NLUJ Law Review

Vini Singh, *Striking the Right (to be forgotten) Balance: Reconciling Freedom of Speech and Privacy – Dignity – Autonomy*, 8(1) NLUJ L. REV. 1 (2021).

STRIKING THE RIGHT (TO BE FORGOTTEN) BALANCE: RECONCILING FREEDOM OF SPEECH AND PRIVACY – DIGNITY – AUTONOMY

*Vini Singh**

ABSTRACT

Technology has transformed the way we share and access information. One only needs to run a simple Google search to meet a person's online persona. The abundant and long-lasting digital memory undoubtedly has its advantages. At the same time, it has far-reaching implications for privacy-dignity-autonomy interests. While there may never have been a time throughout human history when people may have been fully in control of their persona, neither have they been so deprived of control over their public image. The right to be forgotten reflects the claim of an individual to control their persona by offering a chance to reinvent one's online persona by hiding and/or removing personal information from the internet. Since the internet is a primary medium of communication and a valuable source of information, the right to be forgotten poses a significant challenge to the effective exercise of free speech rights. For this reason, it has been the subject of debate across various jurisdictions, including India. The Personal Data Protection Bill, 2019, which is currently being

* The author is an Assistant Professor, Faculty of Law at National Law University, Jodhpur and may be contacted at **vini.hnlu@gmail.com**.

scrutinized by a Joint Parliamentary Committee seeks to introduce the right to be forgotten along with a right to correction and erasure of personal information. While the proposed legislation would mean a step forward in data protection, it fails to strike the appropriate balance between the competing free speech and privacy-dignity-autonomy rights in the context of the proposed right. The author analyses how these competing rights may be reconciled and how the right to be forgotten may be squared with free speech in India.

TABLE OF CONTENTS

I. INTRODUCTION

With the advancement in technology, our lives are becoming less and less private. The electronic devices we use, such as smartphones, fitness trackers, GPS monitors, smart speakers and televisions, constantly keep track of and upload our activities. Technology is so intrusive that to offer a personalised experience, every single search on the internet, every website visited, every video watched online, every song listened to or every post liked or shared by an individual, is compiled to create an online profile for them. This profile can then be used to predict and even manipulate their preferences, ranging from which mobile phone to buy to their political choices.[1]

Further, it is very easy for others to meet this online version of an individual. In fact, it often happens that people meet one's online version and rely on it before meeting them in person – both, in a personal and professional setting. It is not at all uncommon for admission committees or potential recruiters to conduct a google search on the applicants. Thus, making it possible for a single photograph or a social media post depriving a person of an educational or professional opportunity.[2] In extreme cases,

---

[1] Jane Wakefield, *Your data and how it is used to gain your vote*, BBC NEWS (June 11, 2021), https://www.bbc.com/news/technology-54915779.

[2] Dan Levin, *Colleges Rescinding Admissions Offers as Racist Social Media Posts Emerge*, THE NEW YORK TIMES (June 2, 2021), https://www.nytimes.com/2020/07/02/us/racism-social-media-college-admissions.html.

like instances of revenge pornography, it may humiliate, cause immense mental anguish and even drive a person to suicide.[3]

Howsoever reclusive a person might be, they cannot help having an online persona. They may delete their social media accounts out of personal preference, but they would still be required to maintain an online presence to access basic government facilities. For example, to get vaccinated against COVID-19 in India, individuals had to register themselves on the CoWIN web portal.[4] Similarly, payments that they make through credit/debit cards would still be collected and processed. Opting out of internet usage is hardly an option. It is so intertwined with our lives that access to internet services has been recognised as a fundamental right.[5] Moreover, opting out or being cautious on the internet would impede the exercise of their rights to speech and expression, information as well as education. Therefore, it is important that an individual should have control over the personal information that is collected, processed and shared with others.

The Court of Justice of the European Union [*hereinafter* "**CJEU**"] addressed these concerns by recognising the "*right to deindex personal information*" in *Google Spain SL v. Agencia Española de Protección de Datos*

---

[3] Kristen Zaleski, *The long trauma of revenge porn*, OUPBLOG (June 11, 2021), https://blog.oup.com/2019/09/the-long-trauma-of-revenge-porn/.

[4] Shruti Dhapola, *India's COVID 19 vaccine rollout strategy has a digital gap; here are those struggling to plug it*, THE INDIAN EXPRESS (June 11, 2021), https://indianexpress.com/article/technology/tech-news-technology/india-covid-19-cowin-portal-vaccine-rollout-strategy-has-a-digital-gap-those-trying-to-fix-it-7338250/.

[5] Anuradha Bhasin v. Union of India, 2020 SCC OnLine SC 1725; The Constitution of Greece 1975, art. 5A (1); *see also,* Cengiz and Others v. Turkey, [2015] ECHR 1052.

[*hereinafter* "***Google Spain***"].[6] The matter arose in Spain in 2010 when Mr. Mario Costeja Gonzalez brought a complaint before the Spanish Data Protection Agency. He sought the removal of a news item from 1998 regarding his bankruptcy posted on the website of the Spanish newspaper 'La Vanguardia'. The news item was indexed by Google and consequently displayed whenever a Google search for his name was done. He requested the newspaper to take down the news item as it was damaging to his reputation, particularly now that his bankruptcy was old news. When the newspaper refused, he approached Google to deindex the item from search results. Google's refusal to remove the results ensued the legal action. The National High Court of Spain referred the matter to the CJEU seeking a preliminary ruling on the obligation of internet search engines to remove or erase information published by third party websites. The CJEU declared that people have a right to request the removal of information regarding themselves if the said information was "*inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine*."

The CJEU observed that search engines often collect personal information. They index, store, and share such information with other users and "*play a decisive role in the overall dissemination of personal data.*"[7] The CJEU primarily relied on Article 12(b) of the European Union's Data Protection Directive [*hereinafter* "**DPD**"], which confers the right to seek rectification,

---

[6] Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12, ECLI: EU: C: 2014: 317.
[7] *Id.* at 34 – 36.

erasure or blocking of data the processing of which does not comply with the DPD. It also relied on Article 14(a) of the DPD that confers the right to object to processing of data on any of the legitimate grounds specified in the DPD. Further, it referred to Article 6(d) of the DPD that obligates the member states to ensure the relevance, accuracy and currency of personal data. Notably, the CJEU emphasised upon the need for balancing the right to privacy with freedom of expression and access to information. It observed that while considering a request to deindex, the right of the other individuals to access the information in question, the interest of the public in the information depending on the data subject's role in public life, the sensitivity of the information and its impact on data subject's life, and the data subject's right to privacy must be taken into account.[8]

Thereafter, the General Data Protection Regulation [*hereinafter* "**GDPR**"] was implemented in 2018, replacing the DPD. Article 17 of the GDPR guarantees the "*right to erasure (right to be forgotten)*". Subject to certain exceptions and the protection of other rights and interests such as freedom of expression, the right allows the data subjects to request for deletion of personal information held by data controllers "*without undue delay*". There is an obvious tension between the right to be forgotten and freedom of expression and access to information.

