The Right to Erasure

Centre for Communication Governance at
National Law University Delhi

December 2024

The Right to Erasure

CCG Policy Brief

Centre for Communication Governance
National Law University Delhi

Published by
Centre for Communication Governance
National Law University Delhi
Sector 14, Dwarka, New Delhi – 110078

Patrons: Professor (Dr.) G.S. Bajpai (Vice Chancellor, NLUD),
Professor (Dr.) Ruhi Paul (Registrar, NLUD)

Faculty Director, CCG: Dr. Daniel Mathew
Executive Director, CCG: Jhalak M. Kakkar

Authors: Srija Naskar, Sukriti, Nidhi Singh

[Names are mentioned in reverse alphabetical order]

We thank Tavishi and Vignesh Shanmugam for their feedback on this paper.
Reviewed by Shashank Mohan.
Design by Gopika P.

Acknowledgements: This paper was made possible by the generous support we received from the National Law University Delhi (NLUD). The Centre for Communication Governance (CCG) would therefore like to thank our patrons, the Vice Chancellor Professor (Dr.) G.S. Bajpai and the Registrar Prof. (Dr.) Ruhi Paul of NLUD for their constant guidance. CCG would also like to thank our Faculty Director Dr. Daniel Mathew for his continuous direction and mentorship. We would also like to thank Jhalak M. Kakkar, Executive Director at CCG, for her unwavering support, encouragement, and mentorship, which have been instrumental in publishing this research. Special thanks to the ever-present and ever-patient Suman Negi and Preeti Bhandari for the unending support for all the work we do at CCG. Lastly, we would also like to thank all members of CCG for the many ways in which they supported the paper.

Suggested Citation – Srija Naskar, Sukriti, and Nidhi Singh, 'Right to Erasure', (2024) Centre for Communication Governance at National Law University Delhi.

ABOUT THE NATIONAL LAW UNIVERSITY, DELHI

The National Law University Delhi is one of the leading law universities in the capital city of India. Established in 2008 by an Act of the Delhi legislature (Act. No. 1 of 2009), the University is ranked second in the National Institutional Ranking Framework for the last five years. Dynamic in vision and robust in commitment, the University has shown terrific promise to become a world-class institution in a very short span of time. It follows a mandate to transform and redefine the process of legal education. The primary mission of the University is to create lawyers who will be professionally competent, technically sound and socially relevant, and will not only enter the Bar and the Bench but also be equipped to address the imperatives of the new millennium and uphold the constitutional values. The University aims to evolve and impart comprehensive and interdisciplinary legal education which will promote legal and ethical values, while fostering the rule of law.

The University offers a five year integrated B.A., LL.B (Hons.), a one-year postgraduate masters in law (LL.M), and a Ph.D. program, along with professional programs, diploma and certificate courses for both lawyers and non-lawyers. The University has made tremendous contributions to public discourse on law through pedagogy and research. Over the last decade, the University has established many specialised research centres and this includes the Centre for Communication Governance (CCG), Centre for Innovation, Intellectual Property and Competition, Centre for Corporate Law and Governance, Centre for Criminology and Victimology, and Project 39A. The University has made submissions, recommendations, and worked in advisory/consultant capacities with government entities, universities in India and abroad, think tanks, private sector organisations, and international organisations. The University works in collaboration with other international universities on various projects and has established MoU's with several other academic institutions.

ABOUT THE CENTRE FOR COMMUNICATION GOVERNANCE

The Centre for Communication Governance at the National Law University Delhi (CCG) was established in 2013 to ensure that Indian legal education establishments engage more meaningfully with information technology law and policy and contribute to improved governance and policy making. CCG is the only academic research centre dedicated to undertaking rigorous academic research on information technology law and policy in India. It has in a short span of time, become a leading institution in Asia. Through its academic and policy research, CCG engages meaningfully with policy-making in India by participating in public consultations, contributing to parliamentary committees and other consultation groups, and holding seminars, courses and workshops for capacity building of different stakeholders in the technology law and policy domain. CCG works across issues such as privacy and data governance, platform governance, and emerging technologies.

CCG has built an extensive network and works with a range of international academic institutions and policy organisations. These include the United Nations Development Programme, NITI Aayog, various Indian government ministries and regulators, International Telecommunications Union, UNESCO, UNGA WSIS, Paris Call, Berkman Klein Center for Internet and Society at Harvard University, the Center for Internet and Society at Stanford University, Columbia University's Global Freedom of Expression and Information Jurisprudence Project, the Hans Bredow Institute at the University of Hamburg, the Programme in Comparative Media Law and Policy at the University of Oxford, the Annenberg School for Communication at the University of Pennsylvania, the Singapore Management University's Centre for AI and Data Governance, Tech Policy Design Centre at the Australian National University, and the Technical University of Munich.

The Centre has authored multiple publications over the years, including the Hate Speech Report, a book on Privacy and the Indian Supreme Court, an essay series on Democracy in the Shadow of Big and Emerging Tech, a comprehensive report on Intermediary Liability in India, an edited volume of essays on Emerging Trends in Data Governance,

and a guide for Drafting Data Protection Legislation: A Study of Regional Frameworks in collaboration with the United Nations Development Programme, and most recently - a Report on Social Media Regulation and the Rule of Law in Sri Lanka, India and Bangladesh. It has also published reports from three phases of the Blockchain Project conducted in collaboration with the Tech Policy Design Centre at the Australian National University, which maps the blockchain ecosystem in India and Australia.

Privacy and data protection have been focus areas for CCG since its inception, and the Centre has shaped discourse in this domain through research and analysis, policy inputs, capacity building, and related efforts. In 2020, the Centre launched the Privacy Law Library, a global database that tracks and summarises privacy jurisprudence emerging in courts across the world, in order to help researchers and other interested stakeholders learn more about privacy regulation and case law. The PLL currently covers 250+ cases from 20+ jurisdictions globally and also contains a High Court Privacy Tracker that tracks emerging High Court privacy jurisprudence in India.

CCG also has an online 'Teaching and Learning Resource' database for sharing research-oriented reading references on information technology law and policy. The Centre has also offered Certificate and Diploma Courses on AI Law and Policy, Technology Law and Policy, and First Principles of Cybersecurity. These databases and courses are designed to help students, professionals, and academicians build capacity and enable a nuanced engagement with the dynamic space of technology and cyberspace, their implications for society, and their regulation. Additionally, CCG organises an annual International Summer School in collaboration with the Hans Bredow Institute and the Faculty of Law at the University of Hamburg in collaboration with the UNESCO Chair on Freedom of Communication at the University of Hamburg, Institute for Technology and Society of Rio de Janeiro (ITS Rio) and the Global Network of Internet and Society Research on contemporary issues of information law and policy. Most recently, CCG and UNESCO conducted a Workshop on 'AI and the Rule of Law' for stakeholders of the justice sector from India, Bhutan, Maldives, Nepal, and Sri Lanka.

TABLE OF CONTENTS

EXECUTIVE SUMMARY 1

1. Introduction 4

2. Right to Erasure in India 6

2.1. Evolution of the Scope of RTE 7

2.2. Implementation of RTE 12

2.3. Courts in India on the Right to Erasure 13

3. Global Approaches to the Right to Erasure 17

3.1. EU 17

3.2. Asia 22

a. Philippines 23

b. Japan 24

c. South Korea 26

4. Global Trends for the Right to Erasure 28

4.1. Balancing Right to Erasure and Freedom of Speech 29

4.2. Right to Erasure of Public Figures 30

4.3. Public Interest and the Right to be Informed vs. the Right to Privacy 33

4.4. Privacy Rights of Children 35

5. Recommendations for Indian Rules 36

a. Constitutional Protections 36

b. Exemptions for public figures 37

c. De-indexing 37

d. Procedural Safeguards 38

e. Specialised provisions for children 40

f. Transparency reporting of platforms 40

EXECUTIVE SUMMARY

The Right to Erasure ("RTE"), also referred to as the Right to be Forgotten ("RTBF"), enables a data subject to request the Data Fiduciary to correct inaccurate or misleading data, complete incomplete data, and update outdated information. In India, Section 12 of the new Digital Personal Data Protection Act, 2023 ("DPDP Act") provides for RTE. The implementation of the DPDP Act will be provided for through the implementing rules ("Rules"), which are yet to be released. The aim of this policy brief is to lay down recommendations which can help strengthen the discourse around this subject as we look to finalise the implementing Rules.

RTE has emerged as an important right to protect one's personal data, however, its application is not without its challenges. It poses significant tensions with other fundamental rights and freedoms such as freedom of speech and expression, right to information, and freedom of the press. This policy brief aims at bridging the gap in the current iteration of RTE by providing recommendations for its implementation in India. It does so by providing an overview of the evolution of RTE in India and the jurisprudence and implementation of RTE in the European Union ("EU") and Asia (Philippines, Japan, South Korea). Based on an analysis of the different approaches, it identifies common trends that emerge in the enforcement of RTE.

This policy brief starts by introducing the concept of RTE and the idea of 'delisting'. It discusses RTE as provided under Article 17 of the General Data Protection Regulation ("GDPR"). It also discusses landmark cases from Europe which have had a significant impact on the evolution of RTE such as the *Google Spain* case, which recognised the right to request delisting for the first time.

The next section of the policy brief traces the evolution and scope of RTE in the Indian context. It briefly summarises and analyses the previous iterations of RTE throughout the various versions of the data protection bills in India over the years, leading up to the DPDP Act, arguing that the scope of RTE has considerably narrowed over the years. This

is supplemented by a discussion on the manner in which Courts in India have adjudicated different matters pertaining to this right in the past few years.

The policy brief conducts a comparative analysis of RTE in the EU and the Asian jurisdictions of South Korea, Japan and Philippines with existing RTE laws and jurisprudence. Asia and the EU demonstrate two different approaches to data protection generally and the right to erasure more specifically. The EU approach is more uniform and has decades of jurisprudence upon which it is based. The Asian approaches to data protection tend to be more scattered, and some jurisdictions, such as South Korea and the Philippines, have about a decade of jurisprudence in the field of data protection. A comparison of such differing jurisdictions provides a more holistic idea of the development of RTE across jurisdictions and how it may be suitably adapted for implementation in the Indian context. It also allows us to draw from the experiences of countries which are culturally or economically similar to India.

After a comparative analysis, the brief discusses broad trends and conflicts observable globally between RTE and other rights which must be considered for the holistic enforcement of the right. It discusses key issues at the intersection of privacy and freedom of speech and the right to information, and the application of RTE for public figures and children.

Based on its comparative analysis of the frameworks of RTE and a study of the key trends for RTE at the intersection of other rights and freedoms, the policy brief concludes with recommendations for the enforcement of RTE within the impending Rules under the DPDP Act. Briefly, the policy brief recommends the following:

a. *Constitutional Protections*: Need for criteria and a balancing test for deciding delisting or erasure of content to ensure, while ensuring protection of fundamental rights such as freedom of speech and expression and journalistic rights. The Rules should further lay down the kinds of personal information which further public interest and cannot be taken down under an application of RTE.

b. *Exemptions for public figures*: Identify types of data which may not be erased in public interest, such as certain types of information about public figures or government officials and the work done by them in furtherance of their duties.

c. *De-indexing*: Need for establishment of guidelines focussing on the processing of data by search engine providers and delisting requests submitted by data subjects. These would include, 1) the grounds for requesting delisting; 2) exceptions to the right to delisting; and 3) metrics for processing a delisting request.

d. *Procedural Safeguards*: The Rules should prescribe procedural requirements and safeguards for the implementation of RTE by the data fiduciaries. Such measures include 1) a notice requirement at the time of disposal of request for erasure; 2) reasons for rejection of request of erasure; 3) notification of the request for erasure to any third party in possession of the personal data; 4) appeal mechanism against refusal of request of erasure or delisting by the data fiduciary; 5) prescribed time period for disposal of an RTE request by the data fiduciary.

