NAVIGATING THE GDPR-DSA NEXUS: REGULATING PERSONAL DATA IN SOCIAL MEDIA AND SEARCH ENGINES

Assoc.Prof. Denitza Toptchiyska, PhD
New Bulgarian University

Abstract

The Digital Services Act (DSA) brings forth significant new regulations concerning content moderation by intermediary service providers. Specifically, social media platforms and search engines are under scrutiny due to their critical role in disseminating information in modern society. Moreover, the new EU legislation must align with the General Data Protection Regulation (GDPR), which establishes guidelines to safeguard individuals' privacy rights. The article seeks to examine the overlaps between these two regulations and to underscore the main the main points of intersection in their synchronized application.

Keywords: personal data, social media platforms, search engines, DSA, GDPR

In February 2024, the Digital Services Act (DSA)[1] came into full effect bringing significant new legal requirements concerning content moderation by the providers of online intermediary services like social media platforms and search engines that are under specific scrutiny due to their critical role in disseminating information in modern society. DSA together with the General Data Protection Regulation (GDPR)[2] form part of the new modern EU approach towards the regulation of the digital environment aimed to ensure a safe, predictable, and trustworthy online space in which the individual's privacy is protected. The article seeks to examine some of the overlaps between these two regulations and to underscore the main points of intersection in their

[1] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277, 27.10.2022, p. 1-102

[2] 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), OJ L 119, 4.5.2016, p. 1-88

synchronized enforcement referring to the case of social media platforms and search engines.

In 2024 social media platforms shape the characteristics and scope of the contemporary media environment, with active users exceeding 60 percent of the world's population.[3] Social media, as a technology-neutral expression, encompasses a variety of fast-evolving digital technologies and services that enable their users to share ideas and information, text and visuals online. Social media platforms typically feature user-generated content that encourages interactive communication and engagement through likes, shares, comments, and discussions. They offer avenues for community cohesion, individual freedom of expression, and information accessibility, yet they also present challenges such as the spread of misinformation, the proliferation of hate speech, direct or hidden discrimination, and privacy vulnerabilities. In recent years, there have been numerous examples of the influence of social media on the electoral process in European countries, challenging the democratic principles upon which they are built.

Search engines, which are computer software or internet sites used to find information based on user-provided keywords, are another technology with a similarly strong social influence. As gatekeepers to vast amounts of online information, search engines provide users with curated lists of relevant websites, the ranking of which influences the effectiveness of information dissemination to users. Social media significantly impact search result rankings by enhancing visibility and generating links to websites and information shared by users. Both social media platforms and search engines play a central role in enabling freedom of expression and access to information in modern society. However, the risks associated with facilitating access to misinformation and illegal content necessitate the adoption of an effective legal framework tailored to the challenges of the online space.

1. The EU regulatory model for the digital environment

Considering the challenges of regulating the digital space as a technological architecture, the EU aims, as seen in both the GDPR and the DSA, to establish a comprehensive regulatory model to achieve effective governance. This model seeks to combine the expertise of public authorities, private companies, and civil society. From the perspective of regulatory instruments, it encompasses the possibilities of public and private regulation – hard and soft law, self-regulation, and co-regulation – to achieve effective protection of social values in the digital environment.

The EU regulatory model requires the mandatory establishment of a national authority for monitoring and controlling compliance with the respective regula-

[3] Global Social Media Statistics: available at https://datareportal.com/social-media-users (as reviewed on 20.06.2024)

tions. For the GDPR, these are the data protection supervisory authorities, and for the DSA, they are the Digital Services Coordinators. Additionally, the model envisages the cooperation of national authorities within pan-European structures - the European Data Protection Board (EDPB) and the European Board for Digital Services, both of which work closely with the European Commission.

