FREEDOM OF EXPRESSION ON THE INTERNET VS. DIGITAL SERVICES ACT: CHOSEN ASPECTS*

Diana Treščáková, PhD, Associate Professor
Pavol Jozef Šafárik University in Košice, Slovakia, Faculty of Law
Kov.čska 26, 040 75 Košice, Slovakia
diana.trescakova@upjs.sk

ABSTRACT

With the development of information technologies and the digitalization of every area of our lives, we are increasingly encountering violations of individuals' digital rights, which can be classified among fundamental human rights and freedoms. Digital rights are not sufficiently protected on the internet. The use of information technologies also reveals vulnerable areas of our digital space. These vulnerable areas mainly include the field of e-commerce, online shopping, and active or passive participation on social networks, where massive data collection from individuals operating in the online space occurs. This raises questions regarding the adherence to ethical principles in the online environment. However, the issue is not limited to the protection of individuals' personal data and their privacy, but also extends to the overall activities of various entities operating online. It is evident that internet platforms are gaining in power and need to be legally regulated.

At the level of the European Union, a regulation—the Digital Services Act (hereinafter referred to as DSA)—has therefore been adopted with the aim of both regulating online platforms and protecting users themselves.

The aim of this article is to analyze digital rights and their observance on the internet. It is necessary to ask whether these digital rights are adequately protected by current legislation. In this context, the author will focus on the controversial issue of the relationship between freedom of expression and the principles established in the DSA. For this purpose, specific provisions of the DSA will be analyzed, in particular Articles 34 and 35, which introduce the obligation to identify and mitigate systemic risks by very large online platforms (VLOPs) and very large online search engines (VLOSEs).

To achieve the stated goals, standard scientific research methods will be used—primarily those typical of the social sciences, even though the topic overlaps with the field of technology. These methods will be specifically applied in processing the collected data, evaluating them, and formulating conclusions. To examine the raised questions and achieve the defined goals, we

* This article was prepared within the investigation of Grant Project VV-MVP-24-0038 Analysis of liability for internet torts with machine learning methods and APVV 21 – 0336 Analysis of judicial decisions using artificial intelligence.

will primarily use formal-logical methods, comparative methods, and methods of historical, economic, and legal analysis. In addition, methods of induction, deduction, synthesis, interpretation of legal norms, and abstraction will also be employed.

Keywords: *Digital Service Act, digital rights, freedom of expression, illegal content*

1. INTRODUCTION

On October 19, 2022, 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) was adopted, which entered into force on February 17, 2024. Alongside this regulation, its "twin" was also adopted: Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).[1]

The Digital Markets Act (DMA) was adopted with the aim of regulating competition in the digital environment, notably by establishing rules that prevent the abuse of dominant positions by large technolog,ical giants holding the status of gatekeepers (such as Google, Meta, Amazon, etc.). The Digital Services Act (DSA) - the focus of this contributio was adopted as a twin regulation to the DMA. Its primary objective is to regulate content and the accountability of online platforms, to ensure transparency of algorithms and advertising, to strengthen the fight against disinformation, and to enhance user protection.

According to the explanatory memorandum to the DSA Regulation, this legal act constitutes a new pan-European framework for regulating online content within the provision of intermediary services. Based on the principle that "what is illegal offline is also illegal online," it introduces harmonized rules for providers of intermediary services, including social networks, online marketplaces, internet search engines, web hosting and cloud services, online travel and accommodation platforms, app stores, and other types of online platforms. The regulation will also apply to providers from third countries, provided they offer services to users within the EU.

There are several reasons why it became necessary to adopt legislative measures in the form of the Digital Services Act (DSA). First and foremost, recent years have seen a significant increase in risks related to the enforcement of individual

[1] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) available at: [https://eur-lex.europa.eu/eli/reg/2022/1925/oj/eng]. Accessed on 5th of April 2025.

users' rights in connection with the use of digital services. These risks ranged from the dissemination of illegal content online to violations of personal data protection and privacy. It became imperative to create a safe and trustworthy online environment for various categories of users. For this reason, it was necessary to establish clear rules for the use of digital services, ensuring that users' digital rights - particularly the right to privacy, freedom of expression, and protection against discrimination - are respected.

Furthermore, it was essential to curb the spread of illegal content on the internet, as well as disinformation and other forms of content posing societal risks.[2] The DSA introduces mechanisms aimed at minimizing these risks.

Based on the above, it can be concluded that the primary objective of the DSA is to contribute to the development of a safer and more transparent online environment, to improve the conditions for the provision of cross-border intermediary services, to strengthen the position of consumers, and to enhance the protection of fundamental rights of users in the digital space.

