European Union

Author: Joan Barata, Justitia

Joan Barata works on freedom of expression, media regulation, and intermediary liability issues. He is a Senior Fellow at Justitia's Future Free Speech project. He is also a Fellow of the Program on Platform Regulation at the Stanford Cyber Policy Center. He has published a large number of articles and books on these subjects, both in academic and popular press. His work has taken him to most regions of the world, and he is regularly involved in projects with international organizations such as UNESCO, the Council of Europe, the Organization of American States or the Organization for Security and Cooperation in Europe, where he was the principal advisor to the Representative on Media Freedom. Joan Barata also has experience as a regulator, as he held the position of Secretary General of the Audiovisual Council of Catalonia in Spain and was member of the Permanent Secretariat of the Mediterranean Network of Regulatory Authorities.

Country Summary

Several pieces of legislation have been enacted in the European Union (EU) in recent years, aimed at regulating Big Tech companies especially in the areas of copyright, video-sharing platforms, and terrorist content online, contain speech restrictive provisions. The Audio-visual Media Services Directive puts obligations on video sharing platforms to take down illegal hate speech, as well as content that violates their own Terms of Service, thus delegating legal adjudication powers to platforms and creating a regime of liability that might lead to over moderation. One regulation issued during Covid on addressing the dissemination of terrorist content online requires hosting service providers to implement measures which could lead to a general obligation to monitor, to engage in active fact-finding, or to use automated tools, depriving Internet users and hosting service providers of the legal and procedural safeguards applicable to content removal. In the context of the war in Ukraine, a 2022 regulation prohibits

broadcasting, transmitting, or distributing, by any means, of any content by the State-owned and controlled Russian media outlets. The Digital Services Act of 2022 contains problematic provisions including a broad definition of "illegal content," notice-and-action mechanisms without sufficient safeguards for free speech rights of third parties, general obligations for platforms to act upon suspicion of criminal activities, obligation to detect broadly formulated "systemic risks" as well as to adopt mitigation measures which do not only cover illegal but also harmful content, and a so-called "crisis mechanism" that will put significant powers in the hands of the European Commission to control online speech. In a judicial development in 2019, the Court of Justice of the European Union endorsed the creation of a possible general monitoring obligation and the use of automated filters in certain cases, as well as the possible extraterritorial application of European limits to freedom of expression.

Introduction

The EU has a long tradition in its commitment to respect freedom of expression. Not only does the EU Charter of Fundamental Rights protect freedom of expression, but all EU members have also acceded to the European Convention on Human Rights (ECHR) and are bound by the European Court of Human Rights' (ECtHR) jurisprudence, including, of course, decisions on freedom of expression. The most important development is the Digital Services Act (DSA), aiming at establishing a series of horizontal obligations applicable to different types of Internet intermediaries. And there are new proposals at a very advanced stage, such as the European Media Freedom Act (EMFA) or a proposal to regulate political advertising.

I. Legislation

In 2018, the 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[246] (General Data Protection Regulation) came into force. Article 17 enshrines the "right to erasure" which gives the data subject the right to obtain from the data controller the erasure of personal data concerning him or her without undue delay when the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed, among other cases. The controller, in such cases shall take reasonable steps, including technical measures, to inform other controllers that are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data. Exceptions would apply when processing is necessary for exercising the right of freedom of expression and information, for compliance with a legal obligation, for reasons of public interest in the area of public health, for archiving purposes in the public interest,

[246] https://eur-lex.europa.eu/eli/reg/2016/679/oj

scientific or historical research purposes or statistical purposes, and for the establishment, exercise or defense of legal claims.

The "right to erasure" derives from the original formulation of the Court of Justice of the European Union (CJEU) of the so-called "right to be forgotten," in particular in a judgement of May 13th 2014.[247] Right after the publication of the ruling the OSCE Representative on Freedom of the Media, issued a Communique[248] saying that this decision "might negatively affect access to information and create content and liability regimes that differ among different areas of the world, thus fragmenting the Internet and damaging its universality." It also noted that "information and personal data related to public figures and matters of public interest should always be accessible by the media and no restrictions or liability should be imposed on websites or intermediaries such as search engines. If excessive burdens and restrictions are imposed on intermediaries and content providers, the risk of soft or self-censorship immediately appears." These concerns were seconded by other national and international bodies.

