PRIVACY AND ONLINE GATEKEEPERS

András Koltay[*]

INTRODUCTION

Gatekeepers have existed in all historic periods of public communication, and defining their legal status has often caused problems for the law. Generally, newspaper kiosks, postal carriers, and cable and satellite providers were not considered to have a direct impact on the media content they made available to the public. A postal carrier or cable provider could deprive individual readers or viewers from accessing information by refusing to deliver a paper or fix a network error (thereby also hurting his or her own financial interests), but they are not in a position to decide on the content of newspaper articles or television programs. Such actors had limited potential to interfere with the communication process, even though they were indispensable parts of it, and this made them a tempting target for the government seeking to regulate, or at least keep within certain boundaries, the freedom of speech of others by regulating the intermediaries.

Even though the internet seems to provide direct and unconditional access for persons wishing to exercise their freedom

[*] Associate Professor, Pázmány Péter Catholic University Faculty of Law and Political Sciences.

of speech in public, gatekeepers still remain an indispensable part of the communication process. A gatekeeper is defined as a person or entity, the activity of whom is necessary for publishing the opinion of another person or entity, and they include ISPs, blog service providers, social media, search engine providers, entities selling apps, webstores, news portals, news aggregating sites, and the content providers of websites who can decide on the publication of comments to individual posts. Some gatekeepers may be influential or even indispensable, with a considerable impact on public communication, while other gatekeepers may have more limited powers and may even go unnoticed by the public. It is true of all gatekeepers that they are capable of influencing the public without being government actors, and that they are usually even more effective at influencing it than the government itself. As private entities, they are not bound by the Constitution to maintain First Amendment freedom of speech protections, so they can establish their own service rules concerning the freedom of speech.

Natali Helberger and her co-authors identify two fundamental groups of gatekeepers. Gatekeepers of the first group control access to information directly, while gatekeepers of the second group control access to the important services that are needed to connect the user to various types of content.[1] Members of the first group are similar to traditional editors, who decide on the content to be published, while members of the second group become gatekeepers as internet service providers (or cable providers in the context of television) due to the structure of the flow of information.

For freedom of speech purposes, the most important online gatekeepers may belong to any of the following groups, depending on the activities they perform: Social media platforms, search engine platforms and application platforms. The latter two gatekeepers routinely make "editorial" decisions by making content unavailable, or deleting or removing it (either to comply with a legal obligation, to respect certain sensibilities, to protect their business interests or to act on their own discretion). As such

[1] Natali Helberger, Katharina Kleinen-von Königslöw & Rob van der Noll, *Regulating the New Information Intermediaries as Gatekeepers of Information Diversity*, 17 INFO: J. OF POL'Y, REG. AND STRATEGY FOR INFO. AND MEDIA 50, 52 (2015).

decisions have a direct impact on the flow of information, these gatekeepers belong to the first group. When the activities of such gatekeepers are related to sorting content, changing the focus among various pieces of content—that is, the "findability" of such content—or for creating a personalized offering for a user, they belong to the second group.[2]

Thus, as Uta Kohl notes, the most important theoretical questions pertaining to the gatekeepers of the internet relate to whether they play an active or passive role in the communication process, the nature of their "editorial" activities, and the extent of the similarities between their editorial activities and actual editing.[3] The role of gatekeepers covered in this volume is not passive. They are key actors of the democratic public sphere and actively involved in the communication process, including making decisions about what their users can access and what they cannot, or can access only with substantial difficulty. Under the current legal approach, gatekeepers are not considered as "media services" or "content providers." This means that while they do demand protection for the freedom of speech in order to enable their selection activities, they are not bound by the various legal guarantees concerning the right of individuals to access the media,[4] and they are not subject to obligations that are otherwise applicable to the media as a private institution of constitutional value,[5] as it is conceptualized in the European legal approach.[6]

I. THE REGULATION OF SEARCH ENGINES

Online search engines typically perform the following three main activities: (1) Collect information available on the internet using automated programs that follow links to jump from site to

---

[2] *Id*. at 53-54.

[3] Uta Kohl, *Intermediaries within Online Regulation*, *in* INFORMATION TECHNOLOGY LAW 85-87 (Diane Rowland, Uta Kohl & Andrew Charlesworth eds., 5th ed., Routledge 2016).

[4] *See generally* RIGHTS OF ACCESS TO THE MEDIA (András Sajó & Monroe Price eds., Kluwer Law International 1996).

[5] William J. Brennan, Jr., *Address* 32 RUTGERS L. REV. 173, 176-77 (1979).

[6] WILLIAM E. BERRY ET AL., LAST RIGHTS: REVISITING FOUR THEORIES OF THE PRESS 77-100 (John C. Nerone ed., Univ. of Illinois Press 1995); *see generally*, COMM'N ON FREEDOM OF THE PRESS, A FREE AND RESPONSIBLE PRESS (Robert D. Leigh ed., Univ. of Chicago Press 1947).

site (crawling); (2) analyze the collected data, assign various metadata, and build indexes that help to find individual sites later on, and (3) use these indexes to select and present users with pages, ranked on the basis of the available metadata, that meet user-specified query criteria in response to searches run by users by entering a keyword or expression.[7]

Finding information on the internet would be considerably more complicated without search engines. Most users use search engines every day as a matter of course. For all practical purposes, a piece of content not indexed by a search engine does not really exist.[8] As such, search engines can be considered as media, as the information available through them has a fundamental influence on the opinions of users.[9] However, by their nature, they are also different from traditional media; search engines are not the authors or publishers of the content they index and present to users but instead typically collect and rank the contents of others. Nonetheless, this activity can be considered to be protected by freedom of speech. Joris van Hoboken argues that search engines constitute a "meta-medium," because they collect and organize the content of others, but the product of their activities—the search results or rankings displayed in response to a search query—can also be regarded as their own independent content.[10]

The implications of search engines for the protection of human rights are reflected in the recommendations of the Council of Europe. Its 2012 recommendation on the protection of human rights with regard to search engines notes that search engines enable the public to search for, receive, and transmit information online.[11] However, the rights of individuals, especially the right to

---

[7] Oren Bracha, *The Folklore of Informationalism: The Case of Search Engine Speech*, 82 FORDHAM L. REV. 1629, 1636 (2014).

[8] Oren Bracha & Frank Pasquale, *Federal Search Commission? Access, Fairness, and Accountability in the Law of Search*, 93 CORNELL L. REV. 1149, 1164 (2008).