The goal of effectively protecting the fundamental rights in the EU is reflected in the adopted principles regarding the substantive and territorial application of the GDPR and DSA. These principles are tied to the location of the recipients of the provided services or activities conducted within the territory of the EU, which can lead to the extraterritorial application of EU regulations. Thus, social media and search engines can be subject to obligations even if they are not registered or do not have an establishment in an EU member state.

2. Defining social media and search engines in the framework of GDPR

The EU data protection model is based on the concept of a „data controller," which is broadly defined and technologically neutral to ensure effective and thorough protection of data subjects. A data controller is any individual or organization that determines the purposes and means of personal data processing and assumes legal responsibility for the lawfulness of such processing.[4] The GDPR does not contain provisions specifically targeting social media and search engines. This means that in every case of personal data processing, an assessment must be made to determine whether they function as data controllers or data processors within the context of the general legal framework.

Regarding the determination of the role of search engines as data controllers, the CJEU decision from 2014 in the Google Spain case is of key importance.[5] According to the operative part of the decision, search engines are data controllers when the information they process to provide their service contains personal data. Their service includes finding information published or placed on the internet by third parties, automatically indexing it, temporarily storing it, and finally making it available to internet users in a specific order of preference. Furthermore, the Court specifies that the legal basis for personal data processing, in this case, is based on the legitimate business interests of the search engine, which requires a careful balance with the right to privacy and personal data protection of the data subjects.[6] The European Data Protec-

[4] Article 4 (8) and article 5, par. 2 Regulation (EU) 2016/679

[5] CJEU, Case C-131/12, Google Spain SL and Google Inc. v Agencia Espacola de Protecciyn de Datos (AEPD) and Mario Costeja González, judgment of 13 May 2014

[6] CJEU, Case C-131/12, Google Spain SL and Google Inc. v Agencia Espacola de Protecciyn de Datos (AEPD) and Mario Costeja González, judgment of 13 May 2014, paragraph 73, 74

tion Board refers to the CJEU decision when issuing guidelines for determining data controllers, as part of soft law mechanisms aimed at supporting the implementation of the abstract provisions of the GDPR.[7]

Furthermore, in the case law of the CJEU for preliminary rulings, which provide authoritative interpretations of EU law, guidelines for applying the concept of data controller in the context of social media can be found. In a decision from 2018, the CJEU highlights that when determining the purposes and means of data processing, the data controller may act „alone or jointly with others". In such cases, each party involved is qualified as a data controller and is obligated to comply with the relevant data protection provisions.[8] In the context of social media, the primary data controller for processing personal data is the platform itself, but users who create fan pages hosted by the platform also act as data controllers. According to the CJEU interpretation, the mere use of a social network such as Facebook does not automatically render a user jointly responsible as a data controller for the processing of personal data carried out by the platform. It requires a specific assessment to determine whether the social media user qualifies as a data controller, based on their involvement in determining the purposes and methods of data processing. The responsibility of various joint data controllers that may participate at different stages of processing and to varying degrees, should be assessed independently, considering all relevant circumstances of the case.[9]

Considering the growing popularity of social media and their public influence, the European Data Protection Board (EDPB) adopted two documents specifically aimed at social media providers and the application of GDPR in the conduct of their activities. First, the EDPS adopted Guidelines 08/2020 on the targeting of social media users, for the purposes of which it defines social media as online platforms that enable the development of networks of users, creating „accounts" or „profiles", to share information.[10] The document aims to address the application of GDPR principles concerning the collection and use of users' personal data for providing targeted messages as part of the service offered by social media platforms. The EDPS emphasizes that for the provision of this service, the social media platforms use not only information that the user has consciously shared but also information that is „observed or inferred," either by the social media provider or by third parties. It is noted that the processing is possible to include special categories of data within the meaning of Article 9 GDPR, as well as data of a highly personal nature, which requires conducting a Data Protection Impact Assessment (DPIA) and determining whether the processing is „likely to result in a high

---

[7] European Data Protection Board (EDPS), Guidelines 07/2020 on the concepts of controller and processor in the GDPR (adopted on 07 July 2021)

