RIGHT TO BE FORGOTTEN: EU-ROPEAN DATA IMPERIALISM, NATIONAL PRIVILEGE, OR UNIVERSAL HUMAN RIGHT?

Dr. Oskar J. Gstrein, LLM, MA – Department of Governance and Innovation, Data Research Centre – Campus Fryslân, University of Groningen – The Netherlands

Draft accepted for Review of European Administrative Law (REALaw); 2019/2 (Forthcoming)

Abstract

The Digital Age has fundamentally reshaped the preconditions for privacy and freedom of expression. This transpires in the debate about a “right to be forgotten”. While the 2014 decision of the European Court of Justice in “Google Spain” touches upon the underlying issue of how increasing amounts of personal data affects individuals over time, the topic has also become one of the salient problems of Internet Governance. On 24th September 2019 the European Court of Justice delivered its judgment in “Google vs CNIL” (C-507/17) which was supposed to clarify the territorial scope of the right. However, this judgment has raised doubts about the enforceability of the General Data Protection Regulation, and reveals the complex, multi-layered governance structure of the European Union. Acknowledging such complexity at a substantive and institutional level, this article starts by analysing the judgment. Additionally, to better understand the current situation in the European Union and its member states, recently produced draft guidelines by the European Data Protection Board are presented and discussed, as well as two judgments of the German Federal Constitutional Court. Subsequently, the European developments are put in international context. Finally, the insights from these sections are combined which allows to develop several conceptual ideas. In conclusion, it is argued that the right to be forgotten remains complex and evolving. Its success depends on effective multi-layer and multi-stakeholder interaction. In this sense, it has become a prominent study object
that reveals potential venues and pitfalls on a path towards more sophisticated data protection frameworks.

1. INTRODUCTION

The “Right to be Forgotten” (RTBF) became widely known on 13 May 2014 when the decision of the Court of Justice of the European Union (ECJ) in the “Google Spain” Case was announced.¹ Subject to comprehensive academic scrutiny from the start,² Google Spain remained vague on three salient points ever since. Firstly, the rule of law and transparency are not guaranteed, since the decision whether to delist search results from the index of a search engine, as well as its implementation in practice is largely left to Google, or other Search Engine Operators (SEOs). Secondly, it is questionable whether the rights of all parties affected by delisting are safeguarded, since the publisher of the content is not being heard in the process. Thirdly and probably most prominently, the territorial scope of application remains unclear, since it is difficult to assess how far the right of an individual reaches in a virtual landscape without physical borders.

For opponents, delisting has become a prominent example for the seemingly ever-increasing EU-opean data imperialism in the regulatory domain.³ At the same time, proponents demand that delisting should be applied universally since it is an individual (human) right in their view.⁴

---

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


Acknowledging such controversy and complexity on a substantive and institutional level, this article starts with analysing the current situation within Europe (2), continues by comparing international developments (3), and uses the insights from those sections to suggest conceptual ideas (4). The analysis is focused on discussion of Google vs CNIL (2.2, 2.3). Additionally, recently produced draft guidelines by the European Data Protection Board are taken in account (2.4), as well as two corresponding judgments of the German Federal Constitutional Court (2.5).

In conclusion (5), it is argued that the RTBF remains a complex and evolving concept. The continuation of research on this subject is necessary since new cases resulting in more controversial court decisions continue to surface in many countries,\(^5\) including European states,\(^6\) and the highest courts of the EU with cases such as “Google vs CNIL”,\(^7\) as well as others with direct,\(^8\) or indirect connection to delisting and the broader concept of a RTBF.\(^9\) Furthermore, as findings of scholars in Brazil,\(^10\) legislation in Indonesia,\(^11\) or judgments in


\(^7\) Case C-507/17 Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL) EU:C:2019:772.

\(^8\) Case C-136/17, GC and Others v Commission nationale de l'informatique et des libertés (CNIL) EU:C:2019:77.

\(^9\) Case C-18/18, Eva Glawischnig-Piesczek v Facebook Ireland Limited EU:C:2019:821.

\(^10\) Sergio Branco, Memória e esquecimento na Internet, (Arquipélago 2017).

places such as Argentina,\textsuperscript{12} and Canada suggest,\textsuperscript{13} it is over-simplified to consider delisting and the RTBF as a purely EU-ronian affair. Nevertheless, European leadership based on effective collaboration between national, supranational and international governance layers might be essential for delisting to become an undisputedly positive contribution to the Digital Age.

Whether the EU has the ability to provide such strong leadership remains open at this point, particularly due to questions of intra-European power balance. In a sense, the ongoing developments around the RTBF allow to map the relationship between the Union and its member states in areas where the EU aims at fully harmonising legal frameworks. The RTBF can be considered as prototype of the ‘Europeanisation’ of data protection law. This endeavour was ultimately completed with the General Data Protection Regulation (GDPR) that came into force in May 2018. At the end of this project, the abilities of member states to regulate in the area of data protection have been restrained considerably. However, the recent developments on the RTBF raise the issue whether such extensive harmonisation succeeds in the longer run in areas where cultural differences matter, and where effectiveness hinges on enforcement by national authorities.


\textsuperscript{13} An overview of the case with relevant material is available at Global Freedom of Expression – Columbia University, ‘Google Inc v. Equustek Solutions Inc.’ \textit{(2017)}\textsuperscript{13} accessed 24 October 2019.
2. ANALYTICAL SECTION

2.1. Google Spain (C-131/12) in context

While it is certainly true that the 2014 judgment has raised the awareness of a RTBF in Europe and across the world significantly, important aspects of the case are still overlooked by many. Therefore, before analysing the more recent landmark judgment from 2019 and associated issues in detail, it seems necessary to recall some relevant aspects. Firstly, Google Spain had a very narrow focus on a specific setting which required the interpretation of European law by the ECJ according to Article 19 paragraph 1 sentence 2 of the Treaty on the EU. The judgment is based on the 1995 Data Protection Directive of the European Community. Yet, to understand the dynamics of the time, it should be added that critical assessment of the original proposal for Article 17 of the EU GDPR, particularly paragraph 2 of the draft, resulted in the removal of a RTBF in the legislative proposals discussed at the time. When Google Spain was handed down the headline of the draft article had been changed from “right to be forgotten” to “right to erasure”.


