Social Sciences & Humanities Open 13 (2026) 102603

Contents lists available at ScienceDirect

Social Sciences & Humanities Open

journal homepage: www.sciencedirect.com/journal/social-sciences-and-humanities-open

Regular Article

Digital privacy in a fragmented world: Comparative perspectives on the right to be forgotten

Raed Alnimer

College of Business & Law, Royal University for Women – Kingdom of Bahrain, Bahrain

ARTICLE INFO

Keywords:
Rights to Be forgotten GDPR extraterritoriality
data protection
Privacy law
Digital sovereignty
Bahrain PDPL EU laws google Spain
Transborder data flows

ABSTRACT

The European Right to Be Forgotten policy for outdated online content has reshaped privacy regulations across European territories. The regulations enable people to ask for website removal of their personal details. The right to delete data across borders concept has triggered strong debates which spread past European Union territorial boundaries. European Court of Justice decisions and GDPR encounters resistance because it conflicts with current national laws and conventional international working methods.

The research examines privacy norms between Europe and other three nations (Australia, Canada, and Bahrain) that have unique approaches towards personal information protection. The Bahrain data protection law of 2018 obliges organizations to adhere to regulations on information protection but does not have a specific rule for the right to delete data.

The research evaluates personal privacy interactions with free speech and worldwide data management systems through Svantesson's data-privacy rule levels framework. The most suitable solution for safeguarding individual rights and maintaining national control in today's diverse digital landscape appears to be a adaptable multi-layered system.

1. Research problem

Researching this topic is significant as it involves a complex issue: how the EU would like to protect a right to be forgotten, which is a crucial element in privacy policy, but is also trying to impose this policy worldwide, even on non-European countries.It creates problems because some nations prefer to maintain market independence, control their own information, or allow unrestricted speech. Even though the EU has high standards for online privacy, expanding its influence internationally conflicts with the interests of other countries. Bahrain's data protection legislation prioritizes local control over full cross-border transfer freedom. As a result, some significant problems emerge.

- To what extent can the RTBF apply beyond national borders without undermining the regulatory sovereignty of other jurisdictions?
- How do different legal systems balance the RTBF against freedom of expression and public interest considerations?
- Can cooperative or layered regulatory approaches provide a sustainable solution to cross-border RTBF conflicts?

2. Methodology

In this research, the research methodology used is based on the doctrinal perspective of research on laws and their interpretation as a comparative law issue in order to discuss the Right to Be Forgotten (RTBF) and concludes by 2024. The comparative analysis is done on European Union, Canada, Australia and Bahrain. The references to Belgium have been taken out in the previous drafts to address the final comparative set.

It is also a doctrinal research that lacks empirical data collection. It is based on the authority sources of the law solely to make it reproducible and rigorous. The areas of research of the doctrinal inquiry would be key statutes, judicial rulings, regulatory advice, and scholarly commentary in the review. Rulings by lower courts, opinions that are not binding and commentary were omitted so as to focus only on binding and authoritative sources since they offer some clear legal precedents. Using this approach will make the findings of the study based on verifiable law and capable of being recreated by other researchers of the law.

E-mail address: ralnimer@ruw.edu.bh.

https://doi.org/10.1016/j.ssaho.2026.102603
Received 26 November 2025; Received in revised form 3 February 2026; Accepted 17 February 2026
Available online 20 February 2026
2590-2911/© 2026 The Author. Published by Elsevier Ltd. This is an open access article under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/).

2.1. Source

These authorities were recognized by conducting specific searches in one of the legitimate sources of the legislative bodies, court databases, and other general secondary resources. Among the keywords, the following are applicable: Right to be Forgotten, erasure, de-referencing/delisting, extraterritorial, and privacy versus freedom of expression. The inclusion was restricted to the sources that offer important legal advice on these matters.

2.2. Doctrinal analysis

The doctrinal aspect focuses on the issues of primary and secondary sources of law, determining which content, range, or legal rationale is behind the RTBF. As applied to the European Union, this incorporates EU primary law (especially the Charter of Fundamental Rights of the European Union and the Treaty on the Functioning of the European Union) and secondary law (most notably the General Data Protection Regulation), as well as the judicial case law of the CJEU in the European Union (which is leading). Google Spain SL v AEPD and Google v CNIL are some of the key cases that are handled as the landmark authorities that define the content of RTBF as well as its territorial scope.

The doctrinal analysis gives more precedence to authoritative and binding materials, including statute laws, regulations and decisions by apex courts. The rulings of lower courtes, non-binding advice, and policy statements are cited where absolutely required to demonstrate larger patterns, and are not considered as binding. This discriminatory policy brings clarity and coherence to analysis and dogma.

2.3. Comparative legal analysis

The comparative aspect of the research looks at how the three countries Australia, Canada, and Bahrain respond to some of the questions pertaining to data destruction, delisting, and cross-border promotion of privacy rights. The jurisdictions were chosen on basis of the different legal traditions and regulation priorities: The European Union as a rights-based regulatory framework where RTBF is explicitly provided;

Bahrain as a Middle Eastern jurisdiction which takes the stance of a statutory data protection framework that emphasizes sovereignty and localisation of data but does not specifically acknowledge the equivalent of RTBF.In the analysis, there are uniform comparative dimensions, which are as follows; per jurisdiction.

(i) the presence and breadth of a remedy of erasure or of some related remedy;
(ii) the delisting of the search engine, which should be treated differently to data erasure;
(iii) the geographical extension and implementation of the orders connected with the privacy.
(iv) striking a balance between privacy interests on one hand and freedom of expression, public interest and regulatory sovereignty on the other hand.

The consistency of applying the dimensions makes the difference that it will be a systematic and not an illustrative comparison.

2.3.1. Case law selection and identification

Judicial sources were found by subjecting official court databases, legislative portals, and other available secondary sources to targeted searches to uncover such key words as right to be forgotten, erasure, delisting, extraterritoriality, and privacy versus freedom of expression. The analysis is geared towards landmark or leading cases, which describe the broad-based principles in contrast to the legal facts, which increases the probability of the analysis to be reproducible in other researchers in the law field.