The Audiovisual Media Services Directive[249] aims at creating a more level playing field between traditional television and newer on-demand and video-sharing services. The Directive encompasses a series of duties of so-called video sharing platforms (VSPs) concerning the prevention and moderation of content that constitutes hate speech and child pornography, affects children's physical and mental development, violates obligations in the area of commercial communications, or can be considered as terrorist. National authorities (mainly independent media regulatory bodies) are given the responsibility of verifying that VSPs have adopted "appropriate measures" to properly deal with undesirable content. This includes the guarantee that platforms properly revise and enforce their Terms of Service (ToS); have appropriate flagging, reporting, and declaring functionalities; implement age verification or rating and control systems; establish and operate transparent, easy-to-use, and effective procedures to resolve users' complaints; and provide media literacy tools. Platforms will not only have the duty of taking down illegal hate speech, but they will also hold the power to eliminate legitimate (in the sense of fully legal) content that violates their own ToS. Once again, this instrument delegates important legal adjudication powers to platforms as well as creates a regime of responsibility that might lead to over removal.

Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC[250] lays down additional provisions harmonizing EU copyright law, particularly with regards to digital and cross-border uses of protected subject matter. The Directive establishes

[247] *Google Spain SL and Google Inc. vs. Agencia Espanola de Proteccion de Datos and Mario Costeja Gonzalez* C131/12.
[248] https://www.osce.org/fom/118632
[249] https://eur-lex.europa.eu/eli/dir/2018/1808/oj
[250] https://eur-lex.europa.eu/eli/dir/2019/790/oj

that internet service providers will not be able to rely on the hosting safe harbor provided by the Digital Services Act and incur liability for direct copyright infringement, unless it fulfills a number of conditions including making, in accordance with high industry standards of professional diligence, the "best efforts to ensure the unavailability of specific works and other subject matter for which the right holders have provided the service providers with the relevant and necessary information." This has been criticized in terms of impact on freedom of expression in the sense that it forces platforms to use automated filters which might not be able to properly detect protected content. However, this claim was dismissed by the CJEU in the decision of 26 April 2022.[251]

Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online[252] aims to ensure the smooth functioning of the digital single market by addressing the misuse of hosting services for terrorist purposes. The Regulation establishes a definition of "terrorist content" and includes an exception regarding material disseminated for educational, journalistic, artistic or research purposes or for awareness-raising purposes against terrorist activity. The Regulation obliges hosting service providers to ensure that the terrorist content identified in a removal order is removed or access to it is disabled in all Member States within one hour of receipt of the removal order. The removal order should contain a statement of reasons explaining the material to be removed, or access to which is to be disabled as terrorist content and provide sufficient information for the location of that content. Hosting service providers that are "exposed to terrorist content" should, where they have terms and conditions, include therein provisions to address the misuse of their services for the public dissemination of terrorist content, put in place specific measures taking into account the risks and level of exposure to terrorist content as well as the effects on the rights of third parties and the public interest to information, determine what appropriate, effective and proportionate specific measure should be put in place to identify and remove terrorist content. Where the competent authority considers that the specific measures are insufficient to address the risks, it should be able to require the adoption of additional appropriate, effective, and proportionate specific measures. The requirement to implement such additional specific measures should not lead to a general obligation to monitor, to engage in active fact-finding, or to use automated tools. However, the specific nature of the obligations and responsibilities included in the Regulation may de facto determine the (proactive) use of this latter type. With this legislation, Europe seems to move towards a progressive delegation of true law enforcement powers to private companies, depriving Internet users (and hosting service providers themselves) of the legal and procedural safeguards applicable to this kind of decision until now. Moreover, intermediary platforms may increasingly be put in a position where they feel compelled to take overbroad decisions, as the only way to avoid the high penalties and somewhat vaguely defined responsibilities.