The internet is the new marketplace of ideas. Restricting access to information or removing it from the internet could prevent free trade of

[8] *Id.* at 81.

ideas and seems sacrilegious. People worry that an overbroad right in the hands of those wielding public power may distort democratic discourse.[9] It may create a culture of secrecy and be abused to silence the critics of the government, public agencies, and even those wielding huge private power. It may also have a significant chilling effect on freedom of speech and expression.

However, information on the internet is not as permanent as we believe it to be.[10] Search engine results are a product of algorithms and are ranked based on their relevance to the user. They are therefore subject to change. For instance, if user A runs a Google search on "the right to be forgotten" on a given date and time, it is not necessary that they will receive the same search results later. Some results that were displayed prominently before may be de-ranked, while other results may become more prominent. Similarly, OTT platforms, such as Netflix, acquire streaming rights from content providers for TV shows and movies. The content is only available to stream for the period of the license and is removed thereafter.

Further, content is frequently removed from the internet due to various reasons. For example, social media websites like Facebook and Twitter prescribe community standards. Violation of these community standards can lead to the removal of social media posts and in some cases, even blocking of the user's access to their account. Similarly, a notice of

---

[9] KRISTIE BYRUM, THE EUROPEAN RIGHT TO BE FORGOTTEN: THE FIRST AMENDMENT ENEMY (Rowman & Littlefield 2018).

[10] Meg Leta Ambrose, *It's About Time: Privacy, Information life Cycles, and the Right to be Forgotten*, 16 STAN. TECH. L. REV. 369, 372 -373(2013).

alleged copyright violation may lead to the immediate takedown of content.[11]

Therefore, a narrowly tailored right to be forgotten is not likely to bring a drastic change. It is only the remedy of erasure which involves the destruction or removal of personal data and allows takedown of content from the source website.[12] Further, the data that is subject to erasure may still be kept if it is anonymised.[13] Other remedies simply limit the accessibility of information. For instance, delisting/deindexing involves removal of links to the information from search results.[14] The content remains available on the source website. Likewise, de-ranking only makes a search result less prominent.[15] Further, flagging just marks a search result as unreliable or incorrect as the case may be,[16] and the remedies of rectification/correction and updating allow data subjects to correct incorrect personal data[17] and update outdated data, respectively.[18]

---

[11] Lyle Denniston, *Are copyright claims stifling free speech on the Internet?*, CONSTITUTION DAILY (June 11, 2021), https://constitutioncenter.org/amp/blog/are-copyright-claims-stifling-free-speech-on-the-internet.

[12] European Commission, *Do we always have to delete personal data if a person asks* (Oct. 8, 2021), https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/dealing-citizens/do-we-always-have-delete-personal-data-if-person-asks#:~:text=Data%20do%20not%20have%20to%20be%20deleted&text=The%20politician%20requests%20to%20remove,personal%20data%20is%20being%20processed.

[13] *Id.*

[14] CNIL, *The Right to de-listing in questions* (Oct. 8, 2021), https://www.cnil.fr/en/right-de-listing-questions.

[15] Edward Lee, *The Right to be Forgotten v. Free Speech*, 12 I/S: A JOURNAL OF LAW AND POLICY 85, 105(2015).

[16] Hannah Cook, *Flagging the Middle Ground of the Right to be Forgotten: Combating Old News with Search Engine Flags*, VAND. J. ENT. & TECH. L. 1(2020).

[17] The European General Data Protection Regulation 2016/679, art. 16.

[18] *Id.*

Since different jurisdictions reconcile competing rights differently, it is not possible to adopt the right to be forgotten guaranteed under the GDPR universally. Most jurisdictions rely on the context-based proportionality principle to balance competing rights which requires them to minimally impair each right only to the extent it is necessary and proportionate to protect the other rights in each context.[19] However, different jurisdictions ascribe different values to the rights in conflict. For instance, dignity is the most important value in Europe;[20] while Canada lays emphasis on multiculturalism, equality and dignity.[21] While interpreting and balancing fundamental rights this preference takes the spotlight and determines the result.

On the other hand, the USA does not apply the proportionality standard when freedom of speech is pitted against other rights. The First Amendment, which prohibits the US Congress from making a law abridging free speech, always trumps other rights.[22] Therefore, an Indian right to be forgotten would have to be squared with the Constitution of India [*hereinafter* "**the Constitution**"].[23] It would have to be designed in such a way that it effectively safeguards the privacy-dignity-autonomy rights

---

[19] ALEC STONE SWEET AND JUD MATHEWS, PROPORTIONALITY, BALANCING & CONSTITUTIONAL GOVERNANCE: A COMPARATIVE & GLOBAL APPROACH (Oxford University Press 2019); Robert Alexy, *Constitutional Rights, Balancing and Rationality*, 16(2) RATIO JURIS 131(2003).

[20] James Q. Whitman, *The Two Western Cultures of Privacy: Dignity versus Liberty*, 113 YALE LAW JOURNAL 1151(2004).

[21] Peter W. Hogg, *Interpreting the Charter of Rights: Generosity and Justification*, 20 OSGOODE HALL LAW JOURNAL 817(1990).

[22] FLOYD ABRAMS, THE SOUL OF THE FIRST AMENDMENT (Yale University Press 2017).

[23] INDIAN CONST. art. 13(2).

of individuals, and at the same time does not unreasonably encroach upon freedom of speech, expression and information.

While the debate surrounding the right to be forgotten has been focused on whitewashing one's embarrassing past, it is not only about remembering and forgetting, and the harms of extensive digital memory. The right to be forgotten is a corollary of informational autonomy or informational self-determination and represents the control an individual should be able to exercise over their personal data.

Part II of this paper highlights this aspect of the right to be forgotten. Part III traces the right across various jurisdictions. Thereafter, Part IV discusses the proposed design for the right to be forgotten in India. Next, Part V examines whether this proposed framework strikes the appropriate balance between freedom of speech and expression and privacy-dignity-autonomy rights in the context of the right to be forgotten. Finally, Part V also offers suggestions on how the right must be tailored to ensure its constitutional compatibility.

II. DEFINING THE RIGHT TO BE FORGOTTEN

The "right to be forgotten" emerged as a response to the threat posed by technology to privacy, reputation, identity, and memory. It allows for the reinvention of one's online persona by providing the means to hide and/or remove personal information from the internet.