Another key reason for the adoption of the Digital Services Act (DSA) was the need to eliminate the fragmentation of rules governing digital services across individual Member States, which is closely linked to the creation of a Digital Single Market.

Generally speaking, the Digital Services Act (DSA) constitutes a comprehensive legal framework of the European Union aimed at establishing a safer, more transparent, and fairer digital environment. As previously noted, the DSA was adopted with the objective of harmonising divergent legal regulations across Member States, particularly in response to the cross-border nature of online platforms.

An analysis of the DSA's implementation at the national level reveals considerable variation in the approaches adopted by individual Member States following its entry into force. This is particularly evident in relation to the interpretation of issues concerning potential threats to the fundamental right to freedom of expression, especially with regard to the assessment and removal of online content. Even within individual Member States, divergent views may be observed concerning the application of the DSA and the protection of freedom of expression. For example, in Germany, emphasis is placed on the view that the primary aim of the DSA is not censorship, but the safeguarding of freedom of expression. The assessment of online content must not be arbitrary, and legitimate expressions must be

[2] Guide of The Council for Media Services available at: [https://rpms.sk/sites/default/files/2025-02/Prirucka_pre_sprostredkovatelske_sluzby.pdf)]. Accessed 5 April 2025.

duly respected.[3] In France, however, critics have openly expressed the view that the implementation of the DSA is incompatible with the right to freedom of expression.[4] Even in light of these differing perspectives, it must be acknowledged that each Member State will be tasked with implementing the DSA in accordance with its own values and traditions, which inevitably shape this process, while also striving to strike a proportionate balance between the enforcement of the DSA's provisions and the preservation of freedom of expression.

The comprehensive legal framework in the area of digital content established by the DSA is further affirmed by its interaction with other legislative instruments, most notably the Regulation on the transparency of political advertising[5] as well as the Audiovisual Media Services Directive[6] as well as with the General Data Protection Regulation (GDPR), which constitutes a major legal act in the field. The interaction between the DSA and the GDPR is particularly significan because the Regulation also addresses the issue of user profiling, which involves the use of personal data to assess certain personal aspects related to a natural person - most notably the analysis or prediction of aspects such as work performance, economic situation, health status, personal preferences, interests, and other characteristics. This part of the DSA responds to concerns about non-transparent algorithms and recommendation systems, which may reinforce or exacerbate existing societal issues such as discrimination, polarization, or addictive behaviors.[7]

This constitutes one of the reasons why it is imperative to regulate the online environment through appropriate legislation, which will oblige online platforms to implement transparent procedures that are accessible to all users of the platform, thereby enabling them to make an informed and voluntary decision regarding their use of the platform.

---

3 Digital Service Act: Trusted Flagger and freedom of expression available at: [https://www.heise.de/en/background/Digital-Services-Act-Trusted-Flagger-and-freedom-of-expression-9986899.html?utm_source=chatgpt.com], Accessed 18 June 2025.

4 EU digital law restricts freedom of expression, says French whistleblowers group available at: [https://brusselssignal.eu/2024/08/eu-digital-law-restricts-freedom-of-expression-says-french-whistleblowers-group/], Accessed 18 June 2025.

5 Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising available at: [https://eur-lex.europa.eu/eli/reg/2024/900/oj], Accessed 19 June 2025.

6 Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 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) available at: [https://eur-lex.europa.eu/eli/dir/2010/13/oj], Accessed 19 June 2025.

7 Guide of the Council for Media Services available at: [https://rpms.sk/sites/default/files/2025-02/Prirucka_pre_sprostredkovatelske_sluzby.pdf)], Accessed 5 April 2025.

2. DIGITAL SERVICE ACT AND THE PROTECTION OF DIGITAL RIGHTS

The Digital Services Act (DSA) was adopted, among other objectives, primarily to protect the rights of every individual who engages with the online environment and online platforms. These rights can generally be referred to as digital rights, which pertain to individuals who are both active and passive participants in the digital sphere. The DSA is based on the principle that "what is illegal offline should also be illegal online." This could also be paraphrased as follows: if an individual is granted fundamental human rights and freedoms in the offline world, these rights must equally be upheld in the digital world.

Accordingly, it is essential to address the human rights dimension of individual activity in the online environment, as well as how these rights are enshrined in the relevant legislation. In this context, the human rights perspective focuses on safeguarding individual rights in the digital sphere. As digital technologies continue to evolve, we are increasingly confronted with critical questions regarding how to ensure the protection of fundamental human rights - such as the right to privacy, access to information, and protection of personal data from misuse.