Hence, while the negotiations on what would later become GDPR were in full swing, the Judgment was neither focusing on the substance of the final Article 17 GDPR,18 nor addressing the issue of personal data and time as such, as Viktor Mayer-Schönberger had proposed pre-GDPR in his book “Delete”.19 The ECJ was solely focusing on the consequences for an individual (whose life is not of interest to the general public - legal entities such as a company, foundation or political party are excluded as well) in a case where irrelevant,20 yet controversial, personal data of the past was easily retrievable through the use of a search engine. The Grand Chamber of the ECJ found that in such a case, an unjustified distortion of the public image of a person took place. The respective individual should have a right to “delist” (in French “déréférencement”, in German “Nicht-Indexierung”) the referencing Uniform Resource Locator (URL) from the index of a search engine. In this way, the information becomes invisible for the average user when carrying out a search query based on the individual’s name, but the original data remains available at the original source. While there are elements of the issue of personal data and time in the facts of the case and the ultimate decision (interpretation of the legal framework) of the ECJ, the general equalisation of the judgment with the RTBF as proposed originally by Mayer-Schönberger is unprecise, and confusing.21 Additionally, judgments made in line with the procedure of Article 267 of the Treaty on the Functioning of the European Union (TFEU) are formally only binding “inter partes”, not “erga

20 Google Spain SL (n 1) [92] “[…] inadequate, irrelevant or excessive in relation to the purposes of the processing, that they [data] are not kept up to date, or that they are kept for longer than is necessary unless they are required to be kept for historical, statistical or scientific purposes.”
21 This might also be one of the main reasons why discussions on the subject are so controversial, and hardly ever come to compromising results.
This also emphasizes the limited scope of ECJ rulings in an Article 267 TFEU procedure, which means that such mere interpretation neither produces a final decision in the case at stake, nor establishes precedent in accordance with the ‘stare decisis’ doctrine that is typical for many common-law jurisdictions.

Secondly, while it is not surprising that after “Google Spain” the wording RTBF “came back” in the heading of Article 17 GDPR, it remains an open question how precisely the final wording of the regulation addresses delisting as the ECJ has established it through jurisprudence. Unfortunately, this aspect has also not been discussed in detail in the 2019 case of Google vs CNIL, which is the main subject of this article. Arguably, Article 17 paragraph 1 lit. c of the final version of GDPR in combination with Article 21 GDPR reflects the essence of delisting best, whereas Article 17 paragraph 1 lit. d GDPR might offer a less elegant solution. However, there is also a proposal in the literature to consider delisting requests using different legal frameworks such as EU Council Directive 2000/31/EC (e-commerce directive). Nevertheless, it seems appropriate to highlight that Article 17 paragraph 2 GDPR which was presumably drafted by the European Commission as a response to the “original” idea of an actual RTBF as presented by Mayer-Schönberger, remains a provision to erase information with a vague spectrum of rights for the individual, and vague duties for the controller. Regrettably, the history

---


23 Google LLC (n 7).


26 An individual right which allows to erase personal information from the digital sphere entirely. For a detailed analysis see Oskar Josef Gstrein, Das Recht auf Vergessenwerden als Menschenrecht (Nomos 2016) 131-132.
and final wording of Article 17 GDPR have become an example of what remains to be desired in clarity of the regulation in general. This also poses significant challenges for national authorities tasked with enforcement of data protection law, such as national data protection agencies (DPAs). In consequence, the exact definition of the substantive scope, and due process of, as well as necessary exceptions to the RTBF are still inexistent.

Thirdly, delisting is about the distribution, and accessibility of content, not about the “existence” of content as such. Here it is useful to remember the work of Canadian philosopher and media theorist Marshall McLuhan, who famously coined the phrase “the medium is the message.”  He convincingly points out that it is not only the pure content that matters when exchanging information. To the contrary, the form, structure, and accessibility of information also shapes the final message in its essence. While McLuhan was carrying out his analysis predominantly focusing on mass printed books, and mass television, his findings remain valuable in the Digital Age where platforms like Twitter (280 characters per Tweet), Instagram (predominantly picture based), and others meticulously structure the design, presentation, distribution, interaction and accessibility of content for their vast number of users across the world. This aspect should also be remembered when deciding whether a search engine operator is a ‘data controller’ or not, which was an essential question in the Google Spain judgment.  

2.2. National Data Protection Authority versus Internet giant

After the ruling of May 2014, Google setup an advisory council which held several meetings in different cities all over Europe to publicly discuss the RTBF, and the appropriate balance with freedom of expression and the right to information. This advisory council consisted of several


28 *Google Spain SL* (n 1) [35]-[38].
high-profile academics, ex-politicians, and Internet experts. While the initiative started with much momentum, an active observer could not escape the impression that actual policymakers in the EU, and several EU member states were not too happy with the public questioning of a ruling of the EU’s highest court. Nevertheless, the advisory council produced a final report, in which it was focusing particularly on criteria for assessing delisting requests, and procedural elements such as the geographic scope. The advisory council summarized in this report that the issue of territorial application is complex, that it is possible that existing implementation practices at the time might allow for circumvention for certain (skilled) users based in Europe, and that this compromise should ultimately be accepted, keeping proportionality and extraterritoriality in application of European law in mind. Van Alsenoy and Koekkoek have further highlighted, that delisting could be implemented either by using a domain-name based approach, geographic filtering, or through global implementation. Padova argues that the RTBF can be a universal, regional, or ‘glocal’ right. In practice, Google initially only delisted requests based on the domain of the search engine used, but it refined the procedure after concerns by the French Data Protection Authority (Commission Nationale de l'Informatique et des Libertés; CNIL) that it was too easy to circumvent the implementation by using the US-American version of the search engine, for

29 The Advisory Council to Google on the Right to be Forgotten Final Report (Google, 2015)<
accessed 24 October 2019.

30 ibid, section 4.

31 ibid, section 5.4

32 ibid 18-20.


34 Yann Padova, ‘Is the right to be forgotten a universal, regional, or “glocal” right?’ [2019] International Data Privacy Law 9-1, 21-29.

35 Such as google.fr, google.de, google.nl, and similar domains addressing EU/EEA countries. But not google.com.

Considering the aspect of enforcement for a moment, Google vs CNIL is a good example to illustrate the complex relationship between the different variants of harmonised EU law and its execution by national authorities. In absence of clear and precise guidance on the substantive nature of the RTBF in Google Spain, the executing French Data Protection Authority developed an autonomous interpretation of the legal requirements determining technical implementation.