2.4. Analytical framework: Svantesson's layered approach

The research adopts the concept of a layered approach to jurisdiction as an evaluation of the implication of extraterritorial data protection claims through the perspectives of Svantesson. Instead of viewing jurisdiction as a dualistic territorialism concept, the framework is employed to evaluate how the various legal systems distribute regulatory jurisdiction over more than two layers, comprising the interests of the regulating state, the people, the digital intermediaries, and the foreign legal orders. The evaluatory lens around which the jurisdiction is conceptualized is the Svantesson framework which views jurisdiction as a multi-layered structure. These layers are regulating state, data subject, digital intermediaries and foreign legal orders. This framework makes the comparative analysis through the existing distribution of authority and responsibility at these levels, which could be used to consider the conflict between the interests in territorial sovereignty and extraterritorial data protection requirements implicitly.

2.5. Bahrain case study

Lastly, the research is set to adopt a specialized doctrinally-themed scrutiny of the Bahrain Personal Data Protection Law (Law No. 30 of 2018). The review scores the extent of data subject rights, limitations on erasure, and cross-border data transfer regulations, placing Bahrain as a case study of the promotion of privacy versus national control by developing data protection frameworks. The research fails to consider Bahrain as the example of all Gulf or MENA jurisdictions but focuses on it as a situational example to extrapolate the debate about RTBF.

3. Introduction

The definition and limits of privacy have evolved in the digital age in ways that were unthinkable just a few decades ago. Previously kept in local records or physical archives, information is now freely shared across international borders via digital networks. Legal systems now have to reconsider how to strike a balance between state power, corporate interests, and individual protection in light of this new reality. The Right to Be Forgotten (RTBF) is one of the most intricate and contentious legal issues that has surfaced among the many others. (Blume, 2014a).

This paper has three main contributions to the current body of literature on the Right to Be Forgotten (RTBF). First, it transcends the highly EU-centric approach which dominates much of the existing literature by comparatively contrasting the European system with preferred non-EU systems, that is, Canada, Australia and Bahrain. Such a comparative design will allow making the processes by which principles associated with RTBF are tailored, constrained, or challenged in separate constitutional, regulatory settings instead of presuming that they will function in a similar manner across national boundaries.

Second, the research reinforces the doctrinal analysis through locating the discussion on existing EU primary and secondary law and prevailing Court of Justice jurisprudence, such as Google Spain and Google v CNIL, and then comparing them to the comparatively functionally equivalent privacy measures in the respective comparative jurisdictions. Such a method does not presuppose that transplantation of organs legally, but emphasizes the fact that the systems have different balances of privacy protection, freedom of expression, and regulatory sovereignty.

Third, the layered approach goes hand in hand with the use of Swantessons approach, which offers a systematic assessment perspective of the phenomenon of fragmentation in the jurisdiction regulation in the digital context. Instead of offering one standardized model of RTBF to the world, the research shows the usefulness of layered and cooperative reactions to regulation. In this respect, it adds a principled model in measuring cross-border data protection conflict that is attentive to law pluralism and institutional boundaries, and thus provides a more

realistic foundation on further regulation coordination.

4. Aim and objectives

This article aims to determine the extent and boundaries of the Right to Be Forgotten (RTBF) in a fragmented digital space through a comparative analysis of the European Union and the approaches adopted in Australia, Canada, and Bahrain.

4.1. Objectives

1. To clarify the legal distinction between data erasure under the RTBF and search-engine delisting.
2. To analyse EU RTBF jurisprudence and its cross-border implications as a comparative baseline.
3. To compare how Australia, Canada, and Bahrain balance privacy, freedom of expression, and regulatory sovereignty.
4. To evaluate these approaches using Svantesson's layered framework as an analytical tool.

4.2. Structure and scope

The article first examines the EU legal framework, followed by a comparative assessment of Australia, Canada, and Bahrain, and concludes with an integrated evaluation applying Svantesson's framework.

5. Literature gap and contribution

The current literature on Right to Be Forgotten (RTBF) is largely dominated by a European outlook, which is narrowly focused on the case law relating to the European Court of Justice (ECJ) and the jurisdictional applicability of the General Data Protection Regulation (GDPR). However, although these preceding works have been useful in providing foundations for this research work, it is more likely than not that these have not taken into consideration how non-European countries, especially those in the Middle East, have been managing these competing issues. One important case in point that should be considered is the recent PDPL enacted in Bahrain, which is intentionally different from Europe's "Right to be Forgotten" policy. It is indicative of how small countries try to adhere to global regulations while dealing with homegrown problems, such as keeping data within their borders. Rather than focusing on a particular body of regulations, it is necessary to note that it is a struggle between governments trying to protect their hegemony on the internet versus others trying to adopt a unitary notion of privacy on this global resource.(De Hert & Czerniawski, 2016).

The research compares how data regulations in Belgium measure up against others in Bahrain, Australia, Canada, and the European Union. The research offers a new perspective on internet privacy regulation coming out of the Gulf. Moreover, it proposes collaboration between countries as the best way to balance protecting personal information alongside each nation's independence in our increasingly connected world. Ultimately, this work suggests a flexible approach allowing the 'right to be forgotten' to expand internationally, acknowledging different legal systems(Fainmesser et al., 2023).

1 EU Jurisprudence and Law on Data Protection

The EU boasts one of the most advanced data privacy laws in the world at the constitutional level. The European Convention of Fundamental Rights adopted in 2000 introduced the right to data protection as a constitutional right within the European legal system(Bygrave, 2000). A fresh and clear recognition with regard to the right to data privacy has been brought about through Article 8 entitled "Protection of Personal Data," while within the European Convention on Human Rights, the provisions within Article 7 entitled "Respect for Private and Family Life" reiterated that "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."