[9] EMILY LAIDLAW, REGULATING SPEECH IN CYBERSPACE 178 (Cambridge Univ. Press 2015).

[10] JORIS VAN HOBOKEN, SEARCH ENGINE FREEDOM 189 (Wolters Kluwer 2012) (emphasis omitted).

[11] Comm. of Ministers of the Council of Eur., Recommendation CM/Rec(2012)3 of the Committee of Ministers to member States on the protection of human rights with regard to search engines, ¶ 7, 1139th Sess. (2012) https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805caa87 [https://perma.cc/6UEA-M4DC].

privacy and the protection of personal data, may also be violated by search engine services.[12]

In addition to the protection of these rights, other important criteria include guaranteeing access to the service, the diversity of the service and the unbiased treatment of pieces of content. Accordingly, the recommendation calls for increasing transparency regarding search results (e.g., what pieces of content are considered as hits by the service and why, and what is the reason behind the ranking of hits) with a view to ensuring the plurality and diversity of the presented content.[13] Furthermore, the recommendation also invites service providers not to make any piece of content unavailable through their service unless they do so on the basis of a ground for limiting the freedom of expression set forth in Article 10(2) of the ECtHR.[14] Alas, the current regulatory framework permits search engine providers to be invited, but not obliged, to show this kind of respect for freedom of expression.

As Nico van Eijk notes, search engines operate in a legal vacuum because they are a mixture of telecommunications and content services and do not fall into either of these two categories, or possibly they fall into both at the same time.[15] In the context of European law, this duality is also present in the E-commerce Directive, under which search engines are considered information society services, but they are not subject to the liability and exemption rules laid down in Articles 12 to 14 (concerning mere conduit, caching and hosting).

This means that the application of the notice and takedown procedure to search engines is not mandatory in the Member States under the Directive, either. However, the European Court of Justice established in its ruling in *Google France,* by applying Article 14, that certain services provided by search engines (e.g., storing the data and messages of advertisers in relation to sponsored links) could be considered hosting services.[16] The notice

---

[12] *Id.* ¶ 4.

[13] *Id.* ¶ 7.

[14] *Id.* ¶ 8.

[15] Nico van Eijk, *Search Engines: Seek and Ye Shall Find? The Position of Search Engines in Law*, IRIS *PLUS*, at 7 (2006) (Eur.).

[16] Joined Cases C-236/08 to C-238/08, Google France SARL v. Louis Vuitton Malletier SA, 2010 E.C.R. I-2417, ¶ 111.

and takedown procedure, which makes the liability of a service provider dependent on the actions it takes after it becomes aware of a violation, can be applied where those data are illegal.[17] However, this approach cannot be extended to organic search results in general.

European states may draw various conclusions from this situation. They can: (1) impose obligations on search engines by applying general legislation to take action against illegal content, regardless of the provisions of the E-commerce Directive; (2) apply the notice and takedown procedure described in Article 14 to search engines; (3) extend the scope of the liability rules laid down in Articles 12 and 13 to search engines, which afford greater protection to search engines and also permit the application of interim injunctions regarding illegal content; (4) afford absolute immunity to search engines; or (5) create special rules introducing a regulatory framework that is even stricter than the provisions of the directive. An overview of the solutions applied in Europe indicates that options (1) to (3) are commonly applied, while options (4) and (5)—the introduction of more stringent rules concerning search engines, or affording them absolute immunity—are not applied at all.[18]

In addition to resolving the problem of taking action against illegal content in general, search engines are often required to make certain links unavailable in their system if they violate personality rights, personal data, or are used to commit a criminal offence.[19] The United Kingdom introduced a dedicated framework regulating the liability of website operators for defamatory statements as a supplement to the general legal provisions on defamation and the rules of common law.[20]

It is doubtless that the most effective means of regulating search engines is self-regulation, which is already used by Google in connection with numerous subjects that could be dangerous or harmful to users (e.g., pornography and violence). These rules are

---

[17] *Id.* ¶ 120.

[18] Uta Kohl, *Google: The rise and rise of online intermediaries in the governance of the internet and beyond (Part 2),* 21 INT'L J. OF L. & INFO. TECH. 187, 201 (2013); VAN HOBOKEN, *supra* note 10, at 252-56.

[19] Concerning criminal offences, *see* Kohl, *supra* note 18, at 228-30; concerning personality rights, *see* Defamation Act, 2013, c. 26 § 5 (U.K.).

[20] Defamation Act, 2013, c. 26 § 5 (U.K.).

far more restrictive than the constitutionally permitted limitations to the freedom of speech.[21]

In the U.S., Section 230 of the Communications Decency Act affords broad immunity to search engines against legal liability for illegal content that is accessible through their services. However, copyright legislation requires search engines to apply notice and takedown procedures.[22]

In autocratic countries, the introduction of strict rules concerning search engines is one of the most effective means of keeping undesirable opinions from public access. If the activities of search engines were protected by the freedom of speech (meaning in this context the legal corpus originating from the First Amendment of the U.S. Constitution), it would not be possible to object to such practices if they were applied, for example, by the state-owned search engine of China.[23] However, internal "private censorship" is not fully consistent with the European idea of freedom of expression, and private parties can also be expected under legal regulations to serve and support democratic public life.

II. PRIVACY AND SEARCH ENGINES: THE RIGHT TO BE FORGOTTEN

Even before the emergence of the internet, the law had recognized and afforded protection to the legitimate interest of persons in disappearing from the public sphere and making previously published information inaccessible. The perpetrators of criminal offences, for instance, are absolved of the detrimental consequences of their punishment after they serve their sentence, meaning that they may not be confronted with the crimes they

---

[21] *See* VAN HOBOKEN, *supra* note 10, at 237, 245.

[22] Digital Millennium Copyright Act (DMCA), Pub. L. No. 105, 304, 112 Stat. 2860 (codified in scattered sections of 17 U.S.C.); *see* 17 U.S.C. § 512(d) (requiring "notification" and "expeditious[]" removal).

[23] See *Zhang v Baidu.com*, 932 F. Supp. 2d 561, 566 (S.D.N.Y. 2013) (holding, in part, that the district court lacked jurisdiction to address whether the People's Republic of China properly refused to effect service pursuant to Hague Convention on the ground that doing so would infringe its sovereignty or security, in plaintiffs' suit alleging that China and a Chinese Internet search engine service provider conspired to prevent their political speech, in violation of American federal, state, and municipal law).

committed earlier, and they may even start a new life by changing their identity in justified cases.[24] In some European jurisdictions, the veracity of a statement may not be proven in criminal proceedings launched for defamation, unless there is a public interest (e.g., taking a position in a public debate) or a considerable private interest in the publication of that information. In the absence of such an interest, even statements that are in fact true can be considered defamatory, meaning that they result in the truth being forgotten.[25] Privacy, an important aspect of the protection of personality, is afforded protection through the rules of liability for damages and the provisions of private law, and it can also be used under certain circumstances to prevent the publication of otherwise true statements.