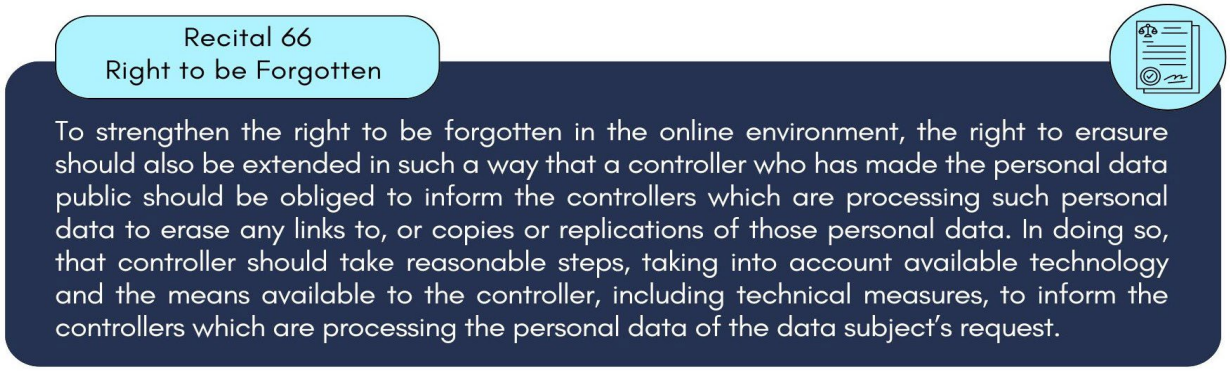
e. *Specialised provisions for children*: The Rules must have special provisions for the erasure of personal data of children, as well as the deletion of personal data uploaded by children if they or their legal guardians request it. This should include rules which allow individuals to erase personal data they uploaded about themselves while they were minors, after they attain the age of majority

f. *Transparency reporting of platforms*: The data fiduciaries should be required to publish transparency reports regularly, providing a comprehensive analysis of the ways in which they assess requests in relation to erasure/delisting.

1. INTRODUCTION

The modern notion of the Right to Erasure ("RTE") has its roots in the French and Italian legal concepts of the 'right to oblivion.'[1] In general terms, it has been viewed as the right for natural persons to have information about them deleted after a certain period of time. At first, the right to oblivion was mostly related to the removal of an individual's judicial and criminal past. However, its current iteration has gone beyond this conception and now forms an integral part of data protection regimes around the world.

The right to erasure is also known as the right to be forgotten ("RTBF") in the European Union ("EU"). Article 17 of the General Data Protection Regulation, 2018 ("GDPR") uses these two phrases interchangeably. Similarly, Recital 66 of the GDPR refers to the right to erasure and the right to be forgotten in an interchangeable way, and does not indicate any distinction between the two.[2]



The guidance released by the UK Information Communication Officer's office ("ICO guidance") provides for the 'right to be forgotten' under Article 17 of the UK GDPR, as the right of individuals to have their personal data erased.[3]

[1] Paul Alexander Bernal, 'A right to delete?', (2011) 2(2) European Journal of Law and Technology.
[2] General Data Protection Regulation, 'Recital 66 - Right to be Forgotten', <https://gdpr-info.eu/recitals/no-66/> accessed 21 November 2024.
[3] Information Commissioner's Office, 'Right to Erasure' <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-erasure/#:~:text=The%20right%20to%20erasure%20is,to%20respond%20to%20a%20request> accessed 21 November 2024.

There does not seem to be a legislative distinction or a consensus in the scope of RTE and RTBF being distinct. Consequently, in this policy brief, we use the terms RTE and RTBF to refer to similar rights under different legal instruments. We will generally use the term RTE, unless specifically termed otherwise in original source or required otherwise for definitional purposes.

In the internet age, as more and more information about individuals becomes available on the internet, the idea of 'delisting' has become an important aspect of RTE. Article 17 of the GDPR has been interpreted to take into account the Right to request delisting. Right to request delisting was first recognised in the *Google Spain* case.[4]

DELISTING

Delisting allows a data subject to request the provider of an online search engine to erase one or more links to web pages from the list of results displayed following a search made on the basis of his or her name. Thus, it allows the data subject to exercise some control over the information available about them on the internet.

The historic ruling in *Google Spain* recognised that search engine operators process personal data and qualify as data controllers. Therefore, as a general rule, the rights of the data subject would prevail over the economic interest of the search engine and that of internet users to have access to the personal information through the search engine. However, a balance of the relevant rights and interests has to be struck and the outcome may depend on the nature and sensitivity of the processed data and on the interest of the public in having access to that particular information.[5]

Since this ruling, other countries have introduced their own versions of the law on the 'right to erasure' and the 'right to request delisting'.

[4] CCG-NLUD, 'Google Spain SL and Google Inc. vs. Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gonsalez' (*Privacy Law Library CCG-NLUD*) <https://privacylibrary.ccgnlud.org/case/spain-sl-vs-agencia-espaola-de-proteccin-de-datos-aepd?searchuniqueid=333115> accessed on 21 November 2024.
[5] *Id.*

Russia, for instance, under its 'right to be forgotten law' gave its citizens the right to request search engines to remove links about them that were in violation of Russian law, inaccurate, out of date, or irrelevant because of subsequent events or actions taken by the citizens.[6] Similarly, Latin American countries such as Brazil and Chile have adopted an array of data subject rights including the right to erasure which allows individuals to seek erasure and delisting of personal data when it is inaccurate or out of date.[7] Various iterations of this right can also be seen in Asian jurisdictions such as the Philippines, Japan, South Korea, and India, discussed in further detail in subsequent sections.

However, the application of this right is not without its challenges as it also poses significant tensions with other fundamental rights and freedoms such as freedom of speech and expression, right to information, and freedom of the press. For this policy brief, we will provide an overview of the jurisprudence and implementation of RTE in the EU and Asia. The EU and Asia offer two different approaches to data protection and the right to erasure. While the EU approach is more uniform with decades of jurisprudence, the Asian approaches to data protection tend to be more scattered and recent. This policy brief further identifies common trends that emerge from an assessment of the manner of implementation of the right across the world and concludes by providing recommendations for its implementation in India.

2. RIGHT TO ERASURE IN INDIA

The primary basis for RTE claim in India stems from the right to privacy, which is a fundamental right under the Constitution of India. The landmark case for the right to privacy in India is *K.S. Puttaswamy vs. Union of India*, which recognised RTE/RTBF

[6] Federal Law No. 264-FZ, Amending the Federal Law "On Information, Information Technologies, and Information Protection" and Articles 29 and 402 of the Civil Procedural Code of the Russian Federation (aka Right to be Forgotten Law), July 13, 2015; 'Duma passes 'right to be forgotten online' law' (*DW*, 7 March 2015) <https://www.dw.com/en/russian-parliament-approves-right-to-be-forgotten-online-law/a-18560565> accessed 21 November 2024; Article 19, 'Legal Analysis: Russia's Right To Be Forgotten' (*Article19.org*, 16 September 2015) <https://www.article19.org/resources/legal-analysis-russias-right-to-be-forgotten/> accessed 21 November 2024.

[7] Arturo J Carrillo and Matías Jackson, 'Follow the Leader? A Comparative Law Study of the EU's General Data Protection Regulation's Impact in Latin America' (2022) 16(2) ICL Journal 177

under the ambit of informational privacy.[8] RTE has been discussed in the various iterations of data protection bills in India, finally culminating into the new Digital Personal Data Protection Act, 2023 ("DPDP Act").[9] The DPDP Act provides for RTE under Section 12. Section 12 of the DPDP Act grants individuals the right to request the Data Fiduciary to correct any data that's inaccurate or misleading, complete any data that's incomplete, and update any data that's outdated. The exact application of this provision will be clarified through the implementing rules ("Rules") under the DPDP Act, which are yet to be released.

Justice K.S. Puttaswamy vs. Union of India (Supreme Court of India, 2017)

In this case, a 9-judge bench reaffirmed the right to privacy as a fundamental right under the Constitution of India. It identified and elaborated on various aspects of the right to privacy, one of which was Informational Privacy.

Justice Chandrachud defined Informational Privacy as "an interest in preventing the information about the self from being disseminated and controlling the extent of access to information." Justice Kaul identified informational privacy to include the right to be forgotten. Justice Kaul noted that such a right would allow an individual, who does not wish their personal data to be processed or stored, to have the option to remove it from the system in cases where the personal data/information is no longer necessary, relevant or correct, and served no legitimate purpose.

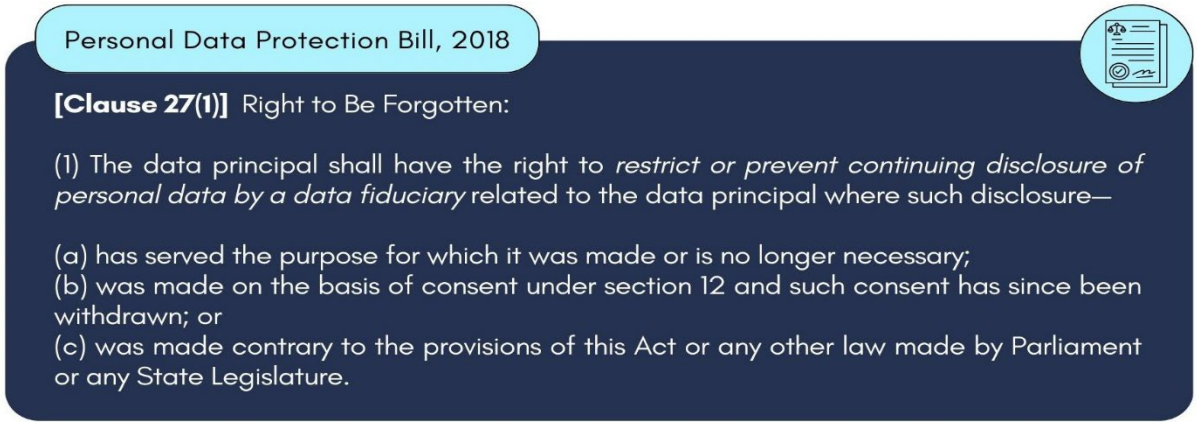
In the iterations prior to the DPDP Act, RTE was a considerably wider right as compared to the narrowed scope in the most recent iterations. In the following subsections, we discuss how the scope and implementation of RTE under Indian data protection law has evolved from 2018 to 2023.

2.1. Evolution of the Scope of RTE

The first mention of RTE in Indian policy can be traced back to the Srikrishna Committee Report of 2018 that included the Draft Personal Data Protection Bill, 2018 ("2018 Bill").[10]

[8] *Justice K.S. Puttaswamy vs. Union of India* (2017) 10 SCC 1, ⁋250, 636.
[9] Digital Personal Data Protection Act 2023
[10] Personal Data Protection Bill 2018, clause 27

The report and the bill termed RTE as the 'right to be forgotten' and defined it as the 'right of individuals to limit, delete, or correct the disclosure of personal information on the internet that is misleading, embarrassing, irrelevant, or anachronistic.'



