

ISSN: 2583-8725

Lex Scripta Journal

Quarterly Online and Print Edition

Law & Policy

“Join the League of
National & International Scholars”



EDITORIAL TEAM

DR. AJAY BHUPENDRA JAISWAL

Professor & Former Head
Department of Law
V.S.S.D. College, Nawabganj,
(C.S.J.M. University, Kanpur)

DR. MEGHA OJHA

Associate Professor | Legal Consultant
| Author | KLEF College of Law

PROF. DR. DEEVANSHU SHRIVASTAVA

Founding Dean and Professor,
GL Bajaj Institute of Law,
Greater Noida

DR. GAURAV GUPTA

Assistant Professor,
Faculty of Law, Lucknow

MR. TUHIN MUKHARJEE

Leadership Strategist | Business Coach
| Author | Speaker

MR. PRAKARSH PANDEY

Author and
Advocate, Allahabad High Court

MR. AMARESH PATEL

Assistant Professor
at Law School,
Amity University, Patna



**LEX SCRIPTA MAGAZINE OF
LAW AND POLICY (VOL-4, ISSUE-1)**

Copyright © 2025, LexScripta

ISSN-2583-8725

Vol - IV, Issue - I

Published by INTEGRITY EDUCATION INDIA

New Delhi

First Floor, 4598/12-B, 1st Floor,
Padam Chand Marg, Daryaganj,
New Delhi, Delhi 110002

Phone: +91 98 11 66 62 16 (M)

Phone: +91 70 11 60 56 18 (M)

Bengaluru

Jallahalli East

Bengaluru, Karnataka. India.

Phone: +91 98 11 66 62 16 (M)

Email: publisher.integrity@gmail.com

USA

New Jersey

14 Grandview Ave, Upper Saddle River,
NJ-07458, USA

Phone: +14805226504 (M)

London

37 Degree Media

64, Hodder Drive, Perivale, London UB68LL.
United Kingdom.

Phone: +44 7950 78 18 17 (M)

Website: integrityeducation.co.in

© Lex Scripta Magazine Of Law And Policy, 2025

Disclaimer

All Copyrights are reserved with the Authors. But, however, the Authors have granted to the Journal (Lex Scripta Magazine of Law and Policy), an irrevocable, non-exclusive, royalty-free and transferable license to publish, reproduce, store, transmit, display and distribute it in the Journal or books or in any form and all other media, retrieval systems and other formats now or hereafter known. No part of this publication may be reproduced, stored, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other non-commercial uses permitted by copyright law.

The Editorial Team of Lex Scripta Magazine of Law and Policy Issues holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not necessarily reflect the views of the Editorial Team of Lex Scripta Magazine of Law and Policy.

[© Lex Scripta Magazine of Law and Policy. Any unauthorized use, circulation or reproduction shall attract suitable action under application law.]

For any Query / Feedback
Phone: +91 98 11 66 62 16 (Vineet Sharma)

Printed in India @ New Delhi

ISSN: 2583-8725

Lex Scripta Journal

Quarterly Online and Print Edition

Law & Policy

"Join the League of National
and International Scholars"



Lex Scripta Journal

Reclaiming Digital Identity: The Concept and Scope of the Right to Be Forgotten

Author
Shailvi Tripathi



Reclaiming Digital Identity: The Concept and Scope of the Right to Be Forgotten

Shailvi Tripathi

Amity law school 5th year
10 sem student BALLB

Abstract

Individuals rights and identity is a responsibility to be protected by law - "All human beings are born free and equal in dignity and rights". In an overstimulated digital system there is an unimaginable amount of information present today on the internet and sometimes this information can be used to tarnish ones identity and further impact their right to live with dignity disrupt Right to privacy. Right to be forgotten ensures that an historical event should not be revitalised due to the length of time elapsed since its occurrence. Right to be forgotten or right to ensure has become popular due to the advent of technology resulting in availability of private information out there related to any individual. This specific sector of law gives individuals the right to control their data usage, including images, videos, etc.