At the same time, it is vital to guarantee equal access to digital services and to prevent discrimination or the misuse of technologies in ways that violate individual rights - such as surveillance, the dissemination of disinformation, or the manipulation of information through opaque algorithmic systems.

In general terms, digital rights can be understood as an extension of fundamental human rights into the online space, and they are essential for protecting individuals from the potential abuses of technological platforms and corporations.

Digital rights are enshrined in several legal acts. The Universal Declaration of Human Rights adopted by the United Nations in 1948 includes fundamental human rights that can also be applied to the online environment. Article 12 of the Declaration defines the protection of privacy and data, stating: "*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks*." Additionally, Article 19 establishes the right to freedom of opinion and expression, which also encompasses the right to seek, receive, and impart information and ideas by any means and regardless of frontiers - rights that can likewise be applied in the digital world.

Similarly, the European Convention on Human Rights defines the protection of privacy in Article 8 and the right to freedom of expression in Article 10. In 2018,

the General Data Protection Regulation (GDPR) came into effect, introducing stringent rules regarding the protection of personal data of EU citizens. Among the fundamental rights it established, which also apply in the digital sphere, is the explicit consent of individuals for the processing of their personal data, easier access to personal data for the data subjects, the right to object to the use of personal data for profiling purposes, the right to erasure (right to be forgotten), and the right to data portability (the ability to transfer data from one service provider to another).

Furthermore, the regulation requires data controllers (those responsible for data processing) to provide individuals with transparent and easily accessible information regarding the processing of their data.

Digital rights can be divided into three basic categories:

1. Violations of right resulting from (the use of) new technologies
2. Conflicting rights from (the use of) new technologies
3. New issues resulting from (the use of) new techlologies for which no rights exist yet[8]

As Custers says a typical examples in the first category are questions regarding the extent to which sophisticated data analytics interfere with someone's privacy, or the extent to which the use of risk profiling is potentially discriminatory against particular groups of people.[9]

Typical examples in the second category are questions regarding the extent to which someone may be wiretapped (privacy interest) for the purpose of criminal investigation (security interest) or the extent to which someone may insult a religion (freedom of religion versus freedom of speech). On all such questions large amounts of literature and case law are available.

The third category, however, is much less discussed in literature, legal practice and academic debates. A typical example in the third category is the 'right to be forgotten', sometimes referred to as the 'right to oblivion'.[10]

The Digital Services Act (DSA) also addresses digital rights, which are reflected in this regulation with the purpose of protecting individuals' rights when using

---

8 Custers, B., *New digital rights: Imagining additional fundamental rights for the digital era,* Computer Law & Security Review, Volume 44, 2022, p.1 [https://doi.org/10.1016/j.clsr.2021.105636], Accessed 11 April 2025.

9 Barocas, S.; Selbst, A.D., *Big Data's Disparate Impact*, 104 California Law Review 671, 2016.

10 Xanthoulis, N., *Conceptualizing a Right to Oblivion in the Digital World: A Human Rights-Based Approach*, 2012, avalilable at: [https://ssrn.com/ abstract=2064503], Accessed 11 April 2025.

online platforms and services. This is in line with the DSA's goal to modernize and improve the rules for digital services in the EU to better respond to the challenges of the digital age. This legislative framework provides stronger tools for the protection of users' digital rights and ensures better regulation and oversight of the digital market in the EU. The aim is to make digital services safer, more transparent, and fairer for everyone.

If we were to approach the basic definition of digital rights, the following core digital rights can be identified:

a) Right to Privacy and Protection of Personal Data, which primarily includes the aspect of controlling one's personal data. This means that every user has the right to control their personal data. Digital platforms must also transparently inform users about how their data is processed. This right also encompasses protection against surveillance and the misuse of data, such as targeted behavioral advertising.

b) Right to Access Information, which can be defined as the right to free and non-discriminatory access to information. On one hand, it includes the fight against censorship, and on the other hand, it protects individuals from disinformation and manipulation through information.

c) Right to Digital Security, or cybersecurity, which involves protection against disruptions in the secure online space caused by security incidents, cyberbullying, and various forms of online fraud. This right also includes communication security, ensuring that it is not accessible to third parties who are not part of the communication, nor will it be controlled from a position of power, e.g., by the state. It should be noted that the responsibility for securing user accounts rests with the platform itself.

d) Right to Be Forgotten, according to which the user has the right to erase or request the deletion of their digital footprints, such as old posts, and the right to remove their personal data from various online databases.

e) Right to Digital Identity, which includes the right to control one's digital identity and protection from the misuse of personal data.

