

Marek Švec, Adam Madleňák, Vladimíra Hladíková, Peter Mészáros

Slovak Mimicry of Online Content Moderation on Digital Platforms as a Result of the Adoption of the European Digital Services Act

DOI: <https://doi.org/10.34135/mlar-24-02-06>

ABSTRACT

The global nature of digital platforms, particularly social media, highlights the lack of a unified legal framework to regulate the content which is distributed to users. This issue is not only about the quality of the content but often concerns its problematic nature, which may conflict with the legal systems of various countries, especially the member states of the European Union. Examples include hate speech, terrorist content, discriminatory material, or images depicting child sexual abuse. Digital platforms frequently argue that they are not responsible for the nature of this content, as they merely facilitate its publication and do not create it themselves, thus claiming they should not be held legally accountable. This article examines the research question of how the recently adopted European Digital Services (*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), 2022*) might change the current paradigm using various legal tools. The Act aims to effectively regulate online intermediaries and platforms, including marketplaces, social networks, content-sharing platforms, app stores, and online travel and accommodation services. Through a critical analysis of the provisions of the Digital Services Act, related legislation, court decisions, and the actual behaviour of digital platforms, the authors reassess the effectiveness of different mechanisms intended for moderating content on these platforms. The primary objective is to determine the shift in the legal boundaries of digital platforms' responsibility for shared content, particularly regarding newly defined obligations related to user safety and new information requirements for digital platforms, such as reporting to European supervisory authorities. Special attention is given to the increased legal protection of minors using digital platforms, particularly regarding the absolute prohibition of profiling them for online advertising, as stipulated in Article 28 of the Digital Services Act. This provision complements the relevant rules set out in Article 22 of GDPR. The general tightening of conditions for presenting advertisements online is intended to curb the use of personalized advertising, which often relies on the (impermissible) profiling of ad recipients using special categories of personal data, such as racial or ethnic origin, sexual orientation, biometric data, and more. In the article, the authors also discuss potential challenges in the practical implementation of the Digital Services Act in individual member states of the European Union, considering the specifics of national legislation. To illustrate these challenges, the article provides an analysis of the legislative realities in Slovakia as a model example.

KEY WORDS

Digital Platforms. Digital Services Act. Moderation of Online Content. Online Advertising. Social Networks.

1 Introduction

Content moderation on digital platforms in a globally interconnected, cross-border environment is inherently challenging. The responsible and diligent conduct of intermediary service providers is crucial for maintaining a safe, predictable, and trustworthy online space. This is also vital for enabling European Union citizens and others to exercise their fundamental rights, as guaranteed by the Charter of Fundamental Rights of the European Union, including freedom of expression, the right to information, freedom to conduct a business, and the right to non-discrimination (*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)*, 2022). Practical application becomes even more difficult when the environment is shaped by different legal frameworks resulting from the fragmentation of national regulations (IFC et al., 2018)¹, not only among EU member states but also across different legal systems, historical traditions, and customs in each country. This situation undermines the fundamental principle outlined in Article 26 of the *Treaty on the Functioning of the European Union*², which aims to create a borderless area within the EU, guaranteeing the free movement of goods and services and the freedom to settle. This issue is further complicated by the cross-border nature of the Internet, which is generally used to deliver digital and information society services, but is subject to varying national regulations (Bulla, 2018).

As a result, efforts to effectively implement measures to prevent the spread of illegal content through digital platforms, search engines, or other services are often ineffective. Due to the fragmentation of legislation across different countries, it is challenging to prevent potential negative impacts on fundamental rights, civil discourse, the electoral process, public safety, and other social issues such as gender-based violence or the protection of minors (Mendoza, 2022). We must recognize that digital platforms serve as instruments driving societal transformation, gradually evolving and redefining exchange relationships between individuals, thus facilitating the shift from a traditional to a collaborative economy. Digital platforms encompass all elements of a collaborative economy, as defined by Felson and Spaethem (1978), which involves socially or legally significant situations where economic goods and services are shared as part of social activities. Botsman and Rogers (2010) expand the definition of a collaborative economy by including innovative elements. They consider traditional activities such as sharing, exchanging, lending, trading, renting, and donating, when facilitated by modern technologies and mutual communities, as integral aspects of a collaborative economy. For the purposes of European law, the European Parliament provides a legally relevant definition of a collaborative economy. It highlights that a collaborative economy should be viewed not just as a collection of new business models offering goods and services, but also as a new form of integration between the economy and society. This integration involves a broad spectrum of relationships, including economic interactions within social contexts, and fosters new forms of community and innovative business models (European Parliament, n.d.).

¹ Authors' note: Due to the varying legal regulations across EU member states, driven by different approaches to regulation and oversight (excluding the impacts on security and trust in digital services), it is estimated that cross-border digital trade could see an increase in value ranging from 1% to 1.8%. This translates to a potential boost in cross-border turnover amounting to between EUR 8.6 billion and EUR 15.5 billion. For comparison, see – Legal analysis of the intermediaries service providers of non-hosting nature – ICF; Grimaldi, The Liabilities Regime and Notice -and- Action Procedures – In European Commission, Directorate -General for Communications Networks, Content and Technology, Overview of the legal framework of notice -and- action procedures in Member States SMART 2016/0039 – Final report, Publications Office, 2018.