[251] Judgment in Case C-401/19, *Poland v Parliament and Council*.
[252] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32021R0784

The Council Regulation (EU) 2022/350 of 1 March 2022[253] concerning "restrictive measures in view of Russia's actions destabilizing the situation in Ukraine" prohibits broadcasting or facilitating any content by the State-owned and controlled Russian media outlets, "including through transmission or distribution by any means such as cable, satellite, IP-TV, internet service providers, internet video-sharing platforms or applications." This is a very problematic ad-hoc legislation for a variety of reasons ranging from the competence of national independent audiovisual regulators in this field, the use of a very broad and general assessment of the information provided by the mentioned outlets rather than specific and properly analyzed pieces of content as well as the lack of proper consultation and participation in the adoption of the regulation.

The DSA[254] or Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC represents and overhaul of EU law governing intermediaries' handling of user content. It builds on the pre-existing eCommerce Directive from 2000 and preserves key ideas and legal structures from that law. The DSA applies to numerous Internet intermediary services. It provides both immunities and obligations. Many of its specific rules apply only to services in specific categories (access, caching, hosting, and marketplace providers, for example). The DSA asserts significant jurisdiction over companies based outside the EU. It reaches services "directed" to EU Member States. It allows enforcers to assess extremely steep fines, in principle reaching up to 6% of annual revenue. It also sets up major new regulatory powers within the European Commission. The DSA contains problematic provisions regarding freedom of expression, including a broad definition of "illegal content" (Article 3.h), notice-and-action mechanisms without sufficient safeguards for free speech rights of third parties (Article 16), general obligations for platforms to act upon suspicion of criminal activities (Article 18), obligation to detect broadly formulated "systemic risks" as well as to adopt mitigation measures (which do not only cover illegal but also harmful content) (Articles 34 and 35), and a so-called "crisis mechanism" that would put in the hand of the European Commission significant powers to control online speech (Article 36).

At the time of preparation of the current analysis, two relevant legislative proposals are under discussion. Firstly, the European Media Freedom Act (EMFA) or Proposal for a Regulation of the European Parliament and of the Council establishing a common framework for media services in the internal market.[255] This aims at tackling at the EU level fundamental issues connected to the exercise of the right to freedom of expression by media actors and media organizations. The EMFA proposal includes safeguards against political interference in editorial decisions and against surveillance. It also tackles the issues of the independence and stable funding of public service media, as well as the transparency of media ownership and of the

[253] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2022.065.01.0001.01.ENG
[254] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R2065
[255] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0457

allocation of state advertising. A key tool introduced by the EMFA is the increased regulatory cooperation and convergence through cross-border coordination tools and EU-level opinions and guidelines. The EMFA has problematic aspects including a very narrow definition of media service providers as well as obligations for very large online platforms to provide a special treatment to media service providers when it comes to content moderation. The latter raises issues of discrimination due to privileged treatment of content based only on the user that posted it and regardless of the public interest of the publication.

Secondly, the Proposal for a Regulation of the European Parliament and of the Council on the transparency and targeting of political advertising[256] aims at framing existing member states' legislation by establishing harmonized rules on the provision of political advertising services, and on transparency and due diligence for sponsors and providers of political advertising services, as well as on the use of targeting and ad delivery techniques in connection with political advertising. The very broad proposal's definition of political advertising is problematic, since it clearly risks restricting a particularly protected area of freedom of expression which is the dissemination of political discourses or "political speech." The proposal grants online platforms the power and responsibility to determine whether a certain publication fits the complex and ambiguous definition of political advertising established in the Regulation. Errors or disagreements with relevant authorities in this area may trigger the imposition of significant financial sanctions. Online platforms are also granted the authority, and even the obligation, to eliminate content where they conclude that a certain promoted message constitutes political advertising, and the sponsor or provider of the advertising service has refused to cooperate, by not providing relevant information. Online platforms also face the responsibility to properly and diligently (in some cases, within 48 hours) assess third-party reports, which in some cases might be filed by malicious actors.