The concept has been controversial since its introduction. It has elicited strong responses from across the world. Some have called it

"censorship"[24] while others have termed it as "rewriting history".[25] Those who argue for this right have also used different terms to describe it. The GDPR also uses the terms "right to erasure" and "right to be forgotten" alternatively. Likewise, the Indian Personal Data Protection Act, 2019 refers to the right as the "right to erasure" and the "right to correction". Viktor Mayer–Schönberger,[26] who is a key proponent of this right and Paul Bernal[27] refer to the right as a "right to delete"; while others call it the "right to oblivion" or "*droit à l'oubli*".[28]

These terms have different connotations and safeguard different interests. For instance, the terms "right to erasure" and "right to be forgotten" used in the GDPR refer to distinct concepts. The former enables a data subject to restrict the unlawful use of their personal data, while the latter allows the data subject to control the usage of their personal data through means like withdrawal of consent.[29] The purpose of the right to be forgotten is to ensure that data subjects have effective control of what they

---

[24] Robert G. Larson III, *Forgetting the First Amendment: How Obscurity Based Privacy and a Right to be Forgotten are Incompatible with Free Speech*, 18. COMM. L. & POL'Y 91, 108(2013)

[25] Antoon De Baets, *A Historian's View on the Right to be Forgotten*, 30 INT'L REV. L. COMP. & TECH. 57(2016).

[26] VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN A DIGITAL AGE (Princeton University Press 2009).

[27] Paul Bernal, *A Right to Delete?*, EJLT 1(2011).

[28] Eloise Gratton and Jules Polonetsky, *Droit a L'Oubli: Canadian Perspective on the Global Right to be Forgotten Debate*, 15 COLO. TECH. LAW JOURNAL 337(2017).

[29] Cecile de Terwangne, *The Right to be Forgotten and Informational Autonomy in a Digital Environment* in Alessia Ghezzi et. al. (eds.) NORBERTO NUNO ET AL, THE ETHICS OF MEMORY IN A DIGITAL AGE 82 (Palgrave Macmillan 2014).

put up online and are able to correct, withdraw or delete it all.[30] Likewise, the "right to oblivion" is distinct from the "right to erasure" and the "right to be forgotten". The "right to oblivion" arises only from a need to protect privacy interests and aims to remedy the potential harms to the "dignity, personality, reputation and identity of an individual."[31] On the other hand, the impetus of the "right to erasure" and the "right to be forgotten" is much broader – they are concerned with the informational flow rather than remembrance and forgetting. They also empower data subjects as there is a power imbalance between data subjects and data controllers.[32] Further, the "right to oblivion" would only cover data that is no longer relevant, while the "right to erasure" and the "right to be forgotten" would encompass inadequate, irrelevant, and excessive personal information as well.[33]

The right to be forgotten thus represents the idea of control over one's personal data. It can be derived from autonomy, dignity, reputation, personality, and privacy rights of an individual.[34] It is broad enough to include the remedies of erasure, delisting/deindexing, de-ranking, flagging, correction and updating that would ensure data subject's control over their personal data.

---

[30] *Fundamental Rights and Citizenship introduced the right to be forgotten along with other data protection reforms in the EU*, VIVIANNE REDING, THE EUROPEAN COMMISSIONER FOR JUSTICE; Steven C. Bennett, *The "Right to be Forgotten": Reconciling E.U. and U.S. Perspectives*, 30 BERKELEY J. INT'L L. 161(2012) ("**Bennett**").

[31] Meg Leta Jones and Jef Ausloos, *The Right to be Forgotten Across the Pond*, 3 J. OF INFO. POL'Y. 1(2013) ("**Meg Leta Jones**"); Aurelia Damo and Damien George, *Oblivion, Erasure and Forgetting in the Digital Age*, 5(2) JIPITEC 71(2014)

[32] Andrea Slane, *Search Engines and the Right to be Forgotten: Squaring the Remedy with Canadian Values on Personal Information Flow*, 55 OSGOODE HALL L. REV. 349(2018).

[33] Meg Leta Jones, *supra* note. 31.

[34] Rolf H. Weber, *The Right to be Forgotten: More than a Pandora's Box?*, JIPITEC 2(2011).

III. TRACING THE RIGHT TO BE FORGOTTEN

While the right to be forgotten is fairly novel, the underlying concept of controlling one's public image is quite well established. The right to autonomy over one's persona has been protected in numerous cases. For example, in the 1867 *Dumas* case, a photographer who had copyright over compromising images of the famous author Alexandre Dumas was prevented from publishing them and was compelled to sell the rights to Dumas. The French court pointed out that privacy, like other aspects of honour, could not be traded off; Dumas had a right to withdraw his consent as he was the subject of those photographs.[35] Similarly, in the Canadian case of *Aubry v. Editions Vice Versa*,[36] the 'Editions' magazine had published the photograph of a teenage girl without her consent. The Canadian Supreme Court upheld her right to privacy, personality and image and granted her damages as there was no predominant public interest in publishing the photograph.

There are several legal predecessors to the right to be forgotten. Different aspects of the right particularly the "right to oblivion" were recognised in several jurisdictions. For example, "Habeas Data" is a writ and constitutional remedy available in many jurisdictions such as Brazil, Colombia, Paraguay, Peru, Argentina, and the Philippines.[37] The remedy can be sought by an individual to find out what information is held about

---

[35] John W. Dowdell, *An American Right to be Forgotten*, 52 TULSA L. REV. 311, 317-318(2017).
[36] Aubry v. Editions Vice Versa, [1998] 1 S.C.R. 591 (Can.).
[37] Sarah L. Lode, *"You have the Data"…The Writ of Habeas Data and Other Data Protection Rights: Is the United States Falling Behind?,* 94 INDIANA L. J. 41, 43 -46(2019).

them, and to seek rectification or destruction of the said personal information. Likewise, in Germany, the rights of human dignity and personality have been expanded to include a "right to informational self-determination".[38] This right allows individuals to determine when and to what extent their personal information is published. Similarly, the French banking sector had the notion of "*droit à l'oubli numerique*".[39] It provided for deletion of information from databases after a certain period of time.

Furthermore, most jurisdictions recognise informational privacy as an important limb of the right to privacy. For example, in the USA, the Constitutions of Alaska, California, Florida, Illinois, and Washington guarantee the right to informational privacy.[40] It has also been recognised in several decisions of the Supreme Court of the United States.[41] Article 8 of the Charter of Fundamental Rights of the European Union also guarantees the right to protection of personal data.[42] It is also regarded as an important limb of the right to privacy-dignity-autonomy in India.[43]

Additionally, almost every jurisdiction, even the USA has a history of legal forgiveness and recognises that rehabilitation of criminals is an

---

[38] Gerrit Hornung and Christoph Schnabel, *Data Protection in Germany I: The population census decision and the right to informational self – determination*, 25 COMP. L. & SEC. REV. 84(2009).
[39] Maryline Boizard, *The right to respect for private life: an effective tool in the right to be forgotten?*, Special Issue: Privacy, MONTESQUIEU L. REV. 20(2015).
[40] Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 BERKELEY TECH L. J. 1085, 1129 – 1144(2002).
[41] Riley v. California, 573 U.S. 373 (2014); Whalen v. Roe, 429 U.S. 589 (1977); Nixon v. Administrator of General Services, 433 U.S. 425 (1977); Ex Parte Jackson, 96 U.S. 727 (1877); Boyd v. United States, 116 U.S. 616 (1886).
[42] The Charter of Fundamental Rights of the European Union, 2000, art. 8.
[43] Justice K.S. Puttaswamy (Retd.) v. Union of India (Privacy), (2017) 10 SCALE 1.