The protection of personal data is also relevant in this context. The EU Directive on the protection of personal data[26] (since repealed) provided that personal data processed by a controller must be "adequate, relevant and not excessive" regarding the further processing of such data,[27] while they must also be accurate and, if necessary, up-to-date.[28] The data subject must be permitted to request from the controller the rectification, erasure or blocking of data the processing of which does not comply with the provisions of the directive.[29] While it caused considerable excitement at its time, the *Google Spain* case[30] did not introduce much novelty in terms of possibly affording any additional right to persons who are concerned about their personal data, though it was certainly novel in that the European Court of Justice held that the obligations laid down in the Directive could also be extended to search engine operators.

---

[24] *See* X (a woman formerly known as Mary Bell) v. O'Brien, [2003] EWHC 1101 [¶ 1] (QB); *Carr v. News Group Newspapers Ltd*, [2005] EWHC 971 [¶¶ 1, 3] (QB).

[25] *See, e.g.*, Code Criminal [C. Crim.] art. 270 (Den.); 2012 Büntető Törvénykönyv [BTK.] § 229 (Act C of 2012 on the Criminal Code § 229) (Hung.); Tryckfrihetsfördningen [TF] [Constitution] 7:14(14) (Swed.).

[26] Council Directive 95/46/EC, 1995 O.J. (L 281).

[27] *Id*. at art. 6(c).

[28] *Id*. at art. 6(d).

[29] *Id*. at art. 12(b).

[30] Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEDP), 2014 E.C.R. 317 (Spain).

According to the European Court of Justice, the activities of search engines constitute data processing for the purpose of Article 2(b) of the Directive, as:

> the operator of a search engine 'collects' such data which it subsequently 'retrieves', 'records' and 'organises' within the framework of its indexing programmes, 'stores' on its servers and, as the case may be, 'discloses' and 'makes available' to its users in the form of lists of search results.[31]

Its activities are, however, different from those of a publisher of websites, the activities of which are involved in a search.[32] Search engines play a decisive role in the global dissemination of data and information, considering that some users would be unable to find a given piece of information without them.[33] This means that the activities of a search engine "have an additional effect" to the activities of the publishers of websites, and they are capable of having a considerable impact on the rights relating to the protection of privacy and personal data.[34] A search engine does not simply facilitate access to information; it also "may play a decisive role in the dissemination of that information, [and] it is liable to constitute a more significant interference with the data subject's fundamental right to privacy than the publication on the web page."[35]As such, a search engine may be required to render personal data in its possession inaccessible, meaning that it would be removed from the list of search results, but it would remain available at its original location (i.e., on the relevant website). However, a search engine may not be required to delete such data:

> if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of

---

[31] *Id*. ¶ 28 (translated to English).
[32] *Id*. ¶¶ 35, 83.
[33] *Id*. ¶ 36.
[34] *Id*. ¶¶ 38, 83 (translated to English).
[35] *Id*. ¶ 87 (translated to English).

> inclusion in the list of results, access to the information in question.[36]

This means that the freedom to discuss public affairs is a limitation of the right to the protection of personal data. The decision caused considerable excitement and triggered a lively debate, as it gave rise to extensive commentaries in legal literature almost immediately upon its being passed.[37]

An interesting detail of the case is that Mario Costeja decided to request that a search engine render its links inaccessible, instead of acting against the newspapers that featured the original 1998 article (pertaining to his old social insurance debt and the forced auction of his property) in their online archives. This fact is telling about the role Google plays in public life. Online archives are far less frequently consulted and, as Filippo Fontanelli points out, Costeja would not have bothered to act if Google had featured the article concerned on the twenty-third page of its list of search results.[38] However, a legal procedure was initiated as the article was featured by Google's algorithm in a prominent place, thereby making the information about the plaintiff easily accessible.

Irini Katsirea is concerned that the logic behind this decision might snowball, possibly affecting online press archives as well, since the limits of the right to be forgotten seem to be vague.[39] It certainly seems to be the case that the court failed to make a clear distinction between archives and the search rankings of a search engine, and the judgment itself does not offer many possible defences against a possible request to delete "irrelevant" or "outdated" data from online archives as well. Dr. Jan Oster also pointed out that the decision does not say much on issues relating

---

[36] *Id*. ¶ 97.

[37] *See* David Lindsay, *The 'Right to Be Forgotten' by Search Engines under Data Privacy Law: A Legal Analysis of the* Costeja *Ruling*, 6 J. MEDIA L. 159 (2014).

[38] Filippo Fontanelli, *The Court of Justice of the European Union and the illusion of balancing in internet-related disputes*, *in* THE INTERNET AND CONSTITUTIONAL LAW 106 (Oreste Pollicino & Graziella Romeo eds., Routledge 2016).

[39] *See* Irini Katsirea, *Search Engines and Press Archives between Memory and Oblivion*, 24 EUR. PUB. L. 125 (2018).

to the freedom of speech (the interests of the public are mentioned in the part quoted above).[40]

Article 9 of the Directive enabled Member States to grant exemptions from the obligations pertaining to the protection of personal data for the processing of such data for "journalistic purposes":

> Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.[41]

However, this provision merely offered a possibility to Member States, and did not impose any obligation to do so. It is also apparent from the approach taken by the European Court of Justice that the data processing carried out by Google is not considered similar or analogous to journalistic activities.[42]

The justification for just this distinction is vehemently challenged by Robert Post.[43] While it seems clear that a search engine makes personal data, among other data, more easily accessible, it is not clear why its activities should be regarded with more stringency than the activities of a press archive, taking into account that, at the end of the day, the publication of the information is a result of the activities of the latter.[44] However, this is not the main concern raised by Post: He argues that Google is an indispensable actor in the infrastructure of communications, and it is absolutely necessary to maintain a vibrant public sphere.[45] Google serves the same public interests as journalism or the media in general,[46] and its activities are similar to newspapers

---

[40] Jan Oster, *Communication, defamation and liability of intermediaries*, 35 LEGAL STUDIES 348, 355-57 (2015) (U.K.); *see also supra* note 36 and accompanying text.

