Technical Solutions Supporting the Online RTBF in the CJEU and ECHR Jurisprudence

Nina Gumzej
University of Zagreb Faculty of Law, Chair of Information Technology Law and Informatics, Zagreb, Croatia
ngumzej@pravo.hr

***Abstract* - Legal solutions toward restricting online accessibility of content relevant to one's privacy are valueless without interdisciplinary cooperation and acknowledgment of technological developments. One example lies in the affirmed use of geo-filtering technology to support the scope of delisting, which ensures the more effective RTBF as a specific right related to the right to erasure, which is reserved for data subjects and implemented by search engines under EU law. Other two concern the measures of rearranging search results, and adding warnings on initiated proceedings in search engine results, which the CJEU acknowledged in certain cases of unsuccessful delisting requests, and which are according to their aim of providing currently accurate data/information traditionally directed toward original content producers. Fourth example lies in the recognized role of de-indexing technology that enables online publishers to restrict accessibility of their own content, and supports the right to private life under ECHR jurisprudence. The paper discusses and critically assesses those solutions. Delisting is shown to be less restrictive than de-indexing for the freedom of expression and at the same time less effective data protection-wise, taking into account also limited territorial scope, and is as such also consumed by de-indexing. Innovative CJEU measures may provide fair solutions for affected data subjects, but still require legal justification and proof of operation in the practice of search engines.**

Keywords - RTBF; geo-filtering; Google v. CNIL; delisting; de-indexing; GC and Others; TU and RE v Google; Biancardi v Italy; Hurbain v Belgium; blocking online content; digital archives; search engine

I. INTRODUCTION

Already in 2011, the European Network and Information Security (ENISA) reported that: „While it is impossible in general to remove data from the Internet once it was published, it might be possible to limit its accessibility (...) A natural way to "mostly forget" data is thus to prevent its appearance in the results of search engines, and to filter it from sharing services like Twitter. EU member states could require search engine operators and sharing services to filter references to forgotten data. As a result, forgotten data would be very difficult to find, even though copies may survive, for instance, outside the EU jurisdiction" [1]. The Court of Justice of the European Union (CJEU) acted on that foresight three years later in the *Google Spain* judgment (C-131/12), where it examined in detail the role of large internet search engines in the dissemination of information relating to individuals in the EU and interpreted the application of the EU data protection law requirements to search engines [2]. Thus, the data subjects may in certain cases request that certain information (personal data) are blocked from search results when users make a search query involving their name. With the exercise of delisting relevant information published on *third-party* websites is neither erased from the Internet nor removed from the index and cache of the Internet search engine. Search results retrieved upon a specific, very narrow name-based search query are merely *blocked*, e.g., they continue to provide links to delisted information in cases of search queries with other keywords [3]. Such a right is colloquially referred to as the "right to be forgotten" (RTBF), as defined and interpreted in the CJEU jurisprudence on the basis of applicable legislation, which is currently Article 17 of the GDPR [4]. Terminology used to denote this right, which data subjects normally invoke before leading search engine operators (Google and Bing being recently declared the very large online search engines [5] pursuant to the Digital Services Act) [6] and as used in this paper is mainly that of the "RTBF" or "delisting", which is also referred to in relevant Guidelines of the European Data Protection Board (EDPB) in [3] and in relevant procedures before Google [7].

Aim of this paper is to explore and discuss the evolution and role of different solutions (geo-filtering, rearranging search results, publishing warnings, de-indexing) impacting, directly or indirectly, the implementation of the online RTBF in the jurisprudence of the CJEU and that of the European Court of Human Rights (ECHR). Analysis in Part 2 sets off with an overview of the path towards the use of geo-filtering technology by Google, which it initially contested but eventually voluntarily implemented, and a discussion on its role in the furthering effect of the territorial scope of delisting, taking into account also relevant aspects of the *Google v. CNIL* judgment [8]. Further examined are innovative measures of rearranging search results and publishing warnings on initiated proceedings, which the CJEU acknowledged in *GC and Others* [9] and *TU and RE v Google* [10] judgments to apply in certain cases of unsuccessful delisting requests - as measures directed toward search engine operators. That analysis concludes with a discussion, on one hand, of the positive outlook for relevant data subjects who are able to and wish to make use of such solutions and on the currently unresolved issues relating to their implementation. Technical solutions relating to implementation of the RTBF have also been discussed in recent ECHR case law in terms of the balancing of the right to respect of private life (including the right to reputation) with the freedom of information by newspaper publishers maintaining online