The Charter has been fully justiciable since 2009 with the entry into force of the Treaty of Lisbon. In addition to that, with the Treaty of Lisbon, there was the introduction of a new paragraph that pointed to the relevance of data privacy rights within the modern constitutional framework that exists within the European Union. Twelve "everyone has the right to the protection of personal data relating to them," as is stated within the provisions of Article 16 within the Treaty on the Functioning of the European Union (TFEU). The Council and European Parliament are authorized within the same article to "lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities."

The principles outlined in the Data Protection Directive applied to bodies within the EU by regulation in 2001 to the protection of persons with regard to the processing of personal data by organism/publications/agencies. The regulation also established the European Data Protection Supervisor (EDPS). In other sectors such as electronic communication and law enforcement/cooperation between law enforcement and the judiciary in criminal matters, there was other regulation within the EU that supported the protection of data privacy (Lynn et al., 2020a).

At last, in 2016, the General Data Protection Regulation (GDPR)20 was adopted by the European Parliament and the Council on the basis of Article 16 TFEU. In the same year, the Directive on the protection of natural persons with regard to the processing of personal data related to criminal offenses or the imposition of criminal penalties was adopted. In an attempt to create an even more complex regulatory environment that takes care of the challenges presented by globalization and technology development, GDPR repealed the Data Protection Directive and adopted rules that had direct and permanent application in all member countries within the European Union(De Hert & Czerniawski, 2016).

Lastly, there is the "ECJ that has proactively taken on the role of the 'human rights court'" to ensure data protection on the level of jurisprudence through the development of its precedents. Specifically: The "ECJ has recently maintained the stringently protected data privacy rights" with an extended understanding of its precedents "to include the invocation of the Charter of Fundamental Rights": 1) horizontally (i.e., with regard to political bodies within the European Union); 2) vertically (i.e., with regard to member states); 3) diagonally (i.e., with regard to private companies that reserve all pertinent authority over the data in question during the data processing process).

First, the ECJ struck down those member states that failed to achieve this objective through national legislation, striking down national laws that incorporated surveillance provisions on the plea that there was an implicit obligation on data protection authorities to be fully independent with regard to Articles 8 of the Charter and 16 TFEU. Second, the ECJ declared that the EU Data Retention Directive that mandated personal data to be retained for law enforcement purposes, and the international understanding reached between the EU and Canada that envisioned the collection of passenger name record (PNR) data to be incompatible with the primacy of EU law due to a violation of Articles 7 and 8 of the Charter that accorded data subjects the right to be protected from systematic state surveillance practices. Third, with the application of data protection laws within the providers offering IT services within the EU internal market and with data subjects' expansive rights arising therefrom, the ECJ has further required that there be a rigorous standard with regard to data protection within the ambit of ICT businesses. In this

regard, the ECJ has further defined the 'right to be forgotten' that was later enshrined within the provisions of GDPR and accepted by other courts(Jerker & Svantesson, n.d.-a).

3 The Right to Be Forgotten

The European Court of Justice made significant progress towards the recognition of the right to be forgotten in the case Google Spain SL vs. Agencia España de Protección de Datos (AEPD), in May 2014. 30 The case concerned Google's and AEPD's requirement to apply the Data Protection Directive in court proceedings. The AEPD received such application from Google to erase any link to the applicant's data in search engine results due to the application of data protection laws. Google appealed an administrative decision in Spanish courts over this application; some questions arose that led to references to the European Court of Justice(Fabbrini & Celeste, 2020).

Indeed, the ECJ has affirmed the existence of the new right to erasure that data subjects may rely upon to get web pages deleted. The search engine provider must therefore delete from the list of search results those websites that are accessible to the public and contain the personal data of the data subject after carrying out a search made with his name. In giving its preliminary ruling on the issue, the European Court of Justice (ECJ) found that search engines such as Google are data processors and joint controllers in the Data Protection Directive(Blume, 2014a).

The European Court of Justice has settled that "a Google search conducted with the intention to obtain 'a more or less detailed profile of the data subject' may be connectable to the 'obligation to remove from the list of results displayed following a search carried out on the basis of a person's name' web pages 'published by third parties' if 'that name or information is still present' there and has not already 'been removed beforehand or simultaneously from those web pages'—regardless whether 'its publication there is lawful(Google Court Decision: The Right to Be Forgotten? - Lexology, n.d.)."

The Google Spain ruling brought about an opportunity to fully codify the "right to be forgotten" in European law. "The data subjects 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 be obligated to erase personal data without undue delay," as stated in Article 17 in the GDPR that enshrines the "Right to erasure (right to forgotten).(CURIA - Documents, n.d.)"

Where "(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based [::]; (c) the data subject objects to the processing [::]," the above provision clearly stipulates that the right to erasure applies. (d) The processing of the personal data was illegal. Furthermore, in line with GDPR Article 17 (2), Furthermore, as per GDPR Article 17(2), "Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller shall take reasonable steps, including technical measures, taking into account the cost of implementation and available technology, to inform controllers which are processing the personal data that the data subject has requested that such controllers erasure any links to, copy, or replication of those personal data.(*Art. 17* GDPR – Right to Erasure *('Right to Be Forgotten') - General Data Protection Regulation (*GDPR – Right to erasure, n.d.)"

The PDPL's Article 23 provides data subjects with the right to obtain the rectification, blocking, or erasure of the data concerned whenever the data's processing is illegal. In this regard, the PDPL limits the right to erasure to cases that are illegal and non-compliant, unlike the GDPR's Article 17 that provides data subjects with the right to erasure if the first data processing was carried out within the provisions of the law. In fact, it must be pointed out that there are no provisions within the PDPL that impose any requirements to de-reference search engines(Bahrain's PDPL vs. GDPR - Securiti, n.d.).

The court writes that "a data subject's right to erasure 'override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in finding that information upon a search relating to the data subject's name.'" The GDPR agreed with this assessment. The right to erasure "shall not apply to the extent that processing is necessary: (a) for exercising the right to freedom of expression and information; (b) for compliance with legal obligations [::] in the public interest" and other purposes related to public health and scientific and historic research, among others, contrary to GDPR article 17(3)(*Art. 17 GDPR – Right to Erasure ('Right to Be Forgotten') - General Data Protection Regulation (GDPR)*, n.d.).

