Martin MACH*

EU Member States' Position on Data Protection

ABSTRACT: *The European Union places a strong focus on the protection of personal data through European law. This is an important and sensitive area that requires clear rules through legal regulation. However, within the same legal area, the Member States can act from different positions. For example, in the case of the right to be forgotten, a State, or its institutions, is only the appellate authority, while private companies are the first decision-makers. Conversely, in the case of the European Commission's proposal to combat child sexual abuse, a relatively strong position is expected from the State, which should be able to intervene at its discretion in the privacy, including the personal data, of its citizens. This article thus focuses on the different legal positions of the Member States in the area of data protection and tries to determine whether a stronger or a weaker position of a Member State is better for the protection of personal data.*
KEYWORDS: *data protection, GDPR, European Union, member state*

1. Introduction

Nowadays, personal data protection is rather associated with European law rather than national law. This is probably partly due to the almost 30-year history of personal data protection of European law, and partly because seems more logical to deal with personal data protection at the level of the European Union (EU) rather than at the individual Member State level. This hypothesis is supported by two facts. First, data protection is currently mainly linked to the Internet and IT systems. Due to the use of modern technologies, it is very difficult to monitor when and if data have crossed national borders and, as the Internet knows no (national) borders, it is more convenient to deal with data protection issues at an international level. Second, there is the need to ensure a uniform approach to data protection. If each Member State were to set its own legal regulation for data protection, the legislative differences would be very difficult to comply with in practice. By contrast, the common rules for EU Member States

* PhD student at the Department of International and European Law, Palacký University in Olomouc. Martin.mach@upol.cz

https://doi.org/10.62733/2024.2.101-119

are clear, easier to comply with in practice and the same for all parties concerned. In addition, they reinforce the so-called "Brussels effect" or "Strasbourg effect" that Lee A. Bygrave uses in the context of data protection.[1] This is one of the positive aspects of data protection at EU level, as data protection decisions have a global impact[2] and the EU has the potential to be a world leader in data protection. At the same time, although legal sources are used in the legislative process involving all Member States and the EU does not legislate as a third party distinct from the Member States, by this delegation, the States voluntarily lose decision-making power in a very sensitive area. Together with the involvement of private companies in data protection, there is the concern that this is a further weakening of the power of Member States. As decisions in this area are taken by the Member States and the EU, it may look like a weakening of the power and sovereignty of the Member States. Is this really the case or is the involvement of Member States in data protection a positive aspect?

2. Personal Data and Their Protection

Nowadays, users' personal data[3] is a "golden egg" for companies who can collect more personal data of a user and predict his behaviour or estimate his character and other characteristics.[4] As it is becoming more difficult to protect one's privacy in the digital age and every user leaves a digital footprint, this is a worrying observation. The truth is that whoever has users' personal data can make money from it. However, the collection of these data can seem unobtrusive. For example, when shopping in an online store, a discount is offered after registration, while physical stores have loyalty cards. An example of the long-term interest and struggle over personal data is the Kiwi vs. Ryanair dispute. The Kiwi flight search engine does not give Ryanair direct contact with the customer, meaning Ryanair cannot send them offers to buy additional services, which form part of the company's earnings. While in 2021, the Czech Constitutional Court dismissed Ryanair's 2019 lawsuit,[5] in 2023, a court in Milan upheld Ryanair in the dispute between the companies.[6] Such disputes dem-

1 Bygrave, 2021.
2 For example, Latin America. Carrillo and Jackson, 2022.
3 'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Art. 4 par. 1 General Data Protection Regulation.
4 Youyou, Kosinski and Stillwell, 2015, pp. 1036-1040.
5 www.expats.cz, 2021.
6 Ryan, 2023.

onstrate how valuable personal data are. Large big tech companies such as Google, Meta,[7] Amazon and others profit from personal data. Although fines for processing personal data in contravention of the law are in the tens or hundreds of millions of euro,[8] the fines are still not high enough and big tech companies are profiting from the data breaches despite the fines.[9]

However, the protection of personal data is not primarily based on preventing data trafficking, but on protecting European users and their rights to the protection of their personality and privacy. The EU recognises the importance of protecting personal data to such an extent that it does not even allow the migration of data outside the EU. The concern about the possible misuse of data by other countries, such as China,[10] is understandable, but the US, which has traditionally been a strong cybersecurity partner and ally of the EU, is no exception. This has already been discovered in practice by Meta, which transferred Facebook users' data to the US.[11]

2.1. Legal Framework

Legislation at the EU level dealing with the protection of personal data existed as early as 1995, namely Directive 95/46/EC of 24 October 1995.[12] This is at a time when Internet search engines already existed, namely Archie (1990), Aliweb and W3Catalog (both 1993), while today's Google (1998), Bing (2009) or Yahoo (1995) did not exist. Additionally, the number of Internet users, and thus search engines, varied widely. Whereas in the year Directive 95/46/EC was issued there were approximately 16 million Internet users (i.e. approximately 0.4 % of the world population),[13] in the year of the Google v. Spain judgment (2014), there were already 3 035 million (42.3 % of the world population) and this figure is still growing. In 2022, for example, there were 5473 million internet users (69 % of the world population).[14] Therefore, although the 1995 Directive regulated data protection at EU the level, shortly after its entry into force, the Internet and its parts reached such a boom that the Directive failed to offer adequate legal regulation. Five years later, in 2000, the Charter of Fundamental Rights of the European Union was presented at the Nice Intergovernmental Conference and became legally binding, together with the Lisbon Treaty, on 1 December