archives. As I will explain in Part 3, the ECHR acknowledges concerns of the prolonged ease of access to published information via search engines and the related responsibility of noted publishers in implementing the technical measure referred to as "de-indexing" in certain cases, as a proper outcome of the balancing between conflicting fundamental rights. Mainly explored in Part 3 is the approach of the Court in *Biancardi v. Italy* judgment [11] and relevant developments in the current referral proceedings before the Grand Chamber in the *Hurbain v. Belgium* case [12]. While both cases certainly merit a detailed academic discussion [13] they are due to scope of paper not examined in substance and detail. Instead, focus is on approach of the Court toward delisting and de-indexing measures, delineation between the two measures and responsible parties to implement them, which further leads the discussion to the issue of the impact of de-indexing on relevant publishers and the exhaustion of the RTBF, from a data subject's perspective, in cases of successfully implemented de-indexing. Analysis in Part 3 is complemented by an overview of current technical documentation and policies, which support website owners toward implementing de-indexing (and other content-blocking measures) on the Google search engine. Part 4 concludes the paper.

II. MEASURES IN CJEU JURISPRUDENCE

A. Role and Evolution of Geo-filtering in Delisting

Google (which is in focus as the world's leading search engine in relation to whom the CJEU's RTBF jurisprudence evolved) currently implements successful delisting requests of data subjects by default across all of its EU domains, and on any other domain where it is established, on the basis of the IP address, that the search originates in the Member State of the data subject. However, this territorial scope issue was legally unresolved and thus left entirely at its discretion for a striking period of 5 years following Google Spain, i.e., up until the CJEU's second RTBF judgment in Google v. CNIL. As I will show, Google's decision to start using the geo-filtering technology resulted from the discussions and pressure of EU DPAs and particularly in light of court proceedings in France, which eventually led to the Google v. CNIL judgment.

Following Google Spain, the Article 29 Data Protection Working Party (Art. 29WP) [14] and Google with its Advisory Council [15] took opposing views on the delisting territorial scope. Art. 29WP considered that delisting should be implemented globally (i.e., on all domains, including .com.), in light of which it *never discussed* in [14] the possible technical measures, such as geo-filtering. Google's Advisory Council considered that the Court's judgment was not sufficiently precise and insisted on regional domain-based delisting. It supported this view with the practice of automatic referrals to local search engine versions when Internet users in Europe entered "google.com" in their browser, and with Google's claim that more than 95% of user searches from Europe are performed on their local versions. The Council also noted the concerns of opposing interests by both the Internet users outside of Europe and individual users within Europe. Unlike with the Art.29WP, the use of measures such as geo-filtering was here raised - though only by independent experts, who noted that there might be technical possibilities to prevent access to delisted content where searches are made in the EU territory. The Council rejected such option in [15] due to "concerns about the precedent set by such measures, particularly if repressive regimes point to such a precedent in an effort to "lock" their users into heavily censored versions of search results", and the lacking clarity on its effectiveness due to possible circumventions.

Google's domain-based delisting practice, which was limited only to its European versions, soon prompted DPAs reactions. In particular, the French data protection authority (CNIL) ordered a global delisting in 2015 [16]. In March 2016, amid the related court proceedings in France Google voluntarily changed its delisting practice to also include geolocation data pinpointing to users attempting to access relevant information from their EU State of residence, which corresponds to that of the data subject [17] ('glocal' implementation of the right to delisting [18]). According to [17], Google implemented these changes, i.e., the use of geo-filtering to such effect also retroactively, thus to all earlier delistings. Still unimpressed, the CNIL fined Google for failing to comply with its global delisting order and noted that while the new geo-filtering measure does constitute an improvement, it remains incomplete (delisted data can still be consulted by users located outside the territory affected by geo-filtering and it is still possible for users concerned to circumvent it, e.g., by use of the VPN) [19].

In Google v. CNIL the CJEU ruled *inter alia* that the "de-referencing" (English term used for delisting/RTBF in its jurisprudence following Google Spain) is in principle supposed to be carried out in respect of all the Member States, but not in cases of diverging public interests in Member States to access the relevant data. As regards global delisting, the EU law does not impose but it also does not prohibit it, whereby such delisting decisions are left to the national DPAs and the courts, i.e., to their balancing between data protection and freedom of information rights in light of their national fundamental rights standards [20]. A detailed analysis of the many complexities discussed and further raised in and as a consequence of this judgment, which attracted immense academic attention [21], falls outside the scope of this paper. To be pointed here is the Court's brief discussion on the role of "measures" such as geo-filtering (explicitly referred to as geo-blocking in the third preliminary question [22]). Specifically, it held that, if necessary, the search engine „may take sufficiently effective measures to ensure the effective protection of the data subject's fundamental rights", which must „meet all the legal requirements and have the effect of preventing or, at the very least, seriously discouraging internet users in the Member States from gaining access to the links in question using a search conducted on the basis of that data subject's name". While not specifying geo-filtering *per se* and criticized in literature for lack of detail on such an important issue [23], this note shows at least the Court's theoretical acknowledgment of technical measures that may be taken, though on pure discretion of the search