National courts, particularly in Germany, look to European Court of Justice precedent with regard to the right to be forgotten. In one case that involved a private party and a broadcasting company, there was a court ruling made in November 2019 that was consistent with European legislation on the right to be forgotten with regard to the applicant's demand to delete his connections to the discovered web pages. The court noted that the demands with regard to the protection of European Union's basic rights are "relevant and assessable" since such rights were governed by full harmonization within the European Union.The court ostensibly dismissed the constitutional case after determining that the usual courts had appropriately balanced the rights that conflict with each other. In the same day that the court made the above ruling, it has set its standard with regard to the right to be forgotten within national law. In adjudging constitutional applications within the national boundaries within Germany, it was made clear that the court would use German constitutional rights if there was the possibility within European law to establish other models within national boundaries "unless it can be shown that either German constitutional rights fall below the level of the minimum standard guaranteed by the Charter or that European law calls for the establishment of the same level of protection."(Friedl, 2020)

In this case, the court holds that "in the light of the constitutional guarantee of the right to individuality consisting inter alia in the right to be forgotten," the private complainant was entitled to "demand that the articles about him be removed from the daily Der Spiegel website." "A balancing act between the freedom of expression and information and the right to be forgotten" was therefore to be carried out in this case. 42 - but "the requirement that time be considered as a relevant contextual factor characterizing information has a new legal dimension due to the realities of information technology and the dissemination of information on the internet." "Given that 'it would have been necessary to consider whether it was possible, and required, to impose an obligation on the media outlet sued before the ordinary courts to take reasonable precautions upon being notified by the complainant, to provide at least some protection against search engines retrieving the articles in question in the context of searches related to the complainant's name, without unduly restricting the general retrievability and accessibility of the articles as such,'" the court finds that there was justification for the constitutional complaint(Friedl, 2020).

4. Extraterritorial Application of EU Data Protection Law

In the present past, the data protection regime in the EU has continued to spread its wings outside the boundaries of the EU. In attempting to establish whether data protection law regimes in third countries became adequate enough to enable data flow from the EU to such countries, the European Court Of Justice (ECJ) made various considerations. Eventually, this led to such countries being persuaded to ensure that data protection regimes in such countries are linked to that of the EU standard(Fabbrini & Celeste, 2020). The European Commission Safe Harbor Decision was set as precedent whereby US data protection law was adjudged to be adequate enough to permit private companies to transfer data from the US to theEU. The European Court Of Justice (ECJ), in the Schrems case, strictly reviewed these Safe Harbor Decisions due to US Mass surveillance activities. But due to the revelation over US Mass surveillance activities' existence, the European Court

Of Justice (ECJ) declared that US laws and activities did not provide enough standards to ensure that the data transferred had enough safeguards. The standards set to limit data protection to national security concerns' use and access; further monitoring and remedy bodies to prevent personal data transferred to be processed illegally or abused are among those extra measures taken by US and EU renegotiate due to the fact that data produced in the EU needs enough personal data protection standards that the European Court Of Justice (ECJ) made US and EU renegotiate (Keele, 2018).

A Facebook user who was disgruntled over the fact that data received had few enough protective measures within the US made the European Court of Justice (ECJ) take the decision. The most updated Privacy Shield Adequacy Decision pronounced by the Commission has enforced these principles. Notwithstanding that this has further been disputed to be inadequate compared to Safe Harbor Decision provisions for US Citizens' data, it seems to be one step forward to note that perhaps data protection law within the EU has significant precedence within international deliberations to ensure that other countries measure up to data protection rights within EU standards(Svantesson, 2013a).

The ECJ has particularly expanded the application of data privacy law within the EU to economic operators that are not incorporated within the EU to data processed within the EU. This has already been noted in Google Spain, "where the European Court of Justice (ECJ) had already concluded that 'on account of the aim to ensure effective and complete protection of the fundamental rights and freedoms of natural persons, and in particular the right to privacy with respect to the processing of personal data'—so as to 'ensure the fundamental rights are protected everywhere in the same way and to the same extent'—'[t]he notion of establishment cannot be interpreted restrictively.' The court therefore concluded that 'although Google is incorporated under US law, Google must comply with the Data Protection Directive since Google has a subsidiary in Spain which is responsible for managing advertising on the Spanish-language version of Google Search'—because Google 'offers goods and services to spanish-speaking users' in the EU." Paragraph 3 (2), entitled "Territorial Scope," declared that "This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behavior as far as such behavior is within the Union."

In effect, the GDPR has further expanded such circumstances. Difficulties arising out of the extraterritorial application of data protection law within the EU—particularly with regard to "right to be forgotten" claims—have reached proportions of concern in attempts by the European Court of Justice (ECJ) to evaluate the circumstances in which requests to delete web data are binding on companies operating worldwide. This was set to occur in September 2019 before the European Court of Justice (ECJ), in the case Google vs. The French data protection authorityCommission Nationale de l'Informatique et des Libertés (CNIL), who had taken Google to court over its failure to delete requested web content from all domains on Google's websites worldwide (*Article 3*† GDPR. Territorial Scope | GDPR-Text.Com, n.d.).

Google had contested the fine that was imposed by the CNIL with the rationale that it was sufficient to remove the content that was accessible only in French from its search engine. In its ruling, the European Court of Justice (ECJ) supported the case on the rationale that Google had geoblocks. The European Court of Justice (ECJ) acknowledged that the "guarantee of a high level of protection of personal data throughout the [EU]" was the objective of GDPR and that undertaking the de-reference on each version of the search engine would ensure this.(*Google Court Decision: The Right to Be Forgotten*? - Lexology, n.d.)