II. Non-legislative developments

The EU Code of Conduct on Countering Illegal Hate Speech Online[257] was originally agreed on May 2016 between the European Commission and Facebook, Microsoft, Twitter and YouTube. Other IT companies joined afterwards. The Code follows the definition of illegal hate speech established by the Framework Decision 2008/913/JHA of 28 November 2008. The Code aims at providing IT Companies with criteria and instruments to support the European Commission and EU Member States in the effort to respond to the challenge of ensuring that online platforms do not offer opportunities for illegal online hate speech to spread virally. The implementation of the Code of Conduct is evaluated through a regular monitoring exercise set up in collaboration with a network of organizations located in the different EU countries.

[256] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0731
[257]https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en

The 2022 Code of Practice on Disinformation[258] is the result of efforts from major online platforms, emerging and specialized platforms, players in the advertising industry, fact-checkers, research and civil society organizations to deliver a strengthened and improved version of the 2018 Code. Signatories committed to take action in several domains, such as demonetizing the dissemination of disinformation; ensuring the transparency of political advertising; empowering users; enhancing the cooperation with fact-checkers; and providing researchers with better access to data. It is important to note that the new Code will become part of a broader regulatory framework, in combination with the legislation on Transparency and Targeting of Political Advertising and the DSA. For signatories that are Very Large Online Platforms, the Code aims to become a mitigation measure and a Code of Conduct recognized under the co-regulatory framework of the DSA.

The existence of such codes, or co-regulatory instruments, has been questioned from a freedom of expression perspective, since they blur the limits between illegal and harmful speech and thus, they may also create added difficulties for users to dispute platforms' interpretations and defend their rights. In addition to this, monitoring mechanisms seem to be based on a quantitative approach versus a more granular and substantive assessment, which makes it particularly challenging to detect and address possible over removals.

III. Enforcement

Enforcement of provisions included in EU law is usually the responsibility of national authorities which, in many cases, may also have the responsibility to adopt legislation necessary to transpose EU rules into domestic regulation. This being said, the CJEU has adopted some relevant decisions regarding the interpretation and enforcement of some of the pieces of legislation mentioned above.

In *Republic of Poland v. Parliament and Council,* the Court validated Article 17 of the Copyright Directive considering that the obligation for platforms to use automated filters to monitor user's speech does not violate freedom of expression since it is accompanied by adequate safeguards. In *Google LLC v. National Commission on Informatics and Liberty (CNIL)*, the CJEU presumes a non-existing uniformity when it comes to the balance between freedom of information and privacy protection across different member States when it comes to the enforcement of the so-called right to be forgotten and uses very ambiguous criteria to refer to the possibility of applying de-referencing requests beyond the limits of the EU. In *Glawischnig-Piesczek v. Facebook Ireland Limited*, the CJEU established that EU law does not preclude a Member State from ordering a host provider to remove information which it stores, the content of which is identical, equivalent to the content of information, which was previously declared to be unlawful, or to block access to that information. It also endorses the creation of a possible general monitoring obligation and the use of automated filters in certain

[258] https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation

cases, as well as the possible extraterritorial application of European limits to freedom of expression.

Conclusion

All the mentioned rules and proposals contain several interesting and innovative provisions, particularly when it comes to providing more certainty and protection to European users of online platforms (and particularly Big Tech) in several areas, including expressing ideas and opinions. The safeguards in question include transparency of terms and conditions, disclosure of algorithms and recommender systems, data protection or accountability and redress mechanisms. However, platform regulation in the EU is particularly focused on tackling risks deriving from the use of social media as a tool to disseminate information by different types of actors, including malicious ones. Such risks tend to be defined in broad terms and encompass content that is not necessarily illegal but labelled as harmful *vis-a-vis* certain political and societal values. Therefore, on the one hand, EU legislation has brought a combination of delegation of private content regulatory measures to be decided by platforms themselves and, on the other oversight by agencies and regulatory bodies, the latter still waiting to be properly identified and mandated in some cases.