[41] Council Directive 95/46, art. 9, 1995 O.J. (L 281) (EC).

[42] *See* Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEDP), 2014 E.C.R. 317, ¶ 85 (Spain).

[43] *See generally* Robert Post, *Data Privacy and Dignitary Privacy:* Google Spain*, the Right to Be Forgotten, and the Construction of the Public Sphere*, 67 DUKE L.J. 981 (2018).

[44] *Id.* at 1010.

[45] *Id.* at 1016.

[46] *Id.* at 1041-43.

in that it serves the public and shapes democratic public opinions. The press plays the same role, with the difference that it publishes the views and opinions of journalists and editors. While this does not apply to a search engine, Post argues that this is an insignificant difference, as the point is that they both convey information to the public (users), which makes the press and search engines highly similar to each other.[47]

The available case law on search engines and the right to be forgotten took off shortly after the decision was passed.[48] It is hardly a surprise that one of the main difficulties resulting from the judgement is the weighing of interests required under the judgement. One difficulty, for example, is the weighing of interests in keeping processing the given piece of information, for the purposes of discussing public affairs openly, against the interests in discarding irrelevant or outdated information. Common law countries have also faced the problem of assessing and weighing the status of the applicant, his or her role in public life at the time of the affair, and the significance of the public interest in preserving a given piece of information.[49] In *NT1 & NT2*, the court had to answer the question whether the right to be forgotten was applicable in cases involving spent criminal convictions. According to Justice Warby, NT1's claims were unfounded as the claimant failed to satisfy the criteria established in *Google Spain*.[50] In the case of NT2, the information available through Google had become "irrelevant and of no sufficient legitimate interest to users of Google Search to justify its continued availability, so that an appropriate delisting order should be made."[51]

In *ML & WW v. Germany,*[52] the European Court of Human Rights (ECHR) held that Article 8 of the Convention was not

---

[47] *Id*. at 1042-43.

[48] *See* THEO BERTRAM ET AL., THREE YEARS OF THE RIGHT TO BE FORGOTTEN, https://pdfs.semanticscholar.org/13f5/e3cd0e8e522238f5df2ce279e6188664165e.pdf?_ga=2.239223555.1447831536.1582150978-883857468.1582150978 [https://perma.cc/3GYX-6JAA].

[49] *See, e.g.*, NT1 & NT2 v. Google LLC [2018] EWHC 799 (QB); *see also* Róisin A. Costello, *The Right to Be Forgotten in Cases Involving Criminal Convictions*, 3 EUR. HUM. RTS. L. REV. 268 (2018).

[50] NT1 & NT2 v. Google LLC [2018] EWHC 799 [¶ 170] (QB);

[51] *Id*. [¶ 223].

[52] *See* M.L. & W.W. v. Germany, No. 60798/10 & 65599/10, Eur. Ct. H.R., ¶ 116 (2018).

violated by the respondent state. The facts of the case were similar to *NT1 & NT2*'s, as the publications by the media concerned a murder conviction. But this was not a case against search engines: The articles appeared in search engine results but the applicants did not make applications in Germany for search engine delisting. However, the decision confirmed the theoretical availability of an Article 8 claim against search engines as well.[53] The ECHR emphasized that the balance of interests may lead to different results depending on whether an individual directs her request for erasure to a search engine operator or primary publisher.[54]

Essentially, the decision of the European Court of Justice in *Google Spain* forced search engines to assume the role of an editor (a somewhat inverted version of the editor's role), as they do not decide on the publication but on the removal of information, and their decision applies to their own system only, even though it is usually indispensable for finding old information. While Google had already been carrying out similar editorial tasks (filtering and ranking content to be presented to users), it had been doing so at its own initiative and in the service of its own economic interests. However, now it is required to do so by law, similarly to the situation of autocomplete search suggestions.

The scope of *Google Spain* was limited to the Spanish version of the search engine (.es domain) as the Spanish authorities believed that their jurisdiction was limited to that scope. However, the Supreme Court of Canada in *Equustek* required Google to perform the removal of links concerning all of its domains, considering that the right to the protection of intellectual property could not be enforced in any other way, for example by removing such links from the .ca domain only.[55] Though *Equustek* was an intellectual property case, it may have some consequences also for

---

[53] *See* Hugh Tomlinson QC & Aidan Wills, *Case Law, Strasbourg: ML and WW v Germany, Article 8 right to be forgotten and the media*, THE INT'L F. FOR RESPONSIBLE MEDIA BLOG (July 4, 2018), https://inforrm.org/2018/07/04/case-law-strasbourg-ml-and-ww-v-germany-article-8-right-to-be-forgotten-and-the-media-hugh-tomlinson-qc-and-aidan-wills/ [https://perma.cc/93FE-V8NB].

[54] M.L. & W.W. v. Germany, No. 60798/10 & 65599/10, Eur. Ct. H.R., ¶ 97 (2018).

[55] Google Inc. v Equustek Solutions, Inc., [2017] 1 S.C.R. 824, 827 (Can.); *see generally* Michael Douglas, *A Global Injunction Against Google*, 134 L. Q. REV. 181 (2018) (Austl.).

the future of the right to forgotten. According to Ronald Krotoszynski, "[it] seems highly likely that a similar kind of analysis could be brought to bear in right to be forgotten cases . . . that involve domestic court orders that require the de-indexing of content not only within the issuing court's territory. . . ."[56] According to him, in the context of the right to be forgotten, this approach would limit the citizens of a country only to the information that the domestic court of *another* country deems appropriate. The issue of the scope of removal will also be faced by the European Court of Justice, as its preliminary ruling on the matter has been sought in a French case.[57]

The General Data Protection Regulation (GDPR) adopted by the EU and replacing the previous Directive introduced considerable changes regarding the right to be forgotten.[58] First, it is significant that the Regulation is directly applicable in each Member State, thus the same provisions are to be applied with the same wording as adopted by the EU. Second, the right to be forgotten is mentioned by exactly this name in the regulation (and as a synonym for the right to erasure). Third, the Regulation seeks to afford greater protection to the freedom of expression, by providing that this right may not be exercised where "processing is necessary . . . for exercising the right of freedom of expression and information."[59] The recognition of this exception is not merely an option but an obligation for each Member State. The vague phrase "journalistic purposes" mentioned in the Directive has now been replaced by the protection of the freedom of speech and the right to information, although only the latter is mentioned in the

---

[56] Ronald J. Krotoszynski, *Privacy, Remedies, and Comity: The Emerging Problem of Global Injunctions*, COMPARATIVE PRIVACY AND DEFAMATION (forthcoming July 2020) (manuscript at 22) (on file with author).