The transfer of data across borders as per the provisions in the PDPL is governed by Articles 12-13 and the 2022 executive resolutions. The transfer rules are governed by Resolution 42/2022 in the case of direct transfers to jurisdictions determined by decision, and Resolutions 43/2022 and 44/2022 take care of the technical and organizational measures as well as approval. The present scenario balances the flow and has reinforced that adequacy measures are internal to every state and are no concern to the process that is followed within the GDPR provisions (*Bahrain Business La*ws | Personal Data Protection Law, n.d.).

"Many third States do not recognize the right to de-referencing or have a different approach to that right," the European Court of Justice (ECJ) pointed out. In light of the decision reached by the European Court of Justice (ECJ), "the GDPR did not reflect the intention 'of the EU legislator to impose on an operator such as Google an obligation to de-reference that applies to the national editions of its search engine which do not correspond to the Member States and to give to rights enshrined in those provisions a scope which would exceed the territory of the Member States'." ECJ concludes that: 'where a search engine operator complies with a request for de-reference in accordance with those provisions, the search engine operator is not required to effect that de-reference on all copies of that search engine, but on the copies of that search engine corresponding to all Member States, by means of measures that, while fulfilling the requirements of the law, prevent or, at the very least, deter an internet user who conducts his search from among the Member States on the basis of the name of the data subjects concerned from accessing through the list shown following that search the links that are the object of that request.')"

A week later, within the boundaries set by October 2019, the European Court of Justice' ruling in the "Eva Glawischnig-Piesczek vs. Facebook" case struck a balance between Google vs. CNIL to some extent since the latter was seen to restrict the extraterritorial application of the right to be forgotten. Although this particular ruling was not mainly related to the right to be forgotten, it was more closely related to the issue that was at stake in other cases regarding whether one can use international companies to erase internationally accessible data that has been found to be harmful to one's honor(Lynn et al., 2020a).

The applicant filed a lawsuit claiming that Facebook had infringed data protection legislation since Austrian politician Mrs. Eva Glawischnig-Piesczeg had successfully obtained an injunction requiring Facebook to delete defamatory posts that had been placed about her on Facebook. Facebook had blocked any further access to the data that had previously been accessible only within AustriaThis was preceded by an analysis by the ECJ on the status accorded to digital service providers within the e-Commerce Directive and then proceeded to investigate if there was any limitation to the measures that member states are permitted to take in the context of information society services within the provisions of EU legislation(Kuner, 2010).

Although it warned that "in view of the global dimension of electronic commerce, the EU legislature has considered it necessary to ensure that EU rules in that area are consistent with the rules applicable at the international level" and that "[i]t is up to Member States to ensure that the measures which they adopt and which produce effects worldwide take due account of those rules," the ECJ ruling gave Austrian courts the "power to oblige Facebook to remove information covered by the injunction or to block access to that information worldwide within the framework of the relevant international law."

5 The Challenges of Extraterritoriality in Comparative Perspective

The issue of extraterritorial application of domestic law in the digital realm is, however, anything but unique to the European Union. The future of free speech on the Internet, the validity of global injunctions, and whether there is to be regulation with regard to web pages across international boundaries are all questions that are highly pertinent to contemporary challenges that are increasingly cropping up before courts across the globe; these are succinctly encapsulated byJennifer Daskal (Black, 1997).

The kind of difficulties that may be posed by the extraterritorial application of data protection laws are evident in other current disputes that concerned US technology firms and resulted in decisions made in

Canada and Australia (Fainmesser et al., 2023).

In 2017, Google was ordered to remove the connection to a company website that infringed the rights of intellectual property by the Supreme Court of Canada in the case Google Inc. vs. Equustek Solutions Inc. A technology company in Canada was Equustek. The company filed an action against Google due to the fact that Google had infringed Equustek's rights to its intellectual property by stealing its trademark and also failed to remove sites belonging to Equustek's competitors from the search engine browser list. Equustek took the issue to the Supreme Court of Canada in 2017 due to the fact that Google had won the case filed by Equustek but was still mandated to remove sites that had infringed Equustek's rights from its international browser list since the court had ordered that Equustek was to win the action filed against Google and that the court was to ensure that the sites are delisted worldwide(Jerker & Svantesson, n.d.-a).

It is pertinent to note that Google later attempted to obtain an injunction from the US District Court in Northern California to prevent the enforcement in the US of the delisting order that had been handed down by the Canadian Supreme Court. The court was more than pleased to grant Google the sought injunction in November 2017. The result was that the decision reached by the Canadian Supreme Court was overturned in the US. Google's case before the Supreme Court of British Columbia in April 2018 failed, notwithstanding the positive decision reached by the Californian court. The court was adamant that it would not entertain Google's claims to restrict the binding effect of its delisting order(Svantesson, 2013b).

Similarly, the Supreme Court of New South Wales in Australia ordered the Californian company and its subsidiary company in Ireland to remove private information shared by a troll all over the world in the case of X vs. Twitter in 2017. The party that went to court, X, was remorseful about the private financial information that had been shared on Twitter by an anonymous troll who had taken up various identities, one of which took up the name of the CEO(Keele, 2018).

Although feeling the initial reluctance to suspend the accounts involved, the court ultimately forced Twitter to reveal the troll's name and delete any illegal data that had been posted on the web. The Australian court was more concerned with international comity principles rather than waiting to see how other countries may decree breach of confidence rather than breach of copyright. In this case, again, the Supreme Court of New South Wales was not reluctant to render an extraterritorial injunction to improve the difficult circumstances that the petitioner faces within his own country. The latest decisions adopted by the ECJ within Google vs. CNIL and Glawischnig-Piesczek vs. Facebook again allowed the transnational application of EU law provisions comparable to that adopted by the Canadian and Australian courts' decisions. The worldwide impact with only one exception—respecting international law principles—was the most important relief that the ECJ was ready to grant to the claimants in Glawischnig-Piesczek vs. Facebook. As was mentioned in the previous section, within Google vs. CNIL, the European Court of Justice (ECJ) made it clear that delisting within the boundaries of the European Union would be enough. The prudent reasoning adopted by the advocate general was fully accepted by the ECJ in Glawischnig-Piesczek vs. Facebook vs. Facebook court press release(Blume, 2014b).