f) Right to Fair Treatment and Non-Discrimination, which requires the application of a ban on discrimination based on digital profiles, e.g., in hiring processes. This right also includes transparency in decision-making algorithms, such as when approving loans, credits, etc. This right can also be linked to profiling, where it is clearly defined that the individual should have the right to avoid decisions based solely on automated processing that evaluates personal aspects affecting them, which have legal

consequences, such as an automatic rejection of an online loan application or electronic recruitment processes without any human intervention. In such cases, appropriate safeguards for the protection of the individual's rights must be established, including the right to review decisions made in a non-automated manner by the relevant authority – recital 71 of the GDPR regulation.[11]

g) Right to Freedom of Expression, based on which users have the right to express their opinions online, provided they do not violate the law. This right also includes protection from arbitrary censorship by digital platforms, with content moderation being transparent and fair. However, it is important to note that the right to freedom of expression on the internet is not unlimited.

Subsequently, it is possible to define the main areas that the protective mechanisms of the Digital Services Act (DSA) are focused on, which reflect the existence of digital rights. The first area is consumer protection. To protect consumers, online platforms will take measures to safeguard them from illegal content, fraud, and manipulation.

Another area that has the potential to infringe upon digital rights is the dissemination of illegal content. According to the DSA (Articles 34 and 35), platforms are obligated to remove or prevent access to illegal content.

Another important area is the transparency of platforms, specifically in disclosing how algorithms work so that users can choose whether they want content to be tailored to them or not. The DSA also introduces mechanisms to give users more control over their personal data and to make it easier for them to request the deletion or correction of their personal data. Under the DSA, platforms are required to ensure that their algorithms do not discriminate against users based on their gender, race, nationality, religion, or other so-called special categories of personal data.

3. FREEDOM OF EXPRESSION ON THE INTERNET VS. DSA

As mentioned earlier, one of the primary digital rights is the right to freedom of expression. In our opinion this right requires particular attention, as it may come into conflict with the principles and mechanisms introduced by the DSA.

[11] 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) avalilable at: [https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=celex:32016R0679], Accessed 5 April 2025.

First of all, it is important to note that freedom of expression, whether in the virtual world or offline, is a fundamental right. The right to freedom of expression is enshrined in many documents, both at the national and international levels. The Charter of Fundamental Rights of the EU regulates it in Article 11, paragraph 1, which states: "*Everyone has the right to freedom of expression. This right includes freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers*."[12]

It is also enshrined in the European Convention on Human Rights in Article 10, paragraph 1, which states: "*Everyone has the right to freedom of expression. This right includes freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.*"[13]

In the Slovak Republic, freedom of expression is enshrined in the Constitution of the Slovak Republic in Article 26, paragraph 1, which guarantees: "*Freedom of expression and the right to information are guaranteed.*" Paragraph 2 complements this freedom as follows: "*Everyone has the right to express their opinions by word, writing, print, image, or by any other means, as well as the freedom to seek, receive, and disseminate ideas and information without regard to state boundaries. The publication of printed matter is not subject to approval. Broadcasting and television activities may be subject to state permission. Conditions shall be established by law*."

In legal theory as well as in practical application, there are ongoing discussions regarding the "tension" that arises between the right to freedom of expression and the new rules introduced by the DSA. In our opinion the conflicts primarily arise because, on the one hand, the new legal framework established through the DSA seeks to regulate the digital space in a way that maximizes the protection of users' rights and ensures that their fundamental freedoms are upheld. On the other hand, it imposes obligations on online platforms, whose activities could potentially lead to restrictions on freedom of expression in the online environment.

Article 34(1)(b) DSA provides a detailed list of potentially affected rights with explicit references to the Charter of Fundamental Rights of the European Union, between which is freedom of expression and information.[14]

---

12 Charter of fundamental rights of the European Union avalilable at: [https://www.europarl.europa.eu/charter/pdf/text_en.pdf], Accessed 10 April 2025.

13 European convention on human rights available at: [https://www.echr.coe.int/documents/d/echr/convention_slk], Accessed 10 April 2025.

14 Manterelo, A., Fundamental Rights Impact Assesment in the DSA in: Hoboken, J. *et al.* (eds.), Putting the DSA into Practice, p. 112. Available at: [https://www.ivir.nl/publicaties/download/vHoboken-et-al_Putting-the-DSA-into-Practice.pdf.], Accessed 15 June 2025.

