.

Haley, Keltie, “Sharenting and the (Potential) Right to Be Forgotten” (2020) 95:3 Indiana Law Journal.

Jain, Srishti, “Right to Be Forgotten and Article 19” (2022) 4:1 Indian Journal of Law and Legal Research.

Joseph, Julia Anna, “‘Sharenting Problem’ in the Backdrop of Indian Legislation” (2023) 7:3 NUJS Journal of Regulatory Studies.

Kelly, Michael J & David Satola, “The Right to Be Forgotten” (2017) 1 UIII Law Review.

Khare, Komal & Devershi Mishra, “Contextualising the Right to Be Forgotten in the Indian Constitution: Juxtaposing Right to Privacy and Right to Free Speech” (2017) 3:2 CALJ.

Koops, Bert-Jaap, “Forgetting Footprints, Shunning Shadows. A Critical Analysis Of The “Right To Be Forgotten” In Big Data Practice” (2011) 8:3 SCRIPTed.

Mali, Prashant, “Privacy Law: Right to Be Forgotten in India” (2018) 7:1 NLIU Law Review.

Matic, Andreea Elena & Valentina Cornea, “The Right to Be Forgotten in the Online Environment” (2022) 18:2 Acta Universitatis Danubius Juridica.

Nunn, Henry, “Consumer Data Privacy and the First Amendment: The Right to Be Forgotten in a Room of Your Own” (2023) 56:4 Creighton Law Review.

Owings, Lisa, “The Right To Be Forgotten” (2016) 9:1 Akron Intellectual Property Journal.

Ramaiah, G V, “Right to Conceive vis-à-vis Right to Birth” (1996) AIR Journal.

Rizzuti, Marco, “GDPR and the Right Be Forgotten” (2020) 2020 European Journal of Privacy Law & Technology.

Rosen, Jeffrey, “The Right to Be Forgotten” (2012) 64 Stanford Law Review.

Singh, Ajay Pal & Rahul Setia, “Right to Be Forgotten: Recognition, Legislation and Acceptance in International and Domestic Domain” (2018) 6:2 Nirma University Law Journal.

Singleton, Shaniqua, “Balancing A Right to be Forgotten with Freedom of Expression in the Wake of Google Spain v. AEPD” (2015) 44 Georgia Journal of International & Comparative Law.

Solove, Daniel J, “Conceptualizing Privacy” (2002) 90 California Law Review.

Tapadia, Vedant & Mridushi Damani, “The Right to Be Forgotten: An Aspect of Data Privacy” (2019) 1:4 LexForti Legal Journal.

Tasar, Ali & Melike Atas, “The Right to Be Forgotten under Protection of Personal Data Law” (2020) 23 GSI Articleletter.

Tejasree, J, “The Need for the Right to be Forgotten in India” (2018) 5:1 RMLNLU Financial and Mercantile Law Review.

Thakur, Naveen, “Right to Privacy — An Implicit Fundamental Right under Article 21” (1998) AIR Journal.

Townend, Judith, “Data Protection and the ‘Right to Be Forgotten’ in Practice: A UK Perspective” (2017) 45:1 International Journal of Legal Information.

Zaman, Shabnam Ahmed, Saptarishi Prasad Sharma & Modhu Chanda Dey, “Right to Be Forgotten: Socio-Legal Study” (2022) 4:1 Indian Journal of Law and Legal Research.

Beloume, Amy, “The Problems of Internet Privacy and Big Tech Companies” (2023), online: *The Science Survey* <<https://thesciencesurvey.com/news/2023/02/28/the-problems-of-internet-privacy-and-big-tech-companies/>>.

Bolton, Robert, “The Right to Be Forgotten: Forced Amnesia in a Technological Age” (2014) Rochester, NY.

Chaturvedi, Siddharth, “Digital Personal Data Protection Bill, 2023: An Incomplete Development” (2023), online: *The Contemporary Law Forum* <<https://tclf.in/2023/08/15/digital-personal-data-protection-bill-2023-an-incomplete-development/>>.

Douglas, Michael, “Questioning the Right to be Forgotten” (13 July 2016) Rochester, NY.

Kayali, Laura, “France Aims to Protect Kids from Parents Oversharing Pics Online” (2023), online: *Politico* <<https://www.politico.eu/article/emmanuel-macron-france-law-aims-to-protect-kids-against-oversharing-parents/>>.

McNealy, Jasmine E, “The Emerging Conflict between Newsworthiness and the Right to Be Forgotten” (2012) Rochester, NY.

Ramesh, Harikartik & Kali Srikari Kancharla, “Unattainable Balances: The Right to be Forgotten” (2020), online: *NLIU Law Review*.