As quoted by the EU, “The need to ensure the efficient protection of fundamental rights and to limit the risk of infringement” is the rationale that led to such extraterritorial application. The way the right to be forgotten has been exercised is outstanding. Borders are no more important in this digital age that we are living in. A search engine can contain one result in one state that is different from the state that the data subjects are in. The right to data protection might still be infringed (Charter of Fundamental Rights of the European Union, n.d.-b).

From the theoretical perspective, taking into consideration the ease with which one has access to data all over the world, it would be ludicrous to restrict such a right to those within the realms of the European Union. If an individual living in France, for example, requests that some results be removed from his search results list through legal means and finds that the results are still linked not only in France but perhaps in Germany and in the US as well without anything had been changed, then that constitutes an infringement of such rights. In fact, there seems to be an implication that data protection rights are extraterritorial, that is outside the European Union(Lynn et al., 2020b).

Despite this, the Google Inc. vs. Equustek Solutions Inc. court case has posed challenges to the extraterritorial application of data protection laws within the European Union. The rules that must be adhered to if one adheres to international comity and is mindful of divergences among various legal traditions are placed in conflict with the extraterritorial application of one's national data protection principles. The reality is that other countries across the globe—those that share similar understandings with regard to democracy, the rule of law, and human rights—subscribe to a different balance between the right to be forgotten, freedom of information, and freedom of expression(*Google Court Decision: The Right to Be Forgotten?* - Lexology, n.d.).

Furthermore, as shown in the most recent court cases in US and Canadian courts, there might come a point that counter-arguments can make the application of data protection laws outside the territorial boundaries invalid. The US Federal District Court has implicitly defined the boundaries within the US jurisdiction with respect to the application of the Canadian writ by forbidding the application of the Canadian Supreme Court'sdecision on the Canadian Google case to the US jurisdiction in particular. In view of these challenges and pitfalls that need to be taken into account, one might argue that the most recent court decisions reached within the European Court of Justice in Google vs. CNIL and Glawischnig-Piesczek vs. Facebook might be regarded as an adequate solution to mitigate the Charybdis of digital sovereignty with that of data protection imperialism.

The conflict that has resulted from the differing opinions seems set to escalate. While there are those who are critical about the European Union's strict data rules, the measures that various countries have taken to manage the data within their countries have shown that there will be more divisions in the digital world in the future. The regulation of the digital world has started to gain prominence even in places such as America and Europe and even among those who are in favor of less freedom. A lack of freedom on the web might result from this development. The development of international laws seems to be key to ensuring that data protection is accorded to people if these international laws are followed by governments in those countries(Jerker & Svantesson, n.d.-a).

6. Interpretation

This paper was aimed at investigating the functionality of the right of Right to Be Forgotten (RTBF) in a divided digital and jurisdictional environment, based on the principles of the European Union and contrasted with similar practices in Canada, Australia and Bahrain.

6.1. *Rebalancing the EU analysis*

The RTBF framework developed by the European Union, based on Article 17 of the GDPR and explained in terms of the landmark cases, including that of Google Spain and Google v CNIL, offers a fine-grained doctrinal background in the understanding of data erasure and search engine delistings (Dpo, 2023). As the analysis confirms, it is undoubtedly proven that EU jurisprudence does not confuse the right to erasure of personal data and the obligation subjected to search engines in cases of such conditions as de-reference of links. Notably, Google v CNIL does not impose a global operation of the delisting requirements, yet it refuses a universal application but instead allows specific actions that secure privacy of the data subjects in the EU in a way that is sufficient.

Instead of repeating the historical progression of EU data protection law, the results highlight that the EU paradigm is a normative framework to be followed and not an immediately transferable tool (Wolford,

2025). It is strong due to its organized balancing of the privacy, freedom of expression, and the public interest, but its weaknesses can be observed, in particular, in case the implementation goes outside the EU borders. This acknowledgement undergirds the comparative judgment that ensues and does not consider the EU experience to be exhaustive and/or possess a universal determination.

6.2. Canada and Australia: doctrinal realities on RTBF

In Canada, no statutory right to be forgotten has been established that might be analogous to the similar provision under GDPR Article 17 of the EU (Toronto Lawyers, 2025). Rather, there is the growing and emerging, and harm-centered right to de-list search results as part of PIPEDA (the federal Personal Information Protection and Electronic Documents Act). In August 2025, the Office of the Privacy Commissioner of Canada decided in a case that people might have a right to removal of specific results of searches where risks of great harm prevail over the public interest, as presented in PIPEDA principles of accuracy and relevance. The search engines were recommended to remove offensive results due to the query of the name of an individual, however, leaving the material of the source behind; this would serve to protect privacy and at the same time allow the freedom of expression and access to information as guaranteed under the Canadian Charter of Rights and Freedoms (Dentons, 2025).

Nonetheless, it is legally debatable whether it is a true RTBF, and others commenting on it believe that as of today, Canadian law does not provide a general prohibition to be forgotten under the data protection law, but only case-specific de-indexing (Law Times, 2018).

Contrastingly, Australia does not as yet acknowledge any formal right to be forgotten or an explicit statutory right of erasure that exists in the privacy Act 1988 (Cth) on the Australian side. The Australian Privacy Principles (APPs) currently provide individuals with the right to request correction of the inaccurate personal data and the obligation of organizations to destroy or de-identify the personal data which are no longer necessary, however, there is also no general right to have the personal data erased or to order the search engine to delist (Gardoce, 2022). A reform of the Privacy Act survey has also appreciated a civil narrow right to de-index search outcomes based on GDPR principles (e.g., sensitive, out-of-date, or misleading information) although to-date such reforms have not produced legally enforceable rights (as of 2025) (Constantine et al., 2023).