engine, upon balancing between the fundamental rights and according to particular circumstances of each case. However, specific technologies used, implementation details and related circumvention concerns have up to today never been discussed, at least under particular interpretative guidelines issued on those points specifically - most importantly by the EDPB. Additional technical measures to address the circumventions to geo-filtering have been pointed to in literature [24]. In any event, even despite its not being fool proof, the use of geo-filtering technology is considered a more acceptable alternative to global delisting orders, whereby the otherwise complex jurisdictional issues and in particular enforcement concerns are minimized [25].

B. Measures in Cases of Unsucccessful Delisting

In two of its other RTBF judgments the CJEU envisaged specific measures to be taken by search engines in cases of delisting requests, which are otherwise unsuccessful, upon balancing (such as due to prevailing public interest to easily access such data via a name-based search query) or due to lacking proof of the manifest inaccuracy of published content. Thus, in the *GC and Others* judgment (which I examined in detail elsewhere [26]) the CJEU considered the measure to be implemented by the search engine after establishing that the de-listing request should be rejected, even though relevant sensitive data are no longer accurate. More precisely, it concerns situations where it is established, upon balancing, that there is a prevailing public interest to easily access, via a name-based search query, published information relating to criminal proceedings brought against the data subject, concerning an earlier stage of the proceedings and no longer corresponding to the current situation. In such cases search engine operators should at the latest upon such examination of the delisting request adjust, i.e., rearrange search results so that the overall picture provided to internet users reflects the current legal position [27]. Such implementation of the "duty to relist" [28] means in particular that the higher ranking is implemented for search results linking to the webpages containing updated information, so that those links appear on top of the list. Measure therefore presupposes that the legal proceedings ended in favour of the data subject (whilst the currently inaccurate data on the earlier phase remain listed upon name-based search results), which issue should be brought to the attention of the search engine operator upon the delisting request.

Many issues remain unclear as regards this measure [29], such as whether this practice should extend to all of the outdated, thus currently inaccurate personal data, starting from the other sensitive data categories to even ordinary data, and to any other type of related legal proceedings. Furthermore, the CJEU did not provide any legal basis for such practice in its judgment (*obiter dictum*) and the issue was raised on its own volition. It may, however, be argued that such a practice might appropriately implement the GDPR data accuracy principle [30]. On the other hand, the resulting concern is mentioned broadening of its scope under that same principle. Otherwise, it is beyond doubt that the practice affects search engine's operations, which needs to be implemented into its automated ranking systems [31].

One of the noted issues that requires further clarification is that of the assumedly large scope of cases in which the updated information (reflecting current legal position) *was not published* [32]. An approach to resolving this lies in another measure, which the CJEU acknowledged in the subsequent *TU and RE v Google* judgment [10]. Specifically, where the operator does not accept the delisting request based on alleged inaccuracy of content (entire content referred to, or a part of it that is not minor in relation to whole content), which is not obvious (manifest), that operator should upon notice by the data subject add warnings concerning existing proceedings (administrative or judicial) disputing accuracy of such content, in relevant name-based search results [33]. Unlike in the previous case, at least according to circumstances of the case and the judgment itself it is possible to argue more clearly that this measure might have a broader scope of application, i.e., that it could cover the various types of situations and data, the current accuracy of which is contested. Furthermore, while the basic tenets *for asserting* the RTBF under Google Spain continue to apply (such as that neither proof of prejudice nor establishment of e.g., illegality of the relevant publication and removal from the source webpage are required) [34], described measure presupposes existence of at least some preliminary action taken in national proceedings toward disputing accuracy of published information (before DPAs or courts).

Both measures aim to provide a fairer outcome for affected data subjects (who wish to call on them) and appear to be a further application of the GDPR to search engines as *sui generis* data controllers, in the context of their own specific data processing activities, and related responsibilities, powers and capabilities [35]. However, the lacking clarity particularly on applicable legal bases is of concern. While as noted the CJEU did not provide explicit basis for rearrangement of search results, but which might be interpreted as implementation of the data accuracy principle, in TU and RE v Google it specified in [33] the purpose of publishing warnings to be ***inter alia*** that of providing the internet users „with information which continues to be relevant and up-to-date". While the latter concern is logical, allowing for a better informative Internet [36] and which could from that point of view justify both here described measures, the void of the crucial *inter alia* continues to potentiate the head-scratching line of "brushed-over" issues concerning the application of GDPR requirements (such as that of data accuracy, right to rectification and right to restriction of processing) [37] to search engine operators.