The Right to be Forgotten enable individuals to request the removal and deletion of personal information that is inaccurate, irrelevant, outdated, unnecessarily excessive content. Right to be forgotten at times be mistakenly assumed similar with right to privacy but they serve a distinctive feature The right to privacy constitutes information that is not known publicly, whereas the right to be forgotten involves revoking of publicly accessible information about any subject to internet. (1)

Background

Right to be forgotten is newly emerging concept, its origins can be traced in EU regulations and in French jurisprudence on the right to be Oblivion or *le droit à l'oubli* (the right to be forgotten) in 2010. (4) This concept gained more recognition during the EU based case Google Spain SL, Google Inc v Agencia Espanola de Proteccion de Costeja Gonzalez in the year 2014. The law under Eu has a limited approach contrary to it the original concept termed as "right to [data] erasure". Right to ensure was more of an addition to the whole case of Google Spain SL, Google Inc v Agencia Espanola de Proteccion de Costeja Gonzalez the main outcome of the case was the codification of General Data Protection Regulations (GDPR). The concepts implements individuals privacy and the desired to be left alone.

Theoretical foundations

1. Philosophical Emergence

While the concept has its recognition through a landmark case its foundation has a more philosophical and ethical legal tradition regarding privacy and its roots. The right to privacy states an right of individual to regulate the collection, use disclosure of his personal information, this can be explained in the form of various activities through its family education, communication clinical and monetary records. This is where right to be left alone comes into picture which is synonym to right to privacy. In the Black law Dictionary "right to be left alone" is the right of a person to be free from unwanted publicity; the right to live without any unwanted interference by the public in matter with which the public is not necessarily concerned. All this defines the right of privacy.

Privacy is recognized as a fundamental human right in several international documents, including:

- Universal Declaration of Human Rights (UDHR): under Article 12 protects the individuals from the arbitrary interference and with their personal lives and personal data.
- International Covenant on Civil and Political Rights (ICCPR): under Article 17 right to protect personal data.
- European Convention on Human Rights (ECHR): under Article 8 states that everyone has the right to respect for their private and family life.

Philosophically, this concept RTBF is linked to the concept of personal autonomy, where individuals should have the ability to manage their digital data and identity most impotently to control their past and what it disseminate.

2. Early Emergence of law in EU

"Right to be Forgotten" was introduced in European law, and gradually moved toward granting individuals control over their data:

- 1981 Convention: The Council of Europe recognised the first legally binding data protection treaty, protecting and guaranteeing individuals right to access stored personal information.
- 1995 Data Protection Directive: This EU directive introduced the concept of data erasure, suggesting that personal information should not be kept if it became unnecessary or doesn't fulfil its purpose and is deemed to become irrelevant. Articles 12 and 14 of this act granted citizens the right to object to data processing (4)(5).

3. Emergence in Europe

Several European nations developed their own versions of this right long before the EU-wide ruling:

- Germany: As early as 1973, the German Federal Constitutional Court ruled in the *Lebach I* case that individuals have a fundamental right to determine how their personal information is used, specifically regarding their reintegration into society after a criminal conviction.
- France: In 1978, France adopted an act allowing individuals to request that data controllers rectify or delete inaccurate or expired personal information. The concept emerged here as the *droit à l'oubli numérique* (right to digital forgetfulness)

4. The Landmark Case: Google Spain v. AEPD (2014)

The specific legal principle of the RTBF was established by the Court of Justice of the European Union (CJEU) following a complaint by a Spanish national, **Mario Costeja González**.

in this landmark case, Mario Costeja González sought removal of search engine results linking his name to an old newspaper notice regarding debt recovery proceedings. The information was legally published but had become outdated and irrelevant over time.

- **The Conflict:** In 2010, Costeja González requested that a newspaper and Google remove links to a 1998 article regarding a debt-related repossession of his home, arguing the matter was fully resolved and the information was now **outdated and irrelevant**.
- **The Ruling:** The CJEU ruled that search engine operators are "**controllers**" of personal data. It held that individuals have the right to request that search engines delist links to information that is "**inadequate, irrelevant or no longer relevant, or excessive,**" even if that information was published lawfully and is factually correct.

5. Codification in the GDPR

Following the *Google Spain* decision, the right was formally codified in the **General Data Protection Regulation (GDPR)**, which took effect in 2018. Under **Article 17**, individuals can request data erasure if:

1. The data is no longer necessary for its original purpose.
2. The individual withdraws their consent.
3. The individual objects to the processing.
4. The data was processed unlawfully.