It should be borne in mind that the legal basis for this interpretation was the ECJ reading of the 1995 data protection directive, which is “[…] binding, as to the result achieved, […] but shall leave to the national authorities the choice of form and methods” according to Article 288 TFEU. This is in contrast to a regulation (such as GDPR) which “shall be binding in its entirety and directly applicable in all Member States” as also stated in Article 288 TFEU. In other words, the new judgment was not only necessary to understand the original meaning of the RTBF as based on the directive better. Since the European data protection regime transitioned from a
directive to a regulation as legal basis, one would expect that the ECJ develops more detailed substantive criteria on the interpretation of rights and duties, since DPAs like CNIL arguably have a weaker mandate to autonomously interpret substantive provisions in the changed legal architecture. Certainly, one might argue that the ECJ also needs to take into account other rights than data protection and privacy when defining the RTBF, particularly freedom of expression. However, formally, the legal proceedings are based on specific secondary European data protection law. It certainly has to be interpreted and applied in compliance with provisions of primary EU law, such as enshrined in the Charter of Fundamental Rights of the EU (CFEU) and relevant national traditions as enshrined in Article 6 paragraph 3 TEU. Nevertheless, from a purely dogmatic perspective more general (primary law) provisions do not outweigh specialised (secondary) laws if they exist and are in force, even when acknowledging that the relationship between primary and secondary law in the EU can be complex.40

Moving on to the parties positions in the case, both sides brought strong arguments to the bench. On the one hand, it was emphasized that extraterritorial application of law is problematic in general, and that insistence of the EU on a global implementation of delisting might ultimately lead to more censorship,41 in Europe and potentially other regions of the world.42 Additionally, and as already mentioned, fragmentation of the regulatory framework is a serious problem for corporate activities on the Internet. On the other hand, if there is an individual right to delist a

---


42 Owen Bowcott, ‘Right to be Forgotten’ could threaten global free speech, say NGOs’ (The Guardian, 2018)<https://www.theguardian.com/technology/2018/sep/09/right-to-be-forgotten-could-threaten-global-free-speech-say-ngos> accessed 24 October 2019; The censorship argument voices a serious concern, but does not ultimately address the fundamental issue. Nevertheless, it voices important concerns regarding the institutions safeguarding that delisting is only granted on the basis of the rule of law, democracy, and human rights.
URL from the index of a search engine, the individual can only benefit from it if it is effectively exercised. In this view, and if it is impossible to implement an individual right effectively, it is non-existent as such. This dispute can also be understood as a case defining whether technology giants have to comply with the law - or vice versa - which certainly complicated the matter, and elevated the likelihood that substantive dogmatic considerations would be severely impacted by political circumstances.

The first question of the request of the Conseil d’État was whether a “right to de-referencing” must be applied by the operator of a search engine on all of the serviced (Internet) domains, irrespective of the place where the search (which is based on a person’s name) is conducted, and even if that territory is not covered by the territorial scope of the old EU data protection directive from 1995. The second question continued from there and focused on a negative answer. Thus, if there was no extraterritorial application of delisting, must such requirement be limited to a specific member state of the EU, or are all member states of the EU covered. The third question focused on technical implementations of delisting.

43 Commission Nationale de l’Informatique et des Libertés (n 38) : « Seule une mesure s’appliquant à l’intégralité du traitement lié au moteur de recherche, sans distinction entre les extensions interrogées et l’origine géographique de l’internaute effectuant une recherche est juridiquement à même de répondre à l’exigence de protection telle que consacrée par la CJUE. »

44 Effectively this means that the territories of the member states of the EU are covered (with some small exceptions for certain oversea territories for some states) as well as Norway, Liechtenstein, and Iceland since they are part of the European Economic Area. For more on the exact territorial application see Jörg Ukrow, ‘Data protection without frontiers? On the relationship between EU GDPR and amended CoE Convention 108’ [2018] European Data Protection Law 240, 240-241.

45 Google LLC (n 7), questions 2, 3. As a side note, the wording “right to de-referencing” which is used in the official English translation of the request for a preliminary ruling, is based on the French term “droit au déréférencement”, and means exactly the same as the concept delisting which is used throughout this text.
On 10 January 2019 Advocate General (AG) Maciej Szpunar presented his opinion in the case.\textsuperscript{46} Although he stated that the idea of global delisting appeals due to “its radicality, its clarity, its simplicity and efficiency”,\textsuperscript{47} he suggests that such interpretation would only consider one side of the coin. Szpunar sees the danger that the authorities of the EU would be overwhelmed with controlling a worldwide application of the right.\textsuperscript{48} Additionally, the EU would be interfering with the right to information of people outside its territories.\textsuperscript{49} In essence, the AG does not see the legal basis for extraterritorial application, and proposes therefore to answer the first question negatively. In combining the second and third question, Szpunar interprets the law in a way that an SEO is required to take all measures at its disposal to make sure the entry cannot be found on Union territory. He mentions and discusses “geo-blocking” in this context, a method that uses the Internet Protocol address and other technological artefacts of a user which allow to draw inferences on the location of a user in order to limit access to content.\textsuperscript{50} Overall, his opinion can be summarized in stating that Szpunar proposed to limit delisting to the territory of the EU, but within it users should not be able to find delisted content by using even advanced methods. The style of his argumentation seems mostly based on formal considerations, rather than the substantive content of provisions.

2.3. \textit{Key points of Google vs CNIL (C-507/17)}

Unlike in Google Spain, the final judgment follows the opinion of the AG and combines it with the known lines of argumentation from the 2014 judgment. In paragraph 54 (out of 74), the ECJ finally seems to make an attempt to add a substantive element to delisting by stating: “It is true

\footnotesize\textsuperscript{46} Google Inc. v Commission nationale de l’informatique et des libertés (CNIL), Case C-507/17, [2019] Conclusions de l’Avocat Général M Maciej Szpunar.
\footnotesize\textsuperscript{47} ibid [36].
\footnotesize\textsuperscript{48} ibid [60].
\footnotesize\textsuperscript{49} ibid [61].
\footnotesize\textsuperscript{50} ibid [70], [71], [78].
that a de-referencing carried out on all the versions of a search engine would meet that objective in full.”

Unfortunately, this is the only sentence in this paragraph, making the entire paragraph and judgment a missed chance to deliver substantive guidance on this crucial issue and the nature of delisting. Hence, the ECJ fails to more clearly define concepts such as necessity and proportionality when applying delisting. A matrix with criteria could have been presented with validity for the EU, potentially building on other existing non-legally binding proposals, as for example developed by the ex-Article 29 Working Party consisting of national DPAs of the EU which has now become the European Data Protection Board (EDPB). To the contrary, the ECJ seemed not to be interested in more substantive top-down harmonisation as it states “it should be pointed out that the interest of the public in accessing information may, even within the Union, vary from one Member State to another”. The Grand Chamber goes on to argue that national data protection authorities should engage in dialogue and cooperation to resolve this issue.