Content regulation on digital platforms by DSA can result in the removal of legitimate content, which can lead to censorship. The issue becomes evident in the process of determining what constitutes illegal content. It is our position that, with regard to freedom of expression, very large online platforms (VLOPs) and very large online search engines (VLOSEs)[15] are required to assess the risk of disproportionate removal of lawful content, particularly in cases where an algorithm or automated system mistakenly deletes content that is not unlawful. There is also a risk of interference with the plurality of opinions, where algorithms may, for example, favor extreme viewpoints while suppressing less popular perspectives in discussions (e.g., on political matters). These concerns arise from the principle of due diligence obligations (such as the ones on the assessment of systemic risks, access to research data and crisis protocols)[16], on which the DSA is based. As noted by Husovec, the real novelty of the DSA lies in the creation of fully fledged tiers of due diligence obligations. Instead of liability, the DSA insists on the responsibility that grows with the service's size and social impact.[17]

In accordance with due diligence obligations, platforms are required to proactively identify risks that may arise in the provision of their services (e.g. dissemination of harmful or illegal content, threats to freedom of expression, manipulation of public opinion), as stipulated in Article 34 of the DSA.

This reflects the application of a risk-based approach within the DSA framework. Subsequently, under Article 35 of the DSA, platforms are also required to implement specific measures to mitigate these risks (e.g. algorithm adjustments, publication of content moderation rules, user control mechanisms). It can be said that the DSA thus shifts responsibility from users and authorities to the platforms themselves.

In addition, platforms are obliged to ensure transparency toward both users and regulatory authorities, which also includes the publication of reports that cover:

- dissemination of illegal content;
- any negative effects for the exercise of the fundamental rights for private and family life, freedom of expression and information, the prohibition of

---

15 Article 34 of the DSA imposes an obligation on providers of very large online platforms (VLOPs) and very large online search engines (VLOSEs) to diligently identify, analyze, and assess all systemic risks within the Union arising from the design or operation of their service and its relevant systems, including algorithmic systems, or from the use of their services.

16 Buri, I., A Regulator Caught Between Conflicting Policy Objectives: Reflections on the European Commission's Role as DSA Enforcer in: Hoboken, J. *et al.* (eds.).: Putting the DSA into Practice, p. 7. Available at: [https://www.ivir.nl/publicaties/download/vHoboken-et-al_Putting-the-DSA-into-Practice.pdf.], Accessed 17 June 2025.

17 Husovec, M., *Principles of the Digital Services Act,* Oxford University Press. 2024, p. 22, ISBN 978 – 0 – 19 – 288245 – 5. [DOI: 10.1093/law-ocl/9780192882455.001.0001].

discrimination, and the rights of the child as set out in the EU's Charter of Fundamental Rights; and

- intentional manipulation of their service with actual or foreseeable negative effects on the protection of public health, minors, civic discourse, or related to electoral processes and public security.[18]

Reports must be submitted to the European Commission alongside an independent audit. When specifying this requirement with regard to freedom of expression, it is evident that the reports submitted by very large online platforms (VLOPs), prepared in accordance with Articles 34 and 35 of the Digital Services Act (DSA), frequently identify systemic risks to freedom of expression. However, the mitigating measures adopted often fail to effectively address these risks, as they tend to be outlined in a general manner without concrete interventions. For instance, Meta's report concerning the Facebook and Instagram platforms highlights risks related to the suppression of political content and the diminished visibility of sensitive societal issues. Nevertheless, the algorithmic adjustments implemented as part of the mitigation efforts were not accompanied by transparent explanations regarding their impact on the visibility of political speech.[19] Similarly, the TikTok platform acknowledged the risk of so-called "filter bubbles" and the potential suppression of minority viewpoints resulting from recommendation algorithms. Yet, the specific measures intended to mitigate these effects remained at the level of broad declarations without demonstrable outcomes.[20]

Closely related to the above is the so-called asymmetric approach of the Digital Services Act (DSA) towards different platforms, which has a direct impact on freedom of expression and its potential restrictions. The asymmetric approach of the DSA means that the obligations imposed by the regulation are not uniform across all digital services but vary depending on the size and type of the provider, as well as the influence and risk profile of the platform. Very large online platforms (VLOPs) and very large online search engines (VLOSEs) are subject to the strictest regime, which includes, for example, the assessment and mitigation of systemic risks (as outlined in

---

18 Latham; Watkins, *The Digital Services Act: Practical Implications for Online Services and Platforms* available at: [https://www.lw.com/admin/upload/SiteAttachments/Digital-Services-Act-Practical-Implications-for-Online-Services-and-Platforms.pdf], Accessed 23 June 2025.

19 Meta's Progress Implementing the Digital Services Act available at: [https://about.fb.com/news/2024/11/metas-progress-implementing-the-digital-services-act/], Accessed 23 June 2025.