[8] CJEU, Case C-210/16, Wirtschaftsakademie Schleswig-Holstein, judgment of 5 June 2018, paragraph 30

[9] CJEU, Case C-210/16, Wirtschaftsakademie Schleswig-Holstein, judgment of 5 June 2018, paragraph 43

[10] European Data Protection Board (EDPS), Guidelines 08/2020 on Targeting of social media users (adopted on 13 April 2021), p. 4

risk".[11] Paying particular attention to the information asymmetry faced by social media users, the EDPS analyses the risks to their fundamental rights, especially in cases where targeting is based not only on data collected by the social media platform itself but also by third parties, such as website visits and browsing history.[12]

Further, in 2022 the EDPS adopted guidelines for recognizing and avoiding deceptive design patterns in social media platform interfaces, looking for a solution to the problem through interpretation of the EU data protection legislation and more specifically GDPR.[13] The document aims to assist social media providers as controllers of social media, that have the responsibility for the design and operation of social media platforms. „Deceptive design patterns" are defined as the various cases when the interface design and user experience design of social media platforms violate the legally permissible limits of the GDPR included in the data protection principles.[14] These patterns are intended to influence users, often on a cognitive basis, into making unintended, unwilling, and/or potentially harmful decisions, particularly regarding their personal data. These decisions typically favour the interests of the social media platforms over the users' best interests. In its guidelines, the EDPS points out that the business model of social media often involves data processing by joint controllers of personal data. It is highlighted that each of them bears legal responsibility for the data processing, aligned with their role in determining the purposes and means of processing. It should be noted that DSA further complements GDPR by prohibiting online platform providers from designing interfaces that deceive or manipulate users, or otherwise distort their ability to make informed decisions.[15]

3. Social media platforms and search engines in the framework of the DSA

The DSA aims to provide more effective protection of consumers' fundamental rights and to address the spread of illegal content and products, hate speech, and disinformation by establishing clear responsibilities for intermediary service providers, including social media and search engines. The goal is to achieve greater transparency with better accountability and oversight, as well as to promote innovation, growth, and competitiveness in

[11] European Data Protection Board (EDPS), Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk" for the purposes of Regulation 2016/679 (Adopted on 4 October 2017)

[12] European Data Protection Board (EDPS), Guidelines 08/2020 on Targeting of social media users (adopted on 13 April 2021), p. 6-8

[13] European Data Protection Board (EDPS), Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them (adopted on 14 February 2023)

[14] Article 5 GDPR

[15] Article 25 Regulation (EU) 2022/2065

the EU's internal market. To achieve its objectives, the DSA establishes harmonized rules regarding the provision of intermediary services in the internal market, a framework for the conditional exemption from liability for providers of intermediary services, and rules concerning specific due diligence obligations.

Both social media and search engines fall within the scope of the concept of „information society services" introduced in Directive 2000/31/EC (Directive on electronic commerce)[16] further amended in Directive (EU) 2015/1535.[17] According to the definition, the concept covers any service normally provided for remuneration, at a distance, by electronic means, and at the individual request of a recipient. For the purposes of the definition, it is clarified that the payment for the services may not come directly from their recipients, as is the case with the services that provide means for searching, accessing, and retrieving data.[18] This is usually the case with social media as well, where users are allowed to create their own „profile" or „account" for free to participate in the community.

Without prejudice to the provisions of other relevant EU legislation, the DSA imposes additional obligations and responsibilities on providers of those information society services that fall within the scope of the category „intermediary service,", that are subdivided into three categories: services for „mere conduit," „caching," and „hosting."[19] These are generally the services, consisting of the transmission or storage in a communication network of information provided by the recipient of the user. Further the DSA defines for the purposes of the regulation what online platforms and search engines constitute as types of intermediary services and introduces specific legal provisions concerning them to protect against the spread of illegal or other harmful information and activities by their users.