While recognising RTBF, the Srikrishna Report recommended balancing it with other rights and freedoms, such as freedom of press and the right to information. Noting that such balancing exercise should not be left to private entities such as the data fiduciaries, it recommended a five-point balancing test which considered:

a) Nature of the personal data sought to be restricted;
b) Scale of disclosure and the degree of accessibility of the personal data;
c) Whether the data principal has a public presence or holds a public office;
d) Relevance of the personal data to the public;
e) Nature of the disclosure and the activities of the data fiduciary.

The assessment under the five-point test was to be done by an Adjudicatory Officer under the 2018 Bill.[11] The 2018 Bill was revised into the Personal Data Protection Bill, 2019 ("2019 Bill"), which contained a similar provision for RTBF as the 2018 Bill, including the five-point balancing test.[12] However, the 2019 Bill introduced an additional and distinct provision termed 'right to erasure of personal data', which was available for erasure of personal data no longer necessary for the purpose for which it was processed.[13] The

[11] Personal Data Protection Bill, 2018, clause 27(2), 27(3) read with clause 68
[12] Personal Data Protection Bill 2019, clause 20
[13] Personal Data Protection Bill 2019, clause 18

request for erasure of data under the latter provision was to be made to the data fiduciary. The data fiduciary was to provide reasons while rejecting an application and was required to have regard to the impact of erasure on the rights and interests of the data principal.

Personal Data Protection Bill, 2019

[Clause 18(1)] Right to correction and erasure:

(1) The data principal shall where necessary, having regard to the purposes for which personal data is being processed, subject to such conditions and in such manner as may be specified by regulations, have the right to—

(d) the erasure of personal data which is no longer necessary for the purpose for which it was processed

In some ways, therefore, the 2019 Bill expanded the scope of RTBF as originally envisaged under the 2018 Bill. The 'right to erasure' read with the 'right to be forgotten' under the 2019 Bill accounted for situations where an erasure of personal data may not lead to removal of data already disclosed elsewhere, while preventing any continued processing of personal data without disclosing the personal data.

Personal Data Protection Bill, 2019

[Clause 20(1)] Right to be forgotten:

(1) The data principal shall have the right to restrict or prevent the continuing disclosure of his personal data by a data fiduciary where such disclosure—

(a) has served the purpose for which it was collected or is no longer necessary for the purpose;
(b) was made with the consent of the data principal under section 11 and such consent has since been withdrawn; or
(c) was made contrary to the provisions of this Act or any other law for the time being in force.

RTBF under the 2019 Bill was further expanded by the Joint Committee Report of 2021 which recommended revision of the right to be forgotten under the 2019 Bill to include 'processing of personal data', along with disclosure. This was suggested to prevent a data

fiduciary from continuing to process data after a restriction on disclosure of data on exercise of the right.

The Data Protection Bill, 2021

[Clause 20] The Right to be Forgotten:

(1) The data principal shall have the right to restrict or prevent the continuing disclosure **or processing** of his personal data by a data forgotten. fiduciary where such disclosure **or processing** —

(a) has served the purpose for which it was collected or is no longer necessary for the purpose;
(b) was made with the consent of the data principal under section 11 and such consent has since been withdrawn; or
(c) was made contrary to the provisions of this Act or any other law for the time being in force.

Unlike all previous iterations of RTE/RTBF, the Digital Personal Data Protection Bill, 2022 ('2022 Bill') contained a limited right to erasure.[14] Under the 2022 Bill, the right to erasure was available to seek removal of personal data no longer necessary for the purpose for which it was processed. It removed extension of the right for disclosures and processing of data as envisaged under the previous bill and provided a narrower reading of RTE.

The Digital Personal Data Protection Bill, 2022

[Clause 13] Right to correction and erasure of personal data:

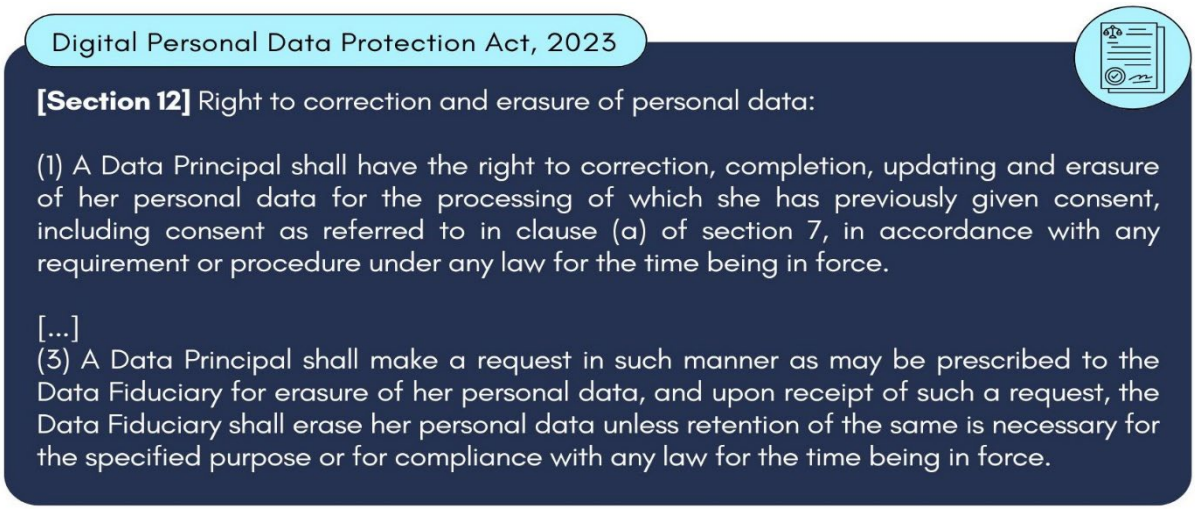
(1) A Data Principal shall have the right to correction and erasure of her personal data, in accordance with the applicable laws and in such manner as may be prescribed.

(2) A Data Fiduciary shall, upon receiving a request for such correction and erasure from a Data Principal:

(d) erase the personal data of a Data Principal that is no longer necessary for the purpose for which it was processed unless retention is necessary for a legal purpose.

[14] Digital Personal Data Protection Bill 2022, clause 13

In its current form under the DPDP Act, RTE is available for erasure of personal data for the processing of which the data principal had previously given consent.



However, under Section 7(a) of the DPDP Act, data may also be processed for purposes where the data principal has not explicitly prohibited the use of her personal data. This impacts the exercise of RTE as it does not account for situations where the data may be processed either for a purpose different from the one originally sought consent for, or where the data is shared with another entity without notice or consent of the data principal. For example, 'X', an individual shares her personal data with a real estate broker 'Y,' to help her find suitable accommodation for rent. 'Y' can process her personal data for the specified purpose of finding 'X' an accommodation. However, if 'Y' further shares 'X's personal data with a third party 'Z', 'X' should be able to exercise her RTE against 'Z'. The DPDP Act also allows retention where it is "necessary for the compliance with any law" in force.

Further, under Section 17 of the Act, the right to erasure, amongst other rights, is not available for exempted entities, including any instrumentalities of the State notified under the DPDP Act. The combined effect of the Act leads to dilution of the strength of RTE in both its scope and effective enforcement, as discussed in detail in the following section.

2.2. Implementation of RTE

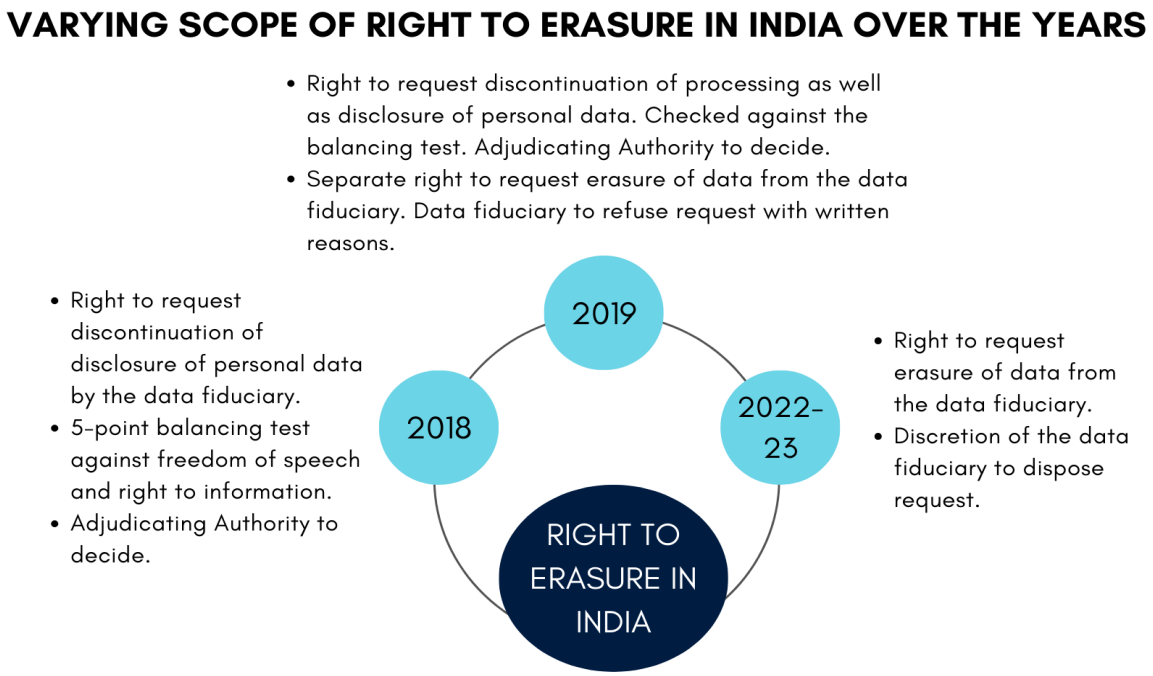
Early iterations of RTE provided for an adjudicatory mechanism keeping in mind the need to balance RTE against other rights and freedoms. The Srikrishna Committee Report had cited practical difficulties associated with implementing RTE by data fiduciaries alone. For instance, it noted that since rejection of delisting requests could involve legal consequences for the data fiduciary, it may disincentivise the data fiduciary from turning down requests. It recommended that the request for removal of personal data should be made to the Adjudicatory Wing of the Data Protection Authority envisaged under the 2018 Bill. Hence, the right was to be available only if the Adjudicatory Authority determined, after conducting the balancing test, that the interest of the data principal overrode the rights to freedom of speech and expression or the right to information of another individual.[15] The 2018 Bill further provided the data principal the option to apply to the Adjudicating Officer to seek review of their decision.[16]

The 2019 Bill, similarly contained safeguards to ensure a balance of rights and freedoms.[17] An application in exercise of the 'right to be forgotten' lay with the Adjudicating Officer who was to decide on the basis of the five-point test. For applications for erasure of data to the data fiduciary, the data fiduciary was required to provide reasons for rejecting an application for erasure of personal data.[18] It further allowed the data fiduciary to dispute the rejection of their request, in which case the data fiduciary was required to indicate against the relevant personal data that the same was disputed.[19] Upon erasure, the data fiduciary was also required to notify the relevant entities or individuals to whom the personal data might have been disclosed.[20]

Unlike all previous iterations, 2022 Bill and the DPDP Act neither provide for review and disputing of the decision of the data fiduciary nor do they envisage a need for an

[15] Clause 27(3) of the Personal Data Protection Bill, 2018
[16] Clause 27(5) of the Personal Data Protection Bill, 2018
[17] Clause 20(2) and Clause 20(3) of the Personal Data Protection Bill, 2019.
[18] Clause 18(2) of the Personal Data Protection Bill, 2019
[19] Clause 18(3) of the Personal Data Protection Bill, 2019
[20] Clause 18(4) of the Personal Data Protection Bill, 2019

adjudicatory body for balancing of rights and freedoms impacted by RTE. The current iteration of the law on RTE has therefore been reduced in scope from its earlier iterations, and it offers more limited protections than originally envisioned.