important public concern. Many states have laws that allow the expungement of criminal records in cases of minor offences.[44] Likewise, Mary Bell injunctions are given in the UK to protect the new identity of rehabilitated criminals.[45] These injunctions ensure that the original identity of the rehabilitated criminal and their family remains hidden to protect them from any likely serious harm that may result from revealing their identities to the public. They are named after Mary Flora Bell who had murdered two children when she was eleven years old. The court had granted an injunction to protect not only her, but her daughter as well who could have been victimised by the public for being the child of a murderer.[46]

The Guidelines on the Protection of Privacy and Transborder Flows of Personal Data by OECD also contain similar principles. For example, the "Data Quality Principle" requires that data must be relevant, accurate, complete and up-to-date.[47] Further, the "Individual Participation Principle" allows an individual to request erasure, rectification, completion

---

[44] The Penal Code of California 1872, § 1203.4; The Texas Code of Criminal Procedure 1965, art. 55.01 – 55.06; Eric Westervelt and Barbara Brosher, *Scrubbing the Past to Give Those With A Criminal Record A Second Chance*, NPR (19 February, 2019), https://www.npr.org/2019/02/19/692322738/scrubbing-the-past-to-give-those-with-a-criminal-record-a-second-chance.

[45] Shamaan Freeman-Powell, *Legal dilemma of granting child killers anonymity*, BBC NEWS (June 11, 2021), https://www.bbc.com/news/uk-47721177.

[46] X (formerly known as Mary Bell) & Y v. News Group Newspapers Ltd. & Ors., [2003] EWHC 1101 (QB).

[47] *OECD Privacy Guidelines* (June 11, 2021), https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

or amendment of personal data.[48] Additionally, the "Principle of Collection Limitation" emphasises upon the consent of the data subject.[49]

The traces of the right to be forgotten can also be found in several instruments. For example, the Canadian Personal Information Protection and Electronic Documents Act, 2000 [*hereinafter* "**PIPEDA**"] provides a right to request correction of personal information.[50] Similarly, the 'Bundesdatenschutzgesetz', Germany's Federal Data Protection Act, 1977, included a right to request the erasure of stored personal data where such storage was impermissible or when the original conditions of data storage were no longer applicable.[51] France's Data Protection Law of 1978, the loi relative à l'informatique, aux fichiers et aux libertés, *i.e.*, "law relating to data processing, files and freedoms", provided a right to correction that also allowed the destruction of data.[52] The Data Protection Act, 1984 of the UK, which was superseded by the 1998 Act and then the 2018 Act, also guaranteed a right to rectification of personal data and a right to erasure.[53] The Privacy Act, 1974 of the USA also guarantees an individual the right to

---

[48] *Id.*
[49] *Id.*
[50] *Draft OPC Position on Online Reputation* (June 11, 2021), https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-on-online-reputation/pos_or_201801/#:~:text=That%20the%20OPC%20proactively%20address,through%20its%20Contributions%20Program%3B%20.
[51] Bundesdatenschutzgesetz 1977, § 4.
[52] Loi relative à l'informatique, aux fichiers et aux libertés 1978, art. 40.
[53] U.K. Data Protection Act 1984, art. 24.

request amendment of their data from the establishments of the executive branch of the federal government.[54]

The CJEU too derived the "right to deindex" in *Google Spain*[55] from the DPD. However, most of these instruments precede the era of big data. They are insufficient to deal with new technology like deepfakes, internet of things, etc. Therefore, the European Union moved towards a new data protection regulation in 2012, and implemented the GDPR in 2018, with the right to be forgotten as one of its pillars.[56] Other jurisdictions have or are in the process of modernising their privacy legislations. For example, in the USA, the State of California passed the California Consumer Privacy Act, 2018 that contains a right to delete personal information and a right to opt-out of processing of personal data.[57] The States of Massachusetts and Nevada have also enacted similar data protection legislations that guarantee the right to delete personal information.[58] The States of New York, Hawaii and Maryland are also poised to enact new consumer privacy legislations. In addition to the right to delete, the proposed New York Privacy Act contains a right of correction as well.[59]

---

[54] 5 U.S.C. § 552 a(d)(2) – (4).
[55] Google Spain SL v. AEPD, Mario Costeja Gonzalez, Case C-131/12, ECLI: EU: C: 2014: 317.
[56] *Fundamental Rights and Citizenship while introducing the right to be forgotten*, OBSERVATIONS OF VIVIANNE REDING, THE EUROPEAN COMMISSIONER FOR JUSTICE; Bennett, *supra* note. 30.
[57] Cal. Consumer Privacy Act 2018, § 1798.105.
[58] Glenn A. Brown, *Consumers' "Right to Delete" under US State Privacy Laws*, THE NAT'L LAW REV. (June 11, 2021), https://www.natlawreview.com/article/consumers-right-to-delete-under-us-state-privacy-laws.
[59] *Id.*

Similarly, Canada is in the process of modernizing its federal privacy legislations, PIPEDA and the Privacy Act, 1983. Its Digital Charter Implementation Act, 2020 would implement the Consumer Privacy Protection Act and the Personal Information and Data Tribunal Act.[60] The Consumer Privacy Protection Act will update PIPEDA which applies to the private sector. The updated law will empower data subjects by enhancing their control over their personal data. It will include a right to request permanent and irreversible deletion of data and a right to request amendment. The UK also has adopted its own General Data Protection Regulation [*hereinafter* "**UK GDPR**"]. The UK GDPR operates under the UK Data Protection Act, 2018. It retains the data protection principles of the European Union's GDPR; it guarantees the right to rectification of incorrect data,[61] the right to request erasure[62] and also the right to object to data processing.[63] Further, it mandates that the data should be relevant, accurate, current and adequate.[64] Additionally, it provides that data can be destroyed if it is no longer required or is excessive for the purpose it was collected.[65]

South Korea has opted for self–regulatory guidelines instead of binding legislation. The Korea Communications Commission issued the

---

[60] *Submission of the Office of the Privacy Commissioner of Canada on Bill C-11, the Digital Charter Implementation Act*, OPC (May 11, 2021), https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_ethi_c11_2105/.
[61] U.K. Data Protection Act 2018, § 46.
[62] *Id.* §§ 47 & 100.
[63] *Id.* § 99.
[64] *Id.* §§ 36, 37, 38, 39, 86 - 91.
[65] *Id.*

Guidelines on the Right to Request Access Restrictions on Personal Internet Postings in 2016.[66] These guidelines enable individuals to request service providers to restrict access to their personal information and to remove information that they cannot delete by themselves. India's Personal Data Protection Bill, 2018, and its revised version, the Personal Data Protection Bill, 2019 also aim to guarantee informational privacy and autonomy to individuals. To that end, they guarantee the right to be forgotten.