III. DE-INDEXING V. DELISTING, DIGITAL ARCHIVES AND TECHNICAL EXPERTISE IN ECHR CASE LAW

Not least on account of lacking EU harmonization in the complex balancing domain between the freedom of information and data protection rights [38] the CJEU's jurisprudence has so far focused strictly on RTBF as exercised by the data subjects before the search engine operators, and on corresponding duties of those operators, regulators and the courts, thereby leaving out the concerns of responsibility of online publishers to themselves take

action by restricting accessibility to disputed content. As I will explain, these issues gained prominence in recent cases before the ECHR. But first it is important to go back to the basics of the RTBF i.e., delisting according to Google Spain, which delineates it from the more traditional legal mechanisms that are directed toward the removal or modification of online content. One of the distinctive features of that right is that it can be asserted against search engine operators regardless of and independently of the data subject's exercise of the more traditional legal institutes against publishers directly (e.g., to have published information removed directly from the source). This is supported by several considerations, all of which are based on reasons of effective and complete protection of *data subjects* [39]. Specifically, they might not be able to succeed in removing their data online for reasons of technical ease of online data reproduction and for jurisdictional reasons where the publisher is not subject to EU law. Also, publishers may keep content online on the basis of their respective laws, including due to prevailing higher regard for the freedom of information [38]. Of relevance here is also the Court's acknowledgment of the fact that it is the publishers who can technically ensure that the data they publish are made unavailable to the search engines, e.g., via exclusion protocols or codes such as 'noindex', although it did not hold such (lack of) action by publishers a condition for establishing the search engine operator's responsibilities for data processing in the context of its own data processing activities, powers and capabilities [40]. Interestingly, in its analysis of the issue if search engine operators may be qualified as data controllers, the Advocate General argued that the only situations in which that operator could be the controller are where it ignored or disobeyed the publisher's (website administrator's) request not to index, i.e. to make the data unavailable for dissemination through the search engine, or where it ignored or disobeyed the publisher's request to update the cache memory (thereby, for example, continuing to show deleted content) [41]. More recently, the EDPB confirmed that search engines operators are themselves bound to carry out actual and full erasure of the URL to third-party content (i.e., de-index) in cases where they disregarded that party's (original publisher's) relevant request (de-indexing / exclusion protocol request) [42]. As a result, such measure has a broader scope than delisting, which is the mere blocking of links displayed in search results following a name-based search query and, as noted earlier, of limited territorial scope.

It is exactly the issue of publishers with online digital archives accessible to the public which is in focus of recent RTBF-related cases before the ECHR, specifically with respect to their role and liability concerning the implementation of noted de-indexing measures. Thus in *Biancardi v Italy* [11] the Court affirmed responsibility of online publishers i.e. owners of online newspaper websites (administrators of newspaper or journalistic archives accessible through the Internet) to deploy "de-indexing" in cases where content of information is itself not challenged nor the way information is published (thereby this case differing from *Węgrzynowski and Smolczewski v Poland* [43] and M.L. and *W.W. v Germany* [44]), but that of *prolonged ease of access to outdated published information via digital archives*. As such, that content is made easily accessible via search engines, thereby harming the individual's right to reputation in the wider context of the right to respect for private life.

In its judgment the Court was commendably attentive to terminological concerns and devoted an entire sub-section of the judgment to the issue of interchangeable uses of de-indexing, delisting and de-referencing concepts in the different sources of EU and international law [45]- which may certainly be confusing. For that reason, technical information on the relevant measure to be employed is vital in order to properly assess its intended aim and scope. It is therefore significant that the Court specifically referred to relevant technical information on de-indexing (as well as other tools enabling the blocking of accessibility of published content via search engines] [46] as a measure available to website owners and thus also to relevant online publishers (administrators of newspaper or journalistic archives accessible through the Internet in this case) [47]. Such technical aspects, most specifically on de-indexing, appear important towards supporting the Court's analysis of facts of the case and its decision that the relevant courts justifiably restricted the publisher's freedom of expression [48]. Specifically, domestic courts found publisher's liability i.a. due to their failure to de-index from the search engine the tags to published article, whereby accessibility to publisher's own content via search engines would be restricted, but would not in itself entail deletion of such content (article).