7 The company that owns Facebook, Instagram and Whatsapp.
8 E.g. Amazon was fined 877m dollars, i.e. approximately 811m Euros. Clark, 2022.
9 In recent years, Google LLC received fines in the order of millions of euros in 2019 (Hanselaer,2019.), 2020 (Hanselaer, 2020.), or 2022 (Brook, 2022.).
10 Hartmann, 2023.
11 edpb.europa.eu, 2023.
12 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995.
13 www.internetworldstats.com.
14 Ibid.

2009. While the latter contains Article 8 on data protection, it is rather a general provision typical of national constitutions and does not respond to the technological developments since Directive 95/46/EC was issued. As such, the case law applies the Directive to current challenges is important, such as the *Google vs Mario Costeja Gonzales* judgment,[15] where the Court derived the right to be forgotten in 2014. This is an expanded right to erasure in light of the great development of Internet search engines and their ability to make greater inroads into the privacy of individuals. As a result, the new right can only be found in the legal source in Article 17 of Regulation (EU) 2016/679,[16] which did not come into force until 2 years after the judgment. Regulation 2016/679, mainly as General Data Protection Regulation (GDPR),[17] takes over all existing principles of protection and processing of personal data that underpin the EU system and confirms that protection travels across borders at the same time as personal data. It also responds to the latest developments in modern technology and further develops and strengthens users' rights. In the context of GDPR, the most frequently mentioned, and most important big tech company in terms of the right to be forgotten, is undoubtedly Alphabet Inc., which owns the Google search engine. This engine accounted for almost 92 % of all searches from users within the EU last year, with Microsoft's second-ranked search engine Bing accounting for just over 4 %.[18]

The development and empowerment of users can be divided into two categories: preventive and remedial. The preventive category includes the possibility for users to obtain information on which of their personal data are processed and for what purpose. The remedial category allows users to seek compliance with applicable legal rules and, where appropriate, seek redress.

These requests are addressed to the counterparty responsible for content on the Internet. The GDPR has introduced the institutes of data controller and data processor,[19] who are responsible for the information disclosed and for any future redress. The institute of the data controller is interesting in that it is not only a guarantor of compliance with the applicable legal rules, but also a first-instance arbitrator in any disputes with the possibility to negotiate redress. These are mostly private big tech companies such as Google, Meta, Amazon or Microsoft and this institute significantly empowers them. As this is a European regulation, one would rather expect an EU body or an EU agency, or even a Member State in the form of a national authority, to be the arbitrator here. The position of private companies with a

15 *Google Spain v. AEPD and Mario Costeja González*, C-131/12.
16 General Data Protection Regulation.
17 Ibid.
18 StatCounter Global Stats.
19 The processor differs from the administrator in that, as part of the activity for the administrator, he can only perform such processing operations that the administrator authorises him to do or that result from the activity for which the processor was authorised by the administrator.

focus on Internet search engine operators has been examined in more detail in *The position of internet search engines as arbitrators of first instance*.[20] However, there is also the current proposal of the European Commission to combat child sexual abuse on the Internet, which goes in a different direction from the current trend. Here, not only is the EU body, the EU Independent Centre for Combating Child Sexual Abuse, represented, but the Member States are also involved by having to designate national bodies to review risk assessments. As such, would it be better in the future to have a more active involvement of the EU and Member States in the protection of the personal data of their citizens, or maintain the current strong position of private big tech companies?

Both approaches have advantages and disadvantages. The greater involvement of private companies and the emergence of the institute of data manager has the same advantages as a *public–private partnership* (PPP). One advantage is the expected faster response of the private sector compared to the public sector. The speed of remediation in the area of data protection that is a key factor, as personal data is a highly sensitive matter and, especially for unauthorised disclosure, the situation needs to be remedied as soon as possible. However, there is also a need for proper legal regulation of what a private partner can and cannot do by defining its powers as well as its obligations. The EU addresses this through the GDPR, which some previous studies evaluate positively and consider it a model for other countries.[21] However, the passage of this procedure in practice remains difficult, for example, in the case of requests for the application of the right to be forgotten by the user in search results through the so-called *watchdog search engines*. These engines draw, among other things, on publicly available information provided by the Member States. In the event of a subject's request for the rectification of personal data disclosed in the search results of watchdog search engines, the data controller is in a situation where it could potentially have to decide on the correctness of a Member State's compliance with the legal rules in the field of personal data. However, this is not legally permissible. The author has addressed this paradox in his research, where he concluded that, in the case of a request by a data subject for redress in the results of a search on a watchdog search engine, where the source of the published information is the State, the accuracy of the information and compliance with the law must again be assessed by the State.[22]

The involvement of the Member States in the protection of users' personal data is necessary because, although data controllers have enhanced powers based on the GDPR, they still face certain limits. At the same time, the Member States need to be

20 Mach, 2023a.
21 For example, Mingyu, 2020.
22 Mach, 2023b.

monitored on how they handle personal data,[23] which is why the involvement of EU institutions is also beneficial. As such, the question remains how to appropriately allocate data protection rights and obligations between the Member States and EU institutions?