20 DSA Risk Assesment Report 2024 available at: [https://sf16-va.tiktokcdn.com/obj/eden-va2/zayvwlY_fjulyhwzuhy[/ljhwZthlaukjlkulzlp/DSA/TikTok_DSA_Risk_Assessment_Report_2024.pdf], Accessed 23 June 2025.

Articles 34–35), algorithm auditing, the establishment of compliance officers, and the obligation to publish data for research purposes. For them, the DSA lists special due diligence requirements (Articles 33-43).[21] Compliance with these due diligence requirements is monitored solely by the Commission (Articles 56, 65-78), with the aim of ensuring a consistent, EU-wide application.[22]

Medium-sized platforms, in comparison to very large online platforms, must fulfill additional requirements regarding transparency, cooperation with relevant authorities, and the implementation of internal control mechanisms. Conversely, small and micro platforms (e.g., small online forums or e-shops) are subject only to basic obligations, such as establishing mechanisms for reporting illegal content. The asymmetric approach thus prevents the disproportionate burdening of small and medium-sized platforms, which under an equal regulatory load might be compelled to engage in preventive censorship out of fear of sanctions. It is argued that such behavior could lead to the so-called chilling effect — a deterrent effect on freedom of expression.

As noted above, to manage the overwhelming volume of online content and comply with the obligations arising from the DSA, it is essential for platforms to employ automated filtering and monitoring mechanisms, which are carried out through algorithmic tools.

As noted by Barata, however, these automated systems can have a very significant negative impact on human rights. He also points out that the regulation lacks clear and binding guidelines on the design and implementation of such technologies, particularly with regard to ensuring effective protection of user rights.[23] The use of artificial intelligence tools to detect illegal and harmful content presents several challenges. Automated filtering based on AI utilizes probabilistic methods and depends on the training data used, which can lead to both false positives (removal of harmless or useful content) and false negatives (leaving harmful content online). Strict parameters can easily lead to a large number of false positives, resulting in the unjust removal or reduced reach of useful information, and even the possible exclusion of valuable contributors.

---

21 Notice also Husovec, M., *Principles of the Digital Services Act,* Oxford University Press. 2024, p. 28, [DOI: 10.1093/law-ocl/9780192882455.001.0001].

22 Jaursch, J., in: Hoboken, *et al.*, Putting the DSA into Practice, p. 93. [DOI 10.17176/20230208-093135-0]. Available at: [https://www.ivir.nl/publicaties/download/vHoboken-et-al_Putting-the-DSA-into-Practice.pdf.], Accessed 17 June 2025.

23 Barata, J.: The Digital Service Act and its impact on the right to freedom of expression: special focus on risk mitigation obligations. In: Platforma por la Libertad de información, 2021, p.12 available at [https://libertadinformacion.cc/wp-content/uploads/2021/06/DSA-AND-ITS-IMPACT-ON-FREEDOM-OF-EXPRESSION-JOAN-BARATA-PDLI.pdf.], Accessed 13 April 2025.

This can have a direct impact on freedom of expression**,** protection from discrimination**,** fair process, and access to information, leading to the erosion of societal value in shared information, media pluralism, and open public discourse.[24] As Atzori points out, the obligations under the DSA that require platforms to assess risks and take mitigation measures can be detrimental to freedom of expression. This is particularly true because they focus on broad and strategic areas, such as public safety, public health, civil discourse, and electoral processes (Article 34, Paragraph 1, Letters a, c, d). The risk of removing politically sensitive content is high, and it is precisely in these areas where freedom of expression and media pluralism should be most protected, as they are key to the functioning of democratic life.[25]

This approach can lead to a contradiction with the freedom of expression, which is enshrined in many legal documents, both at the national and international levels, as discussed at the beginning of this chapter. Actions carried out by online platforms under the DSA could, in some cases, be likened to censorship, which is prohibited (for example, under Article 26, Paragraph 3 of the Constitution of the Slovak Republic).[26]

In summary, it should be noted that for online platforms, it can be problematic to assess whether certain content is illegal or not based on the mechanisms they use to evaluate digital content, as the definition of illegal content can be subject to different interpretations. As a result, there is a risk that online platforms, under the threat of sanctions, may be forced to remove borderline content that is still legal and legitimate, thereby leading to a clear violation of freedom of expression.

4. CONCLUSION

In this article, we focused on the digital rights in the light of the relatively new legal regulation from the EU concerning digital services – the DSA (Digital Services Act). We analyzed the digital rights considered by the DSA, with a particular focus on freedom of expression, which comes into controversy with the application of the rules outlined in the DSA.

---

24 Thiago, D.O., *Content Moderation Technologies: Applying Human Rights Standards to Protect Freedom of Expression*, in: Atzori, M. (ed.), The Digital Services Act and the Freedom of Expression in the European Union: A Political Perspective, 2024, p. 14 available at: [http://dx.doi.org/10.2139/ssrn.4887181.], Accessed 13 April 2025.