There is no statutory right to be forgotten in Canada and Australia that involves a similar level of protection as GDPR in the EU. Canada uses a case-by-case de-indexing strategy under PIPEDA by balancing privacy and the public interest, which is in the case of Google Inc. v. Equustek Solutions Inc. Australia, which provides data remedies and some deletion but no RTBF. The two jurisdictions are concerned with facilitating domestic coherence and proportionality in the law as opposed to blanket elimination. These models are opposed to that of the EU which demonstrates how constitutional habits, judicial interpretation and regulatory priorities make RTBF implementation under non-European circumstances.

6.3. Bahrain and regulatory adaptation

The Personal Data Protection Law (PDPL) of 2018 in Bahrain is a unique regulatory model when contrasting with other comparative regulatory models (Data, 2025). Although the PDPL does not directly enshrine an equivalent to Article 17 of the GDPR, to such a degree, RTBF, data subject rights, i.e. erasure, consent, and lawful processing are partially reflected in the PDPL. To that end, the RTBF should not be described as one hundred per cent and total adoption of Bahrain. Rather, the analysis justifies the more factual analysis, namely that Bahrain exhibits some developing and selective interaction with data protection standards, tailored for home legal frameworks and sovereignty.

It is a qualified reading that removes an inner incongruity between sections of earlier description and wider-scale evaluation. The structure of Bahrain is designed to show a convergence of regulations in principle, and not on wholesale reproduction of the EU model, and must be interpreted as indicative and not representative of that of the broader Gulf or MENA region, on the whole.

6.4. Evaluating extraterritoriality through a layered lens

The use of the layered approach by Svantesson explains why there is neither a realistic nor normative decision of a single and globally consistent RTBF standard (Merete, 2025). The comparative results indicate that every jurisdiction has its own level of legal and regulatory functioning, which is formulated due to constitutional values, institutional potential, and geopolitical backgrounds. The policies of the EU focus on rights-based regulation which has conditional extraterritorial impacts and those of Canada and Australia are oriented to proportionality and domestic legal coherence. The model observed in Bahrain encompasses a regulatory customisation without national sovereignty.

7. Conclusion

There are a number of limitations of this study. It follows the non-experimental, dogmatic methodology and hence is not able to determine the effectiveness or implementation results of RTBF or delisting petitions. It only compares the EU, Canada, Australia and Bahrain and this is not applicable to any generalisation globally, specifically, Bahrain should not be regarded as the representative of the rest of the Gulf or the MENA region.

The comparative analysis indicates that the EU GDPR offers an effective RTBF framework that has limited extraterritoriality, whereas Canada and Australia do not offer a formal RTBF, and the former has a case-based delisting application under PIPEDA, whereas the latter relies on personal protection principles of deletion and correction. The PDPL of Bahrain partially covers the ideas of RTBF (primarily when unlawful processing is involved), but it does not create a deletion or delisting right in search engines in general. These differences underscore the need to use one international standard. A flexible and collaborative model, combining national sovereignty, individual privacy, and freedom of expression, can potentially provide a practical model towards cross-border information security and personal rights.

The danger with this debate is that it can go to the extremes with one side. “One alternative is that one jurisdiction must impose all its law everywhere; thus it gets control over personal data. The other is that it gives paramount importance to the principle of control by nationality possibly to the point that people are placed in danger if data moves beyond national boundaries. Concepts such as ‘layered approach’ referred to by Svantesson indicate th dawn of a bright and intelligent approach. The point that one is sure about is that different countries hold different interests depending on what data is concerned with; who owns it; and whether it has an effect on other people.” In the area of globalization, this appears as a medium between sovereignty and privacy rights.

8. Policy recommendations

- International organizations such as the OECD and UN should facilitate multilateral discussions to develop baseline international norms for data protection, balancing national sovereignty with cross-border cooperation.
- Legislators and jurists should carefully assess the scope of RTBF enforcement abroad, seeking a middle ground between governmental authority and individual freedoms.
- The RTBF should be applied flexibly, considering public interest, freedom of expression, and the context of each jurisdiction.

- Bahrain and other Gulf States should develop tailored data protection laws that address local needs while aligning with international standards, rather than copying EU models.

Indeed, the RTBF reveals how hard it is for there to be a balance between privacy and the omnipresence of the internet. It all relies on global co-operation, following through with these regulations, and giving each individual the right to have control over their information instead of one country with regulations. It is hoped that this will facilitate a balanced global dialogue on managing privacy issues related to digitalization.

8.1. Recommendations for further research

This particular research compared different legal frameworks to investigate "the right to be forgotten," but there are a few issues left unanswered. First, it is necessary to have more empirical information about these requests and how effectively these actually work for individuals. An investigation about how these non-European courts, such as those in Middle East Gulf states, might deal with these matters with similar global elements would also be insightful. Additionally, when it comes to following these regulations, it does become even harder with these Responsible Technology Business Frameworks and new tech concepts such as blockchain, AI, and others. Finally, it is necessary to investigate how society conceives this privacy on matters concerning "our digital memory."

Future studies might then expand on this by exploring the specifics of RTBF's functioning in accordance with changing legislation, technological developments, and cultural differences.

Data availability statement

No new data were generated or analyzed in the course of this study.

Ethics statement

Not applicable.

Ethical statement

This study was conducted in accordance with recognized ethical research standards, ensuring integrity, transparency, and respect for participants. No personal or sensitive data were collected, and all information was handled confidentially and used solely for academic purposes. The authors affirm that the work is original, complies with ethical guidelines, and has not been submitted elsewhere.

Declaration of AI use

No (AI) tools or software were used in the preparation, writing, analysis, or editing of this manuscript.

Funding statement

This research will be supported by funding from the author's university upon final approval and publication.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Raed Alnimer reports financial support was provided by Royal University for Women. If there are other authors, they declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

17 GDPR – Right to erasure ('right to be forgotten') - General Data Protection Regulation (GDPR). (n.d.). Retrieved November 12, 2025, from https://gdpr-info.eu/art-17-gdpr/.

Bahrain's PDPL vs. GDPR - Securiti. (n.d.). Retrieved November 12, 2025, from https://securiti.ai/bahrain-pdpl-vs-gdpr/.