2.2. Positions of Member States in the Protection of Personal Data

As mentioned above, the protection of personal data is found in the EU legal order. However, the protection of personal data is an area of law also represented in national legal orders. This is also the case in both areas of private and public law. In private law, the protection of personal data can be linked to the right to the protection of personality. This includes, for example, the right to be forgotten, the right to the protection of honour and respectability, the right to the protection of likeness, the right to privacy, and the right to informational self-determination. These are rights guaranteed to the individual as the sovereign of his or her personal sphere. In public law, there are regulatory laws for the protection and processing of personal data. In this case, the State regulates the handling of personal data and, as with any legislation issued by it, is the guarantor in this area. This makes it logical that Member States should be actively involved in personal data protection. Insofar as they guarantee the rights in question, regulating them under national law, it is also up to them to enforce them within their own institutions and, where appropriate, negotiate redress. From this viewpoint, it makes sense to involve the Member States in the protection of personal data to a greater extent, in a way similar to what the European Commission is planning to do in the fight against child sexual abuse.

However, the Member States are limited by EU law in the area of personal data protection for a uniform approach. Specifically, European law defines two approaches to the involvement of Member States, or their authorities, in personal data protection. In the first, the Member State is the first decision-maker in cases of personal data protection breaches, while in the other, it is only the appellate authority. In the second case, the role of first decision-maker is played by private big tech companies on the basis of the GDPR. This involves another type of actor in the protection of personal data. Specifically, apart from the Member State and the EU, there is a data controller,[24] usually a large private company falling into the category of big tech companies. However, this competence of big tech companies may seem problematic, especially considering that research points to two facts. The first is the warning of the excessive power of these private companies comparable to that of States. Hongfei Gu

23 Šotová, 2023.
24 Art. 4 par. 7 General Data Protection Regulation.

even argues that big tech companies have created a "digital empire" that is relatively independent of political authority due to their control of data and monopolisation of technology. In terms of data collection and use, private big tech companies are ahead than Member States and have thus gained their own sovereignty.[25] The second fact is that there is a paradoxical situation, where companies that are supposed to decide on data breaches are punished by the EU for doing the same.[26]

2.3. Position of Big Tech Companies in the Protection of Personal Data: Welcome or Unwanted?

The actual position of big tech companies in the area of data protection in relation to the powers and strength of EU Member States is quite interesting. Have big tech companies been given too much power to be the first arbitrators in data breach assessments at the expense of Member States?

To answer this question, it is necessary to focus on procedural application according to legal norms. When big tech companies are the first arbitrators in data breach assessment cases, this is not a substitution of a private company for a Member State. Member States still figure in the adjudication process, but only in an appellate capacity. However, is this "relegation" to the appellate position really a sign of the strong position of private big tech companies and the weakened position of Member States? Before answering, two facts should be highlighted.

As a first fact, the appellate body is usually superior to the first instance body. This relationship of subordination and superiority is necessary for the decision of the appellate body to be considered legally binding by reason of its superior legal force. It has been hypothesised in academia that the weakened position of Member States is visible in the possibility to decide only on cases where the data subject's request for the erasure of personal data is rejected,[27] that is, cases where big tech companies grant applicants' requests are final decisions and there is no possibility to comment or appeal such decisions to delete private data from the Internet. In practice, this means reduced control over cases in which a private company complies. However, this may only be problematic from a State's perspective in the cases mentioned in paragraphs (d) and (e) of Article 17 of the GDPR in the narrower sense, or paragraphs (c), (d) and (e) in the broader sense.[28] In the opinion of the author, this is not direct evidence of greater legal power of private companies than that of Member States. One could choose as a counter-argument the assumption of the application of the

25 Gu, 2023.
26 For example, Zandt, 2023.
27 Finck, 2018.
28 Art. 17 c), d), e), General Data Protection Regulation.

principle of *prohibitio reformatio in peius*,[29] one of the fundamental principles of the right to a fair trial. However, the author is of the opinion that the current state of affairs is due only to an omission in the procedural definition.

The second fact is related to the first and, in the author's opinion, should be mentioned to be the course of appeal proceedings. In the event of an appeal, the private company, as the first-ranking arbitrator, does not have the possibility for a so-called *autoremedy*.[30] Therefore, after the decision and subsequent appeal of the data subject against the rejection of the request, the private company does not have the possibility to reiterate or change the decision. In case of an appeal, the whole process, including the final decision, takes place at the level of the State or its authority. This again, in the author's view, supports the thesis that private companies do not have a stronger position than Member States, although they cannot be denied a strong position in the protection of personal data.

As such, in the author's view, the thesis that private big tech companies have too much power at the expense of Member States in the area of data protection cannot be fully confirmed. However, they do have a significant role in the protection of personal data, especially in the example of procedural involvement in the right to be forgotten mentioned above. This raises the questions of the advantages and disadvantages of involving private companies in the sensitive area as data protection, whether in the end the advantages outweigh the disadvantages and whether the involvement of private companies makes sense.