25 *Ibid.*

26 Constitution of Slovak republic available at: [https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/1992/460/.], Accessed 7 April 2025.

It should be noted that the DSA, as a significant legislative framework, provides stronger tools for protecting users' digital rights and ensures better regulation and oversight of the digital market within the EU. Protecting users from harmful content without excessive interference in their privacy is one of the main challenges of the DSA. It is about finding a balance between protection from harmful information and the preservation of privacy and freedom of expression. From an ideal standpoint, the outcome of applying the rules introduced by the DSA should be that digital services become safer, more transparent, and fairer for all.

Despite the intent behind the DSA, several challenges and problematic areas remain. Among the most prominent ones are:

- Insufficient control over the algorithms used by online platforms to monitor digital content.
- Exploitation of users' personal data by technology giants.
- Excessive interference with users' privacy.
- Infringement of freedom of expression through the removal or blocking of illegal content, which may border on censorship, which is prohibited.

The problematic areas mentioned above, in our opinion, are related to the so-called gaps that can be observed within the framework of the DSA. First and foremost, it is necessary to point out the definition of illegal content within the DSA. The DSA does not provide a legal definition of illegal content on the internet. Recital 12 of the DSA only outlines what could be considered illegal content. It states that, in order to achieve the objective of ensuring a safe, predictable, and trustworthy online environment, the term "illegal content" should broadly reflect existing rules in the offline environment. Specifically, the term "illegal content" should be defined in a broad sense to include information related to illegal content, products, services, and activities. Above all, this term should be understood to cover information that is, according to applicable law, either inherently illegal, such as illegal hate speech, terrorist content, and illegal discriminatory content, or that the applicable rules are illegal due to the fact that they concern illegal activities. The DSA provides demonstrative examples of illegal content.

In relation to the definition of illegal content, a problem may arise when assessing whether the content is already harmful or not, especially if it is evaluated in an automated manner using artificial intelligence tools. A further issue may emerge in the assessment of illegal content by individual Member States. While some Member States may not consider certain expressions harmful or illegal, others may evaluate them as harmful. This discrepancy leads to fragmentation within the

unified digital market, which is one of the objectives of the DSA- removing this fragmentation.

A significant problematic area that arises here, as highlighted in the article, is the collision between freedom of expression and the rules introduced by the DSA. On one hand, there is the protection from harmful content, and on the other, there is freedom of expression. This relates not only to fundamental human rights and freedoms, and the resulting digital rights, but also to ethical dilemmas and challenges. One of the key ethical challenges is finding a balance between maintaining freedom of expression and blocking or removing illegal content. The problem arises when there is excessive moderation of digital content, which may be controversial but not necessarily illegal. Striking a balance between freedom of expression and the regulation of digital content is a critical challenge.

A potential solution could be a clearer and more precise definition of illegal content, which would minimize the room for arbitrary interpretation and thus prevent censorship. Another solution is the introduction of transparent content moderation processes, with the possibility of appealing decisions to remove content. The DSA attempts to address this issue through Article 21. Additionally, a tool for addressing these challenges could be the regular assessment of the regulatory impact on freedom of expression, as well as other digital rights and freedoms.

In our opinion another problematic area that we perceive is the impact of the DSA on other fundamental human rights and freedoms, which could be threatened by the ambiguous provisions of the DSA. As Barata points out, the DSA includes numerous references to the need to uphold freedom of expression and information, the right to non-discrimination, media freedom, and pluralism – all of which are human rights and core European values. However, most of these references are found either in recitals, which have more interpretive than normative value, and/or are still insufficient in practical application. For instance, Article 34(b) requires platforms to consider "any real or foreseeable negative effects on the exercise of fundamental rights" in connection with identifying and managing systemic risks. However, this provision lacks specificity, as it does not specify particular practices or binding guarantees that should be put in place to effectively protect users' rights, whether by platforms or supervisory authorities.[27]

It is necessary to reflect on the future of the online environment, which is already being influenced by the DSA. It is appropriate to pose the question of whether the DSA will be successful in its implementation, and under what conditions?

[27] Barata, *loc. cit.*, note 23.