2.3. Courts in India on the Right to Erasure

While RTE is a recent introduction to the legislative framework in India with the introduction of the DPDP Act, courts have been adjudicating matters pertaining to the right since the past few years. These matters pertain to the removal of personal information about an individual disclosed on the internet, usually based on a violation of the right to reputation and the right to privacy.[21] These orders are usually passed as interim orders directing platforms or search engines to remove the impugned information, often through delisting. Some of the petitions before the court are for

[21] Tellmy Jolly, 'Kerala High Court Directs Removal Of Female Litigant's Name, Details From Court Website, Says It Affected Her Reputation And Dignity' (*LiveLaw*, 1 December 2023) <https://www.livelaw.in/high-court/kerala-high-court/kerala-high-court-direction-remove-female-litigant-details-court-website-243454> accessed 21 November 2024. (The Kerala High Court ordered masking of name of the petitioner who was a female as the issue was sensitive and could affect her reputation and dignity).

masking personal information in court records so that the individuals are not identifiable in the public domain.

One of the first cases on RTE was *Laksh Vir Singh Yadav vs. Union of India*,[22] which called on the Delhi High Court to create a legal regime for the right to be forgotten, including requests for delisting publicly reported court judgements.[23] As of date, the case is pending before the Delhi High Court.

In another case before the Delhi High Court, the plaintiff sought the removal of an Instagram post identifying him in a sexual harassment allegation; the court allowed an ex-parte interim order akin to RTE based on a claim of harm to reputation.[24] The defendant had an anonymous Instagram account that made a post regarding the plaintiff alleging sexual harassment against him during the #MeToo era. The plaintiff claimed that the content was defamatory and sought removal of the Instagram post and the contents available on Google search.[25] In passing its order, the Court reasoned that the anonymous allegations of alleged defamatory nature "cannot be permitted to be made in public domain/published without being backed by legal recourse," else they could lead to mischief.[26]

In other cases, petitioners have sought removal of their details from Google search or from IndianKanoon on grounds such as adverse impact in availing employment opportunities or reputational harm. Petitioners have also sought to delist links with information on criminal cases against them in which they were subsequently acquitted.[27] In one case from July 2023,[28] the Gujarat High Court observed that where an individual was acquitted in

---

[22] W.P.(C) 1021 / 2016

[23] 'Intervention in the High Court of Delhi on the "Right to Be Forgotten" Case' (*Internet Freedom Foundation*, 20 September 2016) <https://internetfreedom.in/intervention-in-the-high-court-of-delhi-on-the-right-to-be-forgotten/> accessed 21 November 2024.

[24] *Subodh Gupta v HERDSCENEAND & Ors.*, CS(OS) 483/2019

[25] 'Subodh Gupta v. Herdsceneand' (*Global Freedom of Expression*) <https://globalfreedomofexpression.columbia.edu/cases/gupta-v-herdsceneand/> accessed 21 November 2024.

[26] Ibid.

[27] *Mr. X vs. Registrar General, High Court of Karnataka* Writ Petition No. 25557 OF 2023 (Karnataka High Court)

[28] Bhavya Singh, 'Once FIR Is Quashed, It Is Duty Of Press To Delete Case-Related News Articles: Gujarat High Court' (*LiveLaw*, 27 July 2023) <https://www.livelaw.in/high-court/gujarat-high-court/gujarat-

a criminal case, any articles published on the case should be deleted. It reasoned that the continued visibility of such articles in the press gives the impression of the criminal case pending against the concerned individual and harms their goodwill. This was in contrast to the opinion of the single judge of the Madras High Court in the case of *Karthick Theodre vs. Registrar General Madras High Court.*[29] The court here declined to grant the right to be forgotten in a petition praying for redaction of name of the petitioner from court records and IndianKanoon publication of a prior criminal case against him in which he was subsequently acquitted.

The court found that alteration of court records or removal of name from all records in public domain in such instances went against the principle of open justice. It further noted the need for a data protection law and rules outlining the criteria for the redaction of names of the accused subsequently acquitted from the criminal proceeding. This opinion was however recently overturned by a division bench of the Madras High Court,[30] which allowed redaction of the name of the petitioner from the case, while noting that a court should exercise discretion in such matters while balancing the right to be forgotten against the right to know. The matter has now been appealed and is pending consideration by the Supreme Court.[31] Most recently, the Delhi High Court allowed a petitioner's name to be masked in a criminal case against him which was subsequently quashed, on all concerned portals including public search engines.[32] The Court noted that no public interest would be served by the continued disclosure of such information on the internet once the case is quashed.

The Criminal Procedure Code, 1973 provides for in-camera proceedings in cases of rape, requires maintenance of confidentiality and prohibits publishing of any personal details

high-court-duty-of-press-case-related-articles-deletion-observations-233756> accessed 21 November 2024.

[29] (2021) 5 CTC 668

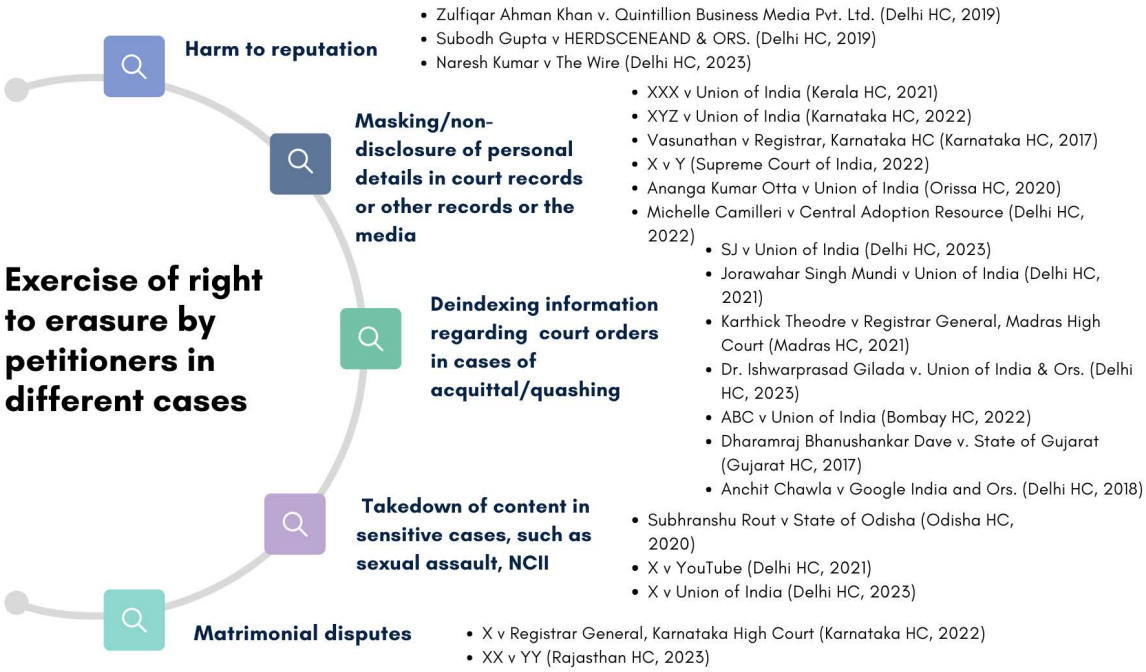
[30] W.A.(MD)No.1901 of 2021 (Madras High Court)

[31] The Supreme Court passed an interim order of stay on the order of the Division Bench of the Madras High Court (Special Leave to Appeal (C) No(s). 15311/2024).

[32] Nupur Thapliyal, 'No Public Interest In Keeping Information Alive On Internet After Quashing Of FIR: Delhi High Court On Right To Be Forgotten' (LiveLaw, 21 November 2024) <https://www.livelaw.in/high-court/delhi-high-court/delhi-high-court-right-to-be-forgtten-privacy-275938> accessed 21 November 2024.

of the parties in the case. In view of this, the Kerala High Court recently allowed RTE against disclosure of personal details of the petitioner in any form of media in a criminal proceeding of rape, except for purposes of court records or the printing and publication of the judgement.[33]

Similarly, in another case[34] concerning a juvenile accused of an offence, the Rajasthan High Court interpreted Section 24 of the Juvenile Justice Act, 2015[35] to contain the right to be forgotten for a 'juvenile in conflict with law'.



[33] *XXX v Union of India* WP(CRL.) No. 318 of 2022 (Kerala High Court)
[34] *Jitendra Meena v State of Rajasthan* S.B. Civil Writ Petition No. 9143/2021
[35] Juvenile Justice Act 2015, s 24 - 'Removal of disqualification on the findings of an offence'
"(1) Notwithstanding anything contained in any other law for the time being in force, a child who has committed an offence and has been dealt with under the provisions of this Act shall not suffer disqualification, if any, attached to a conviction of an offence under such law:
Provided that in case of a child who has completed or is above the age of sixteen years and is found to be in conflict with law by the Children's Court under clause (i) of sub-section (1) of section 19, the provisions of sub-section (1) shall not apply.
(2) The Board shall make an order directing the Police, or by the Childrens Court to its own registry that the relevant records of such conviction shall be destroyed after the expiry of the period of appeal or, as the case may be, a reasonable period as may be prescribed:

Since the DPDPA does not account for the adjudicatory mechanisms or the need for the balance of right to erasure against rights such as access to information, or a mechanism to dispute the decision of the data fiduciary for an RTE request, there is a likelihood for the courts to continue to be a crucial avenue for individuals towards enforcement of RTE.

3. GLOBAL APPROACHES TO THE RIGHT TO ERASURE

Different iterations of RTE can be found across the world. While it is important to look at the developments in the EU, it is equally important to note the development and application of RTE in Asian jurisdictions. We have chosen to focus on Asia and the EU as the two main jurisdictions in this brief as they demonstrate two different approaches to data protection generally and the right to erasure more specifically. The EU approach is more uniform and has decades of jurisprudence upon which it is based. The Asian approaches to data protection tend to be more scattered, and some jurisdictions, such as South Korea and the Philippines, have about a decade of jurisprudence in the field of data protection. India's own data protection law, the DPDP Act, is less than a year old and is yet to come into operation.

Comparing such differing jurisdictions will allow us to have a more holistic idea of how RTE is developing across jurisdictions and how it can be implemented in the Indian context. It also allows us to draw from the experiences of countries which are culturally or economically similar to India.

3.1. EU

The right to erasure, an extension of the EU-wide recognised right to be forgotten, stems from a culmination of various sources in the EU. The roots of RTE can be traced back to the right to privacy under the Charter of Fundamental Rights, 2000 ("EU Charter") of the EU.

Provided that in case of a heinous offence where the child is found to be in conflict with law under clause (i) of sub-section (1) of section 19, the relevant records of conviction of such child shall be retained by the Children's Court."

Charter of Fundamental Rights, 2000

[Article 7] Respect for private and family life

(1) everyone has the right to respect for his or her private and family life, home and communications;

[Article 8] Protection of personal data

(1) everyone has the right to the protection of personal data concerning him or her;
(2) such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified;
(3) Compliance with these rules shall be subject to control by an independent authority.