² Authors' note: Compare with Article 26 of the consolidated version of the Treaty on European Union, 2012/C 326/01.

It is therefore not surprising that digital platforms, which encompass all the defining characteristics of a collaborative economy, have become environments where fundamental social needs are met. From online shopping to social interactions through sharing videos, information, and photos, these platforms address both material and emotional needs. This integration often blurs the line between work and personal life, as well as between activities aimed at fulfilling material needs and those geared towards satisfying emotional needs, such as self-expression and forming social or intimate connections. In this context, digital platforms can create a complex network of relationships through which individuals can fulfil all their needs, regardless of their nature. This complexity often leads individuals to relax established boundaries that traditionally separate their work and personal lives from third parties. As a result, there is a growing tendency to share more information and content online. This expanded sharing can, however, inadvertently lead to violations of fundamental human rights and freedoms, as personal information becomes more susceptible to misuse and exploitation.

The described scenario, where participants share information within the environment of a digital platform, underscores the need for new legal regulations governing the content and scope of shared information on these platforms. Such legislation must address the protection of fundamental rights and freedoms for all online participants, particularly those who are more vulnerable compared to the economically dominant platform operators. The key factor in determining the legal consequences will continue to be the effective protection of individuals' anonymity. This includes not only safeguarding personal data but also defending against negative phenomena such as cyberbullying and protecting minors. The primary requirement for adopting relevant legal regulations is ensuring transparency and accountability for digital service providers regarding the legal or illegal dissemination of inappropriate content online.

2 Theoretical Framework

In response to these requirements, the Digital Services Act was adopted, coming into effect on February 17, 2024 (*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), 2022*). This Act establishes a clear legal framework for the operation of intermediary service providers and, in particular, digital platforms such as social media (Rak & Raková, 2021). Key new obligations include setting up procedures for reporting and addressing illegal content, and providing mechanisms to challenge the decisions made by digital platforms regarding content moderation³. Specifically, this should apply to providers of intermediary services, especially those offering “simple transmission”, “caching”, and “hosting” services. The rapid increase in the use of these services – largely for legitimate and socially beneficial purposes – has also amplified their role in mediating and spreading illegal or harmful content. The requirement for certain online platforms to collect, store, and partially verify and publish information about the businesses using their services aims to enhance the safety and transparency of the online environment for consumers. Additionally, the emphasis on the significant influence of very large online platforms (VLOPs)⁴ in the online space represents a groundbreaking aspect of this regulation. For Very Large Online Platforms (VLOPs), a higher

³ Authors' note: Compare with Art. 24, par. 2 and Recital 77 of the Act on Digital Services, as well as Art. 3, letters m), p) and q) of the Act on Digital Services and Article 33 of the Act on Digital Services.

⁴ Authors' note: The European Commission identified Very Large Online Platforms (VLOPs) based on data provided by the platforms and its own assessment. These VLOPs include social networks such as Facebook, Instagram, TikTok, YouTube, X (formerly Twitter), Snapchat, LinkedIn, and Pinterest; online stores like Amazon, Booking, AliExpress, Zalando, and Google Shopping; as well as Wikipedia, Google Maps, Google Search, and Bing from Microsoft. Additionally, the app stores operated by Google and Apple are also classified as VLOPs.

standard of transparency and accountability has been established regarding content moderation, online advertising, and the use of algorithmic processes. This includes an obligation to assess the risks associated with their systems and to develop effective risk management tools aimed at protecting the integrity of their services against manipulative techniques.⁵ However, Very Large Online Platforms (VLOPs) are also required to ensure transparency in their advertising practices, including the creation of recommendation systems and the decisions related to user self-moderation of content. This commitment is part of the broader regulatory framework established by the Digital Services Act (*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)*, 2022). Complementing this, the Digital Markets Act has been adopted, introducing mechanisms for ensuring compliance with the new rules. This includes market investigations conducted by the European Commission to oversee adherence to these regulations within the digital sector.

The Digital Markets Act is particularly significant because it addresses a range of core platform services that have large economies of scale and low marginal costs for adding new commercial or end users. It also highlights the potential for significant dependency among users, and how this dependency – when combined with unfair practices by platform providers – can severely disrupt market competition. This approach is notably innovative, as earlier definitions, including those in Slovak law, had substantial limitations that allowed digital platforms to evade comprehensive regulation. For example, Section 22h, letter a) of Act No. 442/2012 Coll defined a platform as software, including websites or parts thereof and applications, including mobile apps, that are accessible to users and facilitate connections between sellers and other users to carry out, either directly or indirectly, selected activities for the benefit of these users. It also encompasses all procedures for collecting and processing payments related to these activities (*Zákon č. 442/2012 Z. z. o medzinárodnej pomoci a spolupráci pri správe daní*, 2012).