Discussions are currently developing in the same vein in the referral proceedings before the Grand Chamber in the case of *Hurbain v Belgium* [12]. The relevant court-ordered measure under consideration, which the ECHR Chamber earlier affirmed as proportionate, is that of anonymization of an outdated article available in the newspaper's digital archive. The article contained information on a fatal car accident and included the responsible driver's full name, who was in the meantime formally rehabilitated. In regard to the issue of the less restrictive measures (to anonymization) for the publisher, in the balancing between the right to respect for private life with the freedom of expression, the different content blocking measures such as de-indexing and delisting are discussed. As for delisting, taking into account its effect and key features (RTBF), there is no doubt that it constitutes the least restrictive measure, which only the data subjects may invoke. Interestingly, during the Grand Chamber hearing (09.3.2023) [12] the Belgian Government expressed the position (contrary to that of the publisher) that de-indexing (in the proper sense of adding a no-index tag by the publisher) might in fact be more restrictive for the freedom of the press, as it would lead to "virtual death" of an article (non-availability thereof in the search engines). In contrast, the measure ordered by the judges in national court proceedings (anonymization) would still keep the digital article easily accessible, but in an anonymized form. Technical realities of the online realm with endless redistribution

possibilities of once published content provides good validity (also) to that argument.

Appropriate cognizance of technological options in any case appears critical, particularly since "(evolving) technology can be turned into a virtue as well to better tailor measures and reach more granular verdicts that avoid that radical choices between publicity and deletion must be made" [49]. Taking into account the necessary technical evaluation of the different measures invoked, it is important to point to available documentation and support as provided by the leading search engines.

Thus, according to Google's *current* documentation and policy, website owners may block their article (webpage) from search results (which, as noted also logically include the owners of online newspaper websites) [50]. Currently also *quick removal*s are possible (within a day), but only for those website owners who verified their site in Google's Search Console [51]. These typically last to 6 months [52]. For *permanent removals* (but which do not take effect so quickly), website owners are advised to implement them with a noindex rule [53], which is set with a <meta> tag or HTTP response header, with the result that: "When Googlebot crawls that page and extracts the tag or header, Google will drop that page entirely from Google Search results, regardless of whether other sites link to it" [54]. Upon re-crawling the index, content would no longer be available in search results (options *are available* to speed up the process). It is important to also note the measures to ensure that not only Google but also any other search engine supporting the deindex rule does not index relevant content, and the disclaimer that some search engines *might interpret the noindex rule differently* (which means that content might still appear in their results). Various additional technical options are possible, such as for including (*and excluding*) the *sitelinks search box* in search engine's results, which is promoted as "a quick way for people to search your site or app immediately on the search results page." (…) "Google Search may automatically expose a search box scoped to your website when it appears as a search result, without you having to do anything additional to make this happen. This search box is powered by Google Search. However, you can explicitly provide information by adding WebSite structured data, which can help Google better understand your site (....) If Google Search already exposed a sitelink search box for your site, you can control certain aspects of the sitelink search box by adding WebSite structured data" [55]. Noted possibility of *automatic search-box exposure* by Google is important to take into account in cases of de-indexing.

As regards *non-site owners*, such as private citizens, they cannot use such tools but may submit the *personal data removal request form*s depending on the different types of content/data. They may notify Google also in cases of *outdated content*, if the webpage no longer exists or is significantly different from the current page version. Additionally, and more broadly, content removals are possible for various legal reasons, which include i.a. DMCA copyright violation reports, child sexual abuse imagery, and *requests for removals under the EU RTBF* [56]. Further relevant, but falling outside the scope of this paper are the duties arising from new EU acts such as the Digital Services Act [6] and from the self-regulatory standards, such as those to fight disinformation [57].

Going back to the pending Hurbain v. Belgium case, there appears to be validity in the argument that de-indexing might constitute an even more restrictive measure than article anonymization. However, not least due to entailed consequences of such potential precedent for publisher's operations and freedom of the press in general, the publisher would still prefer that measure to article anonymization. Without prejudice to proper determination of particular circumstances of the case in the current referral proceedings, in theory the revised approach on the balancing and thus on de-indexing, along the lines of that taken in Biancardi v. Italy, appears likely.

IV. Concluding Remarks

Complex relationship between the freedom of information and data protection online, where information once published eventually becomes outdated, irrelevant or incorrect, but still keeps on re-emerging with the simple name-based search queries, and thereby exercising continuing negative effects on affected data subjects, is and will continue to be a growing not only legal, but also general societal and economic problem. Nowadays there is a growing number of paid for services claiming improvement or taking control of one's online reputation, which include employment of various strategies to "push down" negative search results and achieve favorable content prioritizing. The responding legal protection from the point of view of EU data and privacy protection resulted in the RTBF, i.e., the right to delisting, which if successful results in the blocking of search results following a specific and very narrow name-based search queries, and which is implemented by a search engine operator upon request of the data subject. Examined evolution of Google's initially contested but eventually voluntarily and technically even retroactively implemented geo-filtering technology in delisting cases supports the effectiveness of the RTBF when combined with the regional (EU) domain-based delisting. However, the use of such technology and concerns discussed in the paper such as that on possible circumventions, as well as proposed solutions, combined with the related aspects of Google v. CNIL have still not been addressed - at least through EDPB's interpretative initiative. Thereby Google's currently standard delisting approach appears tolerated, possibly in light of its being a "difficult" compromise between the regional, and global domain-based delisting that the EDPB's predecessor insisted on. In any event, from the point of view of data subjects the limited territorial scope is one of the significant drawbacks of the RTBF, i.e., delisting.