RTE was then included within the data protection regime of the now-repealed Data Protection Directive of 1995 ("DPD"). The DPD established that individuals in the EU could request for their personal data to be corrected, erased or blocked once that data was no longer necessary, or if it was of an incomplete or inaccurate nature. Essentially, by virtue of this right, data controllers such as Facebook or Google were obligated to delete all the data of those data subjects who left their services or had "compelling grounds" to request for the erasure of their data.

The current iteration of this right can be found in the General Data Protection Regulation ("GDPR"), which replaced the DPD. Article 17 of the GDPR on the Right to Erasure, outlines the rights of the data subjects and provides them the right to seek erasure of their personal data which has been collected and processed by a data controller, under prescribed circumstances.[36] RTE, under GDPR, is more expansive than its previous iteration, as it does not require the data subject to demonstrate "compelling grounds", thereby reducing the burden of proof on the data subject for the exercise of the right.

[36] General Data Protection Regulation 2018, article 17

General Data Protection Regulation, 2018

[Article 17(1)] Right to erasure ('right to be forgotten')

(1) The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) no longer necessary in relation to the purposes for which the data were collected or otherwise processed;
(b) where data subjects have withdrawn their consent for processing;
(c) where they object to the processing of personal data concerning them;
(d) Where the data has been unlawfully processed;
(e) where the processing of their personal data otherwise does not comply with this Regulation; and
(f) the personal data have been collected in relation to the offer of information society services

While RTE is a crucial tool to ensure that a data subject has control over their data and its processing, a significant focus of the global debate has been on its intersection with privacy and freedom of expression. The origins of this debate can be traced back to the *Google Spain* case.[37]

Google Spain SL and Google Inc. vs. Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gonsalez
(2014 - European Union Court of Justice)

In this case, the European Union Court of Justice interpreted the right to erasure in the context of search engines thereby clarifying the application of data protection law to search engines.

It ruled that an individual could request for the erasure of their data by asking search engines to de-list certain web addresses from search results when a search was conducted using the name of the person making the delisting request.

Thereafter, search engines would have to make a case-by-case analysis in order to determine whether the request is legitimate.

[37] CCG-NLUD, 'Google Spain SL and Google Inc. vs. Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gonsalez' (*Privacy Law Library CCG-NLUD*) <https://privacylibrary.ccgnlud.org/case/spain-sl-vs-agencia-espaola-de-proteccin-de-datos-aepd?searchuniqueid=333115> accessed 21 November 2024.

With this case, the European Union Court of Justice ("CJEU") established a set criteria for search engines to consider while assessing such delisting requests so as to ensure that there was no undue use of powers from their end. Search engines could grant a delisting request only when the personal information provided was "inadequate, irrelevant or no longer relevant, or excessive", and only if the information did not pertain to a public figure or was not of public interest. However, this ruling did not require search engines to remove delisted links from the search index altogether. In other words, the data would still remain on the internet, and users could access it by conducting searches using terms other than the name of the individual making the delisting request.

Following the judgement, the Article 29 Working Party created guidelines for evaluating delisting requests.[38] These guidelines laid down the criteria to be considered by various national data protection authorities while considering delisting requests. These included the nature, accuracy, and the sensitivity of the data sought to be removed, its relevance for public interest, the impact of such data processing on the data subject, and whether the data subject was a minor.

Each of the criteria had to be applied taking into account any conflict between individual privacy and "the interest of the general public in having access to the information." As per the Working Party, in most cases, more than one criterion needed to be taken into consideration in order to reach a decision. In other words, no single criterion in itself stood as determinative.

The Working Party was replaced by the European Data Protection Board in the year 2018 which adopted a new set of guidelines and recommendations to further solidify the right to erasure. These were called the Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR ("Guidelines")[39]. The Guidelines

[38] Article 29 Working Party, 'Guidelines on the Implementation of the Court of Justice of the European Union on Google Spain and Inc v. Agencia Española De Protección De Datos (AEPD) and Mario Costeja Gonzalez' (2014) 14/EN WP225 <https://www.pdpjournals.com/docs/88502.pdf> accessed 21 November 2024

[39] European Data Protection Board, 'Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (Part 1) Version 2.0' (2020) <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201905_rtbfsearchengines_afterpublicconsultation_en.pdf> accessed 21 November 2024.

interpret the RTE in the context of search engines in light of the provisions of Article 17, GDPR. These Guidelines delineate two primary aspects, 1) grounds a data subject can rely on for a delisting request sent to a search engine provider and; 2) the exceptions to the right to request delisting.

Grounds of the right to request delisting under GDPR

(1) When the personal data is no longer necessary in relation to the search engine provider's processing;
(2) When the data subject withdraws consent for the processing;
(3) When the data subject has exercised his or her right to object to the processing of his or her data;
(4) When the personal data has to be erased for compliance with a legal obligation;
(5) When the personal data has been collected in relation to the offer of information society services to a child.

Exceptions to the right to request delisting under GDPR

(1) For exercising the right of freedom of expression and information;
(2) For compliance with a legal obligation;
(3) For reasons of public interest in the area of public health;
(4) For achieving purposes in the public interest, scientific and historical research purposes, statistical purposes;
(5) For the establishment, exercise or defence of legal claims.

Since information on any domain on the internet is generally accessible worldwide, uncertainties arise as to the territorial limitations to the enforcement of a delisting request. On this question, the CJEU in the *Google Spain* case had held that delisting decisions must be implemented to guarantee complete protection of the data subject's rights. In other words, delisting must not be limited to EU domains only so as to ensure that the EU law is not circumvented in any manner. Essentially, this meant that delisting should also be effective on all domains, including *.com* and not just respective national domains.

However, in *Google LLC vs. CNIL*,[40] the CJEU took a different stance.

Google LLC vs. CNIL (European Union Court of Justice, 2019)

In this case, the CJEU declared that search engines such as Google were not required to carry out a delisting request on all the versions of its search engines (globally).

It reasoned that numerous States, outside the EU, did not recognize a right to delisting or that they had adopted an altogether different approach. Consequently, the balance between privacy, data protection and freedom of information varied significantly around the globe.

Therefore, Google and other operators were not required to delistde-reference links containing personal data from search results on their non-EU search engines.

After this case, Google and other operators were not required to delist links containing personal data from search results on their non-EU search engines.

Currently, there is no obligation under the EU law for a search engine operator to enforce a delisting request worldwide. However, there exists an obligation to apply the removal throughout the EU, and not confine it to the Member State where the request originated. The CJEU however clarified that an authority of an EU member state remained competent to order, "where appropriate," a search engine operator to de-reference data from all versions of its search engines worldwide, suggesting that there may be exceptional cases where search engines could be allowed to de-list data globally.

In terms of an appeal mechanism, if a search engine rejects the delisting request, the data subject can either file a complaint with the respective data protection authority (for example in France, it is the CNIL), or the competent judicial authority in each Member State.

3.2. Asia

Asian countries have a different approach towards RTE, and there is no single accepted standard across the continent. The data protection landscape in most Asian countries is

[40] CCG-NLUD, 'Google LLC vs. Commission nationale de l'informatique et des libertés (CNIL)' (*Privacy Law Library CCG-NLUD)* <https://privacylibrary.ccgnlud.org/case/google-llc-vs-commission-nationale-de-linformatique-et-des-liberts-cnil?searchuniqueid=662291> accessed 21 November 2024.

more recent, and lacks the long jurisprudential history which can be found in the EU. In this section we have examined the laws and regulations relating to RTE in the Philippines, Japan, and South Korea. The data protection laws of each of these countries provide for RTE, and they contain valuable policies or cases which speak to the implementation of this law.

a. Philippines

The right to erasure or blocking is contained in section 16(e)[41] of the Data Privacy Act, 2012. The National Privacy Commission of the Philippines ("Commission") has clarified that data subjects have the right to request for the suspension, withdrawal, blocking, removal, or destruction of their personal data from the Personal Information Controller's ("PIC") filing system, in both live and backup systems.[42] The right to erasure or blocking in the Philippines can be applied to all personal data that is publicly available online. In case of a request for removal, the PIC would have to communicate with other PICs, including third party indexes, and request them to erase copies or remove or de-list search results or links to the data subject's pertinent personal data.

The Commission also explains that in certain circumstances, the PIC may refuse, in whole or in part, to delete the personal information of the data subject.[43] The scope of RTE in

[41] Data Privacy Act 2012, s 16(e) - "Suspend, withdraw or order the blocking, removal or destruction of his or her personal information from the personal information controller's filing system upon discovery and substantial proof that the personal information are incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes or are no longer necessary for the purposes for which they were collected. In this case, the personal information controller may notify third parties who have previously received such processed personal information"

[42] National Privacy Commission, 'The right to erasure or blocking', <https://privacy.gov.ph/right-to-erasure-or-blocking/> accessed 21 November 2024.

[43] A PIC may deny your request for erasure or blocking, wholly or partly, when personal data is still necessary in any of the following instances:

1. Fulfillment of the purpose/s for which the data was obtained;
2. Compliance with a legal obligation which requires personal data processing;
3. Establishment, exercise, or defense of any legal claim;
4. Legitimate business purposes of the PIC, consistent with the applicable industry standard for personal data retention;
5. To apprise the public on matters that have an overriding public interest or concern, taking into consideration the following factors:
   - constitutionally guaranteed rights and freedoms of speech, of expression, or of the press;
   - whether or not the personal data pertains to a data subject who is a public figure; and

the Philippines is considerably broader since it requires PIC's to remove information from live and backup systems, and communicate the removal request to third parties as well.

In 2022, the Commission decided the case of *JBA vs. FNT and NNT* where they upheld a broad scope for the existence and the implementation of an individual's right to erasure.[44]

JBA vs. FNT and NNT
(National Privacy Commission of the Philippines, 2022)

In this case, JBA had been an employee of FNT and NNT firm, and her image was used in ad's for their firm even after her departure.

The Commission held that the individuals were acting in the capacity of Personal Information Controllers, and they had violated their obligations under the Data Privacy Act by processing the information after JBA withdrew consent for their data to be used. The Commission clarified that a PIC cannot deny their liability under the Data Privacy Act by arguing that they were not responsible for the auto-renewal of the ad by the advertising website.

This was a wide reading of the right to erasure, where the Commission emphasised on the need for PIC's to make positive efforts to remove information once the data principal withdraws their consent. It also upheld the PIC's obligation to inform third parties of the erasure request from the data subject. The Commission rejected a motion for reconsideration and upheld this decision in 2023.[45]

b. Japan

The applicable data protection law in Japan is the Act on the Protection of Personal Information, 2003 (APPI)[46] which was thoroughly revised in 2015 and came into effect in 2017. The data protection regime in Japan does not very closely resemble either the omnibus protections of the EU or the sectoral approach of the US, and rather falls somewhere in the middle. In 2015, Articles 28-30, granting judicially enforceable rights

- other analogous considerations where personal data are processed in circumstances where data subjects can reasonably expect further processing.