[57] *French court refers 'right to be forgotten' dispute to top EU court*, REUTERS (July 19, 2017), https://www.reuters.com/article/us-google-litigation/french-court-refers-right-to-be-forgotten-dispute-to-top-eu-court-idUSKBN1A41AS [https://perma.cc/XL5Q-JMJ3].

[58] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119), https://eur-lex.europa.eu/eli/reg/2016/679/oj [hereinafter GDPR] [https://perma.cc/3Z7L-AG68].

[59] GDPR, art. 17(3)(a).

preamble, along with audiovisual and news archives.[60] The GDPR seeks to maintain the obligation of search engines to respect the right to be forgotten, even though the text of the regulation in fact reinforces the arguments for their exemption: a search engine is certainly capable of serving both the freedom of expression and the right to information.

Furthermore, the Regulation focuses on the exercise of such rights and indicates where there are exceptions from their exercise, so that these exceptions do not necessarily mean the exercise of any right by a service provider but may apply to users as well. This means that, when considering the situation while bearing in mind the interests of users, a search engine might even be exempted from its erasure obligation, regardless of whether or not a search result is recognized as a form of free expression by the search engine. However, this observation would not apply if irrelevant or outdated pieces of information are not considered to be necessary for the exercise of the freedom of expression or the right to information.

Thus, the criticism offered by Post also remains relevant in the context of the GDPR, although it should be noted that if search engines were considered to be media-like services, as he suggests, it would be an unequivocally welcome change for search engines under the law of the First Amendment. Following such an approach in Europe, however, would mean that the public interest obligations of the media would also apply to search engines, including the requirement of diversity in content, the right to reply for anyone attacked through false factual allegations in the media, and the protection of the audience from harmful content. The situation is ambiguous: on the one hand, the right to be forgotten requires search engines to fulfil a kind of editorial role, while on the other hand, the performance of this task is in part why search engines cannot be considered as media, and, as a key conceptual component of media services, become an actual "editor" in the legal sense of the term.

The U.S. legal system would not be comfortable with recognizing a general right to be forgotten, and Section 230 of the CDA also excludes any kind of liability on the part of search

---

[60] GDPR, recital 153.

engines in this respect.[61] Nonetheless, it is worth pointing out that certain rights akin to the right to be forgotten might exist in certain limited fields of the law, for example under the Fair Credit Reporting Act requiring the erasure of financial data,[62] a Californian statute allowing minors to request the subsequent erasure of data they published online concerning themselves,[63] and other similar provisions and drafts.[64]

III. THE REGULATION OF SOCIAL MEDIA PLATFORMS

Social media platforms have become the primary arena of online public life, but there is no generally accepted definition for such platforms (also known as social networks). For the purposes of this part, social media platforms also include video sharing portals, where users can upload publicly available content, as well as platforms where user-generated content (including videos, texts, images, links, etc.) is made available to, and then shared by, an audience selected by the user. This part applies the same approach towards YouTube, Facebook and Twitter. The main reason for doing so is that, from a freedom of speech perspective, the activities of these platforms are quite similar and can be examined using similar methods. Each of these services is capable of restricting user-generated content, and they are even legally required to do so from time to time. The Audiovisual Media Services Directive[65] of the EU has introduced common rules for these two different services—the scope of the directive extends to audiovisual content that is present on both video sharing platforms and social media platforms.[66]

---

[61] 47 U.S.C. § 230 (2018).

[62] *See* Frank Pasquale, *Reforming the Law of Reputation*, 47 LOY. U. CHI. L.J. 515, 530-31 (2015).

[63] CAL. BUS. & PROF. CODE. § 22581 (West 2020).

[64] Lawrence Siry, *Forget Me, Forget Me Not: Reconciling Two Different Paradigms of the Right to Be Forgotten*, 103 KY. L.J. 311, 331-33 (2014).

[65] Directive 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in the view of changing market realities, 2018 O.J. (L 303/69), ¶¶ 4, 5 [hereinafter New AVMS Directive].

[66] *See* FRANCISCO J. CABRERA BLÁZQUEZ ET AL., *THE LEGAL FRAMEWORK FOR VIDEO-SHARING PLATFORMS*, IRIS *PLUS* (2018).

The matter of legal liability of such platforms raises complex issues. A platform *per se* is not the primary communicator of a harmful opinion, as it only enables others to speak, and sorts and displays such content to other users. The European legal approach dictates that social media platforms must play an active role in the removal of violating content and that they may held be liable if they fail to do so.[67] As such, government regulation involves platform service providers in remedying various violations so that such providers are obliged to decide on the lawfulness of the content concerned. In other words, the task of enforcing the law is shared between the government (courts) and private actors.[68] A rather limited version of the same model is also used in the US, under the aegis of the authorization granted in Section 230 of the CDA. In this way, platform providers become both media companies that decide on the permissibility of content and participants in applying and enforcing the law.[69] While courts naturally play a considerable role in deciding social media related issues that are relevant to the freedom of speech, the moderators and legal counsels of these platforms have a far greater influence on the freedom of discussions and exchanges on the platform than the dedicated government apparatus does.[70]

Under EU law, social media platforms are considered to be hosting service providers, as the users of such services store, sort and make available their own content in and through the system. This means that, pursuant to the E-commerce Directive, the platforms are required to remove any violating content after they become aware of its infringing nature, but they may not be subject to any general monitoring and control obligation.[71] In an Austrian case (which is currently pending, as a preliminary ruling by the

---

[67] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), 2000 O.J. (L 178), art. 14 [hereinafter E-Commerce Directive].

[68] Jack M. Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, 51 U.C. DAVIS L. REV. 1149, 1179 (2018).

[69] *Id*. at 1180-81.

[70] Marvin Ammori, *The "New"* New York Times*: Free Speech Lawyering in the Age of Google and Twitter*, 127 HARV. L. REV. 2259, 2261-63 (2014).

[71] E-Commerce Directive, arts. 14, 15.