If the narrow name-based search query and limited territorial scope of delisting are "sticks", then the CJEU offers the rearranged search results and added warnings on initiated proceedings in search results as "carrots". As such, these measures may lead toward a fairer outcome for those data subjects whose delisting requests were not successful under certain circumstances - and who wish to utilize such options in search engine results. Thereby the

CJEU broadened the scope and type of measures to be taken by very large search engine operators as an arguably further application of the GDPR to them as *sui generis* data controllers (and in the context of their own specific data processing activities, related responsibilities, powers and capabilities), but which still requires proper legal justification. This is so particularly since according to their aim of providing the currently accurate data, such measures are usually directed towards original content producers, also under the more traditional legal institutes.

The role and liability of online publishers in the maintenance (prolongation) of easy access to outdated published information in the digital archives, and their lack of action as regards requested de-indexing to make such content inaccessible to search engines, is an issue gaining prominence in ECHR case law. De-indexing as a technique defined and, in the end effectuated by the search engine operator, at website owner's request (*the functionalities of which may continue to evolve*), signifies the removal of the relevant page from search results regardless of the key word(s) used in the search query. Due to technology involved it also has as an effect the automatic removal of relevant data from search results of more search engines - should they all technically support the deindex rule. When comparing that measure to delisting, it is clear that the latter provides a less restrictive measure in terms of freedom of expression and is at the same much less effective in terms of individuals' data protection and privacy rights, also taking into account its limited territorial scope. In any case upon de-indexing the data subjects normally no longer require delisting from search engines, which is typically consumed by de-indexing and which in any event they might need to separately exercise against more search engines.

On a broader level it has for a while now become clear that any legal solution toward restricting online accessibility of content that is relevant to one's privacy and data protection rights is valueless without interdisciplinary cooperation to support at least the identification, and application of relevant technological developments. Very large internet search engines are certainly key players in that area. In April 2022 Google expanded its policy on removals of personal data that appear in Google Search [58], which it considers to be in line with its aim of helping people take more control of their online presence on its search engine. In fact, it proclaims even more broadly to be continuously "looking for new ways to ensure our policies and built-in safeguards reflect peoples' evolving needs and are easy to use" [59]. This in any case adds to ENISA's early recommendation in [1] on relevant multistakeholder cooperation: "Research communities, industry etc. should develop techniques and coordinate initiatives that aim at preventing the unwanted collection and dissemination of information (e.g., robot.txt, do not track, access control)".

Proper consideration of relevant technological developments and expertise is especially important for relevant regulators and courts in this area. Accordingly, this paper ends with an inspiring note by the German Constitutional Court: "Given that technical developments are ongoing and that they entail uncertainties regarding how and to what extent content providers can influence the dissemination of their articles on the Internet in interaction with search engines, it will fall to the ordinary courts to continue to shape effective and reasonable protective measures. Where reasonable, the courts, which have a considerable margin of appreciation in respect of all these measures, can also require the actors to develop new instruments" [60].

REFERENCES

[1] ENISA, "The right to be forgotten – between expectations and practice," 20.11.2012 (date of deliverable: 18.10.2011), p. 13 (point 4.4.), https://www.enisa.europa.eu/publications/the-right-to-be-forgotten/at_download/fullReport (accessed 06.4.2023).

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

[3] 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, 07.7.2020, pp. 5, 12 (points 8-9, 49).

[4] 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) [2016] OJ L119/1, Corrigendum [2018] OJ L127/2.

[5] European Commission, "Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines," 25.4.2023, https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2413 (accessed 25.4.2023).

[6] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277.

[7] Google, "Right to be Forgotten Overview," https://support.google.com/legal/answer/10769224#zippy=%2Cview-a-list-of-some-common-tools; "Personal Data Removal Request Form," https://reportcontent.google.com/forms/rtbf?visit_id=638185239021320897-1606126095&hl=en&rd=1 (accessed 06.4.2023).

[8] C-507/17 Google LLC v CNIL, ECLI:EU:C:2019:772.

[9] C-136/17 GC and Others v CNIL, ECLI:EU:C:2019:773.

[10] C-460/20, TU and RE v Google LLC, ECLI:EU:C:2022:962.

[11] Biancardi v. Italy (Application no. 77419/16), 25.11.2021.

