From principle to practice: the EU-wide implementation challenges of the 'right to be forgotten' following Google v CNIL (iThenticate Similarity Report)

WORD COUNT	6577	TIME SUBMITTED	31-MAR-2024 10:26AM
		PAPER ID	107951707

Faculty of Law and Administration

STUDIA IURIDICA LUBLINENSIA

From principle to practice: the EU-wide implementation challenges of the 'right to be forgotten' following Google v CNIL

ABSTRACT

While scholarly attention largely gravitates towards the debate on regional v. global delisting under EU law, this paper scrutinizes Google v CNIL concerning the conditions and methods of EU-wide delisting in light of the preliminary reference questions posed. The focus lies in the intricate analysis absent from the dispositif, which leaves many complexities to the evaluation of the national data protection authorities (DPAs) and the courts, and, concerningly, to the solely discretion of the search engine operators. Nuanced analyses absent from the dispositif address the crucial aspects in defining the territorial scope such as the role of geo-blocking, the possible public interest variations within the EU and the regulatory cooperation frameworks, particularly in light of Google's standard delisting procedure. Furthermore, the research highlights the concerns about the varying levels of protection for EU citizens, contrasting the delisting procedure before the search engine operator and the formal proceedings involving data protection authorities and the courts. By exploring a significant decision by the Belgian DPA, the paper illustrates the possibilities for regulatory cooperation among the DPAs to achieve a cohesive and comprehensive approach to EU-wide delisting. The article advocates for regulatory transparency in this legal area and explicit guidance from the European Data Protection Board toward ensuring that the "right to be forgotten" is applied consistently and in a manner that genuinely protects individuals' rights across the EU.

Keywords: delisting; de-referencing; geo-blocking; geo-filtering; EU-wide delisting; EDPB

INTRODUCTION

The *Google Spain* judgment of the Court of Justice of the EU (CJEU) solidified the individuals' (data subjects') right to have the search engine operators cease displaying search results containing links to their specific personal data, which are considered inaccurate, inadequate, irrelevant, or excessive under EU data protection law.[1] This right to delisting[2], colloquially referred to as the 'right to be forgotten', focuses on blocking search results related to the data subject's name or surname, affecting name-specific queries while leaving unaffected

[1] C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, ECLI:EU:C:2014:317.

[2] The relevant case law of the CJEU mainly uses the term „de-referencing", see: C-507/17, *Google LLC v Commission nationale de l'informatique et des libertés – CNIL*, ECLI:EU:C:2019:772; C-136/17, *GC and Others v Commission nationale de l'informatique et des libertés (CNIL)*, ECLI:EU:C:2019:773; C-460/20, *TU, RE v Google LLC*, ECLI:EU:C:2022:962.

those using alternative keywords.[3] As such, this right does not entail the erasure of delisted data from third-party websites and search engine indexes.

Following the ruling the data subjects in the EU gained the ability to directly request delisting from search engine operators, prompting Google and other large operators to swiftly implement relevant procedures. However, the CJEU did not specify in Google Spain the manner in which the search engine operator should terminate inclusion of the links in search results.

Google, whose delisting practice is in focus of this paper, initially implemented delisting across all of the local versions of its search engine (delisting by reference to country code Top-Level Domains - ccTLDs, *i.e.*, "ccTLD-blocking", representing a "natural geographical delineation of the Internet"[4]), targeting the EU/EFTA Member States. Such a regional approach was implemented to ensure EU-wide consistency in line with Google Spain.[5]

However, disagreements emerged regarding the wider scope of delisting. While the data protection authorities grouped within the earlier Article 29 Data Protection Working Party[6] (currently the *European Data Protection Board* – EDPB[7]) advocated for global or universal delisting, which means delisting across all of Google (European and non-European) domain

---

[3] European Data Protection Board - EDPB, *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, July 7, 2020, pp. 5, 12 (points 8-9, 49), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201905_rtbfsearchengines_afterpublicconsultation_en.pdf (access 12.2.2024).

[4] D.J.B. Svantesson, *Delineating the Reach of Internet Intermediaries' Content Blocking – "ccTLD Blocking", "Strict Geo-location Blocking" or a "Country Lens Approach"?*, „SCRIPTed - A Journal of Law, Technology & Society" 2014, vol. 11(2), pp. 157, 161-162.

[5] In his paper, written prior to Google v CNIL, Padova argued that the merit of the regional approach lies in its alignment with the inherently European character of the right to delisting. Firstly, it emphasizes the European origin of the right, highlighting its foundational principles. Secondly, it is consistent with the interpretation by the CJEU that the right to delisting is not absolute. Lastly, the concept of a 'digital territory' for the application of the right to delisting matches the physical territory of the EU. This alignment fosters a strong sense of coherence by reconnecting the geographical location of individuals, their rights as inhabitants of this territory, and the operations of search engines within the same space. Y. Padova, *Is the right to be forgotten a universal, regional, or 'glocal' right?*, „International Data Privacy Law" 2019, vol. 9 (1), p. 26.

[6] The Working Party was established as an independent EU advisory entity concerning data protection and privacy matters. For more, see Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, November 23, 1995, Article 29-30.

[7] With the entry into application of the General Data Protection Regulation (GDPR) on May 25, 2018, the European Data Protection Board (EDPB) replaced the Article 29 Working Party. See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, May 4, 2016; Corrigendum, OJ L 127, May 23, 2018, Article 94, paragraph 2 and Chapter VII, section III.

versions, including "google.com", Google together with its Advisory Council contested such interpretation.

Importantly, an expert consulted by the Advisory Council noted the prospective use of technology to identify the relevant search queries conducted from the EU territory and restrict access to disputed links in such cases. While at the time the Council dismissed this option due to concerns about setting precedents for repressive regimes and uncertainties regarding its efficacy[8], Google eventually did implement such enhanced delisting approach. Thus in March 2016 it voluntarily extended delisting also to any non-EU domain used for the search, but only when the search originated in the same European country where the request for delisting was granted. This new policy relies on geo-blocking technology, whereby users' geolocation data (IP addresses) are utilized to restrict access to delisted content across all domain versions of the search engine.[9]

On a regulatory horizon the disagreement over the territorial scope of delisting escalated in the proceedings against Google in France, in which the French data protection authority (*Commission nationale de l'informatique et des libertés* – CNIL) ordered delisting across all domain versions, leading to a dispute. Despite acknowledging the potential enhancement brought by the new policy (geo-blocking), the CNIL deemed it incomplete. The concern remained that delisted information could still be accessed by any user located outside the region affected by geo-filtering. Additionally, it highlighted the persisting possibility for users to bypass this measure, citing methods such as proxy servers, VPNs, or ToR to mask their EU location (IP address).[10] By way of illustration, Google's territorial delisting policy that has been in effect up until today shows that after delisting across all EU domains and with geo-blocking as explained, the links to delisted data of a person residing e.g. in Croatia, such as their outdated news article or online dating profile[11], would still remain visible to: a) friends and business

[8] The Advisory Council to Google on the Right to be Forgotten, *Report*, February 6, 2015, p. 20, including note with the expert opinion of H. Hijmans, https://static.googleusercontent.com/media/archive.google/en//advisorycouncil/advisement/advisory-report.pdf (access: 2.2.2024). Also see: N. Gumzej, *Technical Solutions Supporting the Online RTBF in the CJEU and ECHR Jurisprudence*, „2023 46th MIPRO ICT and Electronics Convention (MIPRO)" 2023, p. 1468.