Social media as online platforms are defined as a subset of hosting services „that not only store information provided by the recipients of the service at their request, but that also disseminate that information to the public at the request of the recipients of the service."[20] Special attention is directed towards the functionality that defines online platforms, enabling them to disseminate information provided by their users to the public or to a potentially unlimited number of individuals without further action by the user. This capability serves as a primary distinguishing feature from interpersonal communication services,

---

16 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') (OJ L 178, 17.7.2000, p. 1).

17 Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).

18 Preamble, par. 18 Directive 2000/31/EC

19 Article 3 (g) Regulation (EU) 2022/2065

20 Preamble, par. 13 and Article 3 (i) Regulation (EU) 2022/2065

which are designed to facilitate direct interactive communication between specific individuals[21] and are not subject to the specific regulations applicable to online platforms. The DSA also defines the term „online search engine" as an intermediary service for searching information on the internet, where users enter a keyword query and receive results.[22] Specific obligations for their providers are also included.

The DSA provides for a differentiation of obligations for providers of intermediary services according to their role, size, and impact in the online ecosystem. Thus, regarding micro and small enterprises, obligations are foreseen that are proportional to their capabilities and size, while ensuring that they remain accountable. In contrast, special obligations and responsibilities are further foreseen for very large online platforms, including social media, and search engines, which are designated by the European Commission based on the number of their active users in the EU.

4. Balancing of rights under GDPR and content moderation of information including personal data under DSA

The GDPR aims to protect the right to privacy of individuals by adopting a horizontal approach to regulating personal data and assigning broad responsibilities to data controllers regarding the design and implementation of specific measures for ensuring personal data protection. Thus, regarding the application of the right to be forgotten, the EU regulation mandates data controllers to balance the rights of data subjects against the public interest in information accessibility or other legitimate interests. The data controllers are entrusted with the responsibility of determining whether to retain or delete information online. Despite the guidelines provided by the GDPR regarding the balancing of interests, it does not regulate the procedure itself concerning decision-making nor does it impose requirements regarding the standards that must be met. Inquiries regarding the decision-making procedures and the burden of proof were raised before the CJEU and some guidelines were given.[23]

According to the DSA, the providers of intermediary services are not subject to a general obligation to monitor the information they transmit or store, nor are they required to actively seek facts or circumstances indicating illegal activity.[24] However, to ensure a safe, predictable, and trustworthy online environment, the online platforms are required to provide a content moderation process aimed at detecting, identifying, and addressing illegal content and information incompatible with their terms and conditions. The concept of

[21] Article 2 (5) Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast)Text with EEA relevance.

[22] Article 3 (j) Regulation (EU) 2022/2065

[23] Judgment of the Court (Grand Chamber) of 8 December 2022; Case C-460/20

[24] Article 8 Regulation (EU) 2022/2065

'illegal content' encompasses a broad definition, covering all information, irrespective of its form, related to illegal content, products, services, and activities.[25] It also covers information that violates the right to privacy in general or, more specifically, the right to personal data protection. Given their significant social influence, additional obligations related to content moderation are imposed on social media and search engines.

Unlike the GDPR, the DSA establishes specific requirements regarding the procedures for handling user notifications about illegal content, which must be addressed promptly, diligently, impartially, and objectively. Hosting services providers, including online platforms, are obligated to inform both the user who submitted the moderation request and the user who uploaded the moderated content about their decision, including information about legal remedies. Moreover, online platforms must set up an Internal Complaints Handling System, which allows users to challenge decisions made by the online platform. Specific requirements are provided regarding the implementation of complaint procedures: the decision must be made by qualified personnel, not through automated means, and must be justified. Further, the online platforms are obliged to participate in procedures initiated before the certified out-of-court dispute resolution by certified bodies.