Weber, Rolf H. (2011). "The right to be forgotten: more than a Pandora's Box?". *Journal of Intellectual Property, Information Technology and E-Commerce Law*. 2: 120–130. Archived from the original

1. *Mayes, Tessa (2014-05-21). "We have no right to be forgotten online". The Guardian. Retrieved 2014-08-09.*
2. Arthur, Charles (14 May 2014). "Explaining the 'right to be forgotten' – the newest cultural shibboleth". *The Guardian*.
3. https://wjarr.com/sites/default/files/fulltext_pdf/WJARR-2022-1079.pdf
4. <://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?article=2256&context=gjicl>

Objective

The **Right to Be Forgotten (RTBF)** serves a multifaceted **objective purpose** aimed at re-establishing individual control in a digital age, while its **philosophical approach** is rooted in fundamental human rights, personal autonomy, and the concept of social redemption.

Objective Purpose Served

The primary objectives of the RTBF, as established in the sources, include:

- **Empowering Digital Autonomy:** The core intent is to grant individuals greater control over their "digital footprint". This allows people to manage how their personal information is collected, stored, and disseminated by organizations and search engines.(1),(2),(3)
- **Reputation Management and Protection from Harm:** RTBF provides a legal mechanism to minimize personal or professional damage caused by information that is "inadequate, irrelevant or no longer relevant, or excessive". It specifically addresses cases where outdated data—such as old home-foreclosure notices or spent criminal convictions—negatively impacts an individual's current life.
- **Restoring Trust in Digital Systems:** By compelling organizations to delete data upon request, the right aims to strengthen the "bonds of trust between humans and AI" and other data-driven systems that otherwise risk permanent surveillance.
- **Facilitating Social Reintegration:** A critical purpose is to prevent individuals from being "permanently defined by their past". This is particularly relevant in legal contexts, such as criminal rehabilitation, where the continued accessibility of digital records can obstruct a person's reintegration into society.

1. Philosophical Approach

The philosophical framework of the RTBF is built on several key traditions:

- **Privacy as a Fundamental Human Right:** The RTBF is philosophically grounded in international human rights documents, such as Article 12 of the **Universal Declaration of Human Rights** and Article 8 of the **European Convention on Human Rights**, which protect individuals from arbitrary interference with their private lives.
- **Personal Autonomy and Self-Determination:** Philosophically, the right is linked to the concept of **personal autonomy**—the idea that individuals should have the power to shape their own digital identity. This is echoed in German legal tradition as the "fundamental right to determine how their personal information is used".
- **The Right to a "Second Chance":** The RTBF embodies the philosophical belief in **redemption and forgiveness**. It suggests that human dignity requires a "sense of closure," allowing individuals to move forward without the perpetual burden of past mistakes.
- **Balancing Individual Rights against Collective Memory:** The sources highlight a philosophical tension between individual erasure and **social memory**. While privacy advocates emphasize individual control, a counter-philosophy suggests that memory processes are inherently social and that the public has a legitimate interest in accessing truthful information for transparency and history.
- **Human Dignity vs. Informational Democracy:** The RTBF attempts to reconcile the "promise of informational democracy" (democratised access to data) with the need to safeguard "human dignity" from the "unexpected social consequences" of permanent digital archives

The legal and regulatory landscape of the **Right to Be Forgotten (RTBF)**, formally known as the **Right to Erasure**, is primarily defined by European data protection standards that have increasingly influenced global privacy frameworks. While it was established through landmark jurisprudence, it is now codified in major regulations and faces ongoing challenges as it adapts to emerging technologies.

I. Foundational Framework and the GDPR

The modern legal basis for the RTBF is **Article 17 of the General Data Protection Regulation (GDPR)**, which took effect in the European Union in 2018. Under this provision, individuals have the right to obtain the erasure of personal data from a "controller" without undue delay.