[9] The policy was applied also retroactively to all previous delistings under Google Spain. P. Fleischer, *Adapting our approach to the European right to be forgotten*, March 4, 2016, https://blog.google/topics/google-europe/adapting-our-approach-to-european-rig/ (access: 2.2.2024).

[10] Commission Nationale de l'Informatique et des Libertés - CNIL, *Deliberation 2016-054*, March 10, 2016, https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000032291946/ (access: 2.2.2024).

[11] See CNIL's infographic at: *Scope of M. PLAINTIFF's right to be delisted according to Google,* March 24, 2016, https://www.cnil.fr/en/infographic-scope-m-plaintiffs-right-be-delisted-according-google (access: 2.2.2024).

contacts outside the EU, b) friends and business contacts in other EU Member States using non-EU domain versions (e.g., "google.com"), and c) friends and business contacts in Croatia using non-EU domain versions and masking their location by using VPN or other techniques.

The dispute between Google and CNIL led to a preliminary reference procedure before the CJEU and the subsequent *Google v CNIL* ruling.[12] Despite the complexity of the issues, the brief dispositif in Google v CNIL provided that the EU law does not mandate global delisting, but rather delisting across versions corresponding to EU Member States. Additionally, the CJEU pointed to possible measures to prevent the circumventions of delisting, emphasizing their legal compliance and effectiveness in preventing or at minimum discouraging users from accessing delisted content while conducting a search from one of the Member States.

The ruling's ambiguity[13], addressed as the "judgment of Solomon"[14] or even "Pilate's decision"[15] sparked extensive academic discourse. Commentators expressed concerns over potential fragmentation of EU data protection law, undermining intentions of the general Data Protection Regulation (GDPR), and highlighted the legal uncertainty it brings.[16] Scholars like Gstrein warned of diverse interpretations by different data protection authorities and the courts, challenging the GDPR harmonization goals. Moreover, questions arose regarding how the CJEU would convey the varying territorial scope of implementation to EU data subjects, ranging from global delisting to 'glocal'[17] delisting using geo-blocking technology or exclusively national delisting.[18]

Despite concerns, early commentators such as Globocnik expressed optimism, highlighting collaborative efforts, uniformity, and supplementary GDPR mechanisms as

---

[12] C-507/17, *Google LLC v Commission nationale de l'informatique et des libertés – CNIL*, ECLI:EU:C:2019:772 (Google v CNIL).

[13] E. Bougiakiotis, *One Law to Rule Them All? The Reach of EU Data Protection Law after the Google v CNIL Case (August 17, 2020)*, „Computer Law and Security Review" 2021, vol. 42.

[14] M. Bartolomé, *Google v. CNIL and the Right to Be Forgotten: A Judgment of Solomon*, "Global Privacy Law Review" 2020, vol. 1 (1), pp. 61–62.

[15] G. Frosio, *Enforcement of European Rights on a Global Scale*, [in:] *Routledge Handbook of European Copyright Law*, ed. E. Rosati, Routledge 2021, p. 17.

[16] See e.g. M. Samonte, *Google v. CNIL: A Commentary on the Territorial Scope of the Right to Be Forgotten*, „European Papers" 2019, vol. 4 (3), pp. 847-850.

[17] For the expression in the context of delisting, see: Padova, op.cit., pp. 18, 26-27.

[18] O. J. Gstrein, *Right to be forgotten: European data imperialism, national privilege, or universal human right?*, „Review of European Administrative Law" 2020, vol. 13 (1), p. 136. Also see: O. J. Gstrein, *The Judgment That Will Be Forgotten: How the ECJ Missed an Opportunity in Google vs CNIL (C-507/17)*, „VerfBlog" 2019.

potential remedies against arbitrary law application.[19] However, the lack of concentrated efforts in that direction particularly by the European DPAs, nearly five years post-Google v CNIL and almost a decade post-Google Spain, is troubling. While delisting requests against Google have surged[20], discussions on specific measures and technologies such as geo-blocking, implementation details, and associated circumvention concerns at the EDPB level remain lacking, which indicates a concerning gap in addressing critical issues.[21]

While scholarly attention largely gravitates towards the debate on regional v. global delisting under EU law, this paper scrutinizes Google v CNIL concerning the conditions and methods of EU-wide delisting in light of the preliminary reference questions posed by the French court. The focus lies in the intricate analysis absent from the dispositif, which leaves many complexities to the evaluation of the national data protection authorities (DPAs) and the courts, and, concerningly, to the solely discretion of the search engine operators. Nuanced analyses absent from the dispositif address the crucial aspects in defining the territorial scope such as the role of geo-blocking, the possible public interest variations within the EU and the regulatory cooperation frameworks, particularly in light of Google's standard delisting procedure. Furthermore, the research highlights the concerns about the varying levels of protection for EU citizens, contrasting the delisting procedure before the search engine operator and the formal proceedings involving data protection authorities and the courts.

THE NUANCES OF EU DELISTING ACCORDING TO GOOGLE V CNIL

1. The principle of EU-wide domain-based delisting

In addressing the first question regarding the extension of delisting measures across all domain versions of the search engine, the CJEU affirmed the absence of a mandate for global delisting under EU law. This stance stems from the recognition that many third-party states diverge in their approach to such regulations. Moreover, it reflects the nuanced interplay

[19] J. Globocnik, *The Right to Be Forgotten is Taking Shape: CJEU Judgments in GC and Others (C-136/17) and Google v CNIL (C-507/17)*, „GRUR International" 2020, vol. 69 (4).
[20] See: Google, *Google Transparency Report - Requests to delist content under European privacy law*, https://transparencyreport.google.com/eu-privacy (access 2.2.2024).
[21] Gumzej, op. cit., p. 1469. The only guidelines issued by the EDPB so far - but which do not address these concerns, are its Guidelines 5/2019, op. cit.

between the right to data protection, which is not universally absolute, and the concurrent imperative to uphold the freedom of information for internet users, which balance may vary on a global scale.[22]

As explained in the Introduction, in focus of this paper is the Court's analysis concerning EU-wide delisting, addressing the two subsequent preliminary reference questions. The second question pertained to whether the right to delisting, as established in the *Google Spain* and interpreted under EU law (currently the GDPR), obliges the operator to implement delisting solely for the searches conducted on the search engine version corresponding to the EU Member State where the delisting request originated, or more broadly across all EU versions of the search engine. For instance, if a Croatian citizen's delisting request is granted, should the links be suppressed only for searches conducted on the "google.hr" domain, or should it extend to searches on all EU search engine versions (e.g., google.pl, google.es, google.at).

In its response, the CJEU initially affirmed that delisting is generally anticipated to apply to all EU Member States, which is a position it also echoed in the dispositif. Although the focus remains on domain-specific delisting, the approach advocating for delisting across the entire EU aligns with the objective of maintaining a consistent and robust level of personal data protection across the EU, as mandated by the directly applicable GDPR.[23] However, as demonstrated in the following section, the detailed elaborations of the Court in the body of the judgment introduce a significant layer of complexity to the matter.

2. Shaking up the EU domain-based delisting principle: geo-blocking, place of search-based delisting, and the varying public interest shift

2.1. Using geo-location data to localize EU search versions and implement geo-blocking

In order to fully grasp the importance of the posed third preliminary question for resolving the scope of delisting issue it is first necessary to point to Google's localization practice and approach to delisting, which involves geo-blocking. Both practices address the

[22] Google v CNIL, points 53-65.
[23] Google v CNIL, point 66.

attempted circumventions to the domain-based delisting and rely on the user's location when carrying out the relevant search.[24]

Firstly, Google automatically redirects the searches originating in the EU to the relevant local domain of its search engine. In other words, the users are redirected to the country version of its search engine on the basis of their location, regardless of the domain they enter (e.g. "google.com").[25] Next, as noted in the Introduction, due to possibilities of overriding such redirections and masking or hiding the IP addresses associated with the search origin, in March 2016 Google voluntarily implemented in addition to delisting across all European domains also the practice of blocking access to delisted content on any of its domains used for relevant searches, including the widely popular "google.com" domain.