6. As may be provided by any existing law, rules, and regulations

[44] *JBA v FNT and NNT* NPC 20-026 (2022)
[45] *Id.*
[46] Act on the Protection of Personal Information, 2003

to data subjects, were added to the APPI. These included the right to request "disclosure", "rectification", "addition", "erasure", and "cessation of use" of personal data in the private sector.[47]

In 2017, the Supreme Court of Japan decided on a landmark case on the right to privacy in Japan.[48]

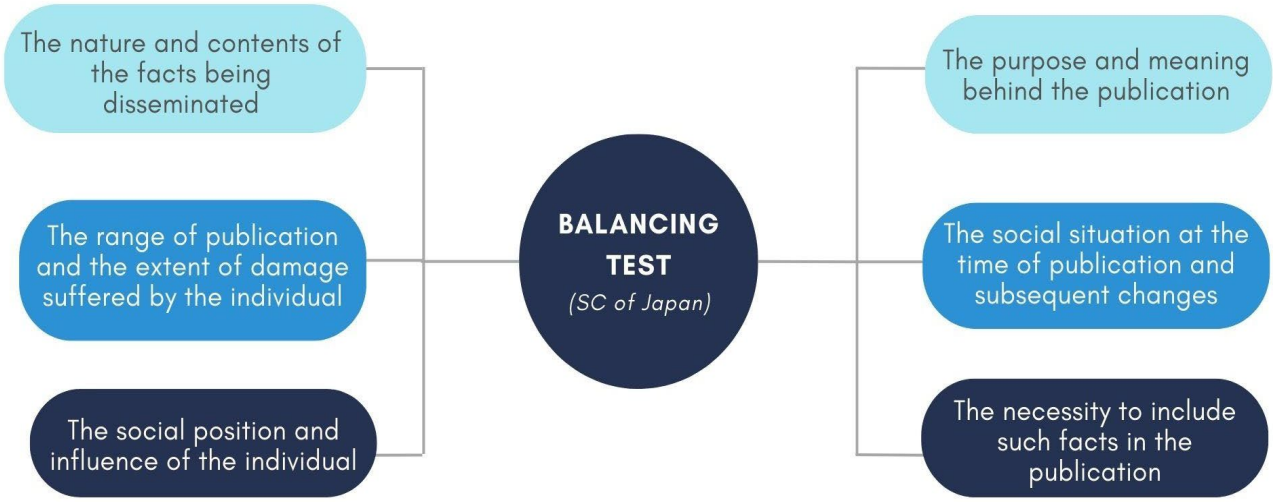
Case of a permitted appeal of the decision to rescind the decision of the second instance concerning the approval and decision on a provisional disposition to delete posted articles
(Supreme Court of Japan, 2017)

In this case, the court balanced the public's interest in knowing about the commission of certain offences against an individual's privacy in taking down URLs which contained personal information about him. The court held that while considering delisting requests, it would have to balance the reasons for preventing dissemination with the public's right to know.

The court held that while a criminal conviction was an intrinsic part of the appellant's privacy, the links in question related to an act committed by him that was strongly condemned by the society and prohibited by law, which made it a matter of public interest.

[47] Article 28, 29, 30 of Act on the Protection of Personal Information, 2003
[48] CCG-NLUD, 'Case of a permitted appeal of the decision to rescind the decision of the second instance concerning the approval and decision on a provisional disposition to delete posted articles' (*Privacy Law Library CCG-NLUD*) <https://privacylibrary.ccgnlud.org/case/case-of-a-permitted-appeal-of-the-decision-to-rescind-the-decision-of-the-second-instance-concerning-the-approval-and-decision-on-a-provisional-disposition-to-delete-posted-articles?searchuniqueid=142989> accessed 21 November 2024.

The court laid down the following factors for consideration:



This case forms a cornerstone of RTE jurisprudence in Japan. It considers the conflict between the right to privacy of the appellant and public interest but does not specifically refer to RTE. Functionally however, the criteria laid down by the Supreme Court of Japan would be useful for search engines while they decide whether to delist certain search results, and enforce the concept of the right to erasure. The case clarifies that RTE is not developing merely as a facet of data protection law, but also as a separate right under the broader umbrella of the right to privacy jurisprudence.

c. South Korea

The primary data protection law in South Korea is the Personal Information Protection Act ("PIPA"), 2011 which was further amended in 2021 and 2023. Article 36 of the PIPA allows a request for the erasure of personal data.[49] South Korea was one of the first

[49] Personal Information Protection Act 2011, article 36 (Rectification or Erasure of Personal Information)
(1) A data subject who has accessed his or her personal information pursuant to Article 35 may request a correction or erasure of such personal information from the relevant personal information controller: *Provided*, That the erasure is not permitted where the said personal information shall be collected by other statutes.
(2) Upon receipt of a request by a data subject pursuant to paragraph (1), the personal information controller shall investigate the personal information in question without delay; shall take necessary

jurisdictions to begin extensive debates around RTE after the *Google Spain* ruling, and the Korea Communications Commission, a government agency, formulated the country's guidelines for delisting.[50] The "Guidelines on the Right to Request Access Restrictions on Personal Internet Postings", were released in 2016, and they allowed individuals to contact search engines to delist or delete data about themselves which they are unable to access.[51]

The Personal Information Protection Commission ("PIPC") of Korea launched a service called 'Eraser' which enforces RTE for minors by deleting or delisting posts which contain their personal data.[52] The service can be used by people under 24 years of age to delete or delist personal information which they had posted about themselves, which they cannot access.

measures to correct or erase as requested by the data subject unless otherwise specifically provided by other statutes in relation to correction or erasure; and shall notify such data subject of the result.

(3) The personal information controller shall take measures not to recover or revive the personal information in case of erasure pursuant to paragraph (2).

(4) Where the request of a data subject falls under the proviso to paragraph (1), a personal information controller shall notify the data subject of the details thereof without delay.

(5) While investigating the personal information in question pursuant to paragraph (2), the personal information controller may, if necessary, request from the relevant data subject the evidence necessary to confirm a correction or erasure of the personal information.

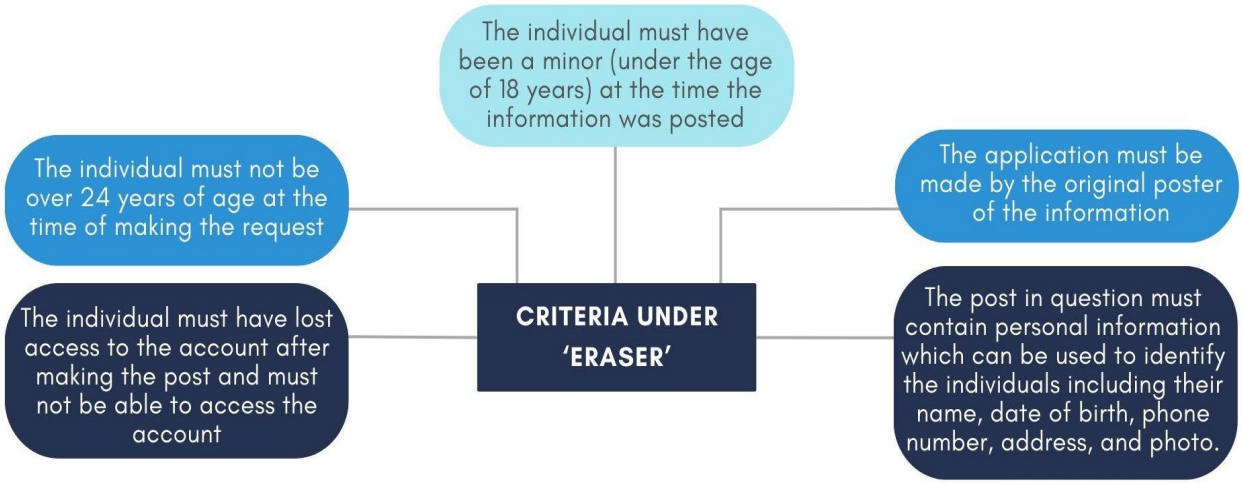
(6) Necessary matters in relation to the request of correction and erasure, notification method and procedure, etc. pursuant to paragraphs (1), (2) and (4) shall be prescribed by Presidential Decree.

[50] Kwon Ji-youn, 'KCC to protect Internet users' 'right to be forgotten'' (*The Korea Times*, 21 February 2016) <https://www.koreatimes.co.kr/www/news/nation/2016/02/113_198532.html> accessed 21 November 2024.

[51] Colleen Theresa Brown, Tasha D. Manoranjan and Samuel Yim, 'South Korea Releases Guidance on Right to Be Forgotten' (*Lexology*, 9 May 2016) <https://www.lexology.com/library/detail.aspx?g=21be3837-0c43-4047-b8b5-9e863960b0b9> accessed 21 November 2024.

[52] Moon Hee-Chul and Cho Jung-Woo, 'Younger Koreans now have the right to be forgotten' (*Korea Joong-Ang Daily*, 24 April 2023) <https://koreajoongangdaily.joins.com/2023/04/24/national/socialAffairs/korea-right-to-be-forgotten-personal-information-protection-commission/20230424160959715.html> accessed 21 November 2024.

In order to avail this service, the following criteria must be met:[53]



The PIPC has further clarified that it would not be possible to remove posts if "there is an obligation to preserve the requested post pursuant to other laws or orders delegated by statute or court orders" or "if the applied post is judged to be related to public interest".

While the current iteration of the project is only applicable to posts made by the individual themselves, the PIPC has announced plans of launching a pilot project in 2024 which would allow individuals to request removal of content posted about them by families and friends while they were minors.[54] This project aims to protect minors who are growing up in the tech age and mitigate the risks of sharing personal information online, including tackling "sharenting", which refers to parents who publicise sensitive content about their children online.

4. GLOBAL TRENDS FOR THE RIGHT TO ERASURE

The implementation of RTE may differ across jurisdictions, however most judicial pronouncements on the issue consider similar tensions in the law. In this section we will

[53] System Guide, 'What is Eraser Service' (*Personal Information Protection*) <https://www.privacy.go.kr/front/contents/cntntsView.do?contsNo=260> accessed 21 November 2024.
[54] Park Boram, 'Government to push for minors' right to be forgotten', (*Yonhap News Agency*, 11 July 2022) <https://en.yna.co.kr/view/AEN20220711007400315> accessed 21 November 2024.

look at some of the most common trends and conflicts between RTE and other rights which must be considered for the holistic enforcement of the right.

4.1. Balancing Right to Erasure and Freedom of Speech

Permanent erasure of data or limiting access to information through delisting has been criticised to pose a threat to the right to information and free speech.[55] Search engines and platforms hosting the given links often argue for freedom of speech in hosting the information.[56] RTE also impacts free press and journalism.

EU's Guidelines for delisting therefore considers, among other things, the relevance of the data, the impact of the data on the privacy of the individual and if the data pertains to a journalistic purpose. Similarly, courts in India carry out a balancing exercise between the right to privacy of the individual concerned, public interest in the information, and freedom of speech of the party against whom RTE is claimed.[57]

Such determination is inherently subjective, requiring not only a case-by-case analysis but also dependent on the standards of protection of privacy and other rights and freedoms in different jurisdictions. Generally, in cases where continued disclosure of information regarding an individual leads to certain harm such as loss of employment or risk of stigmatisation, RTE is likely to be upheld by a court of law.[58] However, there have been some cases, such as the one in Japan referred to above, where factors such as public interest trump considerations of the right to privacy and reputation of an individual. Consequently, it is important for courts to give due consideration to the factors of each

---

[55] Anna Bunn, 'The Curious Case of the Right to Be Forgotten' (2015) 31 Computer Law & Security Review 336; Carla Nunziato, 'The Fourth Year of Forgetting: The Troubling Expansion of the Right to Be Forgotten' 39 University of Pennsylvania Journal of International Law 1011.

[56] Padmakshi Sharma, '"Right To Be Forgotten" Has Various Shapes & Shades, Blanket Orders Cannot Be Passed: Google Argues In Delhi High Court' (*LiveLaw*, 21 July 2022) <https://www.livelaw.in/news-updates/delhi-high-court-right-to-be-forgotten-privacy-google-204440> accessed 21 November 2024.