European Court of Justice has been sought), certain issues were raised concerning the extent of the obligation of removal in the context of Facebook's activities. Briefly, the question is whether a platform may be required under Article 14 of the Directive to remove not only a specifically identified piece of content, but also all other identical and even "similar" content that might be made available in the future. Would such a requirement be inconsistent with the Directive's prohibition on introducing any monitoring obligation?[72]

The proposal of the Austrian court seems reasonable, considering that this particular remedy could be rendered obsolete and useless by the prompt spread and reproduction of harmful content, if a platform were required to remove only specifically identified pieces of content without any such extension. In addition to the E-commerce Directive, more general pieces of legislation also apply to communications through social media platforms, including legislation on data protection, copyright, personality rights, public order, and criminal law. Such legal provisions may also introduce further obligations on hosting service providers in the context of removing violating content.

Offline restrictions of speech are also applicable to communications through social media platforms.[73] Common violating behaviors in social media can be fitted into more traditional criminal categories (i.e., those that were adopted in the context of the offline world) almost without exception, making the introduction of new prohibitions unnecessary.[74] However, this duality gives rise to numerous difficulties as, on the one hand, such limitations are defined as part of the national legislation of each and every country (and the law of free speech is also far from being fully harmonized among EU Member States) while, on the other hand, social media is of its essence a global phenomenon, meaning that it transcends national borders. For example, an opinion that is protected by the freedom of speech in Europe might

---

[72] OGH, Oct. 25, 2017, 6 Ob 116/17b, (2017) (Austria).

[73] Jacob Rowbottom, *To Rant, Vent and Converse: Protecting Low Level Digital Speech*, 71 CAMBRIDGE L.J. 355, 357-66 (2012).

[74] SELECT COMMITTEE ON COMMUNICATIONS, SOCIAL MEDIA AND CRIMINAL OFFENCES, 2014-5, HL 37 (UK), https://publications.parliament.uk/pa/ld201415/ldselect/ldcomuni/37/37.pdf [https://perma.cc/8GP8-MN5A].

constitute punishable blasphemy in an Islamic country. Since harmful content can be made available worldwide and is spread and multiplied on a social media platform quickly, the absence of a uniform standard leads to tension and violence.[75]

As social media platforms spread, it became clear, about a decade after the previous amendment of the directive, that media regulation cannot be interpreted in such a restrictive manner any longer. A proposal for the amendment of the AVMS Directive published in May 2016 introduced the terms "video-sharing platform service" and "video-sharing platform provider."[76] According to the amendment eventually adopted in November 2018, the material scope of the Directive was extended to cover such services.

Even though the original proposal would not have extended the scope of the Directive to social media platforms (in terms of the audiovisual content uploaded to the site), it became clear during the legislative process that they could not be exempted from the Directive, and it could not focus solely on portals used to share videos (e.g., YouTube).[77] This means that, despite their somewhat misleading name, video-sharing platforms include audiovisual content published on social media. An important aspect of the newly-defined term is that service providers do not bear any editorial responsibility for such content; although service providers do sort, display, label, and organize such content as part of their activities, they do not become media service providers.

Article 28(b) of the amended Directive provides that Articles 12 to 15 of the E-commerce Directive (in particular the provisions on hosting service providers and the prohibition of introducing a general monitoring obligation) remain applicable. Member States

---

[75] *See* Uta Kohl, *Islamophobia, "Gross Offensiveness" and the Internet*, 27 INFO. & COMM. TECH. L. 111 (2018).

[76] Proposal for a Directive of the European Parliament and of the Council amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services in view of changing market realities., COM (2016) 287 final (May 25, 2016), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016PC0287&from=EN [https://perma.cc/86N7-BKJ4].

[77] Duncan Robinson, *Social networks face tougher EU oversight on video content*, FIN. TIMES (May 25, 2017), https://www.ft.com/content/d5746e06-3fd7-11e7-82b6-896b95f30f58 [https://perma.cc/W34T-S8RM].

must ensure that video-sharing platform providers operating within their respective jurisdiction take appropriate measures to ensure:

> - the protection of minors from programmes, user-generated videos and audiovisual commercial communications which may impair their physical, mental or moral development;
>
> - the protection of the general public from programmes, user-generated videos and audiovisual commercial communications containing incitement to violence or hatred directed against a group of persons or a member of a group;
>
> - the protection of the general public from programmes, user-generated videos and audiovisual commercial communications containing content the dissemination of which constitutes an activity which is a criminal offence under Union law, namely public provocation to commit a terrorist offence within the meaning of Article 5 of Directive (EU) 2017/541, offences concerning child pornography within the meaning of Article 5(4) of Directive 2011/93/EU of the European Parliament and of the Council, and offences concerning racism and xenophobia within the meaning of Article 1 of Framework Decision 2008/913/JHA;
>
> - compliance with the requirements set out in Article 9(1) with respect to audiovisual commercial communications that are marketed, sold or arranged by the video-sharing platform providers (general restrictions of commercial communications and provisions in order to safeguard minors from commercials).[78]

What constitutes an "appropriate measure" is to be determined with regard to the nature of the content in question, the harm it may cause and the characteristics of the category of persons to be protected, as well as the rights and legitimate interests at stake. These interests include those of the video-sharing platform providers and of the users who created,

[78] New AVMS Directive, *supra* note 65.

transmitted, and/or uploaded the content, as well as the public interest.[79]

The legal situation is somewhat simpler in the U.S., as Section 230 of the CDA also protects social media platforms against government interference.[80] If a platform only provides the facilities needed to upload content, it cannot be held responsible for the possibly infringing nature of that content, even if it encourages users to speak and sorts user content.[81] However, if a platform controls, generates, actively edits, or modifies such content, it loses its immunity.[82] The scope of exceptions from this rule can also be extended, as happened in April 2018, when a recently adopted law permitted taking action against websites, including hosting service providers, promoting trafficking in human beings for sexual exploitation.[83]

IV. PRIVACY AND SOCIAL MEDIA PLATFORMS

Freedom of opinion means that people are free to form their own convictions and hold their own opinions on the basis of the information available. It follows that this freedom is also related to the protection of private life, freedom of religious beliefs and the freedom of speech. However, social media platforms tend to ignore this aspect of privacy. The business model of such platforms is based on the targeted display of advertisements, and they need to know their users to fulfil this goal. Knowing their users means, on the one hand, knowing the information users share and publish,

---

[79] *Id*. art. 28b(3).

[80] 47 U.S.C. § 230 (2018).

[81] Claire Ballentine, *Yelp Can't Be Ordered to Remove Negative Posts, California Court Rules*, N.Y. TIMES (July 3, 2018), https://www.nytimes.com/2018/07/03/technology/yelp-negative-reviews-court-ruling.html [https://perma.cc/GJP7-NY7U].