While the situation makes it clear that the country code domain name is not the sole suitable territorial link to the EU, especially since ".com" domain is utilized by users throughout the EU[26], such Google's practice only affects the searches originating in the EU State of residence of the successful requesting party. In other words, geo-blocking is not applied in cases of searches by users located in all other EU countries, where they are using any non-EU domain for that search.[27]

Compared to solely EU domain-based delisting, the geo-blocking practice introduced by Google increases the protection of the person requesting delisting, and its initiative to do so should be commended. For instance, if a friend, relative, or business contact located in the same EU Member State conducts a search using a non-EU domain like "google.com", bypassing Google's automatic redirection to the local search engine domain, they could easily retrieve the

[24] The CJEU was duly aware of both. Google v CNIL, points 32 and 42.
[25] In connection with this, see: E. Kao, *Google Blog - Making search results more local and relevant*, October 27, 2017, https://www.blog.google/products/search/making-search-results-more-local-and-relevant/ (access 2.2.2024).
[26] J. H[illegible]le, *Internet Jurisdiction: Law and Practice*, New York 2021, p. 251.
[27] (1) „For example, in the European Union we delist URLs from versions of Google's search results for countries applying European data protection law. We'll also use geolocation signals (like IP addresses) to restrict access to the delisted URL on all Google Search services for users we think are in the requester's country." Google, *Legal Help, Right to be Forgotten Overview*, https://support.google.com/legal/answer/10769224?hl=en (access 2.2.2024). (2) "We delist URLs from all European Google Search domains (google.fr, google.de, google.es, etc.) and use geolocation signals to restrict access to the URL from the country of the person requesting the removal. For example, let's say we delist a URL as a result of a request from John Smith in the United Kingdom. Users in the UK would not see the URL in search results for queries containing [john smith] when searching on *any* Google Search domain, including google.com. Users outside of the UK could see the URL in search results when they search for [john smith] on any *non-European* Google Search domain." Google, *European privacy requests Search removals FAQs*, https://support.google.com/transparencyreport/answer/7347822?hl=en (access 2.2.2024).

delisted data. Conversely, individuals conducting the same search using the local version of the search engine would not have access to delisted content.

However, Google's approach may still raise concerns of incomplete and ineffective protection from the data protection law perspective. Commentators such as Taylor argue that while the current territorial delisting implementation by Google is not unreasonable (since there are connections between Google's activities, EU territory and the EU residents), it is not sufficient since the rights of data subjects according to EU law are not sufficiently protected, taking into account the easy circumvention and especially since the rights of the data subjects are not protected EU-wide.[28]

Both these approaches to delisting, which are based on the users' search location, were presented to the Court as additional measures to EU domain-based delisting.

2.2. The convoluted perspective on the place-of-search based delisting

With the noted Google' practices in mind, which acknowledged the fact that domain-specific restrictions can be bypassed, the third preliminary question sought clarity on whether as an adjunct to EU domain-based delisting, delisting should extend to all versions of the search engine based on the location of the search in the EU, through measures such as geo-blocking, either according to the location of the successful delisting applicant (as then and nowadays still implemented by Google through geo-blocking) or even wider, across the entire EU territory.

Even though the issue of geo-blocking is essential to the question of territorial limitations and variations in delisting[29], the Court's discussion of the relevant third preliminary question was minimal and without reference to Google's geo-blocking practice.[30] While

[28] M. Taylor, *Transatlantic Jurisdictional Conflicts in Data Protection Law. Fundamental rights, privacy and extraterritoriality*, Cambridge 2023, pp. 183-185.
[29] S. Wrigley, A. Klinefelter, *Google LLC v. CNIL: The Location-Based Limits of the EU Right to Erasure and Lessons for U.S. Privacy Law*, „North Carolina Journal of Law and Technology" 2021, vol. 22 (4), p. 71.
[30] For criticisms of the Court's lacking regard of technological possibilities of geo-blocking, see e.g.: J. Quinn, *Geo-location technology: restricting access to online content without illegitimate extraterritorial effects*, "International Data Privacy Law" 2021, vol. 11 (3), pp. 305-306. Also see analysis by della Valle, who argues that the Court failed to sufficiently consider technological aspects and inappropriately burdened Google with the sole responsibility of implementing the 'sufficiently effective measures', while "being totally disinterested in the technical feasibility of protecting the right to be forgotten thus configured and not taking into consideration the easy circumvention that could derive from it." The Court's lack of engagement with the more technical details is evident primarily through its notable omission in addressing the third question, showing no concern to specify

acknowledging the need for a technologically neutral approach[31], the Court has not at minimum recognized, in comparison to its previously proclaimed principle of EU domain-based delisting, the impact that any such technologically enabled delisting might have on the goal of the complete and effective protection of data subjects under EU law.[32] In any case, a structured discussion on the third preliminary question would have been beneficial for legal clarity and certainty reasons.[33]

The approach of the Advocate General in his Opinion was easier to follow in terms of structure and focus on the preliminary reference questions posed. That analysis relied significantly on the noted Google's policies of automated redirections and geo-blocking practice. If properly implemented, and in line with the law, the AG considered such practice would render the issue of domain-based delisting obsolete.[34] In other words, the focus is not on the domains on which delisting is implemented, but on the *place from which the search is carried out*. Consequently, along the lines also of the CJEU's justification of the domain-based delisting as a principle under EU law, the AG opined that any user making the relevant search in the EU should not access delisted information regardless of the domain used for the search. In order for that to happen, the operator must be *obliged* to ensure effective and complete delisting for all relevant name-based searches originating in the EU. In accordance with the case at hand, and the relevant third preliminary question, such ensuring of effective and complete delisting for all searches made in the EU presupposes the operator's *mandatory* use of geo-blocking measures, in line with the law.[35]

The pathway toward recognizing the place of search-based delisting principle was far more convoluted in the CJEU's ruling. Its formation began with the Court's relativization of the previously proclaimed EU-domain-based delisting principle.

---

whether the use of geo-blocking technique is necessary or adequate for ensuring the intended protection. A. Iannotti della Valle, *The (In)Adequacy of the Law to New Technologies: The Example of the Google/CNIL and Facebook Cases before the Court of Justice of the European Union*, "European Journal of Privacy Law & Technologies (EJPLT)" 2020, vol. 2020 (2), p. 178.

[31] Globocnik, op. cit., p. 385.

[32] See Google v CNIL, point 39 (questions 2 and 3).

[33] Court decided to address all questions jointly. Google v CNIL, point 43.

[34] Opinion of Advocate General Szpunar delivered on 10 January 2019, Case C-507/17, ECLI:EU:C:2019:15, point 72.

[35] *Ibidem*, points 70-78.