As Hoboken et al. points out a crucial aspect of the success of the DSA relates to the application of its due diligence requirements in practice and the effective implementation of its enforcement framework. The enforcement framework includes a combination of new regulatory authorities at the national (Digital Services Coordinators) and EU level (as part of the European Commission). These elements will be decisive as to whether the DSAwill deliver on its goals, and whether its rules will be capable of meaningfully protecting fundamental rights.[28]

To conclude, we may express the view that it is necessary to state that society must avoid two extremes – on one hand, the complete absence of regulation, which could lead to the spread of harmful content, and on the other hand, overly strict regulation, which could suppress legitimate freedom of expression and restrict public discourse. Finding this balance will require continuous dialogue between legislators, platforms, civil society, and users of digital services.

REFERENCES

BOOKS AND ARTICLES

1. Atzori, M., *The Digital Services Act and the Freedom of Expression in the European Union: A Political Perspective*, SSRN, 2024, available at: [http://dx.doi.org/10.2139/ssrn.4887181.]
2. Barata, J., *The Digital Service Act and its impact on the right to freedom of expression: special focus on risk mitigation obligations*, Platforma por la Libertad de información, 2021, available at: [https://libertadinformacion.cc/wp-content/uploads/2021/06/DSA-AND-ITS-IMPACT-ON-FREEDOM-OF-EXPRESSION-JOAN-BARATA-PDLI.pdf.], Accessed 13 April 2025
3. Barocas, S.; Selbst, A.D., *Big Data's Disparate Impact*, 2016, 104 California Law Review 671
4. Custers, B., *New digital rights: Imagining additional fundamental rights for the digital era*, Computer Law & Security Review, Vol. 44, 2022. [https://doi.org/10.1016/j.clsr.2021.105636]
5. Hoboken, J.: Quintais, J. P.; Appelman, N.; Fahy, R.; Buri, I.; Straub, M., *Putting the DSA into Practice*, available at: [https://www.ivir.nl/publicaties/download/vHoboken-et-al_Putting-the-DSA-into-Practice.pdf], Accessed 15 June 2025
6. Husovec, M., *Principles of the Digital Services Act*, Oxford University Press. 2024. [DOI: 10.1093/law-ocl/9780192882455.001.0001]
7. Latham; Watkins, *The Digital Services Act: Practical Implications for Online Services and Platforms*, available at:

[28] Hoboken, *et al. Putting the DSA into Practice*, available at [https://www.ivir.nl/publicaties/download/vHoboken-et-al_Putting-the-DSA-into-Practice.pdf], Accessed 15 June 2025.

[https://www.lw.com/admin/upload/SiteAttachments/Digital-Services-Act-Practical-Implications-for-Online-Services-and-Platforms.pdf], Accessed on 23rd of June 2025

8. Xanthoulis, N., *Conceptualizing a Right to Oblivion in the Digital World: A Human Rights-Based Approach*, 2012.
[https://ssrn.com/ abstract=2064503], Accessed 11 April 2025

COURT OF JUSTICE OF THE EUROPEAN UNION

1. Judgement of CJEU from 04 July 2023. C-252/21 Meta Platforms Inc., before Facebook Inc.,Meta Platforms Ireland Ltd, before Facebook Ireland Ltd,Facebook Deutschland GmbH against Bundeskartellamt. ECLI:EU:C:2023:537. Available at:
[https://curia.europa.eu/juris/document/document.jsf?text=&docid=275125&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1], Accessed 14 April 2025.

EU LAW

1. European convention on human rights available at:
[https://www.echr.coe.int/documents/d/echr/convention_slk], Accessed 10 April 2025.
2. Charter of fundamental rights of the European Union avalilable at Charter of fundamental rigts of European Union available at:
[https://www.europarl.europa.eu/charter/pdf/text_en.pdf], Accessed 10 April 2025.
3. 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) available at:
[https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=celex:32016R0679], Accessed 5 April 2025.
4. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) available at:
[https://eur-lex.europa.eu/eli/reg/2022/1925/oj/eng], Accessed 5 April 2025.

LIST OF NATIONAL REGULATIONS, ACTS AND COURT DECISIONS
WEBSITE REFERENCES

1. Constitution of Slovak republic available at:
[https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/1992/460/.], Accessed 7 April 2025.
2. DSA Risk Assesment Report 2024 available at:
[https://sf16-va.tiktokcdn.com/obj/eden-va2/zayvwlY_fjulyhwzuhy[/ljhwZthlaukjlkulzlp/DSA/TikTok_DSA_Risk_Assessment_Report_2024.pdf], Accessed 23 June 2025.
3. Guide of The Council for Media Services available at:

[https://rpms.sk/sites/default/files/2025-02/Prirucka_pre_sprostredkovatelske_sluzby.pdf)], Accessed 5 April 2025.

4. Meta's Progress Implementing the Digital Services Act available at: [https://about.fb.com/news/2024/11/metas-progress-implementing-the-digital-services-act/], Accessed 23 June 2025.