[82] Tom Jackman & Jonathan O'Connell, *Backpage has always claimed it doesn't control sex-related ads. New documents show otherwise.*, WASH. POST (July 11, 2017), https://www.washingtonpost.com/local/public-safety/backpage-has-always-claimed-it-doesnt-control-sex-related-ads-new-documents-show-otherwise/2017/07/10/b3158ef6-553c-11e7-b38e-35fd8e0c288f_story.html [https://perma.cc/S74R-U8UX].

[83] 18 U.S.C. § 2421A (2018). For an overview, *see* Tom Jackman, *Trump signs "FOSTA" bill targeting online sex trafficking, enables states and victims to pursue websites*, WASH. POST (April 11, 2018), https://www.washingtonpost.com/news/true-crime/wp/2018/04/11/trump-signs-fosta-bill-targeting-online-sex-trafficking-enables-states-and-victims-to-pursue-websites/?noredirect=on&utm_term=.faccd8cf7174 [https://perma.cc/4LK3-FW76].

so that their profile can be charted for targeted marketing, and, on the other hand, knowing (or at least guessing) the ideas users do not speak of or do not even have at the time. This is how advertisements—which suggest what to buy, which hotel to book or which website to visit—become shown to users.

The opinions of users can not only be guessed, but they can also be influenced and directed by suggestions. Users may be able to control such suggestions through their free will, but their freedom to decide for themselves is clearly restricted. The more information is available on a given user, the more detailed a profile is built up by a platform, and the more targeted the advertisements shown to him are, and consequently the more restricted that freedom becomes.[84] It seems particularly worrisome that data collection may also extend to opinions that are not communicated and which exist only as thoughts—as happens when the analysis of messages never sent and content never posted is also used to develop the profile of a user.[85] This means that not even the content of unsent messages remains secret, as it would otherwise remain in the offline world. Nonetheless, most users permit platform providers to process their personal data without being particularly concerned, in exchange for a high-quality personalized service. This phenomenon raises fundamental questions regarding the future of privacy protection and the practicality of its basic principles.[86]

Measures to protect privacy, various torts, and the provisions of a civil code may be applied in the context of disputes among social media users. Such means and measures must be applied with due regard to and in line with the values of free speech and the open discussion of public affairs.[87] Privacy concerns and

---

[84] Susie Alegre, *Rethinking Freedom of Thought for the 21st Century*, EUR. HUM. RTS. L. REV. 221, 226-27 (2017).

[85] *See* Sauvik Das & Adam Kramer, *Self-Censorship on Facebook*, *in* PROCEEDINGS OF THE SEVENTH INTERNATIONAL AAAI CONFERENCE ON WEBLOGS AND SOCIAL MEDIA (2013), https://www.aaai.org/ocs/index.php/ICWSM/ICWSM13/paper/viewFile/6093/6350 [https://perma.cc/EFC9-3N5K].

[86] *See* Lee Rainie & Janna Anderson, *The Future of Privacy*, PEW RES. CTR., (Dec. 18, 2014), http://assets.pewresearch.org/wp-content/uploads/sites/14/2014/12/PI_FutureofPrivacy_1218141.pdf [https://perma.cc/TMC5-785F].

[87] *See* Von Hannover v. Germany, No. 59320/00, Eur. Ct. H.R., ¶¶ 56-58, 64 (2004); Campbell v. MGN Ltd, [2004] 2 AC 457 (HL).

violations by social media platforms are not covered here, as they are only indirectly related to free speech issues. Platforms do not publish the data they collect on their users, but such information is used subsequently to determine the content (e.g., Facebook news feed) provided to each user concerned. If such content is considered the "opinion" of the platform, it becomes clear that free speech issues can be closely related to various privacy issues.[88]

It is difficult for social media platforms to decide what to do with information uploaded by their users after their death. The right to privacy dictates that the photographs, messages and other content of a deceased person are to be protected, even against any next of kin, but this consideration is often in conflict with the family members' right to respect for the deceased. To date, this conflict seems irresolvable at the level of principles.[89]

The notice-and-takedown procedure laid down in the E-commerce Directive is a specific area where the liability of a platform for a privacy violation may have a direct impact on free speech. Generally, the procedure is conducted in a similar way to the removal of any other infringing content, meaning that the platform is required to decide on the permissibility of a specific piece of content if it receives a privacy violation notice.[90] This means that the platform has to play the roles of both editor and judge; it has to decide on whether to remove a piece of content or keep it accessible, thereby also passing a decision on its permissibility. This form of regulation raises some obvious concerns. If a platform decides not to remove a piece of allegedly violating content, the claimant may sue the platform as well as its author.

For example, a dispute between private parties turned into a dispute between a platform and a private individual in *CG v.*

---

[88] *See* Case C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH, 2018 E.C.R. 388 (The Grand Chamber of the European Court of Justice holding that both the platform and the administrators of a fan page are liable for the privacy violations committed by Facebook concerning user data managed by the fan page operators on Facebook.).

[89] *See* Damien McCallig, *Facebook after death: an evolving policy in a social network*, 22 INT'L J. OF L. & INFO. TECH. 107 (2014); Bo Zhao, *Posthumous Defamation and Posthumous Privacy Cases in the Digital Age*, 3 SAVANNAH L. REV. 15, 16-17 (2016).

[90] E-Commerce Directive, *supra* note 67, art. 14.

Facebook Ireland Ltd. in Northern Ireland.[91] A Facebook user set up two sites on the platform where he published the personal data of persons convicted of committing pedophile offences (sex crimes against children). A photograph and the home address of the claimant (referred to by the abbreviation "CG" in the case documents) were also displayed next to an exchange. The claimant had indeed been convicted of a pedophile offence, but he had served his sentence, had been released, and was not considered a threat to society any more by public authorities.

However, he was harassed and received threats against his life because of the Facebook page. The communication concerning the claimant was considered a clear misuse of private information, but Facebook refused to remove the information after receipt of a notice on the grounds that the notice was not submitted in the required form (it had been sent by post instead of using Facebook's own system). The court pointed out that a platform provider may not specify a required form for sending a notice, and that the only relevant factor was whether or not a notice was received. During the period between receipt of the notice and the removal of the infringing content (as it was removed eventually), Facebook was committing a violation.[92]

In addition to enabling their users to express their opinions, social media platforms also provide employers with means of controlling their employees. When an employer believes that a published opinion about it is harmful to its interests, it may impose a sanction on the employee who expressed this opinion. This is exactly what happened in *Bland v Roberts*.[93] It appears from UK case law that the freedom of speech of employees is afforded extensive protection, as an opinion presented regarding a private or public matter may not be followed by sanctions where it did not violate the interests of the employer.