The relativization was initiated by a recognized absence of comprehensive harmonization under EU law in reconciling the balance between the data protection and the freedom of information rights.[36] This stems from the potential conflict between divergent public interests in various EU Member States seeking access to pertinent information (via a search engine and a very narrow name-based search query). Though, as Hörnle rightfully commented, with this the clarity of the judgment was diminished[37], the CJEU underscored the imperative for balancing these competing rights and interests even in the context of the otherwise rather limited right to delisting.[38]

In light of this, the CJEU directed attention to the cooperation and consistency instruments and mechanisms provided under the GDPR, and emphasized the practical application of these mechanisms in reconciling data protection and freedom of information rights across the EU Member States. According to the CJEU, that procedure could result in a delisting decision of the DPAs, which would cover all relevant name-based searches that are carried out *from the EU territory*.[39]

As observed, despite its previously proclaimed principle of EU domain-based delisting, it is here that the Court makes its first reference to the *EU place of search criterion* for delisting that covers all searches from the EU territory. Thereby it indicates, on one hand, that the geographical location from which the searches are conducted within the EU may well play a crucial role in determining the scope of delisting. On the other hand, determination of such a wider scope according to the Court appears possible only following prior coordination of the DPAs, due to possible public interest variations throughout the EU.

Importantly, most of these vital arguments remain absent from the dispositif.

---

[36] Google v CNIL, point 67. See Article 85 GDPR as well as Art 17(3)(a) GDPR, which both leave it to the Member States to reconcile the right to data protection with the right to freedom of expression and information. H. Kranenborg, *Article 17. Right to erasure ('right to be forgotten')*, [in:] *The EU General Data Protection Regulation: A Commentary*, eds. C. Kuner, L. A. Bygrave, C. Docksey, New York 2020, p. 481.

[37] Hörnle, op. cit., p. 252.

[38] The freedom of information for internet users is here exemplified through the ease with which they can obtain pertinent data about the data subject by entering their name in a search engine. This data remains easily accessible to internet users using alternative search terms and is not removed from its original source of publication.

[39] Google v CNIL, points 68-69. Also see Chapter VII of the GDPR. As Streinz notes, similar mechanisms are absent in other areas of EU data law, which opens the door to specific decisions by national courts that impact the accessibility of delisted content also within the EU. T. Streinz, *The Evolution of European Data Law*, [in:] *The Evolution of EU Law*, eds. P. Craig, G. de Búrca, New York 2021, pp. 925-926.

3. A critique of the Court's approach to EU-wide delisting

The Court's approach to EU-wide delisting should be criticized.

Firstly, it is because by logic of its own determination on the possibly diverging public interest throughout the EU to access delisted information, determination of both the EU domain-based and place of search-based delisting as supported by geo-blocking, should be preceded by a prior analysis of potential public interest variations in individual Member States. To be precise, there is no difference as regards the scope of intrusion that the delisting might have on the users' freedom of information in the cases of domain-based and place of search-based delisting (including geo-blocking). Affected search engine users are in both cases the users who are carrying out relevant searches in the territory of the EU, as identified by Google on the basis of geolocation data.

As a result, same procedural requirements noted by the Court for ordering delisting on the basis of the location data of search users throughout the EU as the EU(-wide) domain-based delisting would then be required, i.e. employment of the cooperation mechanism under the GDPR in cases of doubt on the varying public interest to access delisted information throughout the EU.

Thus a delisting decision based on a harmonized approach of the European DPAs would appear to be a prerequisite for implementing EU-wide delisting even in the cases, as argued previously in the paper, where the more restricted delisting in scope is concerned, such as that limited to European domains.

This also means that where the collaborative regulatory process under the GDPR is not initiated following a delisting request, the level of protection of users' rights throughout the EU as affected by an EU-wide delisting decision may significantly vary. Of course, the DPAs could also decide that the delisting takes place in only one of several Member States (e.g. if there is a substantially higher interest to access relevant information in some Member States).[40]

In light of the preceding analysis it is difficult to understand why the Court left out from the dispositif the vital considerations on the balancing of data protection and privacy rights with

[40] Globocnik, op. cit., p. 386.

the interest of the EU public and the related possibility of DPA decisions. This is also taking into account the fact that these concerns directly relate to the posed preliminary reference questions and may affect interpretations of EU domain-based delisting as a principle under EU law.

Secondly, though ensuring, on one hand, the easy and quick access of individuals to delisting requests and procedure, which resulted in a streamlined procedure before the search engine operators themselves, the CJEU appears to have disregarded the unintended consequences of the possibly varying level of protection depending on the choice and ability of such individuals to take action against the operator's decision, thereby involving the DPAs and ultimately the courts in the decision-making process. Specifically, a private company such as Google cannot itself be entrusted with the assessment of the complex public interest considerations and nuances throughout the Member States that the Court highlighted in the body of its judgment. Thus there is no comparable procedure in the assessment of public interest variations where the search engine operator is the sole venue for the delisting decision without further involvement of the DPAs and the courts (i.e. upon a legal remedy against the operator's delisting decision).

Thirdly, it is the premise of this paper that the proper addressal of circumventions is what ultimately defines the scope of delisting. Thus a delisting order that covers *all relevant searches from the EU territory* implies the mandatory use of technical measures such as geo-blocking for any IP address used for the search within the EU, regardless of the domain on which the search was conducted. In other words, as Globocnik argued already early, effective *EU-wide delisting* may only be ensured by a standard application of geo-blocking measures.[41]

However, while advocating for a technologically neutral approach, the Court entrusted the assessment of measures to address circumventions to the DPAs and ultimately the courts, in terms of both the legality and purpose. Critically, where regulatory authorities and the courts are not involved, it left these issues and therefore determination of the scope of implementation to the sole discretion the search engine operator. Simultaneously, the Court recognized the significance of the aim in determining the scope of delisting based on the users' search location.

[41] *Ibidem*; Wrigley, op. cit., p. 716.

EU-WIDE DELISTING ORDER: CASE EXAMPLE

The Belgian DPA's decision from 2020 provides a rarely thorough, publicly available analysis of the conditions for EU-wide delisting, which also focuses on the important issues of discerning between, and combining the domain-based and place of search (geo-blocking) delisting approaches.[42] Though the decision was subsequently annulled by the Brussels Court of Appeal for lacking explanation on DPA's jurisdiction over Google Belgium (instead of Google LLC), the DPA's assessment of the conditions for the issuing of an EU delisting orders that include the delisting from non-EU domains for data subjects in the EU, was itself not subject to examination by the Court.[43]

According to the Belgian DPA, the purpose of consulting other DPAs is to consider the public interest in other Member States regarding access to delisted content. This is relevant when deciding on delisting across all Google domain names (e.g., "google.be", "google.fr", "google.de") and European residents. In cases of more restricted delisting, such as limiting it to Google's top-level Belgian domain name (".be") and implementing geo-blocking for Belgian users, residents of other Member States would still have access to delisted content. Other situations may arise where collaboration with only two authorities could be satisfactory. For instance, if a request for delisting pertained to only two Google country extensions (e.g. ".fr" and ".lu"), and included geo-blocking measures for residents of these nations, the consultation process would entail reaching out solely to the authorities of those particular countries.[44]

In light of the lacking clarity and a more general determination in Google's Privacy Policy on determination of the relevant data controller (generally)[45], the DPA's finding on the

[42] Litigation Chamber (Chambre Contentieuse), Decision on the merits 37/2020 of July 14, 2020, Case no.: DOS-2019-03780, https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-37-2020-eng.pdf (access 2.2.2024).

[43] Cour d'Appel Bruxelles, 2020/AR/1111, June 30, 2021, https://www.gegevensbeschermingsautoriteit.be/publications/arrest-van-30-juni-2021-van-het-marktenhof-ar-1111-beschikbaar-in-het-frans.pdf (access 2.2.2024).