[57] *Anchit Chawla v Google India and Ors*. 2018 SCC OnLine Del 13516; *SJ v Union of India* W.P.(C) 5608/2023 (Delhi High Court); *Jorawer Singh Mundy v Union of India* 2021 SCC OnLine Del 2306; *Karthick Theodre v Registrar General*, Madras HC (2021) 5 CTC 668; *Vysakh KG v Union of India* 2022 SCC OnLine Ker 7337.

[58] This entails a case-by-case assessment. One of the foremost considerations for balancing free speech and privacy is public interest in the information. In certain cases, such as those pertaining to sexual abuse or involving minors, the courts are likely to privilege privacy and anonymity of the individual over other freedoms.

case, and ensure that RTE is not being used by people in dominant positions to remove victim's accounts or whistleblower testimony. Additionally, since the internet enables individual expression, any exercise of right to erasure should not lead to a chilling effect for speech and expression. For instance, accounts of alleged crimes committed by public personalities should be removed for harm to reputation only after due consideration to the weight and context of such accounts as being a crucial form of expression enabled by the internet - in some instances, as an integral means for victims to voice themselves.

4.2. Right to Erasure of Public Figures

There lies a significant conflict between the right to know and free speech and the right to privacy, including image, name and reputation in the case of public figures or public officials. [59]

In the United States, there is an emphasis on personal liberty and freedom of speech as opposed to a right to privacy for public figures.[60] This has implications for how the courts adjudicate claims on the basis of the right to privacy for public figures.[61] In the United States, 'newsworthiness' of information may be a key consideration for the court in deciding a RTE claim.[62]

On the other hand, the EU follows a personal dignity approach to privacy, which emphasises a right to one's image, name, and reputation and a right to control one's public image and shield against unwanted public exposure. Unlike the US, which has derived individual privacy from various constitutional rights,[63] the EU recognises privacy as an independent fundamental right.[64] This also extends to the manner in which the EU

[59] Shlomit Yanisky-Ravid and Ben Zion Lahav, 'Public Interest vs. Private Lives — Affording Public Figures Privacy in the Digital Era: The Three Principle Filtering Model' (2017) 19(4) Journal of Constitutional Law 975.
[60] *New York Times Co. v. Sullivan* 376 U.S. 254 (1964); *Associated Press v. Walker* 389 U.S. 28 (1967)
[61] Amy Gajda, 'Privacy, Press, and the Right to Be Forgotten in the United States' (2018) 93(1) Washington Law Review 201.
[62] *Id.*
[63] Nehmat Kaur, 'Right to Privacy in the United States of America', (*The Leaflet*, 28 May 2018) <https://theleaflet.in/specialissues/right-to-privacy-in-the-united-states-of-america-by-nehmat-kaur/> accessed 21 November 2024.
[64] EU Charter of Fundamental Rights 2000, article 7, 8

perceives posting information and pictures about public figures. For instance, European courts have imposed liability on internet service providers that housed nude images of celebrities.[65] Unlike the courts in the EU, US courts have shown more restraint in issuing injunctions once images have been irrevocably diffused over the Internet.[66]

In Latin American countries, courts may generally be more careful in granting a RTE. In the case of public figures, courts may be less inclined to order take down of content impacting their reputation in furtherance of the public's right to know and freedom of expression.[67] However, in a case from Brazil,[68] the Superior Court of Justice upheld the right to be forgotten for removal of links in the case of a public prosecutor who was charged with fraud ten years prior. The Court in this case considered that upholding private interest over the access to information so as to allow an individual to follow their life with "reasonable anonymity".

[65] James Q. Whitman, 'The Two Western Cultures of Privacy: Dignity Versus Liberty' (2003) 113 The Yale Law Journal 1151.
[66] Id.
[67] Eduardo Bertoni, 'Right to Be … Forgotten? Trends in Latin America after the Belé n Rodriguez Case and the Impact of the New European Rules', *Oxford Handbook of Online Intermediary Liability* (Oxford University Press) <https://doi.org/10.1093/oxfordhb/9780198837138.001.0001>. 'Denegri v. Google Inc (Appellate Court)' (*Global Freedom of Expression*) <https://globalfreedomofexpression.columbia.edu/cases/denegri-v-google-inc/> accessed 21 November 2024. (In this case, a public figure, embarrassed by an old footage of her from a talk show, petitioned the court to have the links with the footage deindexed. The court refused to grant her relief. the Argentinian Supreme Court gave precedence to the ability of people to search information on the internet.); 'Maureira Álvarez v. Google' (Global Freedom of Expression) <https://globalfreedomofexpression.columbia.edu/cases/maureira-alvarez-v-google/> accessed 21 November 2024.(The Chilean Supreme Court considered the de-indexation of news articles concerning a criminal matter against a former Regional Minister of Education for misappropriation of public funds in which he was subsequently acquitted.)
[68] 'DPN v. Google Brasil Internet Ltda' (*Global Freedom of Expression*) <https://globalfreedomofexpression.columbia.edu/cases/dpn-vs-google-brasil-internet-ltda/> accessed 21 November 2024..

Based on a review of cases and existing literature from different jurisdictions, we can classify the broad observations from our analysis below,

	US	EU	Brazil
Approach	Emphasis on personal liberty and freedom of speech as opposed to a right to privacy for public figures.	Follows a personal dignity approach to privacy	Courts may generally be more careful in granting a RTE and, in the case of public figures
Aspects / Factors Considered	Newsworthiness	Right to one's image, name, and reputation and a right to control one's public image and shield against unwanted public exposure	Balance between reputation and the right to privacy against the public's right to know and freedom of expression
Illustration	In order to sue for libel and recover damages, the Court held that public figures must prove 'highly unreasonable conduct' that departed from normal standards.	Court imposed liability on internet service providers that housed nude images of celebrities	Court allowed the right to be forgotten for removal of links in the case of a public prosecutor who was charged with fraud ten years prior to enable him to lead life with anonymity.

Courts in India have been relatively flexible in granting RTE. In one case,[69] the Delhi High Court allowed the plaintiff, a well-known personality in the media industry, to seek delisting or removal of publications or re-publications containing allegations of sexual harassment against him in the wake of the #MeToo movement. The plaintiff argued loss of reputation and personal grief due to the "one-sided accounts." The court took into account the fact that the original publications had already been taken down from the platform and observed that the #MeToo campaign should not transform into a sullying campaign. The court considered that continued republication would jeopardise the rights of the plaintiff and allowed the plaintiff to use its order to prevent any further republications of the original articles.

While the global trends on the balance between the right to reputation and the freedom of information vary depending on the jurisdiction, it can be seen that public figures

[69] *Zulfiqar Ahman Khan v Quintillion* (2019) SCC OnLine Del 8494

generally do have a lower expectation of privacy online. The internet can serve as an important forum where people can gather to discuss affairs of public importance and exercise their democratic rights such as the right to freedom of speech and association. Many times these rights are exercised through criticism or increased scrutiny of public officials or public personalities in online spaces. In these cases, courts could uphold legitimate criticism of public figures as critical and not take down information which furthers debates on matters of public importance.

4.3. Public Interest and the Right to be Informed vs. the Right to Privacy

Public interest considerations are of particular concern in petitions seeking removal of information regarding past criminal records or other court matters. In such cases, courts weigh the right to information and the public interest in continued disclosure against one's right to privacy.[70]

Passage of time may impact the extent of public interest held in the information, as was also held by the court in the *Google Spain* case. For instance, in *Don Alfonso vs. Google Spain*,[71] the Supreme Court of Spain upheld the right to be forgotten for an individual who prayed for removal of information regarding a crime for which he was pardoned back in 1981.

Public interest considerations may however be impacted by the facts of the case, such as the status of the individuals concerned. In *M.L. and W.W. vs. Germany*,[72] the European Court of Human Rights rejected an application for delisting of links containing information regarding the unsuccessful reopening of the case of murder of a German

[70] 'Don Dionisio v. Google' (Global Freedom of Expression) <https://globalfreedomofexpression.columbia.edu/cases/don-dionisio-v-google/> accessed 21 November 2024. (The Supreme Court of Spain refused de-indexation of links for a criminal investigation against the director of a high value enterprise. The court noted that there was a public interest in the information regarding an individual of his status and therefore right to information prevailed.).

[71] 'Don Alfonso v. Google Spain' (*Global Freedom of Expression*) <https://globalfreedomofexpression.columbia.edu/cases/don-alfonso-v-google-spain/> accessed 21 November 2024.

[72] CCG-NLUD, 'M.L. and W.W. vs. Germany' (*Privacy Law Library CCG-NLUD*) <https://privacylibrary.ccgnlud.org/case/ml-and-ww-vs-germany> accessed 21 November 2024.

actor, in which the accused was convicted. Despite the passage of time, the court found that there was ongoing public interest in the events.

Determination of public interest may further depend on the type of information sought to be removed. For instance, while acknowledging the individual can seek delisting, the Supreme Court of Japan refused to allow delisting of links containing information on a man who was fined for paying for child prostitution in 2011.[73] The court reasoned that "child prostitution was strongly condemned by the society and prohibited by law", making it a matter of public interest.

In India, removal of links containing past actions against individuals are determined on similar considerations such as, the passage of time, nature of the information sought to be removed, impact on other rights and freedoms such as dignity, privacy or access to information. In sensitive matters such as those of rape and sexual assault, the details of the victim are redacted from the court records. Courts have also allowed non-disclosure of personal details or delisting in matrimonial matters where the courts privilege the privacy of the concerned individuals.[74] In other cases, where the individual had been acquitted and availability of information online is harming their reputation or causing economic despair, courts have been inclined to allow delisting.[75]

Consequently, there may be cases in which courts may deny an erasure or a delisting request, even if it causes reputational harm to an individual, if it is a matter of public concern. While the information of victims may often be removed or redacted to protect their privacy, the courts must balance the RTE of the perpetrator with the public's broader right to be informed.

---

[73] CCG-NLUD, 'Case of a Permitted Appeal of the Decision to Rescind the Decision of the Second Instance Concerning the Approval and Decision on a Provisional Disposition to Delete Posted Articles' (*Privacy Law Library CCG-NLUD*) <https://privacylibrary.ccgnlud.org/case/case-of-a-permitted-appeal-of-the-decision-to-rescind-the-decision-of-the-second-instance-concerning-the-approval-and-decision-on-a-provisional-disposition-to-delete-posted-articles?searchuniqueid=252352> accessed 21 November 2024.

[74] 2022 SCC OnLine Ker 7337; X v Registrar General, Karnataka High Court and Ors. WP 22994 of 2021 (Karnataka High Court); XX vs. YY 2023 SCC OnLine Raj 4173.

[75] *XXX v Union of India* WP(CRL.) No. 318 of 2022 (Kerala High Court); *Naresh Kumar v The Wire* CS(OS) 749/2023 (Delhi High Court); *SJ v Union of India* W.P.(C) 5608/2023 (Delhi High Court).

4.4. Privacy Rights of Children

Data protection regimes often contain special provisions to safeguard children's privacy. For instance, the European criteria for delisting[76] requires the data controllers to consider whether the data subject in question is a child. In India, the Protection of Children from Sexual Offences Act, 2012[77] and the Juvenile Justice (Care and Protection of Children) Act, 2015[78] forbids disclosure of children's details by the media.[79] Courts therefore mask the personal details of the child in its records. A similar policy is also followed in the Philippines for victims of child sexual abuse.[80] However, so far, there is no guidance under the DPDP Act on the exercise of the right to erasure by children for their personal data.