2.3.1. Benefits

As personal data is a very sensitive area for any data subject (i.e. an individual), this topic must be treated with the utmost seriousness. It is necessary to ensure that the situation is remedied as quickly as possible, so that the interference with personal rights is as short and causes as little damage as possible. It is the speed of the response, coupled with the ability to negotiate a remedy, which, in the author's view, is the strongest argument for the involvement of private companies in the protection of personal data. The GDPR imposes the obligation on the data controller to *erase personal data without undue delay*.[31] Although the definition of "*without undue delay*"

29 It expresses the prohibition of changing the decision for the worse, that is, to the detriment of the person who was affected by the contested decision and filed the appeal himself or in whose favour the appeal was made.

30 A special possibility of correcting the decision issued by the authority in the first level of decision-making. This usually happens after the decision has been appealed. In the case of the right to be forgotten, this is thus an appeal.

31 Art. 17 par. 1, General Data Protection Regulation.

is a vague legal concept, not a specific timeframe,[32] in first instance decision-making practice for requests to apply the right to be forgotten, Google can make a decision within a month of a request to delete personal data.[33] It is precisely the one-month time limit for dealing with requests to remove personal data from the Internet that Member State authorities probably need.[34] For completeness, one law firm has stated on its website: 'Unfortunately, search engines often take significantly longer as they are inundated with requests. It is therefore important to seek legal advice as soon as you become aware of the information being available online'.[35] However, the author of has not been able to trace these cases and believes that this may be the case with smaller local companies, not large search engine companies to whom the majority of all right to be forgotten requests arrive.

The second half of the quotation is also interesting from the viewpoint of this article, due to mentioning the importance of finding "*legal advice*" as soon as possible. Indeed, the right to be forgotten is well understood, as any individual can apply for it without the need for in-depth legal knowledge. Moreover, this is one of the positives of the involvement of private companies in data protection. In the case of the right to be forgotten, the origin of this right dates back to the judgment of *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*.[36] However, only one criterion, or exception, can be found in this judgment, where it is necessary to assess whether there is an "overriding public interest" in the specific information that the data subject wishes to have removed. If the answer is in the affirmative, the information in question is not deleted and the interference with the applicant's fundamental rights is justified by the overriding public interest of society in having access to the information in question.[37] The total of six conditions[38] and five exceptions[39] currently applied are legally defined in the GDPR. As such, this constitutes a significant difference from the single criterion set out in the judgment. However, the first to extend the criteria from the Costeja judgment was not the EU or any public administration representative but a private company, namely Google. On 30 May 2014, just 17 days after the judgment in the Costeja case of 13 May 2014, Google

32 Only the maximum period is traceable. In par. 3 of Art. 12, the maximum period is up to 1 month and in complex cases, up to 2 months.
33 British law firm confirms the decision within weeks and also reports a record for a response from Google within 10 minutes of sending a request. The unwanted material is then removed from the search results that same day. See: www.samuels-solicitors.co.uk.
34 A shorter period can only be considered in cases of the creation of new departments dealing only with this activity, which would incur significant financial expenses.
35 Matthews, 2020.
36 *Google Spain v. AEPD and Mario Costeja González.*
37 *Google Spain v. AEPD and Mario Costeja González*, p. 97.
38 Art. 17 par. 1, General Data Protection Regulation.
39 Art. 17 par. 3, General Data Protection Regulation.

introduced the first web form[40] available in 25 languages for sending requests for the right to be forgotten from users,[41] as well as an initial scheme for the procedural processing of users' requests for the right to be forgotten.[42] This made the right to be forgotten available to the general public without the need for legal training or legal representation. The importance of this step can be assesses by comparing it with the USA, that is, if a data subject in the EU and the US were to make the same request. In the US, there is generally very little that an individual can do because they have to disclose which law has been violated. Even a reference to the violated law is a barrier for a layman to make his or her request due to the legal ignorance of the procedure or the law being violated in his or her case.[43] Again, one can see the speed of the response from a private company in creating a form, which would probably have been much longer for a public administration. If we look at the US, a great example of this in practice was the creation of a website for the purposes of *The Patient Protection and Affordable Care Act* (PPACA), known as Obamacare.[44] What the public administration failed to do was to create a functional system, which private companies did in 5 months.[45]

If a big tech Company can work faster than the public administration and can meet expectations in terms of the planned goals, this brings another argument for engaging these companies, namely financial savings. Replacing the big tech company with a Member State institution would mean new costs for salaries, IT equipment, training, energy and more to achieve the same result, but over a longer period of time. This is in direct contrast with the principle of efficiency and economy of each Member State. Alternatively, the State would not have to worry about being replaced by a private company and, thus, losing its power or sovereignty. Member States are still involved in the protection of personal data, even in the case of the right to be forgotten. They serve as an appellate body, which, as previously mentioned, is superior to the first instance. Therefore, the sovereignty or power of the State cannot be construed as being under threat from big tech companies. Conversely, the involvement of public institutions up to the level of the appellate body can be seen as an additional sub-advantage. For the resolution of trivial cases already at the level of first instance decision making, the resulting decisions are obvious and State institutions would be overwhelmed by them. They thus only decide in appeal cases, where there is a presumption of more difficult decisions. Looking at Google's *Transparency*

40 reportcontent.google.com.
41 Par. 22, https://www.wsj.com/public/resources/documents/google.pdf.
42 Lee, 2016, p. 1038.
43 Mach, 2023c, p. 648.
44 Patient Protection and Affordable Care Act, Public Law 148, U.S. Statutes at Large 124 (2010): 119-1024.
45 See Contorno, 2014.