[44] Litigation Chamber, op. cit., point 87 and footnote 44.

[45] It is only with the amendment of its Privacy Policy on July 1, 2021 that Google transparently declared Google LLC (based in California, USA) as the data controller responsible for processing information indexed and displayed in Google Search services regardless of the data subject's location. See: *Google Privacy Policy*, *European requirements – Data controller*, https://policies.google.com/privacy (access 2.2.2024) - compare to earlier versions. Also see the adjusted data removal request form: *Personal Data Removal Request Form*,

inapplicability of the one-stop-shop mechanism in that case is here not discussed in detail.[46] In absence of such mechanisms, the DPA relied on Article 61 of the GDPR to carry out informal consultations with the other DPAs on the scope of territorial delisting in its intended delisting decision. Thus it viewed their feedback as the needed procedural requirement toward its ordering of the EU domain-based and EU-wide place of search-based (i.e. geo-blocking) delisting measures.[47]

Taking into account that the large majority of DPAs responded in agreement to the DPA's intended EU-wide delisting decision, and its view that delisting cannot be effective if it also does not apply to searches performed outside of Belgium[48], the DPA ordered the search engine operator to „implement any effective technical solutions required to remove search listings (…), for all the search engine's websites in every language, but only for users visiting them from the European Economic Area (…).[49]

Consequently, here the DPA established here that the territorial scope of delisting should extend to all of the EU/EEA member countries. That decision is based on the recognition that searches conducted from locations beyond Belgium, whether physically or via a proxy server accessing alternative search engine versions, could potentially present a substantial risk to the data protection rights of the person seeking delisting. The DPA found it entirely plausible that within the context of that person's professional activities they might have connections in other European countries, especially those neighbouring Belgium. Individuals in these regions may seek information about the data subject using Google versions specific to their countries, rather

---

https://reportcontent.google.com/forms/rtbf?visit_id=638253262036290912-1897396507&hl=en&rd=1 (access 2.2.2024).

[46] A recent digest covering one-stop-shop cases under the GDPR shows that the DPAs have issued relatively few decisions under the cooperation mechanism of Article 60 of the GDPR which likely stems from the fact that the majority of such cases are processed as local matters. A. Mantelero, *One-stop-shop thematic case digest: right to object and eight to erasure*, December 9, 2019, p. 5, https://edpb.europa.eu/system/files/2023-02/one-stop-shop_case_digest_on_the_right_to_object_and_right_to_erasure_en.pdf (access 2.2.2024).

[47] Litigation Chamber, op. cit., point 89.

[48] „In a borderless Europe, it would be futile to order that the delisting apply only to searches performed from Belgian IP addresses." Litigation Chamber, op. cit., point 90.

[49] Litigation Chamber, op. cit., operative part of the decision: item 2.

than the Belgian one (".be"). Given this scenario, restricting the delisting to Belgium alone would lack efficacy.[50]

This case exemplifies the potential for effective regulatory cooperation among the European DPAs, which leads to a genuinely comprehensive EU-wide delisting order. Such cooperation, as demonstrated by the Belgian DPA's initiative, transcends the mere domain-based delisting to include geo-blocking measures based on the searcher's location within the entire EU/EEA territory. Despite the annulment of the DPA's decision by the Brussels Court of Appeal due to jurisdictional issues, the collaborative approach towards considering the varying public interest across Member States highlights a path forward for achieving a balance between the right to data protection and the freedom of information. The positive response from the majority of DPAs to the proposed EU-wide delisting approach reinforces the feasibility of broader geo-blocking measures than those, which are currently standard in Google's practice.

CONCLUDING REMARKS

According to some authors it is because of the possible overriding of geo-filtering, particularly the advancement and easy of use of technologies such as the VPN, that the right to delisting is in fact an impossible right[51] and for others this may justify the approach towards global delisting.[52] While possible solutions to avoid the localization circumventions are being discussed in literature[53], geo-blocking (or other relevant technological measures) must according to the CJEU only be *sufficiently effective*[54] to prevent or at least seriously discourage internet users in the Member States from accessing delisted content. As argued in this paper, it is the geo-blocking based on the IP location of users across the EU, regardless of the domain

[50] Litigation Chamber, op. cit., point 91.
[51] J. Friesen, *The impossible right to be forgotten*, „Rutgers Computer and Technology Law Journal" 2021, vol. 47 (1), pp. 192-196.
[52] K. Carrara, *The Right to Be "almost" Forgotten. What are the limits of a territorial interpretation of data protection*, Tilburg University, LL.M.thesis, 2020/2021, http://arno.uvt.nl/show.cgi?fid=154901 (access 2.2.2024). Also see: P.T.J. Wolters, *The territorial effect of the right to be forgotten after Google v CNIL*, „International Journal of Law and Information Technology" 2021, volume 29 (1), p. 69.
[53] See D. Erdos, *Search engines, global internet publication and European data protection: a new via media?*, „The Cambridge Law Journal" 2020, vol. 79 (1), pp. 26-27. Additionally, see Wolters, op. cit., pp. 70-71.
[54] Wolters, op. cit., p. 70.

used for the search, which directly addresses the issue of accessibility of delisted content by EU residents. Coupled with EU domain-based delisting, such a place-of-search based delisting, which acknowledges the technical realities of overriding automated redirections to local versions of the search engine and the use of VPN and other technologies to hide one's location, entails a wider and therefore more effective and complete scope of protection for the data subject in terms of EU data protection law.

At the same time there should be no difference in the *Google v CNIL* requirement to assess the balance between public interest in accessing information and the protection of personal data rights, whether delisting is applied across all EU domains or across all domains based on searches originating within any EU Member State. Affected search engine users are in all cases the users who are carrying out relevant searches within the EU, as identified by Google on the basis of geolocation data. Consequently, delisting on the basis of EU domains as a proclaimed principle under EU law in Google v CNIL should apply also to extended delisting on the basis of location of search users in the EU. As Birnhack noted, "geolocation is an important tool in applying the legal decision, but it is only a tool at the service of the law".[55] Thus in both scenarios, the fundamental considerations remain consistent. The distinction lies in the technical implementation and scope of the delisting, not in the underlying legal and ethical principles.

While focusing on domain-based delisting, the CJEU appears to have implicitly relied on the search engine's mechanism of automated redirections to the local EU versions, which would suffice to prevent access to delisted information by EU residents. However, this presumption does not consider potential circumventions, which compromise the effectiveness of delisting, but which considerations were at the heart of the third preliminary question posed. The Court's approach can be critiqued for not providing a clear reply to the third preliminary question as regards the implementation of measures, additionally to EU domain-based delisting, according to which access to delisted data would be restricted, based on the search origin being the data subject's Member State or any EU Member State, regardless of the domain version consulted. Furthermore, the absence in the dispositif of vital concerns regarding the possibly

[55] M. Birnhack, *Symposium: The Glocal Net: Standing on Joel Reidenberg's Shoulders*, „Fordham Law Review" 2022, vol. 90 (4), pp. 1453-1454.

varying public interest and regulatory cooperation under the GDPR might suggest an assumption that the EU domain-based delisting could uniformly address the GDPR's objectives without necessitating a nuanced analysis of public interest variations.

In consequence, but particularly on account of lacking harmonized approach and guidance at the regulatory (EDPB) level even up until today, Google's delisting practice as voluntarily extended by geo-blocking as of 2016, remains standard. Paradoxically, while acknowledging domain-based delisting limitations and aiming to provide a harmonized level of data protection for EU data subjects, Google's delisting practice appears to *exceed Google v CNIL*. At the same time, the approach still fails to take into account that disabled access to delisted data on any domain used for the search, where the search originates only in the data subject's Member State is largely pointless for most data subjects and falls short of ensuring the complete and effective data protection under the GDPR.