- **Grounds for Erasure:** Data must be deleted if it is no longer necessary for its original purpose, if the individual withdraws consent, if the data was processed unlawfully, or if the individual objects to the processing.
- **Legal Precedents:** The right has roots in earlier European laws, such as the **1995 Data Protection Directive** (Articles 6, 12, and 14) and the **1981 Convention for the Protection of Individuals**. National traditions also played a role, notably Germany's **1973 Lebach I case** and France's **1978 Act on Information Technology**.

II. Landmark Jurisprudence: Google Spain

The specific principle of digital erasure gained worldwide prominence through the 2014 ruling in **Google Spain v. AEPD**.

- **The Ruling:** The Court of Justice of the European Union (CJEU) determined that search engine operators are "**data controllers**" because they locate, index, and disseminate information.
- **The Responsibility:** The court held that individuals could request search engines to delist links containing personal data that is "**inadequate, irrelevant or no longer relevant, or excessive,**" even if the original publication was lawful and factually correct.
- **Jurisdictional Limits:** A subsequent 2019 case, *Google v. CNIL*, clarified that search engines are **not obligated to apply delisting globally**; they are only required to remove results within EU domains.

III. Global Comparative Landscape

The adoption of RTBF-like regulations varies significantly across jurisdictions, reflecting differing philosophical approaches to privacy and free speech.

- **United States:** The U.S. lacks a federal RTBF law, as the right is seen as conflicting with **First Amendment** protections for free speech and the press. However, state-level laws like the **California Consumer Privacy Act (CCPA)** grant residents limited rights to request the deletion of data held by businesses.
- **Asia and Latin America:** Several countries have incorporated RTBF into their legal systems, including **South Korea** (PIPA), **Japan** (APPI), **Brazil** (LGPD), and **Argentina**.
- **Developing Regions:** Nations such as **Nigeria** (NDPR) and **South Africa** (POPIA) have emerging provisions for data deletion, though they often face challenges regarding regulatory oversight and enforcement.

IV. Legal Balancing and Controversies

The RTBF is not an absolute right and requires a **balancing test** against other fundamental interests.

- **Freedom of Expression:** Regulatory bodies must weigh the individual's privacy against the public's right to access information. Requests are often denied if the data involves **public interest**, historical research, or information regarding public figures.
- **The "Memory Hole" Effect:** Critics argue that enforcing erasure can amount to **online censorship**, potentially creating a revisionist digital archive that undermines historical accuracy and public accountability.

V. The Frontier: AI and Blockchain

The legal landscape is currently expanding to address how erasure applies to decentralized and generative technologies.

- **Large Language Models (LLMs):** LLMs present a challenge because they "memorize" training data. Legal experts are debating whether "Machine Unlearning"—technical methods to make AI models "forget"—can satisfy Article 17 requirements.
- **Blockchain:** The **immutability** of blockchain directly contradicts the requirement for data to be editable or deletable. Proposed solutions include **off-chain storage** or technical "mutability" workarounds to allow for regulatory compliance.

- **Sparse Models:** Researchers have proposed "**un-pruning**" algorithms to eliminate the influence of deleted data on a model's pruned topology, ensuring users can withdraw their data's influence from the pruning process

Google Spain v. AEPD (2014)

The landmark case of **Google Spain v. AEPD (2014)** established the legal foundation for what is now known as the **Right to Be Forgotten (RTBF)** or the **Right to Erasure**.

1. Origins of the Conflict

The case began in March 2010 when **Mario Costeja González**, a Spanish lawyer, filed a complaint with the Spanish Data Protection Agency (AEPD). His grievance concerned a 1998 announcement in the newspaper *La Vanguardia* regarding a real estate auction for the recovery of social security debts.

Costeja González argued that the proceedings had been fully resolved for years and the debt had been paid in full. He contended that the continued appearance of this information in Google search results was **outdated, irrelevant, and defamatory**.

He requested that:

- The newspaper remove or alter the pages.
- Google Spain or Google Inc. remove his personal data so it would no longer appear in search results.

2. Legal Journey

The AEPD dismissed the complaint against the newspaper, ruling that the original publication was **legally justified** as it was done pursuant to a government order. However, the Agency **upheld the complaint against Google**, asserting that search engines are subject to data protection laws and have an independent duty to protect personal information. Google appealed this decision to the Spanish National High Court, which referred several questions regarding the interpretation of EU data protection law to the **Court of Justice of the European Union (CJEU)**.