Certainly, the restraint of choosing a clear direction in territorial application is understandable when considering the delicate nature of the topic with is manifold political and economic implications. The judges need to navigate the waters between Scylla and Charybdis since Article 3 GDPR effects in extraterritorial application of the regulation which provokes the expectation of universal applicability of individual rights, yet leaves open how enforcement outside the territory of the EU should be handled by national DPAs. The ECJ recognizes this

51 Google LLC (n 7).


54 Google LLC (n 7) [67].

55 ibid [68], [69].
reality by stating that delisting cannot be enforced on a worldwide scale by national DPAs in the EU.\textsuperscript{56}

However, this finding results in many uncomfortable questions: Has the European legislator factually overburdened its institutions, especially the national ones enforcing the majority of EU law? What does that say about the existence and importance of individual rights of data subjects residing in the EU, after almost a decade of promises that they are protected against the multinational giants GDPR was drafted to regulate? Certainly, the ECJ adds that SEOs must take measures “seriously discouraging internet users”,\textsuperscript{57} but the judges do not develop criteria how this should technically work. Arguably, this is a big problem since we have seen in the past that it leaves the enforcement of delisting effectively to SEOs,\textsuperscript{58} which lead to this case in the first place. Hence, the problematic aspects threatening the rule of law and democratic control of digital space are neither resolved, nor addressed by this judgment, which is worrying since the digital domain is already heavily influenced by the forces of “surveillance capitalism”\textsuperscript{59}.

Still, the real disappointment about this judgment comes at the very end, where the ECJ seems to completely blur the line between the harmonisation of data protection law and the margin of appreciation for national authorities when interpreting and executing it. Rendering its own preceding elaborations practically meaningless, the ECJ adds that national authorities might in the light of national standards of protection of fundamental rights require SEOs to carry out universal delisting (!).\textsuperscript{60} This is against the spirit of the GDPR and giving back the power of regulation to member states and their authorities. It is also potentially very dangerous, since

\textsuperscript{56} ibid [64], [65].

\textsuperscript{57} ibid [70].

\textsuperscript{58} Julia Powles and Enrique Chaparro, ‘How Google determined our right to be forgotten’ (\textit{The Guardian}, 2015) \url{<https://www.theguardian.com/technology/2015/feb/18/the-right-be-forgotten-google-search>} accessed 22 October 2019.


\textsuperscript{60} \textit{Google LLC} (n 7) [72].
different DPAs might develop different interpretations of delisting when balancing it with other rights, taking into account national traditions and established practices. In light of this statement and considerable efforts made to promote GDPR as a fully harmonised framework protecting data subjects all across a unified Europe, one wonders how the judges in Luxembourg explain to those data subjects in the future that they might have a right to delist information from the index of a search engine universally in one country (e.g. France), ‘glocally’ with the application of geo-blocking technology in another (e.g. The Netherlands), and only nationally in the third (e.g. Germany). It is also unclear whether there will be the possibility for ‘forum shopping’ for European data subjects, picking and choosing the kind of delisting that they prefer themselves. With this looming threat of fragmentation, one might argue that even SEOs like Google cannot be content with the outcome of the proceedings.61

2.4. 2019 Decisions of the German Federal Constitutional Court

While the primary focus of this analytical section is on the Google vs CNIL judgment, it is important to augment it with two developments that followed shortly after the publication of the ECJ decision. These developments underline the finding that the judges in Luxembourg left the space to define delisting largely to national authorities.

On 6 November 2019 the German Federal Constitutional Court (FCC) issued two decisions on the RTBF, which are entitled RTBF I and RTBF II, respectively.62 The decisions have also been published in English,63 which can be seen as another indicator for their intended international


62 Case 1 BvR 16/13, Recht auf Vergessen I, [6 November 2019]; Case 1 BvR 276/17, Recht auf Vergessen II [16 November 2019].

relevance. Focusing first on the institutional perspective, it has been argued that the decisions should be interpreted as a contribution of the FCC to the further development (or perhaps recalibration) of the fundamental rights system in the EU and Europe. As Gärditz and Polakiewicz argue,64 the FCC is leaning towards an understanding of the fundamental rights framework in Europe which resembles the kinetic structure of a “mobile”. Such a flexible and egalitarian model of interchange is an alternative to the model of a pyramid which symbolizes clear legal competences and power structures, with the European organisations and institutions on top. The mobile is supposed to give courts on the national, supranational and international level enough room to develop and interpret human rights autonomously, while not threatening interconnectedness and interdependency. Polakiewicz describes that this concept has been suggested by current FCC president Voßkuhle in a speech held in January 2014.65 Hence, and according to the case law references in the decisions themselves,66 this German jurisprudence has to be understood as a continuation of the complicated and long-standing discourse on the status of European integration of the German legal order in the fundamental rights systems of the EU and the Council of Europe. While other member states of the EU tend to show their friction with European institutions mostly on a political level, Germany has a tradition of


66 Case BvR 16/13, paras 48-65; BvR 276/17, paras 88-94.
defining the relationship in the form of systematic case-law. In this regard it is also interesting to see how the FCC judges explain in detail why the two cases do not require referral to the ECJ according to the European and German jurisprudence on Article 267 TFEU.

This procedural autonomy leads to more detailed description of delisting on a substantive level. Before describing the main aspects of how the FCC interpreted delisting in the two decisions, it is important to briefly outline the respective backgrounds of the decisions. RTBF I is based on a dispute about the accessibility of press reports in an online archive of a large German news magazine. These articles describe a spectacular case of murder that has been subject to extensive media coverage on a national level. At the time of writing of this article, the details of the case can still be found online by searching for the ship that was involved, or other circumstances which are described in the decision itself. The person that has been convicted for murder and reported on in the years 1982 and 1983 in the magazine, as well as other news sources afterwards, demands in its application that a search with an internet search engine based on its name should not contain links to the articles from the 1980ies which have become part of an online archive of the magazine. The person argues that this is unwarranted since it was released from jail after serving the sentence and since it has started to re-integrate in society. Maybe it should be borne in mind that this re-integration process is already ongoing several years by the time this case is discussed before the FCC.