Google's practice raises the question of whether and how it incorporates Google v CNIL nuances into its delisting decisions, especially in the absence of explicit guidance or a coordinated mechanism among the EU data protection authorities. In particular, it raises questions about the capacity of a private entity to independently assess and balance public interest considerations across diverse legal jurisdictions without direct coordination with the DPAs. The absence of explicit guidance on addressing public interest variations and the reliance on the cooperation and consistency mechanism among the EU data protection authorities under the GDPR, therefore, highlight a critical gap where search engine operators act as the sole venue for delisting requests.

The Belgian Data Protection Authority's (DPA) decision illustrates a successful instance of regulatory cooperation leading to an EU-wide delisting order that encompasses not just EU search domains but also takes into account the searcher's location within the entire EU. This case accentuates the potential for a substantive evaluation process and agreement on broader geo-blocking measures than Google's current standard practice, offering a more complete protection of data subjects' rights without unduly compromising the freedom of information. This offers a model for more comprehensive protection but also indicates that wider protection might require DPA involvement, challenging Google's standard practice.

On the other hand, employment of DPA cooperation mechanisms for each and every EU delisting is not sustainable in light of the immense burden that this would impose on the DPAs and the courts. That is a concern possibly reciprocating the reasons behind the delegated decision-making authority under Google Spain to the large search engines.[56] Consequently, the nuances of Google v CNIL, Google's implementation of delisting requests and the need for ensuring a more complete and effective data protection in the EU emphasizes the need for further dialogue between search engine operators, DPAs, policymakers, and stakeholders. This dialogue should aim to refine the balance between privacy protection and freedom of information, ensuring that delisting practices are transparent[57], consistent, and adequately responsive to the varying legal, cultural, and public interest contexts within the EU. At minimum clear guidelines by the European Data Protection Board (EDPB) should help the search engine operators navigate these complexities more effectively, ensuring a more consistent and legally compliant approach across the EU.

At the same time, DPA's decisions, participation in pertinent legal proceedings as needed and their other relevant activities in this legal area require proper monitoring. A comparative overview shows insufficient regulatory coverage in this area, with certain exceptions[58]. It is imperative that the DPAs make these decisions and their accompanying guidance accessible and transparent to both the general public and the academic community. This need becomes particularly urgent in light of the CJEU's approach, which left most of the implementation requirements to the national DPAs and the courts. Without such transparency and active engagement, the "complete and effective" protection of individuals' data protection

[56] R. A. Hulvey - Carr Center for Human Rights Policy, Harvard Kennedy School - Harvard University, *Companies Courts? Google's Role Deciding Digital Human Rights Outcomes in the Right to be Forgotten*, 2022, p. 10, https://carrcenter.hks.harvard.edu/files/cchr/files/22_hulvey_companies-as-courts.pdf (access 2.2.2024). As Obedniek notes, the disparity in financial resources and administrative limitations perpetuates a situation in which blic actors acquiesce to the implementation and regulatory influence exerted by tech companies. A. S. Obendiek, *The Right to Be Forgotten: Moral Hierarchies of Fairness*, [in:] *Data Governance: Value Orders and Jurisdictional Conflicts*, Oxford 2022, p. 191.

[57] For earlier calls to Google for greater transparency on the substantive criteria used for delisting decisions snd developments, see: J. ss, *Dear Google: open letter from 80 academics on 'right to be forgotten'*, „The Guardian", May 14, 2015, https://www.theguardian.com/technol 2015/may/14/dear-google-open-letter-from-80-academics-on-right-to-be-forgotten (access 2.2.2024); M. Smith, *Updating our "right to be forgotten" Transparency Report*, „Google Blog", https://blog.google/around-the-globe/goog urope/updating-our-right-be-forgotten-transparency-report/, February 26, 2018 (access 2.2.2024); T. Bertram *et al*, *Five Years of the Right to be Forgotten*, „Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security" 20 pp. 959-972..

See e.g. Agencia Española de Protección de Datos (AEPD), *Memoria Annual 2022*, pp. 42 *et seq*., https://www.aepd.es/documento/memoria-aepd-2022.pdf (access 2.2.2024).

rights across Member States risks being inconsistent. This inconsistency does not only depend on the individuals' choice of legal recourse against Google's decisions but also on the capacities and research skills of their DPAs and the judiciary, which are navigating this relatively new legal area.

REFERENCES

LITERATURE

Bartolomé, M., *Google v. CNIL and the Right to Be Forgotten: A Judgment of Solomon*, "Global Privacy Law Review" 2020, vol. 1 (1), **DOI: https://doi.org/10.54648/gplr2020008**.

Bertram, T. *et al*, *Five Years of the Right to be Forgotten*, „Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security" 2019, **DOI: https://doi.org/10.1145/3319535.3354208**.

Birnhack, M., *Symposium: The Glocal Net: Standing on Joel Reidenberg's Shoulders*, „Fordham Law Review" 2022, vol. 90 (4).

Bougiakiotis, E., *One Law to Rule Them All? The Reach of EU Data Protection Law after the Google v CNIL Case (August 17, 2020)*, „Computer Law and Security Review" 2021, vol. 42, **DOI: https://doi.org/10.1016/j.clsr.2021.105580**.

Carrara, K., *The Right to Be "almost" Forgotten. What are the limits of a territorial interpretation of data protection*, Tilburg University, LL.M. thesis, 2020/2021, http://arno.uvt.nl/show.cgi?fid=154901 (access 2.2.2024).

Erdos, D., *Search engines, global internet publication and European data protection: a new via media?*, „The Cambridge Law Journal" 2020, vol. 79 (1), **DOI: https://doi.org/10.1017/S0008197320000197**.

Friesen, J., *The impossible right to be forgotten*, „Rutgers Computer and Technology Law Journal" 2021, vol. 47 (1).

Frosio, G., *Enforcement of European Rights on a Global Scale*, [in:] *Routledge Handbook of European Copyright Law*, ed. E. Rosati, Routledge 2021, **DOI: https://doi.org/10.2139/ssrn.3650521**.

Globocnik, J., *The Right to Be Forgotten is Taking Shape: CJEU Judgments in GC and Others (C-136/17) and Google v CNIL (C-507/17)*, „GRUR International" 2020, vol. 69 (4), **DOI: https://doi.org/10.1093/grurint/ikaa002.**

Gstrein, O. J., *Right to be forgotten: European data imperialism, national privilege, or universal human right?*, „Review of European Administrative Law" 2020, vol. 13 (1), **DOI: https://doi.org/10.7590/187479820X15881424928426**.

Gstrein, O. J., *The Judgment That Will Be Forgotten: How the ECJ Missed an Opportunity in Google vs CNIL (C-507/17)*, „VerfBlog" 2019, **DOI: https://doi.org/10.17176/20190925-232711-0**.

Gumzej, N., *Technical Solutions Supporting the Online RTBF in the CJEU and ECHR Jurisprudence*, „2023 46th MIPRO ICT and Electronics Convention (MIPRO)" 2023, **DOI: https://doi:10.23919/MIPRO57284.2023.10159696.MIPRO 2023**.

Hörnle, J., *Internet Jurisdiction: Law and Practice*, New York 2021, **DOI: https://doi.org/10.1093/oso/9780198806929.001.0001**.