3. The CJEU Ruling (May 13, 2014)

The CJEU reached several historic conclusions that redefined the responsibilities of internet intermediaries:

- **Search Engines as "Data Controllers":** The court ruled that search engine operators are "controllers" of personal data because they locate, index, store, and disseminate information.
- **Processing of Data:** The act of indexing and displaying third-party content constitutes the "processing" of personal data.
- **Right to Delink:** Individuals have the right to request that search engines remove links to information that is "**inadequate, irrelevant or no longer relevant, or excessive**" in relation to the purposes for which it was processed.
- **Accuracy vs. Relevance:** Crucially, the court held that this right applies even if the information has been published **lawfully** and is **factually correct**.

4. The Balancing Test

The court emphasized that the RTBF is **not an absolute right**. It must be balanced against:

- The **public's interest** in accessing the information.
- The **freedom of expression** of the original publishers.

- The **nature of the individual's role** in public life (e.g., public figures have a lower expectation of privacy regarding relevant information).

5. Legacy and Modern Influence

The *Google Spain* decision was the direct precursor to **Article 17 of the General Data Protection Regulation (GDPR)**, which formally codified the Right to Erasure across the European Union in 2018. Since the ruling, Google has processed millions of requests—over **3.2 million** between 2014 and 2019 alone—with a removal rate of approximately **43%**.

Criticism

The **Right to Be Forgotten (RTBF)** has faced significant criticism from legal scholars, business executives, and technical experts, primarily revolving around its impact on free speech, the integrity of public records, and the practical challenges of implementation in a digital environment.

1. Conflict with Freedom of Expression and Press

The most prominent criticism is that the RTBF directly constrains the **freedom of expression** and the public's right to access information.

- **Online Censorship:** Critics argue the right represents a form of **online censorship** and is viewed by some as the single biggest threat to free speech in the digital age.
- **Journalistic Integrity:** A significant portion of delisting requests involves journalistic material, which is usually produced in the public interest. Forcing the de-indexing of news items can rattle the capacity of a story to tell a **complete picture** and undermines the role of the press as a public watchdog.
- **The "Memory Hole" Effect:** Opponents fear that the RTBF allows for the suppression of legitimate public records, creating a "memory hole" that results in **historical revisionism** and harms the transparency of digital archives.

2. Operational and Procedural Problems

The practical mechanisms for enforcing erasure have been widely questioned for creating perverse incentives and bypassing due process.

- **Burden on Intermediaries:** Search engines are forced to act as "judges" in assessing removal requests, a process that is highly resource-intensive and subjective. This creates an incentive for search engines to **"over-remove"** content to avoid potential legal liability, rather than defending the public's right to access it.
- **Lack of Due Process:** In many jurisdictions, de-indexing procedures occur without involving the **original publishers** of the information, depriving them of the right to be heard and defend their content.
- **Jurisdictional Overreach:** Critics highlight the issue of **extraterritoriality**, noting that a universal order to delist content globally could reduce global freedom of expression standards to the "lower common denominator" of the most restrictive domestic laws.

3. Technical Feasibility and "Machine Memory"

As the RTBF moves beyond search engines into AI and decentralized systems, critics point to fundamental technical contradictions.

- **Blockchain Immutability:** The core value of **blockchain** is its immutability; the requirement to edit or delete data for RTBF compliance strikes at the heart of the technology's security and is often deemed impracticable.
- **AI and Large Language Models (LLMs):** It is technically difficult to make a machine learning model "forget" specific training data without frequent and costly retraining. Furthermore, the "undue delay" requirement of one month in the GDPR is often **impossible to achieve** for LLMs that take several months to train.
- **Catastrophic Unlearning:** Technical methods to force a model to unlearn data (Machine Unlearning) can lead to a sudden and exponential degradation of the model's overall performance, a phenomenon known as "**catastrophic unlearning**".

4. Unintended Consequences (The Streisand Effect)

Attempts to exercise the RTBF can ironically lead to a loss of privacy through the **Streisand effect**.