Under the DSA, online platforms are required to submit their decisions and statements of reasons for content moderation to the Data Transparency Database (https://transparency.dsa.ec.europa.eu/) established by the European Commission in September 2023. By July 2024, more than 12 billion statements of reasons have been submitted, indicating instances where online platform providers have identified illegal content or violations of their platform terms of use. In over 30 million cases, it is indicated that the identified violation falls under the category of data protection and privacy violations that led to reduced visibility of the content or its removal.

5. Targeted advertising based on special categories of personal data

The processing of special categories of personal data under Article 9 of the GDPR, such as data revealing racial or ethnic origin, political opinions, or sexual orientation, is governed by specific rules due to the significant risks to the fundamental freedoms and fundamental rights of data subjects. In its case law, the CJEU upholds the fundamental prohibition on processing special categories of data established by the GDPR, stating that such processing is permissible only in the exceptional cases outlined in the Regulation, which must be interpreted strictly.[26] The CJEU also confirms that when an online

[25] Article 3 (h) Regulation (EU) 2022/2065

[26] CJEU, Judgment of 4 July 2023, Meta Platforms Inc and Others v Bundeskartellamt (Case C-252/21), par. 74-76

social network operator collects data from websites or applications related to special categories of personal data visited by the user and links this information to the user's social network account, it constitutes processing special categories of personal data. It also acknowledges that the digital traces left by users during visits to websites or apps related to Article 9 of the GDPR categories do not constitute making their data public and therefore, they cannot be freely and unconditionally processed by the service providers.[27]

The DSA builds upon GDPR to reinforce the high level of protection concerning the processing of special categories of personal data. It prohibits online platform providers from targeting advertisements using user profiling based on the special categories of data outlined in Article 9 (1) of the GDPR. Additionally, the DSA prohibits the use of profiling for targeted advertising when providers can reasonably ascertain that the user is a minor, regardless of whether the profiling is based on special categories of personal data or not.[28]

Conclusions

Both GDPR and DSA constitute a European legal framework designed specifically to regulate the digital environment, combining hard and soft law instruments. Their effectiveness relies on activating and integrating the diverse tools they encompass, alongside the collaborative engagement and participation of public institutions and private organizations targeted by these regulations. Following their role in the technological architecture of the digital space, private companies are entrusted with decision-making responsibilities concerning the protection of fundamental rights and freedoms, including limiting the dissemination of illegal content and safeguarding personal privacy. This approach necessitates the adaptation of traditional legal systems based on hard law, where public institutions play a pivotal role, to ensure the effectiveness of the new legal framework.

Bibliography:

- CJEU, Case C-210/16, Wirtschaftsakademie Schleswig-Holstein, judgment of 5 June 2018 European Data Protection Board (EDPS), Guidelines 08/2020 on Targeting of social media users (adopted on 13 April 2021)
- CJEU, Judgment of 13 May 2014, Google Spain SL and Google Inc. v Agencia Espacola de Protecciyn de Datos (AEPD) and Mario Costeja Gonzólez (Case C-131/12)
- CJEU, Judgment of 4 July 2023, Meta Platforms Inc and Others v Bundeskartellamt (Case C-252/21)

[27] CJEU, Judgment of 4 July 2023, Meta Platforms Inc and Others v Bundeskartellamt (Case C-252/21)

[28] Article 26 and 28 Regulation (EU) 2022/2065

- CJEU, Judgment of 8 December 2022, TU and RE v Google LLC (Case C-460/20)
- European Data Protection Board (EDPS), Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them (adopted on 14 February 2023)
- European Data Protection Board (EDPS), Guidelines 07/2020 on the concepts of controller and processor in the GDPR (adopted on 07 July 2021)
- European Data Protection Board (EDPS), Guidelines 08/2020 on Targeting of social media users (adopted on 13 April 2021)
- European Data Protection Board (EDPS), Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk" for the purposes of Regulation 2016/679 (Adopted on 4 October 2017)
- 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), OJ L 119, 4.5.2016, p. 1-88
- Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277, 27.10.2022, p. 1-102