Iannotti della Valle, A., *The (In)Adequacy of the Law to New Technologies: The Example of the Google/CNIL and Facebook Cases before the Court of Justice of the European Union*, "European Journal of Privacy Law & Technologies (EJPLT)" 2020, vol. 2020 (2).

Kranenborg, H., *Article 17. Right to erasure ('right to be forgotten')*, [in:] *The EU General Data Protection Regulation: A Commentary*, eds. C. Kuner, L. A. Bygrave, C. Docksey, New York 2020, **DOI: https://doi.org/10.1093/oso/9780198826491.003.0049.**

Obendiek, A. S., *The Right to Be Forgotten ... oral Hierarchies of Fairness*, [in:] *Data Governance: Value Orders and Jurisdictional Conflicts*, Oxford 2022, **DOI: https://doi.org/ 10.1093/oso/9780192870193.001.0001**.

Padova, Y., *... right to be forgotten a universal, regional, or 'glocal' right?*, „International Data Privacy Law" 2019, vol. 9 (1), **DOI: https://doi.org/10.1093/idpl/ipy025**.

Quinn, J., *Geo-location technology: rest... access to online content without illegitimate extraterritorial effects*, "International Data Privacy Law" 2021, vol. 11 (3), **DOI: https://doi.org/10.1093/idpl/ipab016**.

Samonte, M., *Google v. CNIL: A Commentary on the Territorial Scope of the Right to Be Forgotten*, „European Papers" 2019, vol. 4 (3), **DOI: 10.15166/2499-8249/332**.

Streinz, T., *Evolution of European Data Law*, [in:] *The Evolution of EU Law*, eds. P. Craig, G. de Búrca, New York 2021, **DOI: https://doi.org/10.1093/oso/9780192846556.001.0001**.

Svantesson, Dan Jerker B., *Delineating the Reach of Internet Intermediaries' Content Blocking – "ccTLD Blocking", "Strict Geo-location Block..." or a "Country Lens Approach"?*, „SCRIPTed - A Journal of Law, Technology & Society" 2014, vol. 11(2), **DOI: https:// dx.doi.org/10.2966/scrip.110214.153**.

Taylor, M., *Transatlantic Jurisdictional Conflicts in Data Protection Law. Fundamental rights, privacy and extraterritoriality*, Cambridge 2023, **DOI: https://doi.org/10.1017/9781108784818**.

Wolters, P.T.J., *The territorial effect of the right to be f...otten after Google v CNIL*, „International Journal of Law and Information Technology" 2021, volume 29 (1), **DOI: https://doi.org/10.1093/ijlit/eaaa022**.

Wrigley, S., Klinefelter, A., *Google LLC v. CNIL: The Location-Based Limits of the EU Right to Erasure and Lessons for U.S. Privacy Law*, „North Carolina Journal of Law and Technology" 2021, vol. 22 (4).

LEGAL ACTS

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, November 23, 1995.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, May 4, 2016; Corrigendum, OJ L 127, May 23, 2018.

CASE LAW

C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, ECLI:EU:C:2014:317.

C-136/17, *GC and Others v Commission nationale de l'informatique et des libertés (CNIL)*, ECLI:EU:C:2019:773.

C-507/17, *Google LLC v Commission nationale de l'informatique et des libertés – CNIL*, ECLI:EU:C:2019:772.

C-460/20, *TU, RE v Google LLC*, ECLI:EU:C:2022:962.

Commission Nationale de l'Informatique et des Libertés - CNIL, *Deliberation 2016-054*, March 10, 2016, https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000032291946/ (access: 2.2.2024).

Cour d'Appel Bruxelles, 2020/AR/1111, June 30, 2021, https://www.gegevensbeschermingsautoriteit.be/publications/arrest-van-30-juni-2021-van-het-marktenhof-ar-1111-beschikbaar-in-het-frans.pdf (access 2.2.2024).

Litigation Cham (Chambre Contentieuse), Decision on the merits 37/2020 of July 14, 2020, Case no.: DOS-2019-03780, https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-37-2020-eng.pdf (access 2.2.2024).

Opinion of Advocate General Szpunar delivered on 10 January 2019, Case C-507/17, ECLI:EU:C:2019:15.

ONLINE SOURCES

Agencia Española de Protección de Datos (AEPD), *Memoria Annual 2022*, https://www.aepd.es/documento/memoria-aepd-2022.pdf (access 2.2.2024).

Commission Nationale de l'Informatique et des Libertés - CNIL, *Scope of M. PLAINTIFF's right to be delisted according to Google*, Ma 24, 2016, https://www.cnil.fr/en/infographic-scope-m-plaintiffs-right-be-delisted-according-google (access: 2.2.2024).

European Data Protection Board - EDPB, *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, July 7, 2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201905_rtbfsearchengines_afterpublicconsultation_en.pdf (access: 2.2.2024).

Fleischer, P., *Adapting our approach to the European right to be forgotten*, March 4, 2016, https://blog.google/topics/google-europe/adapting-our-approach-to-european-rig/ (access: 2.2.2024).

Google, *European privacy requests Search removals FAQs*, https://support.google.com/transparencyreport/answer/7347822?hl=en (access 2.2.2024).

Google, *Google Privacy Policy*, *European requirements – Data controller*, https://policies.google.com/privacy (access 2.2.2024).

Google, *Google Transparency Report - Requests to delist content under European privacy law*, https://transparencyreport.google.com/eu-privacy (access 2.2.2024).

Google, *Legal Help*, *Right to be Forgotten Overview*, https://support.google.com/legal/answer/10769224?hl=en (access 2.2.2024).

Google, *Personal Data Removal Request Form*, https://reportcontent.google.com/forms/rtbf?visit_id=638253262036290912-1897396507&hl=en&rd=1 (access 2.2.2024).

Hulvey, R. A. - arr Center for Human Rights Policy, Harvard Kennedy School - Harvard University, *Companies Courts? Google's Role Deciding Digital Human Rights Outcomes in the Right to be Forgotten*, 2022, https://carrcenter.hks.harvard.edu/files/cchr/files/22_hulvey_companies-as-courts.pdf (access 2.2.2024).

Kao, E., *Google Blog - Making search results more local and relevant*, October 27, 2017., https://www.blog.google/products/search/making-search-results-more-local-and-relevant/ (access 2.2.2024).

Kiss, J., *Dear Google: open letter from 80 academics on 'right to be forgotten'*, „The Guardian", May 14, 2015, https://www.theguardian.com/technology/2015/may/14/dear-google-open-letter-from-80-academics-on-right-to-be-forgotten (access 2.2.2024).

Mantelero, A., *One-stop-shop thematic case digest: right to object and eight to erasure*, December 9, 2022, https://edpb.europa.eu/system/files/2023-02/one-stop-shop_case_digest_on_the_right_to_object_and_right_to_erasure_en.pdf (access 2.2.2024).

Smith, M., *Updating our "right to be forgotten" Transparency Report,* „Google Blog", https://blog.google/around-the-globe/google-europe/updating-our-right-be-forgotten-transparency-report/, February 26, 2018 (access 2.2.2024).

The Advisory Council to Google on the Right to be Forgotten, *Report*, February 6, 2015., https://static.googleusercontent.com/media/archive.google/en//advisorycouncil/advisement/advisory-report.pdf (access: 2.2.2024).