The background of the RTBF II decision is an episode of a television magazine which has been produced and broadcast by a publicly founded TV station in Germany. The episode describes unfair practices of employers against their employees. One of the persons portrayed is the


68 Case BvR 16/13, paras 71-74; BvR 276/17, paras 64-94.

69 Case BvR 16/13, paras 1-12.
applicant in this case. It requires that an internet search based on its name should not show links to an archived version of the episode which has become available online, and which still shows the person acting on behalf of an employer. The person fears that users of the search engine would be led to believe that it has a bad character and argues that the consistent availability of the episode illegitimately limits its capacity for further personal development.\footnote{Case BvR 276/17, paras 1-19.}

In result, the FCC accepted the complaint of the applicant in RTBF I, whereas it denied success to the complaint in RTBF II. It would go beyond the scope of this submission to discuss the complex integration of delisting in the German legal order with all its side-effects through these two decisions in detail, although much is to be analysed and discussed in terms of updated fundamental rights dogmatic. Especially when it comes to the relationship between technology corporations and individuals in the light of the German concept of informational self-determination,\footnote{Case BvR 16/13, paras 84-95.} Zuboff’s ‘surveillance capitalism’ seems to resonate with the judges of the FCC.\footnote{Shoshana Zuboff, 28-1 New Labor Forum 10-29.} Two other substantive key aspects of the decisions relate to the balance with freedom of expression and the decision on what is part of collective history.

publisher with the interest of the SEO to run its business very strongly.\(^74\) Hence, the SEO becomes a medium to integrate the interests of the original content publisher in the balancing exercise of the judges. This means that data protection considerations are not per se overriding other rights when it comes to delisting. Furthermore, when it comes to deciding which information becomes part of collective history, the FCC underlines that the decision on which personal information is of historic interest is not only a question that has to be considered from the perspective of the affected individual. Rather, the meaning of the specific action to society and its changing nature over time are also important. This is particularly emphasized in relation to RTBF I and the underlying case that has become subject to widespread media coverage.\(^75\) When considering these two decisions in conclusion, one might argue that the national legal order, with its fully developed criminal and media law provisions might be more appropriate to explore the detailed nature of delisting than the legal sphere of the EU, where a fully harmonized data protection framework exists, yet a corresponding media and publication framework is lacking. However, as interesting and dogmatically clear these FCC decisions are, little is being stated about the geographical scope of delisting. Therefore, one might suggest that the FCC assumes that its decisions will be enforced by German authorities, which in return means that the substantive dimension of the German version of delisting will largely be restrained to the territorial borders of Germany. Whether this is the best possible outcome for German data subjects in a Digital Age with largely cross-territorial data flows, remains to be seen.

2.5. Draft Guidelines of the European Data Protection Board

It is not only national high courts that have become active after the Google vs CNIL judgment. On 2 December 2019 draft guidelines ‘on the criteria of the Right to be Forgotten in the search

\(^74\) Case BvR 276/17, 1.

\(^75\) Case BvR 16/13, paras 107-113.
engines cases under the GDPR where adopted by the EDPB, the successor of the Article 29 Working Party. For clarification it should be added that at the time of writing the draft guidelines were still in the stage of public consultation. As mentioned in the section 2.3., the Article 29 Working had already produced guidelines on the implementation of delisting in 2014.

While such guidelines are not legally binding and merely interpret existing laws and court judgments, they have had considerable factual authority in the past. Frequently, they are considered as (politically?) binding consent of data protection authorities in the EU, which have strategically aligned their positions to increase the impact of their work over many years now. However, the forum of the Art 29 Working Party has been transformed with the emergence of GDPR, strengthening the idea of ‘distributed governance’. Compared to the Art 29 Working Party the new EDPB has gained increased powers and competences.

The first public version of the guidelines on delisting only covers the grounds a data subject can use to request delisting from an SEO based on Article 17 paragraph 1 GDPR, as well as corresponding exceptions stemming from Article 17 paragraph 3 GDPR. However, the EDPB confirms in the introduction that both Article 17 GDPR and Article 21 GDPR (Right to object) can serve as legal basis for delisting, which mirrors the stance taken earlier in this piece when


77 Article 29 Data Protection Working Party, ‘Guidelines on the implementation of the Court of Justice of the EU judgment on “Google Spain and inc v. Agencia Espanola de Proteccion de datos (AEPD) and Mario Costeja Gonzalez” C-131/12’, (2014) 14/EN WP 225.


exploring options for a detailed legal basis in the GDPR.\textsuperscript{80} This first public version of the guidelines was planned to be supplemented with an appendix containing criteria for data protection authorities to handle complaints for refusals of delisting.\textsuperscript{81}

It is premature to speculate on the exact outcome of this process. Nevertheless, the guidelines are already relevant since they contain detailed arguments on how a specific legal ground for delisting in Article 17 GDPR works.\textsuperscript{82} While this part seems to be worked out in detail already, the draft also contains some analysis why delisting might be refused according to Article 17 paragraph 3 GDPR. Here, the section on balancing the right to privacy with freedom of expression stands out. Still, since it refers mainly to the original Google Spain Case, as well as a 2018 decision of the European Court of Human Rights in Strasbourg that will be discussed in more detail below,\textsuperscript{83} novel arguments or more detailed instructions for the balancing exercise are largely missing. Nevertheless, the tendency to align the right to freedom of expression of the original publisher increasingly with the interest of the SEO can also be seen in this document,\textsuperscript{84} which mirrors what has been described in the previous section.

3. INTERNATIONAL CONTEXT

3.1. Delisting as a global phenomenon

The 2019 decision in Google vs CNIL is particularly disappointing, since the judges seem to miss the bigger picture: the RTBF and delisting are not purely European concepts. While the

\textsuperscript{880}Oskar Josef Gstrein [2017] Privacy in Germany 13.


\textsuperscript{883}M L and W W v Germany App no 60798/10 and 65599/10 (EChHR, 28 June 2018). Although this case relates to Germany it is not unreasonable to expect that individuals from countries outside the EU bring similar claims to Strasbourg.