Project Eraser of the South Korean PIPC,[81] as discussed above, is a useful precedent for the exercise of the right to erasure by children. It offers more control to children over their personal information and is a useful way to empower children with more decisional autonomy as a data subject. This project is however applicable only for content posted by the individual themselves. A similar right is considered applicable for children under the UK GDPR.[82] It further provides that in a case where a parent requests erasure of the child's personal data, the child's wishes should still be taken into account. However, where

---

[76] European Data Protection Board, 'Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (Part 1) Version 2.0' (2020)
(1) When the personal data is no longer necessary in relation to the search engine provider's processing;
(2) When the data subject withdraws consent for processing;
(3) When the data subject has exercised his or her right to object to the processing of his or her data;
(4) When the personal data has to be erased for compliance with a legal obligation;
(5) When the personal data has been collected in relation to the offer of information society services to a child.

[77] Protection of Children from Sexual Offences Act 2012, s. 23

[78] Juvenile Justice (Care and Protection of Children) Act 2015, s. 24

[79] *Eric Ranee & 2 Ors. v State of Meghalaya & Anr.* Crl. Petn. No. 79 of 2023 (Meghalaya High Court)

[80] *People v. Cabalquinto* G.R. No. 167693 of 2006 (Supreme Court of the Philippines)

[81] Personal Information Protection Commission, 'New Service Empowers Children and Adolescents to Control Their Online Personal Information' (PIPC, 26 April 2023) <https://www.pipc.go.kr/eng/user/ltn/new/noticeDetail.do?bbsId=BBSMSTR_000000000001&nttId=2151> accessed 21 November 2024.

[82] Information Commissioner's Office, 'How Does the Right to Erasure Apply to Children?' (*ICO*, 19 May 2023) <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/children-and-the-uk-gdpr/how-does-the-right-to-erasure-apply-to-children/> accessed 21 November 2024.

the child wishes for their data to be erased without the parent's knowledge or where there is a dispute between the parent and the child regarding the erasure, the ICO Guidance suggests that the best interest and the level of understanding of the child should be considered.

Consequently, informational privacy of children in the digital age should provide greater autonomy to children over their data. Data protection regimes must allow for mechanisms to allow the erasure or delisting of content of children, either by their guardians, or by the children themselves. Decisions made about children's data should also build in safeguards to consider the best interest of the child.

5. RECOMMENDATIONS FOR INDIAN RULES

The DPDP Act has made a positive contribution towards enhancing the rights of data principals in India. The data protection law in India was passed following long periods of discussion over several iterations of the law and provides a good basis for the protection of rights such as the right to erasure. These laws will have to be further supported by implementing rules which will clarify the scope and the ambit of these laws. These recommendations are based upon an assessment of the emerging trends in RTE in Asia and the EU, which are applicable to the Indian legal context. These recommendations broadly cover important factors to be considered while framing Rules for the implementation of RTE under Section 12 of the DPDP Act.

a. Constitutional Protections

From the previous section we can see that many jurisdictions including the EU and jurisdictions in Asia are grappling with the effects of RTE on other constitutional rights including the right to access information and the right to freedom of speech and expression. The Rules for DPDP Act must clearly lay down the criteria which must be kept in mind while deciding whether to retain, delist or erase content. Specifically, the Rules must lay down special provisions to protect fundamental rights such as the right to freedom of speech and expression, and the journalistic rights. They should lay down the

kinds of personal information which further public interest and cannot be taken down under an application of Section 12 of the DPDP Act.

This would involve a case-by-case analysis of the facts to implement the balancing test between various fundamental rights, which may require judicial expertise.

b. Exemptions for public figures

The Rules may also lay down certain kinds of data which may not be erased in public interest. This could include certain types of information about public figures or government officials and the work done by them in furtherance of their duties. Individuals holding public office or doing work in the public sector may be considered to have a diminished right to privacy.[83]

c. De-indexing

Courts in India have enforced RTE based on the right to privacy and the right to reputation. Consequently, they have passed orders directing platforms to ensure the erasure of data or search engines to delist the impugned information.

Delisting is an aspect of RTE where the data would still remain on the internet, however the users could access the same by conducting searches using terms other than the name of the individual making the delisting request. In other words, such requests do not result in a complete erasure of information.

Therefore, the Rules must establish guidelines which should solely focus on the processing of data by search engine providers and delisting requests submitted by data subjects. The Rules should establish three primary points 1) the grounds under which a data subject could request delisting; 2) exceptions to the right to delisting; and 3) metrics on which the delisting request should be processed. These grounds/metrics could be based on the five point balancing test laid down by the Srikrishna Committee report and the EU guidelines on evaluating delisting requests.

[83] *R Rajagopal v State of Tamil Nadu* (1994) 6 SCC 632, ¶26

The balancing test laid down by the Srikrishna Committee included the nature of the personal data sought to be removed and its relevance for public interest, scale and accessibility of its disclosure and the status of the data principal in having a public presence or holding a public office.[84] The EU guidelines, on the other hand, primarily relied on withdrawal of consent to remove personal data. It also highlighted certain exceptions to the right to request delisting under the GDPR which included complying with a legal obligation, exercising the right to freedom of expression and information and for reasons of public interest.[85]

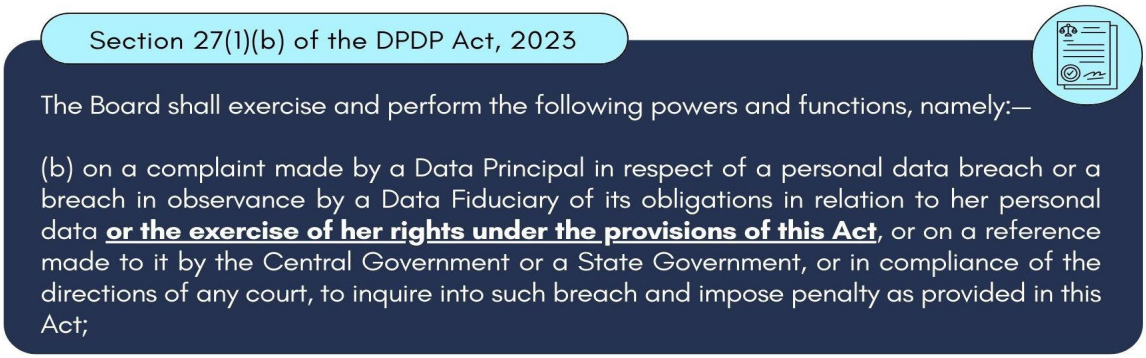
d. Procedural Safeguards

The implementing rules should prescribe procedural requirements and safeguards for the implementation of RTE by the data fiduciaries, such that a data principal can exercise this right effectively. Such measures should include:

- Notice requirement - While disposing a request for erasure, the data fiduciary should disclose to the data principal all the personal data in its possession, including information on any third parties that may be in possession of the data. It should further include the status of all personal data collected by the fiduciary. This would allow the data principal to understand where their data is being processed and stored, and to meaningfully exercise their RTE.
- Reasons for rejection of request of erasure - A data fiduciary may refuse a request of erasure if it does not meet the requirements for erasure or delisting prescribed in the law. A data fiduciary should be required by the implementing rules to provide reasons in writing for refusing a request of erasure or delisting. Reasons should indicate the grounds for refusal of the request and provide the mechanism by which they may appeal to the DPB.

[84] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (2018)
[85] European Data Protection Board, 'Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (Part 1) Version 2.0' (2020) <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201905_rtbfsearchengines_afterpublicconsultation_en.pdf> accessed 21 November 2024.

- Notification to third parties - The data fiduciary should notify of the erasure to any third party in possession of the personal data. Such notification should contain the description of the request made and the grounds of erasure. This can reduce the burden on the data principal to approach multiple fiduciaries.
- Appeals process - The Rules should provide for appeal against refusal of request of erasure or delisting by the data fiduciary. Under Section 27(1)(b) of the DPDP Act, the DPB would be the appropriate forum for appeal. The Rules can further lay down the procedure for a second appeal to the Appellate Tribunal.



- Time period for disposal of request of erasure/delisting - The Rules should prescribe a time period of 30 days within which the data fiduciary should dispose of a request of erasure or delisting. The said time period allows adequate time to the data fiduciary to comply while ensuring a speedy disposal of request of the data principal.
- Streamlined procedure for making requests - The data fiduciaries should be required to have an accessible and well-publicised means of making an application for erasure of data by the data principal. The application page should explain the grounds for exercise of the right to erasure in a simple and accessible manner. Data fiduciaries should be required to provide for alternative mechanisms of application processes to accommodate for various forms of disabilities, multiple languages, and differing levels of education and access to technology.

e. Specialised provisions for children

The Rules must have specialised provisions for children. This would include specialised provisions for information uploaded about children, as well as information uploaded by children. There is a growing recognition of increased danger to children due to the increasing influence of the internet in their formative years.[86] More children are now online on social media platforms like Instagram, TikTok or X, posting images and personal information about themselves. Children may share information about themselves online without fully understanding the implications of the same. Additionally, there is also a growing trend of 'family influencers' on social media channels, where parents post images and information about their children online, often without their consent.[87] Therefore, the Rules must have special provisions for the erasure of personal data of children, as well as the deletion of personal data uploaded by children if they or their legal guardians request it. Additionally, there can also be rules which allow individuals to erase personal data they uploaded about themselves while they were minors, after they attain the age of majority. The South Korean example of 'Eraser' is one of the models which could be implemented, allowing children the ability to remove information about themselves off the internet.

f. Transparency reporting of platforms

Data fiduciaries implementing erasure requests must be transparent about their internal compliance process. As a part of transparent reporting, the data fiduciaries should be required by the Rules to publish transparency reports regularly, providing a comprehensive analysis of the ways in which they assess such requests in relation to erasure/delisting.

---

[86] UK House of Commons Committee Report, 'Screen time: impacts on education and wellbeing', <https://publications.parliament.uk/pa/cm5804/cmselect/cmeduc/118/summary.html> accessed 21 November 2024.

[87] Irena Zervas, 'Profit without Privacy: Family Content Creators and Child Influencers' (Northeastern University Political Review) <https://nupoliticalreview.org/2024/03/19/profit-without-privacy-family-content-creators-and-child-influencers/> accessed 21 November 2024

Among other data, the transparency reports must provide the aggregate statistics on the number of erasure/delisting requests received by them and how often they are rejected. It must show the rate at which the data fiduciaries erase/delist content by category on a quarterly basis. The Rules must also require such reports to provide for an analysis of the evaluation mechanism. In other words, the data fiduciaries should show a breakdown of all the grounds basis which they process such requests. Additionally, data fiduciaries should provide a detailed set of safeguards that are in place to ensure that individuals' rights to privacy and other fundamental rights like free expression are respected.

The right to erasure or the right to be forgotten has existed in India prior to the enactment of the DPDP Act and has been enforced by courts, such as through the right to privacy. It also has a history of legislative deliberation up until the enactment of the new DPDP Act. This jurisprudence provides useful insights for the implementation of RTE. The Rules should further be in consonance with existing laws and judicial pronouncements.

Centre for Communication Governance

National Law University Delhi

Sector 14, Dwarka

New Delhi – 110078

011- 28031265

ccgdelhi.org

privacylibrary.ccgnlud.org

twitter.com/CCGNLUD

ccg@nludelhi.ac.in