Report,[46] half of the applications are resolved by Google. Assuming that every unsuccessful applicant for the right to be forgotten appeals, the State institution decides on "only" half of the applications. In this way, it is not overwhelmed by applications and can deal with them more quickly at a lower cost. However, the real percentage will be less than 50 % of all requests, as the author considers it unrealistic that every data subject whose request is rejected would actually appeal.

2.3.2. Disadvantages

The previous subsection mentioning the advantages of involving private companies in data protection suggested that their involvement is desirable and necessary. However, to have an overall perspective on the subject, it is also necessary to mention the disadvantages of such involvement. Here, the author's previous published research will also be considered.[47] In addition to the speed with which a situation can be rectified, the protection of personal data requires that the decisions on these matters be taken in accordance with the applicable legislation. As this is a sensitive area of interference with the personal rights of the individual, it would be desirable to make the decision-making process as transparent as possible, as this also increases trust in the decision-maker. However, for private companies, transparency is not at the level it could ideally be. For completeness, the first instance decision-making process is not completely non-transparent. In addition to the form, Google has also come up with a procedural scheme for decision-making, as already mentioned.[48] However, there are still too many uncertainties, which should be explained more to the general public. The application process has been briefly but clearly developed, for example, by a collective of authors in *Five Years of the Right to be Forgotten*.[49] However, it is important that each application is manually assessed by at least one employee of the search engine company. These decisions could still be changed retrospectively by the Google Advisory Council, made up of 10 independent experts.[50] The problematic fact is that the last traceable meeting of the Advisory Council was in Brussels on 4 November 2014.[51] Since then, there was no further mention of a meeting, as the Google Advisory Council was intended to serve mainly in contentious cases, which should no longer occur, because since 26 November 2014, the EU issued detailed Guidelines on the implementation of the Court Of Justice of the European Union

46 transparencyreport.google.com.
47 Mach, 2023a.
48 Lee, 2016, p. 1038.
49 Bertram et. al., 2019, p. 960.
50 archive.google.
51 www.youtube.com, 2015.

judgment's of the Costeja case.[52] The final report of the Advisory Council is dated 6 February 2015.[53]

Transparency was also addressed by Google, in section 5.5 of the Google Advisory Board's final report,[54] where it was divided into four points:

1) transparency to the public regarding the completeness of name searches;
2) transparency to the public on individual decisions;
3) transparency to the public on anonymised statistics and general search policy;
4) transparency to the data subject on the reasons for refusing his or her request.

Peripherally related to the criticised transparency of the decision-making process and concise justification in case of denial of a request is point 4), on which the report further states that '... some experts have suggested that Google is also responsible for providing detailed explanations of its decisions'.[55] However, these expert recommendations were already redundant and outdated by 6 February 2015 (i.e. at the time of the report's publication), as the Implementation Guidelines of 26 November 2014 already contained a requirement for sufficient justification for the rejection of the request, which would be made available to the national data protection authority in the event of an appeal.[56] Search engines must thus provide sufficient justification in the event of a refusal and, if this is not the case, which is sometimes criticised, recourse should be made to the national data protection authority, which is also a logical follow-up of the refusal; that is, if the data subject is not satisfied with the outcome of the assessment and the justification does not seem sufficient, an appeal against the decision to the national authority is a procedural step to which he or she has the right. Therefore, the subjective assessment of the sufficiency and completeness of the applicant's reasoning does not change the facts and, as the data subject has the right to appeal the decision, any insufficient reasoning cannot be considered as a denial of the individual's right to be forgotten. However, an objective assessment of the facts must contain sufficient reasons for the decision on the grounds of the right to a fair trial.

The second point of criticism of the transparency of the decision-making process on applications concerning the failure to disclose details of internal procedures. It is, at least as a basic outline, clear how the application is processed and handled. Once the search engine receives it, it is assessed by at least one member of staff on the basis of

52 WP225 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, 2014.
53 The Advisory Council to Google on the Right to be Forgotten, 2015.
54 Str. 21, tamtéž.
55 Ibid.
56 WP225 Guidelines on The Implementation, 2014, p. 15, b).

the criteria given. The request is then either approved, the search results are modified and the third party on whose website the personal information in question appears is informed of the deletion from the search results, or the request is rejected and the applicant is informed of this, along with the reasons why the request was rejected. However, the author of this paper notices an absence of more detailed information about the staff who decide on the requests. This does not mean a list of the names of employees; in administrative proceedings for traffic offences, it is not the name of the official concerned that is important, but his or her professional qualifications for the post. In case of private companies that decide whether to keep sensitive personal data publicly available, it is not known what qualifications or minimum requirements the employees deciding on the applications have. However, the author considers this to be a very important piece of information, because even if the criteria by which applications are assessed are given, this assessment cannot be described as a purely monotonous activity, but also requires a sense of detail, good analytical thinking, knowledge of the law and more. Therefore, it would be useful for the public to know the minimum standards required for these positions and how they are observed.