In addition to the CJEU ruling in *Google Spain,*[67] the right to be forgotten has also been upheld by national courts. Her Majesty's High Court of Justice in England recognised the right to be forgotten and provided guidance for its application in *NT1 and NT2 v. Google LLC.*[68] The Court directed Google to delist the information concerning the applicant NT2 as per the provisions of the Data Protection Act, 1998. The Court relied on *Google Spain*[69] and Article 29 Working Party Guidelines on Implementation of Google Spain to balance freedom of speech with privacy concerns. It allowed NT2's request since the information pertaining to him had no connection with his current professional and personal life.

---

[66] *KCC takes measures to guarantee "Right to be Forgotten"*, KOREA COMMUNICATIONS COMMISSION, https://www.kcc.go.kr/user.do;jsessionid=u95SDTNn2bk-8xJxpU3DpOa8kxymjESdivHgBfVc.servlet-aihgcldhome10?mode=view&page=E04010000&dc=E04010000&boardId=1058&cp=2&boardSeq=42538.

[67] Google Spain SL v. AEPD, Mario Costeja Gonzalez, Case C-131/12, ECLI: EU: C: 2014: 317.

[68] NT1 and NT2 v. Google LLC, [2018] EWHC 799 (QB).

[69] Google Spain SL v. AEPD, Mario Costeja Gonzalez, Case C-131/12, ECLI: EU: C: 2014: 317.

However, it denied NT1's request as the information in question could play a determinative role in assessing his current professional capabilities.

The Canadian Federal Court also crafted an equivalent remedy in *A.T. v. Globe24h.com.*[70] It directed the Romanian website Globe24h.com to remove Canadian decisions containing personal, financial, medical, and other sensitive information from its website, from search engine caches and to refrain from republishing of such decisions. While these decisions were already available on the Canadian Legal Information Institute's website, these decisions were not indexed by search engines. When Globe24h.com published them, they were indexed and as a result, sensitive information about individuals was displayed as search results. Coupled with this remedy, the Federal Court also awarded damages for the loss of privacy and reputation.

The Supreme Court of India [*hereinafter* "**the Supreme Court**"] in *Justice K.S. Puttaswamy (Retd.) v. Union of India* [*hereinafter* "***Puttaswamy (Privacy)***"][71] observed that the right to be forgotten is concomitant to the right to privacy. The Karnataka High Court too paved the way for the right to be forgotten in *(Name Redacted) v. Registrar General.*[72] Herein, the father of a woman had sought the removal of the woman's name from the digital records of court proceedings she had initiated against a person and from the search results regarding the same as this information was damaging to her current marital relationship and reputation. The High Court acquiesced

---

[70] A.T. v. Globe24h.com, 2017 FC 114 (Can.).
[71] Justice K.S. Puttaswamy (Retd.) v. Union of India (Privacy), (2017) 10 SCALE 1.
[72] (Name Redacted) v. Registrar General, 2017 SCC OnLine Kar 424.

and recognised a "right to be forgotten" on the lines of foreign jurisdictions. However, the High Court failed to provide any sound basis or any guidance for the implementation of the right. Thereafter, the Delhi High Court in *Zulfiqar Ahman Khan v. Quintillion Business Media (P) Ltd.*[73] held the right to be forgotten as a key aspect of the right to privacy. It observed that both rights were integral to an individual.

The Orissa High Court came to the rescue of a woman whose objectionable pictures and videos were posted on social media.[74] The High Court noted that while strong penal action was available against the accused who had raped and blackmailed the victim, there was no mechanism that could prevent the dissemination of her photos and videos on the internet. Lamenting on the insensitive behaviour on social media towards such victims, the High Court pointed out the need for legislating the "right to be forgotten" as it was not possible in every case for a victim to approach the courts. It further held that it was imperative to recognise the right to be forgotten in such cases lest any accused outrage the modesty of a woman and misuse the same in cyberspace unhindered to harass her.

Recently, the Delhi High Court once again recognised the right to be forgotten of an American citizen by passing an interim order directing online platforms such as Indian Kanoon to block a judgement concerning him from being accessed from search engines.[75] The individual had been acquitted by the Indian courts, yet the judgement which was available on a

---

[73] Zulfiqar Ahman Khan v. Quintillion Business Media (P) Ltd., 2019 (175) DRJ 660.
[74] Subhranshu Rout v. State of Odisha, 2020 SCC OnLine Ori 878.
[75] Jorawer Singh Mundy v. Union of India, 2021 SCC OnLine Del 2306.

single Google search to any potential employer was hampering his employment prospects causing irreparable harm to him. Therefore, recognising his right to privacy and the right to be forgotten, the Delhi High Court granted him interim relief. Further, the Supreme Court also made certain observations regarding the right to be forgotten in its recent judgement in *Jigya Yadav v. CBSE.* [76] It directed the Central Board of Secondary Education to amend its by-laws and include a mechanism to ensure that corrections or changes may be made in the certificates that it will issue or has already issued. It observed that the new certificates could retain old information with disclaimers, except if the change was effected in the exercise of the right to be forgotten. Notably, it held that the right to control one's identity is a fundamental right.

IV. THE PROPOSED FRAMEWORK FOR THE RIGHT TO BE FORGOTTEN IN INDIA

The Supreme Court in its nine-judge bench decision in *Puttaswamy (Privacy)*[77] upheld the "*fundamental right to privacy*." The judgement marks the beginning of a new era in Indian constitutional law.[78] It places the individual at the heart of fundamental rights jurisprudence and closely interlinks dignity and liberty-based rights. It also clarifies and embeds the "proportionality standard of review" which ensures that fundamental rights are not unduly curtailed.

---

[76] Jigya Yadav v. CBSE, 2021 SCC OnLine SC 415.
[77] Justice K.S. Puttaswamy (Retd.) v. Union of India (Privacy), (2017) 10 SCALE 1.
[78] Shreya Atrey & Gautam Bhatia, *New Beginnings: Indian Rights Jurisprudence After Puttaswamy*, 3(2) U of OxHRH J 1 (2020).

The first step of this standard requires that limitations on fundamental rights must only be imposed to achieve a legitimate purpose. This legitimate purpose must be "rationally connected" to the means adopted for achieving the said purpose. Further, such means must impair the fundamental right in question as minimally as possible. The means also must be necessary and sans any alternatives that may similarly achieve the said purpose with a lesser degree of impairment of the right. The final step requires a contextual balancing of competing interests to ascertain that the cost of impairment is not greater than the benefit of achieving the legitimate purpose. This standard has opened up several possibilities for realizing the transformative character of the Constitution.[79]

Acknowledging the importance of safeguarding informational privacy in the era of big data, the court-mandated steps must be taken to guarantee effective data protection rights. Consequently, a committee chaired by Justice (Retd.) B.N. Srikrishna was constituted to draft a data protection regime for India.[80] The Personal Data Protection Bill, 2018 [*hereinafter* "**2018 PDP Bill**"] was drafted on the recommendation of this committee. The 2018 PDP Bill was debated upon and revised as Personal Data Protection Bill, 2019 [*hereinafter* "**2019 PDP Bill**"]. This 2019 PDP Bill is currently under consideration before a Joint Parliamentary Committee.