\textsuperscript{884}EDPB Guidelines 10-11.
RTBF is frequently associated with the EU and GDPR, a comparative perspective on the topic suggests that this is clearly a misconception. In South America, both Argentina (*Virgina da Cunha* case)\(^{85}\) and Brazil (*Daniela Cicarelli* case)\(^{86}\) have significant developments in the area, which partly precede the 2014 judgment of the ECJ to 2010 or earlier. At the time of writing, appearances of the right in court judgments, statutes, or draft legislation are further documented for Canada,\(^{87}\) Chile,\(^{88}\) Colombia,\(^{89}\) Indonesia,\(^{90}\) Israel,\(^{91}\) Mexico, Peru, Kenya, Russia,\(^{92}\) and Turkey.\(^{93}\) Additionally, a 2018 judgment of the European Court of Human Rights in Strasbourg invites speculations whether delisting and the broader concept of a RTBF are not only relevant for the member states of the EU, but the larger Europe with states such as Switzerland.\(^{94}\) Even before this judgment specifically relating to delisting the Strasbourg court produced considerable amount of case law addressing this area.\(^{95}\) Japan has a vivid discussion on the

---

86 Branco (n 10) 130-131.
87 Supreme Court of Canada, Google Inc. v Equustek Solutions Inc. (2017) 2017 SCC 34.
88 Apers (n 5) 7-8.
90 Rahman (n 11).
94 M.L. and W.W. v Germany App no 60798/10 and 65599/10 (ECtHR, 28 June 2018). Although this case relates to Germany it is not unreasonable to expect that individuals from countries outside the EU bring similar claims to Strasbourg.
nature and implementation of the right, and there is considerable jurisprudence on the topic in the country.96 Finally, it has recently been discussed and argued that a RTBF should also be existing for children in Australia.97

If one counts the number of states mentioned in this section it can be assumed that more than 25 percent of the nations on earth have seen considerable developments in the area of delisting and the RTBF.98 It needs be emphasized at this point that while the research supporting this claim has been carried out by observing the regulatory landscape over several years, it cannot be claimed that this list is complete, nor that all of the mentioned developments are considered desirable when measured on the scales of human rights, rule of law, and democracy. However, without more thorough study it also seems unwarranted to conclude that the appearances of delisting and the RTBF outside Europe are predominantly negative in terms of their impact on the rights and freedoms of internet users.

Finally, these findings should be read together with comparative research from Erdos and Garstka from 2019, which is looking at the compatibility of a RTBF with the data protection frameworks of all G20 nations. They conclude that “fifteen out of the nineteen G20 States (almost 80%) have now adopted data protection laws which establish a general framework for most forms of personal data processing. Moreover, all of these laws include rectification rights enabling individuals to require action in relation to ‘inaccuracy’ and all bar one explicitly empower individuals to raise broader challenges as regards the legitimacy of an ongoing

---


97 Anna Bunn, ‘Children and the ‘Right to be Forgotten’: what the right to erasure means for European children, and why Australian children should be afforded a similar right’ (2019) 170(1) Media International Australia 37.

98 Of the approximately 200 countries in the world, the council of Europe alone has 47 member states including the member states of the EU and the European Economic Area. Together with the countries mentioned in Latin America, Africa, and Asia this number raises to the indicated threshold.
dissemination of personal data.” Delisting relates to a serious problem that requires detailed, and concrete answers. Certainly, these answers are not easy to find, but the main question is probably not any longer whether delisting should exist as such. It would be more important to consider which procedures and safeguards need to be in place to guarantee proper application of this complex “tool”, particularly when it comes to necessity and proportionality of its application.

3.2. “Repurposing” of the right to be forgotten

Since the Google Spain judgment delisting as a tool has also been “tested” in different settings by many actors, and courts in different countries. To provide a broader perspective this section will outline the most significant developments in this regard. Soon after the judgment in May 2014 a discussion started whether delisting could be a useful remedy for victims of “revenge porn”, or similar sensitive content that has been produced and shared without consent. Indeed, for many victims whose intimate pictures, or videos are being spread all across the internet, it seems impossible to stop the increase of harm without an intervention of intermediaries such as search engines or video platforms. On 19 June 2015 the ex-senior vice president of Google Inc., Amit Singhal, announced in a blog post that “going forward, we’ll honor requests from people to remove nude or sexually explicit images shared without their consent from Google Search results. This is a narrow and limited policy, similar to how we treat removal requests for other highly sensitive personal information, such as bank account numbers and signatures, that may surface in our search results. In the coming weeks we’ll put up a web form people can use to

---


submit these requests to us, and we’ll update this blog post with the link.”101 While the post itself does not mention delisting or the Google Spain case, the connection to the issue was obvious, and perceived as such by commentators.102

Furthermore, in 2013 the State Legislature of California passed two laws which relate to revenge porn establishing arguably comparable individual rights. One of these laws prohibits dissemination of sexually explicit images without consent, while the other affords juveniles the right to delete data provided by themselves which is being reposted or -published by others.103 Additionally, the emergence of ‘deepfake revenge porn’ videos using artificial intelligence and machine learning to transfer the portrait of the victim into a seemingly realistic ‘recording’ might also become relevant in the context of delisting, and is already subject to regulatory activities in California.104 From 2017 onwards, and connected to a law suit from a young woman who became a revenge porn victim in New York City, the issue again sparked a broader discussion of a RTBF in the United States.105 A bill containing a variation of a RTBF was discussed in the State Assembly.106 It remains to be seen whether this translates into a more comprehensive and federal approach. The urgency of this issue has been most recently

---


underlined by another scandal in the United States, where producers of an adult content website coerced young women into participating in videos. Even after the women were granted millions in compensation following legal procedures, it turned out to be practically impossible to remove the videos from the internet.\textsuperscript{107} In contrast to the cases of Virgina da Cunha, or Daniela Cicarelli, it can also not be argued that there is any public interest in this material.

The second related area keeps the spotlight on the United States and is connected to law enforcement and the publication of “mugshots”.\textsuperscript{108} These are portrait pictures taken by law enforcement agencies after people have been taken into custody. Most of these unflattering and potentially (mid- to long-term) problematic portraits are the result of minor crimes, or misdemeanour. Many law enforcement agencies publish these pictures online which are then aggregated by dedicated portals,\textsuperscript{109} or news outlets. Some of these outlets charge money in order to remove the portraits, which is heavily debated and raises the question of the role of websites in this area.\textsuperscript{110} Proponents of delisting might argue that this practice shows that the non-existence of the right creates a void that is being used for the development of an industry built on a business model of removing content. The end-result often is the same as with delisting, but the concerned individual has to pay a considerable amount of money for its privacy. Due to different regulatory traditions in the area of data processing it seems unlikely a North American


\textsuperscript{109} See for example the website <https://mugshots.com> accessed 24 October 2019.

version of delisting or a RTBF will be created in the short term,\textsuperscript{111} but it also has been argued that it would be consistent and possible when focusing on natural law and human dignity.\textsuperscript{112} The third area of unforeseen “repurposing” has nothing to do with personality or privacy, but keeps the connection to the North America, and Google as a search engine operator. Back in 2011 two small Canadian corporations, Equustek Solutions Inc. and Datalink, got into a fierce dispute related to intellectual property rights.\textsuperscript{113} Datalink used to distribute networking devices of Equustek, but eventually acquired confidential information and trade secrets, and began to re-label own products as Equustek’s.\textsuperscript{114} Despite Canadian courts ordering a prohibition of the sale of inventory, and the use of Equustek’s intellectual property, the operations of Datalink continued from an unknown location via the internet. Since removing individual listings of Datalink’s illegal offers by Google proved ineffective, and since it was impossible to identify the physical location of Datalink’s operations, the Canadian courts ordered Google to delist the relevant search results. Google, which was a non-party in the dispute, appealed against this decision. Eventually, the case had to be considered by the Canadian Supreme Court which upheld the obligation of Google to keep delisting Datalink’s offers.\textsuperscript{115} What followed was a territoriality dispute between a Californian court and the Canadian Supreme Court, which ended with the latter again insisting on the delisting obligation in a decision on 28 June 2017. In this last verdict, the Canadian Supreme Court found that Google had to comply with the ruling although it had to effectively comply in the United States: “[…] On balance, therefore, since the interlocutory injunction is the only effective way to mitigate the harm to Equustek pending

\textsuperscript{111} Keller (n 25) 315-318.