Greater openness of the requirements for the positions of employees assessing right to be forgotten requests serves, among other things, as good public relations for the companies that own the search engines. Moreover, these individual steps may signify openness and could alleviate the concerns about abuse of the position of private companies, which is the third category of criticism of private companies as first-party arbitrators. These concerns are not specific to the right to be forgotten, and there is significant research on the possible abuse, or proven abuse, of dominance by big tech companies.[57] Specifically, the right to be forgotten is about the aforementioned paradoxical situation of search engines deciding on the availability of information, but it is on this availability and mediation of information that they have built their business model. Mark Leiser has written extensively on this topic in his paper *Private jurisprudence and the right to be forgotten balancing test*,[58] which examines how Google approaches the balancing test between the right to be forgotten and the public's right to be informed. This balancing test can also be interpreted as Google's dilemma of whether to delete personal information, thereby applying the right to be forgotten, or to keep it, thereby supporting its business model. Other researchers also conclude that these balancing tests should be carried out by States, but are decided by search engines, which replace the judicial process, thus weakening the role of the State at the expense of the private search engine.[59] In addition, search engines have their own archives and geological mutations, which may ultimately

57 For example, Félix, 2022, p. 137, Dembrow, 2022, Hutchinson, 2022.
58 Leiser, 2020.
59 Chenou and Radu, 217, p. 76.

raise suspicions of the abuse of their positions, or at least the attempt to circumvent the original meaning of the right to be forgotten. Julia Powles and Enrique Chaparro consider Google's solution of removing only links on its domains to be trivial and undermining the Costeja vs. Google ruling, and Google's decision to create the aforementioned Advisory Board to be tactical. In their view, Google's intention was merely to move the discussion away from the core issue (i.e. the introduction and protection of digital rights), and rather create a conflict between the apparently divergent views of the EU and the US.[60] However, with all these critical comments, it is important to highlight an important factor that features strongly and has already been mentioned. Search engine companies are primarily set up to make a profit and are, on the one hand, willing to submit to regulation, but on the other hand, will try to operate within the rules so that they can maximise their profits. Therefore, if they are criticised that their procedures and processes are not identical to those of public authorities, this is not such a surprising finding. It is on these differences that the PPP method works, which brings the advantages already mentioned, but there are also disadvantages or risks arising from it.

3. Conclusion

It is already obvious that the involvement of private big tech companies in data protection has its advantages and disadvantages. With the ever-increasing influence of modern technology on our lives, the power of private companies tied to modern technology is also increasing. The more we use the Internet, for example, the bigger the digital footprint we will leave. Companies with a business model built on these digital footprints which contain users' personal information have strong positions in this area and may appear to be becoming adversaries of the State, or certain monsters that need to be defeated. Alternatively, the current trend, to which the author agrees, is that there is the possibility of seeking cooperation between States or the EU and private companies. Big tech companies have strong positions in this day and age, where it is commonplace to be online, and have become an overlooked force that would be too much work to eliminate completely. However, as power increases, so should responsibility. That is, the EU, Member States and big tech companies should all get involved in protecting individuals' personal data. It is thus more beneficial for not only the States and the EU to be involved in the protection of personal data, but also the big tech companies, which can be more effective in the online world than the States themselves.

60 Powles, Chaparro, 2015.

However, what needs to be checked in the case of granting powers to these companies is whether they are operating in compliance with the law and it is also necessary to set up an adequate legal framework. If some powers are delegated to private entities because of their strong positions, there is also the need for a strong position of the legislator to ensure that this delegation produces the desired results through appropriate regulation. Moreover, modern technologies are specific due to their current rapid evolution, so developments need to be constantly monitored and new challenges in the form of risks need to be assessed. The EU is trying to respond to current developments with the DMA and DSA legislative proposals, but the question is whether these acts will prove beneficial in curbing abuses of power by large big tech companies. The need for constant monitoring must continue, as big tech companies are in a strong position, meaning that a strong EU or Member States are needed to regulate and set boundaries. This is because the big tech companies, within their business model, are testing the limits of the rules set and interpreting them to their own best advantage.