---

[79] *Id.*

[80] Justice B.N. Srikrishna Committee, *Report of the Committee on Data Protiection – A Free and Fair Digital Economy Protecting Privacy, Empowering Indians*, MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY (2018).

Several significant changes were made in the new bill including the addition of a right to erasure to supplement the right to be forgotten.

The 2019 PDP Bill is applicable vertically, *i.e.*, to State and its instrumentalities as well as horizontally, *i.e.*, to private entities. It regulates the processing of personal data "*within India, by Indian persons whether corporate or natural, whether in India or otherwise, and those data fiduciaries or data processors outside India in connection to business in India, the systematic activity of offering goods and services to Indian data principals, or profiling of data principals in India*."[81] However, it would not apply to the processing of personal data of Indian data principals outside India by data fiduciaries or data processors outside India.[82] This creates a gap in the regulatory net. For instance, the 2019 PDP Bill will not apply if say a major data fiduciary like Facebook collects and processes or transfers for processing the personal data of an Indian data principal while they are living abroad. If they wish to exercise any of the data protection rights like the right to be forgotten, the only recourse available to them would be an equivalent framework, if any in the foreign jurisdiction, provided it applies to them.

It borrows extensively from the GDPR and recognizes various informational privacy principles such as purpose limitation, limitation on the period for which data can be stored, right of individuals to access data, right to port personal data, privacy by design, etc. It creates a fiduciary relationship between individuals and entities that collect, store, and process

---

[81] Personal Data Protection Bill 2019, §2.
[82] *Id.*

their personal data. It uses the term "*data principal*"[83] and "*data fiduciary*"[84] to depict this relationship instead of the terms "data subject" and "data controller" used in the GDPR. It imposes a duty of care on data fiduciaries and requires them to process data in a "*fair and reasonable manner*".[85] Data fiduciaries are supposed to ensure that the personal data that is processed is complete, accurate and is not misleading or outdated.[86] They must not retain the data longer than necessary for the purpose for which it was collected unless legally bound to do so.[87] Depending on the volume and sensitivity of the data, the 2019 PDP Bill creates a special class of data fiduciaries termed "*significant data fiduciaries*".[88] They are subject to higher penalties in case of violation of the provisions of the proposed bill.

The consent of the data principal is central to its framework. Barring certain exceptions, personal data can only be processed on the basis of "*free, informed, specific and clear consent of the data principal*."[89] The consent must be capable of being withdrawn and has to be taken before processing.[90] Consent requirements are more stringent for the processing of sensitive personal data.[91] Further, the 2019 PDP Bill creates the Data Protection Authority of India [*hereinafter* "**DPAI**"] to ensure enforcement

---

[83] *Id.* § 3(14).
[84] *Id.* § 3(13).
[85] *Id.* § 4.
[86] Personal Data Protection Bill 2019 § 8.
[87] Personal Data Protection Bill 2019 § 9.
[88] *Id.* § 36.
[89] *Id.* § 11.
[90] *Id.*
[91] *Id.* § 11(3).

of its provisions.[92] It confers extensive powers on the DPAI, such as the power to call for information, search and seizure, etc.[93] The adjudicatory division of DPAI imposes penalties for violation of compliance requirements and offences under the proposed bill.[94]

In addition to the right to be forgotten[95] and the right to erasure,[96] the 2019 PDP Bill also guarantees a right to correction of incorrect or misleading data,[97] completion of incomplete data,[98] and updating of outdated data.[99] The right to be forgotten enables the data principal to request the DPAI to restrict or prevent the continued disclosure of his data by a data fiduciary only on the three specified grounds. *First*, the disclosure of data has served the purpose for which it was collected and is no longer necessary for that purpose. *Second*, the consent has been withdrawn by the data principal for the disclosure of data that was collected and processed with the consent of the data principal. *Third*, when the disclosure is contrary to the provisions of any legislation in force. Further, the data principal must establish that his right to restrict disclosure overrides the freedom of speech, expression, and information of others. Hence creating a presumption in favour of freedom of speech and expression.

---

[92] *Id.* § 41.
[93] *Id.* §§ 51-55.
[94] *Id.* §§ 57-66.
[95] *Id.* § 20.
[96] *Id.* § 18.
[97] *Id.*
[98] *Id.*
[99] *Id.*

While considering such a request, the Adjudicating Officer of the DPAI is required to take into account the sensitivity of the data, the role of the data principal in public life, the scale of disclosure, the degree of accessibility sought to be restricted and the activities of the data fiduciary and whether they would be significantly impeded. An appeal lies from the decision of the Adjudicating Officer to the Appellate Tribunal and thereafter to the Supreme Court. Unlike the GDPR which allows data subjects to request the data controllers directly, the 2019 PDP Bill has avoided conferring the responsibility of balancing speech and privacy on private entities. However, the DPAI under the 2019 PDP Bill is no longer independent and it is doubtful if it would not be biased when the request is directed to the government or its instrumentalities as data fiduciaries.[100]

The right to erasure on the other hand is only available when the data is no longer necessary for the purpose for which it was collected.[101] The requests for erasure, correction, completion and updating can be made directly to the data fiduciary. If the data fiduciary accepts the request of erasure, it must notify all other entities to whom the disclosure was made regarding such erasure. If it refuses such a request, then it has to offer reasonable justifications for the same.[102] Failure to do so can attract a penalty of up to INR 5,000 (five thousand) per day with a maximum cap of

---

[100] Lakshya Sharma and Siddharth Panda, *Into the Orwellian Dystopia: A Comparative Analysis of Personal Data Protection Bill 2019 vis-à-vis Indian Privacy Jurisprudence,* 7(2) NLUJ L. REV. 1, 27(2021).
[101] Personal Data Protection Bill, 2019 § 18.
[102] *Id.* § 21(4).

INR 10,00,000 (ten lakh) for significant data fiduciaries and INR 5,00,000 (five lakh) for other data fiduciaries.[103] There is no specific provision for appeal. However, the general right to complaint to the DPAI for contravention of the provisions of the 2019 PDP Bill[104] is available to the data principal in case of refusal. On receiving such a complaint, the DPAI would appoint an Inquiry Officer. Based on the report submitted by the Inquiry Officer and after hearing the data fiduciary, the DPAI can give appropriate directions in writing.[105] The data principal can appeal against such an order to the Appellate Tribunal.[106]

It is questionable whether the current framework would strike an appropriate balance with freedom of speech and expression and be constitutionally compatible. Apart from the lack of independence of DPAI, there are other issues that plague this framework. For example, the Adjudicating Officer has hardly been given any guidance regarding the application of grounds on which the right to be forgotten can be availed. The factors provided leave a lot of room for discretion and need clarification. There is no distinction between data posted by the data principal himself and data posted by other people about the data principal in either of the provisions. This should be a very important factor in considering a request regarding these rights as the latter would implicate the right to free speech of others while the former would only implicate their right to access the information. The right to erasure can be handy in other

---

[103] *Id.* § 58.
[104] *Id.* § 53.
[105] *Id.* § 54.
[106] *Id.* § 72.