- **Increased Publicity:** Attempting to censor or hide a piece of information often has the unintended consequence of publicizing it more widely. Data-driven studies have shown that for some requesters, the republication of delisted links by media outlets (as a form of transparency protest) actually **increased their visibility** on social media and search trends.
- **Susceptibility to Attacks:** Transparency activists can use inference attacks to rediscover delisted URLs and requester names, potentially exposing the very information the individual wanted hidden and putting the **efficacy of the law** in question.

References

1. Weber, Rolf H. (2011). "The right to be forgotten: more than a Pandora's Box?". *Journal of Intellectual Property, Information Technology and E-Commerce Law*. 2: 120–130. Archived from the original
2. https://wjarr.com/sites/default/files/fulltext_pdf/WJARR-2022-1079.pdf
3. <://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?article=2256&context=gjicl>
4. Weber, Rolf H. (2011). "The right to be forgotten: more than a Pandora's Box?". *Journal of Intellectual Property, Information Technology and E-Commerce Law*. 2: 120–130. Archived from the original
5. https://wjarr.com/sites/default/files/fulltext_pdf/WJARR-2022-1079.pdf
6. Arthur, Charles (14 May 2014). "Explaining the 'right to be forgotten' – the newest cultural shibboleth". *The Guardian*.
7. Arthur, Charles (14 May 2014). "Explaining the 'right to be forgotten' – the newest cultural shibboleth". *The Guardian*.
8. Mayes, Tessa (2014-05-21). "We have no right to be forgotten online". *The Guardian*. Retrieved 2014-08-09.
9. Mayes, Tessa (2014-05-21). "We have no right to be forgotten online". *The Guardian*. Retrieved 2014-08-09.

EDITORIAL TEAM

PROF. (DR.) BANSHI DHAR SINGH

Professor,
Ex. Dean & Head,
Faculty of Law,
University of Lucknow

DR. KALPESHKUMAR L GUPTA

Founder ProBono India, Legal Start-ups,
Law Teachers India

DR. SUDHANSHU CHANDRA

Assistant Professor, Manuu Law
School, Maulana Azad National Urdu
University (Central University),
Hyderabad

PROF. (DR.) SANJAY SINGH

Director
of IIMT College of Law

INTERNATIONAL EDITORIAL TEAM

PROF. DR. MARC OLIVER OPRESNIK

President and CEO
Opresnik Management Consulting
and Opresnik Business School

*PROF. DR . COMRADE AMB.
CHUKWUNONSO C
HARLES OFODUM ESQ*

Chancellor, ALSA University.
Legal Director for Nigeria, World
Association for Humanitarian Doctors

ABOUT LEX SCRIPTA JOURNAL

Lex Scripta Magazine is a premier peer-reviewed online and print journal dedicated to advancing scholarly research in law, policy, and social sciences. With the vision of promoting academic excellence and fostering a culture of intellectual exchange, the magazine provides a distinguished platform for academicians, researchers, legal professionals, and students to publish their original work and contribute to contemporary legal discourse.

Each submission undergoes a rigorous double-blind review process conducted by a panel of eminent national and international professors, ensuring the highest standards of quality and academic integrity. Lex Scripta not only encourages original and innovative research but also strives to bridge the gap between theoretical insights and real-world applications in the legal domain.

Contributors and editorial members receive global recognition through certificates and publication opportunities, while readers gain access to insightful, authoritative, and thought-provoking content across diverse areas of law and policy.

Now managed by Integrity Education India, Lex Scripta Magazine is committed to expanding its academic footprint through enhanced digital presence, global collaborations, and university partnerships. Upholding its ISSN identity, Lex Scripta continues to evolve as one of India's most trusted and respected journals in the field of legal research and education.

KEY FEATURES

- | **Scholarly Insights** – Access in-depth, peer-reviewed research articles written by distinguished academicians and legal experts.
- | **Global Perspectives** – Explore diverse viewpoints on law, policy, and governance from national and international scholars.
- | **Authentic Content** – Read verified and academically sound articles that uphold the highest standards of research quality.
- | **Knowledge Enhancement** – Stay updated with emerging trends, case studies, and policy developments across multiple legal domains.
- | **Easy Accessibility** – Enjoy seamless access to online editions and exclusive hardcover issues for academic and professional use.



CONNECT WITH US **9811 666 216**
7011 605 618