Black, J. (1997). Free speech & the internet: The inevitable move toward government regulation. *Richmond Journal of Law and Technology, 4*(2). https://scholarship.richmond.edu/jolt/vol4/iss2/2.

Blume, P. (2014a). Dan Jerker B. Svantesson, Extraterritoriality in data privacy law, copenhagen: Ex Tuto publishing, 2013, 240 pp, DKR395. *International Data Privacy Law, 4*(2), 171–173. https://doi.org/10.1093/idpl/ipu003

Blume, P. (2014b). Dan Jerker B. Svantesson, Extraterritoriality in data privacy law, copenhagen: Ex tuto publishing, 2013, 240 pp, DKR395. *International Data Privacy Law, 4*(2), 171–173. https://doi.org/10.1093/idpl/ipu003

Bygrave, L. A. (2000). *European Data Protection European Data Protection Determining Applicable Law Pursuant To European Data Protection Legislation, 1*.

Charter of fundamental rights of the European Union. (n.d.-a).

Charter of fundamental rights of the European Union. (n.d.-b).

Constantine, J., Fiddian, S., & Benson, D. (2023). Australian privacy law reforms: How will expanded. *Clayton Utz. Claytonutz.com*. https://www.claytonutz.com/insights/2023/june/australian-privacy-law-reforms-how-will-expanded-individual-privacy-rights-impact-your-practices-and-procedures.

CURIA - Documents. (n.d.). Retrieved November 12, 2025, from https://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=en.

Data, B. (2025). Bahrain data protection law explained | VComply. *VComply*. https://www.v-comply.com/glossary/bahrain-data-protection-law-bdpl/.

De Hert, P., & Czerniawski, M. (2016). Expanding the European data protection scope beyond territory: Article 3 of the general Data protection regulation in its wider context. *International Data Privacy Law, 6*(3), 230–243. https://doi.org/10.1093/idpl/ipw008

Dentons. (2025). Canada's emerging "right to be forgotten": Federal privacy commissioner rules on de-listing. *Dentons.com*. https://www.dentons.com/en/insights/articles/2025/november/11/canadas-emerging-right-to-be-forgotten.

Dpo. (2023). *The right to be forgotten vs. AI's Infinite memory: A regulatory dilemma. Dpo-India.com*. https://www.dpo-india.com/Blogs/right-to-forgot/.

Fabbrini, F., & Celeste, E. (2020). The right to be forgotten in the digital Age: The challenges of data protection beyond borders. *German Law Journal, 21*, 55–65. https://doi.org/10.1017/glj.2020.14

Fainmesser, I. P., Galeotti, A., & Momot, R. (2023). Digital privacy. *Management Science, 69*(6), 3157–3173. https://doi.org/10.1287/mnsc.2022.4513

Friedl, P. (2020). A new European fundamental rights court: The German constitutional court on the right to be forgotten. *European Papers - A Journal on Law and Integration, 5*(1), 447–460. https://doi.org/10.15166/2499-8249/343, 2020.

Gardoce, R. (2022). What is the right to be forgotten? *Sprintlaw*. https://sprintlaw.com.au/articles/right-to-be-forgotten/.

Google court decision: The right to be forgotten? - Lexology. (n.d.). Retrieved November 12, 2025, from https://www.lexology.com/library/detail.aspx?g=ef282556-4483-4757-a8b5-613348f5356c.

Jerker, D., & Svantesson, B. (n.d.-a). Extraterritoriality and targeting in EU data privacy law: The weak spot undermining the regulation. http://idpl.oxfordjournals.org/.

Jerker, D., & Svantesson, B. (n.d.-b). Protecting privacy on the "Borderless" internet - Some thoughts on extraterritoriality and transborder data flow. In Bond Law Review (Vol. 19). http://epublications.bond.edu.au/blr.

Keele, B. J. (2018). Information sovereignty: Data privacy, sovereign powers and the rule of law. In Radim Polčák, B. Dan Jerker, & Svantesson (Eds.), *International journal of legal information* (Vol. 46, pp. 123–124). Northampton, MA: Edward Elgar. https://doi.org/10.1017/jli.2018.28, 2017. Pp. xvii, 268. ISBN: 978-1-78643-921-5. US$ 135.00(2).

Kuner, C. (2010). Data protection law and international jurisdiction on the internet (part 2). *International Journal of Law and Info Technology, 18*(3), 227–247. https://doi.org/10.1093/ijlit/eaq004

Law Times. (2018). The case against a right to be forgotten. Www.lawtimesnews.com. https://www.lawtimesnews.com/archive/the-case-against-a-right-to-be-forgotten/263214.

Lynn, T. G., Mooney, J., & Van Der Werff, L. (2020a). Data privacy and trust in Cloud computing. https://www.researchgate.net/publication/344810026.

Lynn, T. G., Mooney, J., & Van Der Werff, L. (2020b). Data privacy and trust in cloud computing. https://www.researchgate.net/publication/344810026.

Merete, C. (2025). *Dan jerker B. Svantesson - Nobel peace prize*. Nobel peace prize. https://www.nobelpeaceprize.org/research/visiting-fellows-program/visiting-fellows/dan-jerker-b-svantesson.

Svantesson, D. J. B. (2013a). A "layered approach" to the extraterritoriality of data privacy laws. *International Data Privacy Law, 3*(4), 278–286. https://doi.org/10.1093/idpl/ipt027

Svantesson, D. J. B. (2013b). A "layered approach" to the extraterritoriality of data privacy laws. *International Data Privacy Law, 3*(4), 278–286. https://doi.org/10.1093/idpl/ipt027

Toronto Lawyers. (2025). The "Right to be Forgotten" arrives in Canada. *Tlaonline.ca; Toronto Lawyers Association*. https://www.tlaonline.ca/?pg=News&blAction=showEntry&blogEntry=133133.

Wolford, B. (2025). *What is GDPR, the eu's new data protection law?* GDPR.EU. https://gdpr.eu/what-is-gdpr/.