\textsuperscript{113} Supreme Court of Canada (n 87).

\textsuperscript{114} ibid 5-6.

\textsuperscript{115} Global Freedom of Expression (n 13).
the resolution of the underlying litigation, the only way, in fact, to preserve Equustek itself pending the resolution of the underlying litigation, and since any countervailing harm to Google is minimal to non-existent, the interlocutory injunction should be upheld.”

4. CONCEPTUAL SECTION

4.1. Multi-level governance and territorial scope

The governance of the internet is typically characterised as “multi-stakeholder mechanism”, influenced by seven different groups. Those are states/governments, private sector commercial entities, civil society, intergovernmental organizations, other international private sector organizations, the academic community, and the technical community. Nevertheless, how this multi-stakeholder governance works in detail remains unclear for the most part. While it seemed for years that developments related to governmental surveillance, such as the EU-US negotiations on “Privacy Shield”, would predominantly determine the territorial scope of individual rights in the digital domain, the adoption of the US CLOUD Act combined with the vacation of the US Supreme Court judgment in the “Microsoft Ireland Case” has arguably moved the spotlight on cases such as Google vs CNIL. A proposal for a “framework for responsible data protection regulation” published by Google Chief Privacy Officer Keith

116 ibid [53].
117 Such as the “Global Network Initiative” which is an alliance of Internet and telecommunications companies, human rights and press freedom groups, investors, and academic institutions from around the world. More information can be found via <https://globalnetworkinitiative.org> accessed 25 September 2018.
Enright in September 2018 emphasized once more that potential fragmentation of the internet is a serious concern for all private corporations,\textsuperscript{121} regardless of their size, or influence. However, as has been outlined above in the section on key points of Google vs CNIL, the judgment itself does not deliver a clear answer. While the ECJ seems to favour a ‘glocal’ solution, limiting the existence of a RTBF to the territory of the EU with the addition of SEOs applying technical measures “seriously discouraging internet users” from accessing delisted links at any other version of the search service,\textsuperscript{122} it remains unclear how this should be implemented technically. At the same time the ECJ leaves it to member states and their authorities to interpret delisting at the end of the judgment. As has been outlined in the analytical section, it remains to be seen whether national high courts will fill this gap in the governance structure of a ‘mobile’, or whether the ‘distributed governance’ of the EDPB will prevail. Hence, it has to be concluded that there is no clear path of progress on this aspect. It is unlikely that this issue can be solved without more international consensus on the substantive nature of delisting, although it might seem unrealistic to expect that a forum could be gathered enabling such political engagement and agreement. Arguably, it would have been the role of the ECJ to continue to provide the groundwork for such deliberations, living up to its role as “motor of integration” in the EU, and potentially abroad.\textsuperscript{123} Nevertheless, and regardless of the activity of high courts, it remains first and foremost the role of legislators to


\textsuperscript{122} Google LLC (n 7) [70].

\textsuperscript{123} Michael Blauberger and Susanne K. Schmidt, ‘The European Court of Justice and its political impact’ (2017) 40(4) West European Politics 907.
add substantive elements to delisting, which is a task that was largely ignored in the development of GDPR.  

4.2. Revisiting the purpose of the balancing exercise

Considering all these developments, it seems unlikely that the debate about delisting and the RTBF in the broader sense has ended with Google vs CNIL. Certainly, at least for the EU it will remain challenging to understand the dimensions of the right. On the same day that Google vs CNIL was handed down, the ECJ also published its verdict in GC and Others vs CNIL, where the court had to deal with several cases in which it was unclear how sensitive personal information (e.g. political or philosophical beliefs, ethnic backgrounds, etc.) ought to be delisted. Several days later on 3 October 2019, in a case concerning hateful comments on the social network Facebook against the ex-leader of the Green party in Austria, the ECJ found that such comments need to be removed worldwide on the platform if necessary and proportionate.

It is beyond the scope of this submission to discuss both of these judgments in detail. However, in light of all of these proceedings covering similar issues, one wonders whether the existing dogmatic framework needs not be recalibrated in order to develop a holistic perspective which would promote (restore?) legal certainty. Traditionally, it is established practice to start with the consideration of one specific human right (privacy, data protection, freedom of expression, etc.) and balance it with other rights. As the regularly updated factsheets of the European Court of Human Rights in Strasbourg demonstrate, these balancing exercises need to take into account

124 Gstrein (n 26).

125 GC and Others (n 8).

126 Facebook Ireland Limited (n 9).

account the circumstances of each individual case and can be difficult. It is particularly challenging to deduct a common paradigm from the plethora of proceedings dealing with similar issues. This is the same in Luxembourg, with each of the judgments being formally only binding “inter partes”, and not “erga omnes”.128 Hence, it might be useful to consider the addition of an argumentative meta-layer in order to create an overarching framework for the jurisprudence, and more certainty for concerned parties who usually have to start costly and lengthy proceedings before ending up in European high courts.

Considering the setup of modern human rights law and the EU’s fundamental rights system, the principle of human dignity is arguably at its core,129 as enshrined in Article 1 CFEU. Therefore, it seems possible to argue that the principle of human dignity can serve as a guiding paradigm when establishing the balance between different rights such as freedom of expression and privacy. Keeping in mind that the end-result of the balancing process has to respect and protect human dignity, it might be possible to replace the balancing scale - adding a little bit more of one right at the cost of another - with a spiral in which the emphasis of the jurisprudence keeps oscillating between the poles of pure privacy and freedom of expression. The inherent aim of such jurisprudence is to strive upwards, achieving a higher level of human dignity as it evolves.