Bibliography

- Archive.google. *The Advisory Council to Google on the Right to be Forgotten*. [Online].
- Available at: https://archive.google.com/advisorycouncil/ (Accessed: 29 October 2023).
- Bertram, T., Bursztein, E., Caro, S., Chao, H., Chin Feman, R., Fleischer, P., Gustafsson, A., Hemerly, J., Hibbert, C., Invernizzi, L., Kammourieh Donnelly, L., Ketover, J., Laefer, J., Nicholas, P., Niu, Y., Obhi, H., Price, D., Strait, A., Thomas, K. and Verney, A. (2019) Five Years of the Right to be Forgotten. *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. Available at: https://doi.org/10.1145/3319535.3354208 (Accessed: 29 October 2023).
- Brook, C. (2022) *Google Fined $57M by Data Protection Watchdog Over GDPR Violations*, Digital Guardian [Online]. Available at: https://www.digitalguardian.com/blog/google-fined-57m-data-protection-watchdog-over-gdpr-violations (Accessed: 29 October 2023).
- Bygrave, L.A. (2020) The 'Strasbourg Effect' on data protection in light of the 'Brussels Effect': Logic, mechanics and prospects, *Computer Law & Security Review*, 40 [Online]. Available at: https://www.sciencedirect.com/science/article/pii/S0267364920300650 (Accessed: 29 October 2023).
- Carrillo, A.J., Jackson, M. (2022) Follow the Leader? A Comparative Law Study of the EU's General Data Protection Regulation's Impact in Latin America. *ICL Journal*, 16(2), pp.177–262 [Online]. Available at: https://doi.org/10.1515/icl-2021-0037 (Accessed: 29 October 2023).
- Chenou, J.-M., Radu, R. (2019) The "Right to Be Forgotten": Negotiating Public and Private Ordering in the European Union. *Business & Society*, 58(1), pp. 74–102 [Online]. Available at: https://doi.org/10.1177/0007650317717720 (Accessed: 29 October 2023).
- Clark, K. (2022) *Google's $400m penalty and impact of the 5 heftiest data privacy fines on 2023 ad plans* [Online]. Available at: https://www.thedrum.com/news/2022/11/15/googles-400m-penalty-the-impact-the-5-heftiest-data-privacy-fines-2023-ad-plans (Accessed: 29 October 2023).
- Contorno, S. (2014) *Is* healthcare.gov *working 'great' now?* [Online]. Available at: https://www.politifact.com/article/2014/mar/14/healthcaregov-working-great-now/ (Accessed: 29 October 2023).
- Dembrow, B. (2022) Investing in Human Futures: How Big Tech and Social Media Giants Abuse Privacy and Manipulate Consumerism, *University of Miami Business Law Review,* 30(3), pp. 324–349 [Online]. Available at at: https://repository.law.miami.edu/cgi/viewcontent.cgi?article=1402&context=umblr (Accessed: 29 October 2023).
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

- edpb.europa.eu. (2023) *1.2 billion euro fine for Facebook as a result of EDPB binding decision | European Data Protection Board* [Online]. Available at: https://edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en (Accessed: 29 October 2023).
- Félix, A. S. (2022) Big Tech Companies' Unprecedented Success and the Abuse of Dominance in the EU and the US: A Comparative Analysis, *Southampton Student Law Review*, 12(1), pp. 137–179 [Online]. Available at: https://www.southampton.ac.uk/~assets/doc/law/SSLR%20Vol%2012%20Issue%201%20Final.pdf (Accessed: 29 October 2023).
- Finck, M. (2018) Google v CNIL: Defining the Territorial Scope of European Data Protection Law. Oxford Business Law Blog [Online]. Available at: https://www.law.ox.ac.uk/business-law-blog/blog/2018/11/google-v-cnil-defining-territorial-scope-european-data-protection-law (Accessed: 29 October 2023).
- Gu, H. (2023) Data, Big Tech, and the New Concept of Sovereignty. *Chinese Political Science Review* [Online]. Available at: https://link.springer.com/article/10.1007/s11366-023-09855-1 (Accessed: 29 October 2023).
- Hanselaer, S. (2019) *The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC – European Data Protection Board – European Data Protection Board*. European Data Protection Board – European Data Protection Board [Online]. Available at: https://edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en (Accessed: 29 October 2023).
- Hanselaer, S. (2020) *The Swedish Data Protection Authority imposes administrative fine on Google*. European Data Protection Board – European Data Protection Board [Online]. Available at: https://edpb.europa.eu/news/national-news/2020/swedish-data-protection-authority-imposes-administrative-fine-google_en (Accessed: 29 October 2023).
- Hartmann, T. (2023) *TikTok must accelerate work to comply with new EU digital regime, Breton says* [Online]. Available at: https://www.euractiv.com/section/platforms/news/tiktok-must-accelerate-work-to-comply-with-new-eu-digital-regime-breton-says/ (Accessed: 29 October 2023).
- Hutchinson, S. Ch. (2022) Potential abuses of dominance by big tech through their use of Big Data and AI, *Journal of Antitrust Enforcement*, 10(3), pp. 443-468 [Online]. Available at: https://doi.org/10.1093/jaenfo/jnac004 (Accessed: 29 October 2023).
- Judgment on "Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12 (2014) [Online]. Available at: https://ec.europa.eu/newsroom/article29/items/667236 (Accessed: 29 October 2023). Published 26. November 2014.
- Lee, E. (2016) Recognizing Rights in Real Time: The Role of Google in the EU Right to Be Forgotten. *UC Davis Law Review,* 49(3), pp. 1017-1094 [Online]. Available at