From principle to practice: the EU-wide implementation challenges of the 'right to be forgotten' following Google v CNIL (iThenticate Similarity Report)

ORIGINALITY REPORT

35%
SIMILARITY INDEX

PRIMARY SOURCES

1	docs.mipro-proceedings.com Internet	328 words — 3%
2	carrcenter.hks.harvard.edu Internet	166 words — 2%
3	academic.oup.com Internet	165 words — 2%
4	www.gegevensbeschermingsautoriteit.be Internet	156 words — 2%
5	dokumen.pub Internet	130 words — 1%
6	tribunajuridica.eu Internet	118 words — 1%
7	arno.uvt.nl Internet	112 words — 1%
8	ebin.pub Internet	112 words — 1%
9	www.google.com Internet	109 words — 1%

10	universitypress.unisob.na.it Internet	101 words — 1%
11	www.idp.al Internet	92 words — 1%
12	research.bond.edu.au Internet	75 words — 1%
13	www.homepages.ucl.ac.uk Internet	67 words — 1%
14	ous.repo.nii.ac.jp Internet	62 words — 1%
15	www.strausscenter.org Internet	57 words — 1%
16	ir.lawnet.fordham.edu Internet	55 words — 1%
17	cyelp.com Internet	54 words — 1%
18	rozkotova.cld.bz Internet	51 words — 1%
19	www.dataguidance.com Internet	50 words — 1%
20	scholar.smu.edu Internet	49 words — < 1%
21	link.springer.com Internet	44 words — < 1%

22	lup.lub.lu.se Internet	42 words — < 1%
23	www.thedialogue.org Internet	41 words — < 1%
24	btlj.org Internet	40 words — < 1%
25	flifl.pravo.hr Internet	40 words — < 1%
26	www.dyskurs.inp.uz.zgora.pl Internet	40 words — < 1%
27	www.researchgate.net Internet	40 words — < 1%
28	ueaeprints.uea.ac.uk Internet	37 words — < 1%
29	www.techethos.eu Internet	37 words — < 1%
30	bc.umcs.pl Internet	36 words — < 1%
31	www.medialaws.eu Internet	34 words — < 1%
32	cris.tau.ac.il Internet	33 words — < 1%
33	rankingdigitalrights.org Internet	30 words — < 1%
	repository.uel.ac.uk	

34	Internet	30 words — < 1%
35	www.itm.nrw Internet	29 words — < 1%
36	dione.lib.unipi.gr Internet	28 words — < 1%
37	hpaied.org Internet	28 words — < 1%
38	www.diva-portal.org Internet	28 words — < 1%
39	private-law-theory.org Internet	27 words — < 1%
40	cnil.fr Internet	26 words — < 1%
41	lauda.ulapland.fi Internet	25 words — < 1%
42	www.iusinitinere.it Internet	25 words — < 1%
43	inplp.com Internet	24 words — < 1%
44	s-space.snu.ac.kr Internet	24 words — < 1%
45	www.europarl.europa.eu Internet	22 words — < 1%
46	www.utupub.fi	

	Internet	21 words — < 1%
47	science.law.muni.cz Internet	20 words — < 1%
48	cris.unibo.it Internet	19 words — < 1%
49	ctlj.colorado.edu Internet	19 words — < 1%
50	www.matrixlaw.co.uk Internet	19 words — < 1%
51	"The Right To Be Forgotten", Springer Science and Business Media LLC, 2020 Crossref	18 words — < 1%
52	fdslive.oup.com Internet	18 words — < 1%
53	www.coursehero.com Internet	18 words — < 1%
54	era-comm.eu Internet	16 words — < 1%
55	iris.unitn.it Internet	16 words — < 1%
56	pure.uva.nl Internet	15 words — < 1%
57	Brown, Abbe, Kheria, Smita, Cornwell, Jane. "Contemporary Intellectual Property", Contemporary Intellectual Property, 2023 Publications	14 words — < 1%

58	Laroussi Chemlali, Leila Benseddik. " The right to de-referencing ‘manifestly inaccurate’ information: ", Journal of Media Law, 2023 Crossref	14 words — < 1%
59	Orla Lynskey. "Complete and Effective Data Protection", Current Legal Problems, 2023 Crossref	14 words — < 1%
60	etheses.lse.ac.uk Internet	13 words — < 1%
61	www.nsf.ac.lk Internet	13 words — < 1%
62	Nina Gumzej. "Technical Solutions Supporting the Online RTBF in the CJEU and ECHR Jurisprudence", 2023 46th MIPRO ICT and Electronics Convention (MIPRO), 2023 Crossref	12 words — < 1%
63	scholarship.law.duke.edu Internet	12 words — < 1%
64	"Handbook of Communication Rights, Law, and Ethics", Wiley, 2021 Crossref	10 words — < 1%
65	beta.bailii.org Internet	10 words — < 1%
66	myassignmenthelp.com Internet	10 words — < 1%
67	one-web.t4staging.qmul.ac.uk Internet	10 words — < 1%

68	journals.umcs.pl Internet	9 words — < 1%
69	pure.rug.nl Internet	9 words — < 1%
70	scholarship.law.unc.edu Internet	9 words — < 1%
71	www.utrechtjournal.org Internet	9 words — < 1%
72	"EU Internet Law in the Digital Single Market", Springer Science and Business Media LLC, 2021 Crossref	8 words — < 1%
73	Franz C. Mayer. "Rebels Without a Cause? A Critical Analysis of the German Constitutional Court's OMT Reference", German Law Journal, 2019 Crossref	8 words — < 1%
74	Luca Tosoni. "Rethinking Privacy in the Council of Europe's Convention on Cybercrime", Computer Law & Security Review, 2018 Crossref	8 words — < 1%
75	Noémi Nagy. ""Humanity's new frontier": Human rights implications of artificial intelligence and new technologies", Hungarian Journal of Legal Studies, 2023 Crossref	8 words — < 1%
76	docslib.org Internet	8 words — < 1%
77	econeng.sogang.ac.kr Internet	8 words — < 1%

78	ns2.journals.umcs.pl Internet	8 words — < 1%
79	pub.law.uaic.ro Internet	8 words — < 1%
80	script-ed.org Internet	8 words — < 1%
81	seer.uscs.edu.br Internet	8 words — < 1%
82	www.accessnow.org Internet	8 words — < 1%
83	www.diva-portal.se Internet	8 words — < 1%
84	www.jdsupra.com Internet	8 words — < 1%
85	www.ru.nl Internet	8 words — < 1%
86	zenodo.org Internet	8 words — < 1%
87	"Use and Misuse of New Technologies", Springer Science and Business Media LLC, 2019 Crossref	7 words — < 1%
88	David Erdos. " SEARCH ENGINES, GLOBAL INTERNET PUBLICATION AND EUROPEAN DATA PROTECTION: A NEW ? ", The Cambridge Law Journal, 2020 Crossref	7 words — < 1%

89 Eugenia Politou, Efthimios Alepis, Maria Virvou, Constantinos Patsakis. "Privacy and Data Protection Challenges in the Distributed Era", Springer Science and Business Media LLC, 2022 — 7 words — < 1%
Crossref

90 Melisa Liana Vazquez. "Neither Matter Nor Spirit: The Ambivalent Substance of Digital Legal Personhood and Its Theological Antecedents", International Journal for the Semiotics of Law - Revue internationale de Sémiotique juridique, 2023 — 6 words — < 1%
Crossref

91 Yann Padova. "Is the right to be forgotten a universal, regional, or 'glocal' right?", International Data Privacy Law, 2019 — 6 words — < 1%
Crossref

EXCLUDE QUOTES	OFF	EXCLUDE SOURCES	OFF
EXCLUDE BIBLIOGRAPHY	OFF	EXCLUDE MATCHES	OFF