[12] Hurbain v. Belgium (Application no. 57292/16), 22.6.2021 - referred to the Grand Chamber, hearing held on 09.3.2023: https://www.echr.coe.int/Pages/home.aspx?p=hearings&c= (accessed 20.4.2023).

[13] M. R. Allegri, "Dimenticare, rievocare, rappresentare: dove conduce la via dell'oblio," MediaLaws - Rivista di Diritto dei Media, vol. 2, 2022, pp. 81-123.

[14] Article 29 Data Protection Working Party, "Guidelines on the implementation of the Court of Justice of the European Union judgment on 'Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González' C-131/12," WP 225, 26.11.2014, p. 9.

[15] The Advisory Council to Google on the Right to be Forgotten, 06.2.2015, pp. 18-20 (point 5.4.), https://static.googleusercontent.com/media/archive.google.com/en//advisorycouncil/advisement/advisory-report.pdf (accessed 06.4.2023).

[16] CNIL, "La CNIL met en demeure Google de procéder aux déréférencements sur toutes les extensions du moteur de recherche," 12.6.2015, http://www.cnil.fr/linstitution/actualite/article/article/la-cnil-met-en-demeure-google-de-proceder-aux-dereferencements-sur-toutes-les-extensions-du-mote/ (accessed 12.6.2015).

[17] P. Fleischer, "Adapting our approach to the European right to be forgotten," 04.3.2016, https://blog.google/topics/google-

europe/adapting-our-approach-to-european-rig/ (accessed 06.4.2023).

[18] Y. Padova, "Is the right to be forgotten a universal, regional, or 'glocal' right?," International Data Privacy Law, vol. 9, pp. 15-29, 2019 at p. 18.

[19] CNIL, Délibération n° 2016-054, 10.3.2016.

[20] C-507/17 in [8] paras 53-73.

[21] 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, vol. 69, pp. 380–388, April 2020; J. Quinn, "*Google v CNIL*: Circumscribing the Extraterritorial Effect of EU Data Protection Law," in Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty, F. Fabbrini, E. Celeste and J. Quinn, Eds. Oxford: Hart Publishing, 2020, pp. 47–62; G. Frosio, "Enforcement of European Rights on a Global Scale (July 13, 2020)", in Routledge Handbook of European Copyright Law, E. Rosati, Ed. Routledge, 2021, pp. 413-440, http://dx.doi.org/10.2139/ssrn.3650521; P.T.J. Wolters, "The territorial effect of the right to be forgotten after Google v CNIL," International Journal of Law and Information Technology, vol. 29, pp. 57–75, spring 2021; A. Klinefelter and S. Wrigley, "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, vol. 22, pp. 681-734, 2021; I. Hadjiyianni, "The Global Reach of EU Law in the Digital Age: The Territorial Scope of Data Protection," in EU Internet Law in the Digital Single Market, T.-E. Synodinou, P. Jougleux, C. Markou and T. Prastitou-Merdi, Eds. Springer Nature Switzerland AG, 2021, pp. 311-335; E. P. Maat, "Google v. CNIL: A Commentary on the Territorial Scope of the Right to Be Forgotten," European Review of Private Law, vol. 30, pp. 241-262, 2022; M. Taylor, Transatlantic Jurisdictional Conflicts in Data Protection Law. Fundamental rights, privacy and extraterritoriality. Cambridge University Press, 2023, pp. 165-188.

[22] C-507/17 in [8] para 39.

[23] O. J. Gstrein, "Right to be forgotten: european data imperialism., national privilege, or universal human right?," Review of European Administrative Law, vol. 13, pp. 125-152, 2020 at p. 135; Wolters in [21]; J. Quinn, "Geo-location technology: restricting access to online content without illegitimate extraterritorial effects," International Data Privacy Law, vol. 11, pp. 294-306, 2021 at p. 303; Klinefelter and Wrigley in [21] at p. 717.

[24] D. Erdos, "Search Engines, Global Internet Publication and European Data Protection: a New *via Media*?," Cambridge Law Journal, vol. 79, pp. 24-27, 2020 at pp. 26-27; Wolters in [21] at pp. 70-71.

[25] B. V. Alsenoy and M. Koekkoek, "Internet and jurisdiction after Google Spain: the extraterritorial reach of the 'right to be delisted'," International Data Privacy Law, vol. 5, pp. 105-120, 2015 at p. 114; D. J. B. Svantesson, Solving the Internet Jurisdiction Puzzle. Oxford University Press, New York: NY, 2017 at p. 214; Quinn in [23] at pp. 305-306; G. E. M. Perez, "Global or Local? Freedom of Speech and Some Extraterritorial Court Decisions on the Internet," Queen Mary Law Journal, vol. 3, pp. 70-91, 2022 at p. 89; Klinefelter and Wrigley in [21] at pp. 717-718; Taylor in [21] at pp. 177-185.