https://lawreview.law.ucdavis.edu/issues/49/3/Articles/49-3_Lee.pdf (Accessed: 29 October 2023).
- Leiser, M.R. (2020) 'Private jurisprudence' and the right to be forgotten balancing test, *Computer Law & Security Review*, 39 [Online]. Available at: https://www.sciencedirect.com/science/article/pii/S0267364920300637 (Accessed: 29 October 2023).
- Mach, M. (2023a) Postavení vyhledávačů jakožto prvoinstančních rozhodců v právu být zapomenut. www.iurium.cz [Online]. Available at: https://www.iurium.cz/denik/denik-odborne-clanky/postaveni-vyhledavacu (Accessed: 29 October 2023).
- Mach, M. (2023b) The 'Right to Be Forgotten' by Watchdogs and Open-Source Search Engines in Šišková, N. (ed.). *Legal Issues of Digitalisation, Robotization and Cyber Security in the Light of EU Law.*
- Mach, M. (2023c) Komparace práva být zapomenut a placených alternativ, *Právník,* 162(7), pp. 644-656 [Online]. Available at: https://www.ilaw.cas.cz/casopisy-a-knihy/casopisy/casopis-pravnik/archiv/2023/2023-7.html?a=3783 (Accessed: 29 October 2023).
- Matthews, A. (2020) *Removing your information from Google search results: what is the 'right to be forgotten'?* [Online]. Available at: https://www.farrer.co.uk/news-and-insights/removing-your-information-from-google-search-results-what-is-the-right-to-be-forgotten/ (Accessed: 29 October 2023).
- Mingyu, S. (2020) *Personal Data Protection from the Perspective of Public-Private Partnership* [Online]. Available at: https://www.clausiuspress.com/conferences/AETP/ICEIPI%202020/70.pdf (Accessed: 29 October 2023).
- Patient Protection and Affordable Care Act, Public Law 148, U.S. Statutes at Large 124 (2010): 119-1024.
- Powles, J., Chaparro, E. (2015) How Google determined our right to be forgotten [Online]. Available at: https://www.theguardian.com/technology/2015/feb/18/the-right-be-forgotten-google-search (Accessed: 29 October 2023).
- 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).
- reportcontent.google.com. *Report content on Google* [Online]. Available at: https://reportcontent.google.com/forms/rtbf (Accessed: 29 October 2023).
- Ryan, E. (2023) *Ryanair wins case against travel site Kiwi* [Online]. Available at: https://www.businesspost.ie/news/ryanair-wins-case-against-travel-site-kiwi/ (Accessed: 29 October 2023).
- StatCounter Global Stats. *Search Engine Market Share Europe* [Online]. Available at: https://gs.statcounter.com/search-engine-market-share/all/europe (Accessed: 29 October 2023).

- Šotová, Z. (2023) *Zprávy o boji s evropskou korupcí: Jak země EU špehují své občany* [Online]. Available at: https://www.investigace.cz/boj-s-evropskou-korupci/?fbclid=IwAR28d_SmvR5Vgy7jBGMRzChzQrAc4Z7nCKC4253odhKJTWV4QxcmmDVTndo (Accessed: 29 October 2023).
- The Advisory Council to Google on the Right to be Forgotten (2015). Available at: https://static.googleusercontent.com/media/archive.google/cs//advisorycouncil/advisement/advisory-report.pdf [Accessed: 29 October 2023].
- transparencyreport.google.com. *Google Transparency Report* [Online]. Available at: https://transparencyreport.google.com/eu-privacy/overview?hl=cs (Accessed: 29 October 2023).
- *Wall Street Journal. Available at:* https://www.wsj.com/public/resources/documents/google.pdf (Accessed: 29 October 2023).
- WP225 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, 2014. [Online]. Available at: https://ec.europa.eu/newsroom/article29/items/667236/en (Accessed: 29 October 2023).
- www.expats.cz. (2021) *Kiwi vs. Ryanair: Czech ticket platform wins dispute over handling of passenger data* [Online]. Available at: https://www.expats.cz/czech-news/article/czech-ticket-seller-kiwi-com-wins-dispute-with-ryanair-over-handling-of-passenger-data (Accessed: 29 October 2023).
- www.internetworldstats.com. *Internet Growth Statistics 1995 to 2023 – the Global Village Online* [Online]. Available at: https://www.internetworldstats.com/emarketing.htm?fbclid=IwAR2DVQgzwksJuQ9uBZfhFZcLWw00SJiOVnHrwyYQbQW8McjtwoX76gGq2L0 (Accessed: 29 October 2023).
- www.samuels-solicitors.co.uk. *Right to be Forgotten Assistance from Expert Solicitors* [Online]. Available at: https://www.samuels-solicitors.co.uk/right-to-be-forgotten (Accessed: 29 October 2023).
- www.youtube.com. (2015) *Advisory Council Meeting, 4 November, Brussels* [Online]. Available at: https://www.youtube.com/watch?v=OTAbo3n3BJ8&t=1030s (Accessed: 29 October 2023).
- Youyou, W., Kosinski, M., Stillwell, D. (2015) Computer-based personality judgments are more accurate than those made by humans. *Proceedings of the National Academy of Sciences*, 112(4), pp. 1036–1040 [Online]. Available at: https://www.pnas.org/doi/10.1073/pnas.1418680112 (Accessed: 29 October 2023).
- Zandt, F. (2023) *Infographic: Big Tech, Big Fines*. [Online] Available at: https://www.statista.com/chart/25691/highest-fines-for-gdpr-breaches/ (Accessed: 29 October 2023).