situations like revenge porn and should have been drafted to encompass such a situation. The present provision seems superfluous considering that the data fiduciaries are anyway not allowed to retain the data beyond the period necessary for the purpose it was collected.[107] If they do so, the DPAI may suo motu or on a complaint received by it, initiate an inquiry and take action against them.[108] Further, for non-compliance with this requirement, they would be subject to a penalty of up to INR 15,00,00,000 (fifteen crores) or four per cent of their total worldwide turnover of the preceding financial year, whichever is higher.[109] Further, a data principal can also complain to the DPAI and seek compensation from the data fiduciary if the data principal suffers harm as a result of contravention of this requirement.[110]

Moreover, the 2019 PDP Bill does not specify what remedies may be given to restrict disclosure of personal data in the context of the right to be forgotten. Is only delisting/deindexing permitted or remedies like de-ranking may be given? It also does not clarify if takedown of information from the source website can be done to restrict disclosure. Further, it also does not leave room for other remedies like flagging of information as unreliable or under-review which may sometimes be enough to prevent the harm to the data principal or could be used as an interim relief while the

[107] *Id.* § 9.
[108] *Id.* §§ 53(1) (b) – 54.
[109] *Id.* § 57(2).
[110] *Id.* § 64.

request for the right to be forgotten or erasure, completion, correction or updating is pending.

The following sections explore how competing rights are balanced in India and offer suggestions for designing a constitutionally compatible right to be forgotten in India.

V. RECONCILING FREEDOM OF SPEECH AND EXPRESSION AND PRIVACY IN THE CONTEXT OF THE RIGHT TO BE FORGOTTEN

The Constitution of India is a "transformative document".[111] The provisions of Part III of the Constitution are interpreted as a whole and in a progressive manner.[112] There are some rights like freedom of religion which have been subjected to other rights[113] and there are some rights that have been expressly qualified.[114] However, there is no hierarchy of rights in the Constitution. Nor is precedence given to one constitutional value over the other.

When two rights compete against one another, there is no clear winner. The competing rights are contextually balanced against each other to determine the outcome. For instance, in the case of *Mr X. v. Hospital Z,*[115] the Supreme Court was called upon to balance the right to privacy of an HIV patient against the right to life and health of his fiancée. Herein, a

---

[111] GAUTAM BHATIA, THE TRANSFORMATIVE CONSTITUTION: A RADICAL BIOGRAPHY IN NINE ACTS (HarperCollins India 2019).
[112] Maneka Gandhi v. Union of India, AIR 1978 SC 597.
[113] INDIAN CONST. art. 25.
[114] *Id.* art. 19, art. 25.
[115] Mr X. v. Hospital Z, AIR 1999 SC 495.

doctor had disclosed the appellant's HIV positive status to his fiancée which ultimately led to the cancellation of his marriage. The Supreme Court acknowledged that the appellant had a right to privacy and the doctor owed a duty of confidentiality to his patient. However, in the given circumstances his fiancée had a greater interest in knowing this information.

Similarly, in *in re Noise Pollution and Restricting Use of Loudspeakers,*[116] the Supreme Court balanced the right to life and a clean environment under Article 21 of the Constitution against freedom of speech and expression. Once again, the Supreme Court contextually balanced the conflicting rights and observed that while there was freedom of speech and expression, the same was not absolute. Nobody had the right to engage in "*aural aggression*" as others had an equal right not to be compelled to listen and enjoy a peaceful life. The harmful effects of noise on health also tilted the balance in favour of the right to a clean, pollution-free environment in this case.

Hate speech and defamation jurisprudence inevitably involve a balancing exercise between freedom of speech and dignity.[117] The requirement of reasonability for restrictions on Article 19 freedoms has always required proportionality and therefore contextual balancing. Therefore, while the landmark cases of *Modern Dental College*[118] and *Puttaswamy (Privacy)*[119] formally introduced the proportionality standard in

---

[116] In re Noise Pollution and Restricting Use of Loudspeakers, AIR 2005 SC 3136.
[117] Subramanian Swamy v. Union of India, (2016) 7 SCC 221.
[118] Modern Dental College and Research Centre v. State of Madhya Pradesh, (2016) 7 SCC 353.
[119] Justice K.S. Puttaswamy (Retd.) v. Union of India (Privacy), (2017) 10 SCALE 1.

our constitutional jurisprudence for testing limitations on rights, it was never an alien concept. For instance, in *State of Madras v. V.G. Row*,[120] a case regarding freedom of association, the Supreme Court pointed out the link between the reasonableness of a restriction and proportionality. It observed that while assessing the reasonability of a restriction, it would consider the nature of the right in question and the purpose of the restriction imposed. Further, it would consider the extent and urgency of the mischief sought to be remedied, *i.e.*, the necessity. Lastly, it would examine whether the restriction was proportionate as per the prevailing circumstances at the time.

Freedom of speech and expression is a precious right in India considering its history during the freedom movement. And while free speech jurisprudence in India borrows heavily from the First Amendment jurisprudence, it has never been regarded as a superior right. As discussed above, it does not automatically trump other fundamental rights in case of a conflict. Even in the USA, scholars have been clamouring for reading the First Amendment with the Thirteenth and Fourteenth Amendment, particularly in the context of hate speech.[121] In contrast, the requirement of reasonableness under Article 19 closely resembles the balancing exercise undertaken by the Supreme Court of Canada in cases like *Oakes*,[122] *Hill*[123]

---

[120] State of Madras v. V.G. Row, AIR 1952 SC 196.

[121] RICHARD DELGADO AND JEAN STEFANCIC, MUST WE DEFEND NAZIS? WHY THE FIRST AMENDMENT SHOULD NOT PROTECT HATE SPEECH SUPREMACY (NYU Press 2018).

[122] R v. Oakes, [1986] 1 S.C.R. 103 (Can.).

[123] Hill v. Church of Scientology, [1995] 2 S.C.R. 1130 (Can.).

and Dagenais,[124] the European Court of Human Rights in *Axel Springer*,[125] the House of Lords in *Campbell*,[126] and the South African Constitutional Court in *NM v. Smith*.[127]

The underlying principle in this reconciliatory exercise is that of proportionality. Both sets of conflicting rights are defined in the light of each other, as neither is considered superior to the other.[128] In fact, it is understood that each of these rights informs and is informed by the other. Under this exercise, it is first determined that the limitation is imposed through law, and that it is for a legitimate interest since a fundamental right is at stake. Thereafter, it is seen whether the limitation imposed on one right is necessary in order to prevent a real and substantial risk to the other and that reasonably available alternative measures would not prevent the risk. And finally, it is seen that in the given context the salutary effects of the limitation in safeguarding one fundamental right should outweigh the deleterious effects of limiting the other.