While such dogmatic interpretation is new to the discourse on delisting that has been segregated between those arguing either for more privacy and against freedom of expression or vice versa, such a different approach could be rooted in the discourse on the establishment of a right to “informational self-determination”. This is based on the principle of human dignity, in combination with the right to personal development, originating from a census discussion in

128 Prete (n 22).

(West-)Germany in 1983. More recently, it has also been suggested to understand informational self-determination as a right to control the digital narrative of one’s life. Furthermore, in 2017 the United Nations have elaborated on the interconnection and interdependence of these rights by “[r]ecognizing that the right to privacy can enable the enjoyment of other rights and the free development of an individual’s personality and identity, and an individual’s ability to participate in political, economic, social and cultural life, and noting with concern that violations or abuses of the right to privacy might affect the enjoyment of other human rights, including the right to freedom of expression and to hold opinions without interference, and the right to freedom of peaceful assembly and association,...” To give the law and jurisprudence such a “mission” is particularly fitting for the regulatory framework of the EU, considering its particular “sui generis” nature, and the importance of the “effet utile” principle.

4.3. Rule of Law and Transparency of the procedure

Google took the lead in the implementation of the ruling of the ECJ after Google Spain. This has also revealed interesting perspectives on the corporation as a political actor. Furthermore, Google also setup a dedicated transparency report for “search removals under European privacy

---

132 UNHRC Res A/HRC/34/L.7/Rev.1 22.03.2017 p. 3
135 Chaparro (n 58).
This reporting has been improved over the years, up to the point where information is updated on a daily basis. Up to 24 October 2019, Google has received approximately 866,000 requests to delete approximately 3.4 million URLs, of which it delisted about 45 percent.\textsuperscript{138} The ratio of decisions for and against delisting have remained remarkably stable over the years. Furthermore, the SEO also provides sample cases from different European countries, and how it finally decided on those applications. While the information provided seems highly comprehensive, and illustrative, the predominantly quantitative material provided does not allow for comprehensive qualitative review of the individual decisions taken. What happens in practice and how, remains virtually unknown to the public. In 2015 an open letter was sent by eighty academics to Google in which it was demanded to open up the “blackbox”.\textsuperscript{139} To date, little has happened in this respect, although Google has published an academic article with analysis and discussion of ‘five years of the right to be forgotten’ in late 2019.\textsuperscript{140} While this paper delivers interesting insights on cultural sensitivities and differences in several European states, it is also mostly based on quantitative data analysis.

It is understandable that the corporation took care of the implementation mechanism itself, since it is directly responsible to comply with court judgments. Still, it might be more preferable to establish a publicly run online dispute resolution mechanism, which would take over the role of deciding on delisting requests in a transparent manner. Such a platform might also be used by other smaller search engine providers. This dispute resolution system might also be able to


\textsuperscript{138} ibid.


address critical aspects such as unification of standards between different SEOs, and the sharing of the burden of compliance costs.

4.4 Rights of the parties involved in the decision

Additionally, the establishment of such a public mechanism could also contain a procedural element which provides the original content creator the opportunity to be heard. Delisting requires to consider the right to privacy of one person, the freedom of expression of another, and/or the public interest in being informed.\textsuperscript{141} Currently, a request for delisting is based on the assessment of a form which needs to be filled out by the applicant. In the past aspects such as the procedure used to confirm the residence of the applicant were discussed,\textsuperscript{142} or the requirement to provide proof of identity since processing of such information might be prohibited by certain national laws.\textsuperscript{143} More recently, Erdos highlights that the standardised notification practice of Google for webmasters, end users and public databases should be reconsidered and limited to what is appropriate and strictly necessary in a specific individual case.\textsuperscript{144}

Nevertheless, the arguably biggest concern in this respect remains that original content creators do not have the possibility to voice an opinion on the legitimacy of the request. Hence, while the applicant will receive notification of the effectiveness of the effort, the original creator of the content is currently not involved in the decision-making process. As described, the German FCC has recently tried to solve this problem by tying the right to freedom of expression of such


\textsuperscript{142} Gstrein (n 26) 103.

\textsuperscript{143} ibid 104.

a third party to the freedom to conduct business of the SEO. However, while this might strengthen the consideration of the value of expression in the balancing exercise with privacy, it also means that the interests of the original content creators can only be mediated by the SEO, national public authorities, or courts.

5. CONCLUSION

As has been outlined in the analytical section, delisting and the broader concept of a RTBF remain complex. Whereas the ECJ took a very bold step with its Google Spain decision in 2014, the judges in Luxembourg seem to have become much more careful in defining the substantive scope with the 2019 Google vs CNIL verdict. At first this seems surprising, especially when considering the enactment of GDPR in 2018 which enshrines a specific - albeit vague - provision on the ‘right to be forgotten’ in Article 17. With more harmonised and enforceable secondary European Union law, one would expect the ECJ to be more confident. However, as several national judgments following Google Spain, the recent draft EDPB guidelines, and two corresponding FCC judgments in Germany suggest, the substantive development of delisting has become a multi-layer and multi-stakeholder exercise with some space for diversity, also within Europe. The governance model of a kinetic sculpture in the form of a “fundamental rights mobile” (“Grundrechts-Mobile”) prevails for the moment.145 This “mobile” consists of several interacting actors on different connected layers, which engage in a process based on restraint, implicit rules, and mutual respect. With its egalitarian character it stands in contrast to more hierarchical concepts based on competence and delegation of power, such as proposed by the legal philosopher Hans Kelsen.146


On the institutional level, the recent ECJ judgment and its “aftermath” demonstrate that even with substantively harmonised European data protection rules in the form of a directly applicable regulation, effective enforcement in practice hinges on sound collaboration of supranational and national institutions. Furthermore, the interests and specific features of the European and member state level need not only be carefully weighed against each other, but also in context of international political and economic developments.

To conclude, it seems that while the ECJ was predominantly focused on sending a signal beyond the shores of the Union in 2014, it was much more concerned about internal balance in 2019. The substantive void of the Google vs CNIL judgment is now filled by bodies of regulators and national courts within European states. As has been highlighted throughout the conceptual section of this article much remains to be done. Issues such as territorial scope and effective enforcement, balancing human rights in the light of human dignity, transparency of the procedure and the rule of law, as well as individual procedural rights remain to be resolved. The final question is how much harmonisation is desirable when it comes to delisting and the right to be forgotten in the broader sense. Especially when looking beyond Europe, where the concept is widespread as the presented comparative research suggests, it will be seen whether the lack of clear leadership of the ECJ results in more fragmentation towards the national level, or more dialogue towards universal rights for data subjects.

Electronic copy available at: https://ssrn.com/abstract=3530995