[26] N. Gumzej, "'The Right to Be Forgotten' and the Sui Generis Controller in the Context of CJEU Jurisprudence and the GDPR," Croatian Yearbook of European Law and Policy, vol. 17, pp. 127–158, 2021 at pp. 142-156.

[27] C-136/17 in [9] para 78.

[28] F. Giovanella, "From the "right to delisting" to the "right to relisting," MediaLaws - Rivista di Diritto dei Media, vol. 2, pp. 124-144, 2022.

[29] Globocnik in [21]; Gumzej in [26] at pp. 154-155.

[30] GDPR in [4] Art. 5(1)(d); Globocnik in [21].

[31] "A guide to Google Search ranking systems," https://developers.google.com/search/docs/appearance/ranking-systems-guide?hl=en (accessed 06.4.2023).

[32] Globocnik in [21].

[33] C-460/20 in [10] para 76 (in connection with paras 68-75).

[34] C-131/12 in [2] paras 84-88, 96, 99.

[35] Gumzej in [26].

[36] Giovanella in [28] at p. 137.

[37] GDPR in [4] Art. 5(1)(d), Art. 16 and Art. 18.

[38] GDPR in [4] Art. 23(1); Art. 85; Art. 17(3)(a); Notifications under Art. 85(3) GDPR: "EU Member States notifications to the European Commission under the GDPR," <https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu/eu-countries-gdpr-specific-notifications_en> (accessed 06.4.2023); D. Erdos, "Special, Personal and Broad Expression: Exploring Freedom of Expression Norms under the General Data Protection Regulation," Yearbook of European Law, vol. 40, pp. 398–430, 2021.

[39] C-131/12 in [2] paras 84-86.

[40] C-131/12 in [2] para 39.

[41] "Opinion of Advocate General Jääskinen," 25.6.2013, ECLI:EU:C:2013:424, paras 91-93, 99.

[42] EDPB in [3] p. 5 (point 10).

[43] Węgrzynowski and Smolczewski v. Poland (Application no. 33846/07), 16.7.2013.

[44] M.L. and W.W. v Germany (Applications nos. 60798/10 and 65599/10), 28.6.2018.

[45] Biancardi v. Italy in [11] paras 53-56.

[46] Biancardi v. Italy in [11] para 50 incl. n. 2.

[47] Biancardi v. Italy in [11] para 51.

[48] Biancardi v. Italy in [11] paras 70-71.

[49] S. Verschaeve, "Going dark or living forever: the right to be forgotten, search engines and press archives," Master's thesis, KU Leuven Faculty of Law, p. 43, 25.5.2020, http://dx.doi.org/10.2139/ssrn.3669865 (accessed 06.4.2023).

[50] "Crawling and Indexing," "Removals," https://developers.google.com/search/docs (accessed 06.4.2023).

[51] "About Search Console," https://support.google.com/webmasters/answer/9128668?hl=en#zippy=%2Cproduct-requirements (accessed 06.4.2023).

[52] "Removals and SafeSearch reports Tool," https://support.google.com/webmasters/answer/9689846 (accessed 06.4.2023).

[53] "Remove a page hosted on your site from Google," https://developers.google.com/search/docs/crawling-indexing/remove-information (accessed 06.4.2023).

[54] "Block Search indexing with noindex," https://developers.google.com/search/docs/crawling-indexing/block-indexing (accessed 06.4.2023).

[55] "Sitelinks search box (WebSite) structured data," https://developers.google.com/search/docs/appearance/structured-data/sitelinks-searchbox (accessed 06.4.2023).

[56] "Remove your personal information from Google," https://support.google.com/websearch/troubleshooter/3111061; "Remove outdated content," https://support.google.com/websearch/answer/6349986; Remove "Outdated Content tool," https://support.google.com/webmasters/answer/7041154; "Personal Data Removal Request Form" in [7] (accessed 06.4.2023).

[57] "The Strengthened Code of Practice on Disinformation 2022," https://ec.europa.eu/newsroom/dae/redirection/document/87585 (accessed 06.4.2023).

[58] "Remove select personally identifiable info or doxxing content from Google Search," https://support.google.com/websearch/answer/9673730 (accessed 06.4.2023).

[59] M. Chang, "New options for removing your personally identifiable information from Search," 27.4.2022, https://blog.google/products/search/new-options-for-removing-your-personally-identifiable-information-from-search/ (accessed 06.4.2023).

[60] BVerfG, 1 BvR 16/13, 06.11.2019, http://www.bverfg.de/e/rs20191106_1bvr001613en.html at para 142 (related see also paras 133-135), accessed 06.4.2023.