Likewise, while testing the reasonability of restrictions on Article 19(1)(a) of the Constitution, the first stage is to determine whether the restriction has been imposed by a law. The next is to see if the limitation has been imposed on the basis of one of the grounds mentioned in Article 19(2), a legitimate state interest. The rational nexus of the limitation with one of the mentioned grounds also entails the necessity of the restriction

---

[124] Dagenais v. Canadian broadcasting Corp., [1994] 3 S.C.R. 835.
[125] Axel Springer AG v. Germany, 39954/08 [2012] ECHR 227 (7 February 2012).
[126] Campbell v. MGN Ltd., [2004] UKHL 22.
[127] NM v. Smith, [2007] ZACC 6.
[128] Subramanian Swamy v. Union of India, (2016) 7 SCC 221.

to achieve the aim mentioned in Article 19(2) and the lack of equally effective alternative means. And finally, the elements of proximity and proportionality require that the limitation must be narrowly tailored to achieve the legitimate aim and must not be an overbroad restriction. For instance, in *Romesh Thappar v. State of Madras*,[129] Section 9(1-A) the Madras Maintenance of Public Order Act was struck down as it did not have a rational nexus with any of the legitimate aims mentioned in Article 19(2) and was overbroad. Similarly, in *Shreya Singhal v. Union of India*,[130] Section 66A of the Information Technology Act, 2000 was struck down as overbroad, vague, arbitrary and disproportionate. Recently, in *Anuradha Bhasin v. Union of India*,[131] the Supreme Court reiterated that orders for internet shutdowns must comply with the proportionality standard.

Restrictions on the right to privacy also need to pass the touchstone of proportionality. The standard has been applied since *Puttaswamy (Privacy)*[132] in various decisions like *Puttaswamy (Aadhar)*,[133] *Navtej Singh Johar*[134] and *Joseph Shine*[135] to test the validity of restrictions on privacy-dignity-autonomy. As the right to be forgotten represents privacy-dignity-autonomy interests, it can be restricted only as per the proportionality standard.

---

[129] Romesh Thappar v. State of Madras, AIR 1950 SC 124.
[130] Shreya Singhal v. Union of India, AIR 2015 SC 1523.
[131] Anuradha Bhasin v. Union of India, 2020 SCC OnLine SC 1725.
[132] Justice K.S. Puttaswamy (Retd.) v. Union of India (Privacy), (2017) 10 SCALE 1.
[133] Justice K.S. Puttaswamy v. Union of India (Aadhar), (2019) 1 SCC 1.
[134] Navtej Singh Johar v. Union of India, AIR 2018 SC 4321.
[135] Joseph Shine v. Union of India, (2019) 3 SCC 39.

Hence, while balancing both freedom of speech and expression and privacy-dignity-autonomy in the context of the right to be forgotten, both sets of rights would have to be informed by each other. They would have to be read in a manner that minimally impairs each right while simultaneously effectively safeguarding both. This is clearly a delicate task and requires sufficient guidance. In this process, the first step should be to regard both sets of rights at equal footing since the Constitution does not give preference to either, nor does it prefer liberty over dignity or vice-versa. Further, both sets of rights are liberty as well as dignity based and are correlated.

Protecting both sets of rights is a legitimate state interest, and since Part III of the Constitution is read as a whole, both sets of rights should be harmoniously interpreted. At the next stage of necessity, restrictions imposed on freedom of expression and access to information on the one hand, and privacy-dignity-autonomy on the other hand, must be examined for their effectiveness and need. If there are equally effective, less restrictive measures available, then those should be resorted to. Thus, when de-ranking of information in search results can suffice, delisting should not be given as a remedy. On the other hand, there may be cases of revenge porn or cases involving information about a minor that warrant the remedy of erasure of the information from the source. At the same time exceptions meant to ensure freedom of speech and expression like "journalistic purposes"[136] must be clearly defined through an inclusive list to prevent an

[136] Personal Data Protection Bill 2019 §36.

overbroad interpretation. Particularly, the government's power to grant such exemptions to its agencies[137] must be limited.

Finally, while examining the proportionality, it must be ensured that both the right to be forgotten and the exceptions to safeguard speech and expression are tailored narrowly to effectively safeguard the underlying rights. Taking a cue from these principles, the next section offers certain suggestions regarding drafting a constitutionally compatible "right to be forgotten" provision.

VI. SUGGESTIONS AND CONCLUSION

To reconcile freedom of speech and expression with privacy-dignity-autonomy in the context of the right to be forgotten, the author recommends the following amendments. *First*, there shouldn't be separate provisions and procedures for the right to be forgotten and erasure, correction, completion and updating.

The provision for the right to be forgotten must offer a combination of catalogue and standards. The catalogue should enlist fact situations with corresponding remedies to be granted as a rule. For example, in cases involving intimate photos or videos, the remedy of irretrievable erasure from the source and other links should be given as a rule. Similarly, matters pertaining to marital relationships or discords may be delisted after a reasonable period of three to five years. This catalogue can be revisited from time to time as jurisprudence develops. If the data

---

[137] *Id.* § 37.

principal's case falls within the catalogue, he should be allowed to approach the data fiduciary directly with a mechanism of appeal to the Appellate Tribunal in case of refusal.

The rest of the requests by should be determined according to standards. The data principal must not bear the burden of proving that his privacy-dignity-autonomy interest overrides the free speech and access to information rights of others. This should, however, be a determinative factor during balancing. It should be seen that who is has authored the information. If the author was the data principal then the balance should shift in favour of the right to be forgotten; if however, the information was posted by others, it should shift in favour of freedom of speech. It should also be seen if the data principal was a minor when the information was posted; this should shift the balance towards the right to be forgotten. Next, the newsworthiness of the data must be assessed having regard to factors such as time elapsed, the sensitivity of the information, the role of the data principal in public life and the relevance of that information to his public life. And if the information pertains to his private life, whether the data principal had deliberately courted publicity by exposing his private life or if that information is associated with his role in public life despite its sensitivity.

As a general rule, de-ranking relevant search results should be the preferred remedy unless making them inconspicuous cannot prevent harm to the data principal. In those cases, delisting may be granted as a remedy as it would further limit access to the information by removing relevant links from the search results. The remedy of erasure and takedown from

the source must only be granted in exceptional circumstances when there are compelling privacy-dignity-autonomy interests. Additionally, when a request if pending, the information can be flagged as under review so that those accessing it do not rely upon it. Also, when a request is denied for exceptions like "journalistic purposes", then too the information can be flagged to indicate so.

These requests should be heard by a DPAI panel consisting of a technical and a judicial member having significant experience with a mechanism of appeal to the Appellate Tribunal. Further, the independence of the DPAI must be ensured by modifying the process of composition and appointment. The DPAI members must be selected by a panel consisting of representatives of the government, industry, and the judiciary to counterbalance any influence they may exercise. The term of five years for the members must be a rule and members should be removed only under the specified grounds.

It is imperative that freedom of speech and expression is not impeded and that the right to be forgotten does not remain a paper tiger. Both sets of rights are valuable and must be zealously guarded in the era of big data. A narrowly tailored right to be forgotten would not only ensure the privacy-dignity-autonomy of individuals but also prevent the chilling effect on speech on the internet due to lack of informational autonomy. The author believes that the above suggestions may be helpful in achieving this objective.