That is the situation, for example, where an opinion remains within the protected boundaries of free speech and it may not be

---

[91] CG v. Facebook Ireland Ltd., [2016] NICA 54 (N. Ir.).

[92] Lorna Woods, *When is Facebook liable for illegal content under the E-commerce Directive? CG v. Facebook in the Northern Ireland courts*, EU LAW ANALYSIS (Jan. 19 2017), http://eulawanalysis.blogspot.com/2017/01/when-is-facebook-liable-for-illegal.html [https://perma.cc/RJ2M-JWDG].

[93] *See* Bland v. Roberts, 730 F.3d 368, 373-74 (4th Cir. 2013).

considered the employer's opinion or an "official" position published in its name and on its behalf.[94] In the context of U.S. law, Cara Magatelli argued that employees are free to pursue any kind of activity outside work as long as such activities are not illegal and do not violate the legitimate business interests of their employer.[95] Other rules apply when Facebook is used during working hours, but in such cases any possible sanctions are not based on the content of a message but on the misuse of working time. The judgment of the Grand Chamber of the European Court of Human Rights (ECHR) in the case of *Bărbulescu v Romania*[96] found that the monitoring of an employee's email account resulted in the violation of his right to respect for private life and correspondence within the meaning of Article 8 of the ECHR.

Though this was not a case related to social media usage, the decision has important implications generally to employees' online privacy rights at the workplace, and so it is relevant for our purposes. According to the ECHR, the applicant was not informed on the extent and the nature of the monitoring activities or the possibility of his employer having had access to the content of the communications. The Court observed that the domestic courts did not pay attention to the scope of the monitoring, the degree of the intrusion nor to whether the monitoring was justified by legitimate reasons. The specific aim of such strict monitoring was not identified, while neither the seriousness of the consequences for the applicant nor alternative less intrusive measures were examined.

Mary-Rose Papandrea raised the interesting issue of whether or not an employee may communicate with others through social media concerning a work-related matter (as if doing so were part

---

[94] *See* Smith v. Trafford Housing Trust, [2012] EWHC 3221 (Ch) (Eng.). For more details on case-law, *see* Dominic McGoldrick, *The Limits of Freedom of Expression on* Facebook *and Social Networking Sites: A UK Perspective*, HUM. RTS. L. REV. 125, 139-49 (2013). Regarding the difficulties in protecting free speech rights in the workplace, *see* Paul Wragg, *Free Speech Rights at Work: Resolving the Differences between Practice and Liberal Principle*, INDUS. L. J. 1 (2015); *see also* David Mangan, *Online Speech and the Workplace: Public Right, Private Regulation*, 39 COMP. LAB. L. AND POL'Y J. 357 (2018) (Eng.)

[95] Cara Magatelli, *Facebook is Not Your Friend: Protecting a Private Employee's Expectation of Privacy in Social Networking Content in the Twenty-First Century Workplace*, 6 J. OF BUS., ENTREPRENEURSHIP & THE LAW. 103 (2012).

[96] Bărbulescu v. Romania, No. 61496/08, Eur. Ct. H.R., ¶ 56 (2017).

of his or her job).[97] This issue is particularly sensitive in the context of exchanges between teachers and students. If an employer prohibits teachers from communicating with students (e.g., to prevent inappropriate communication and relationships), the prohibition might limit the teachers' freedom of speech, even in situations where they wish to discuss a non-educational matter with a student.

Naturally, the freedom of speech may be restricted in justified cases, but only if doing so satisfies the appropriate laws and tests.[98] Regulating the use of social media is a possibility, and is an established practice in some work communities; furthermore, it does not seem to be an objectionable one where the legitimate interests of an employer require the regulation of those activities of its workers in situations where their posts and tweets could be regarded as the opinion of the employer.

This is why the *New York Times* introduced guidelines for the use of social media by its journalists.[99] It may seem ironic that the social media presence of journalists working for a traditional medium is subject to such regulation, but the reasons for regulation can easily be appreciated. As is also admitted by the journalists themselves, whatever they publish, even as a private individual, might be construed as the position of the paper which they work for.

CONCLUSION

It seems hard to dispute that search engines should be considered "editors". This position is supported by: (1) the preliminary and self-regulatory filtering of content that could offend users (pornography, violence etc.); (2) the role search engines play in the removal of links to content violating copyrights, personality rights or other rights, and (3) the possibility of manipulating their search results in their own or someone else's interest. However, such activities should not be

---

[97] *See* Mary-Rose Papandrea, *Social Media, Public School Teachers, and the First Amendment*, 90 N.C. L. REV. 1597 (2012).

[98] *Id*. at 1600-02.

[99] *The Times Issues Social Media Guidelines for the Newsroom*, N.Y. TIMES (Oct. 13, 2017), https://www.nytimes.com/2017/10/13/reader-center/social-media-guidelines.html [https://perma.cc/8QKW-S39J].

confused, as the activities mentioned in points (1) and (3) are conducted by a search engine at its own initiative, while the activities mentioned in point (2) are required by the government.

Even though all of these activities are similar, in that each of them represents a deviation from the mission of the search engine, the compilation of search rankings that are most relevant to users is influenced by external considerations. This is a kind of editorial activity, which, coupled with the special role search engines play in the online public sphere, makes search engines highly influential entities that cannot be considered passive at all.

The advent of social media platforms has brought about fundamental changes in the structure of the public sphere, the communication of opinions, the range of means of accessing information and the rules pertaining to the freedom of speech. It is a significant fact that all of the most influential platforms operate out of the U.S., and their owners, executives and developers follow an approach toward the freedom of speech that is deeply rooted in the principles and doctrines of the First Amendment.

It is also noteworthy that the major platforms have a global presence, meaning that they have significant numbers of users in many different countries and that the rules of multiple jurisdictions can be applied to the content they make available. As a result, the functioning of these platforms is influenced by a number of different approaches toward the freedom of speech. These circumstances have various and sometimes contradictory consequences. On the one hand, the platforms sometimes try to make the First Amendment the law of the entire world. On the other hand, the platforms limit free speech much more strictly upon government request than they normally do in the U.S., merely to maintain a comfortable "safe space" for users and to ensure a peaceful business environment. U.S.-based global companies, which are used by countless U.S. citizens for daily communication and exchange, are also subject to European free speech rules and regulations that follow a different tradition.[100]

---

[100] Ammori, *supra* note 70, at 2263.