In this context, considering the European framework for defining a digital platform, Article 9, par. 1 and par. 2 of Act No. 264/2022 Coll., the Media Services Act, offers a more detailed legal definition, specifying that content sharing platform is an information society service whose primary purpose, or one of its main purposes, is to store and distribute a large volume of works and other protected items uploaded by users, in accordance with specific regulations (*Zákon č. 264/2022 Z. z. o mediálnych službách*, 2022). However, none of the provided legal definitions fully satisfy the requirement for a comprehensive legal basis to regulate online content. Additionally, these definitions only apply to the legal relationships covered by the relevant regulations. In this context, a notable positive element for regulating online content is found in Section 2, letter a) of the Electronic Commerce Act. This section offers a broader definition of “information society service”, under which the activities of digital platforms can also be categorized. According to this provision, an information society service is understood to be a service provided remotely through electronic communication networks, typically for payment upon the request of the recipient. This includes activities such as commercial communication, data processing, transmission, storage, search, collection, and electronic mail, excluding personal electronic mail (*Zákon č. 22/2004 Z. z. o elektronickom obchode*, 2004). In light of the above, the definition in Article 2, letter h) of the Digital Services Act appears to be broadly applicable and positively suited to regulating the online content in question. It accommodates a wide range of entities by including hosting service providers, which store and publicly distribute information at the request of the service recipient. This definition is effective unless the hosting activity is a minor and ancillary component of another service that cannot function objectively or technically without it.

⁵ Authors' note: For example, there is a prohibition for digital platforms against using inducement techniques designed to influence user behaviour through so-called dark patterns.

This broader definition of digital platform activities is closely aligned with, yet does not undermine, existing European legal regulations. However, the new legal framework introduced in the Digital Services Act marks a significant shift, offering a more precise approach to regulating online content by expanding both its personal and substantive scope.

The Digital Services Act thus serves as a new, secondary tool for regulating online content and establishing a “horizontal framework” that applies to all categories of content, products, services, and activities within intermediary services. Its integration into the hierarchy of legal norms complements existing regulations, particularly GDPR (*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, repealing Directive 95/46/EC (General Data Protection Regulation)*, 2018). From the perspective of its intended purpose, the Act clarifies and broadens the scope of regulation by including a new range of entities that might have previously evaded the original legal framework due to its ambiguity or perceived insignificance in the relevant economic market. For instance, while the Act’s measures on online advertising complement rather than alter existing regulations regarding consent to personal data processing and the right to object, they introduce new obligations for transparency towards users of online platforms. This increased transparency will help users exercise their rights as data subjects more effectively. Additionally, it will enable authorities and verified researchers to monitor how advertising is displayed and targeted (Mendoza, 2022).

3 Methods

The aim of this article is to evaluate the social and legal consequences of applying the new Digital Services Act to the activities of digital platforms engaged in various intermediary functions, which fall under the broader categories of hosting and information society services. To achieve this objective, the article employs a scientific method that includes critical analysis of relevant European legislation, examination of legal conclusions from pertinent courts, and review of factual actions by stakeholders, as documented through statistical research and legally relevant documents. To achieve the objectives of this article, we employed several research methods that collectively contributed to a thorough assessment of user protection on digital platforms, particularly social networks that facilitate online (personalized) advertising. This advertising is created through the automatic processing of information and personal data using computer algorithms and profiling. By carefully selecting information sources, we aim to emphasize the interdisciplinary nature of the topic. Our research drew on insights from sociology, psychology, management, marketing, and especially legal sciences to explore the commercial functioning of digital platforms and their role in addressing the social needs of their users. The various sections of the article are organized to logically lead to comprehensive conclusions. In summary, alongside analytical and synthetic methods, we employed inductive, deductive, and comparative research techniques. Finally, scientific abstraction was used to define key terms based on a review of domestic and international literature, including monographs and peer-reviewed journals. We also incorporated our own insights from expert research in digital marketing communication, along with practical experience in personal data protection, commercial law, and privacy on digital platforms.

4 Results

To achieve the goal of creating a safe, predictable, and trustworthy online environment under the Digital Services Act, the term “illegal content” should be broadly defined (Laclavíková & Olšovská, 2018). This definition should encompass not only the content itself but also any associated information related to illegal content, products, services, and activities. Specifically, “illegal content” should include, regardless of its form, information that is illegal in itself or connected to unlawful activities under applicable law. This includes, but is not limited to, hate speech, terrorist content, discriminatory material, images depicting sexual abuse of children, and online harassment.⁶ The main challenge of regulating content on digital platforms lies in their operation across various legal frameworks. Digital platforms can navigate different regulations and apply specific legal rules (*lex specialis*) for each. Within a single platform, it is possible to encounter varying regulations depending on the type of business activity, such as mediating the sale of goods and services. This complexity makes the creation of a unified approach to content regulation difficult. At the same time, the platform will provide opportunities for social interaction among users and access to various media content, thereby qualifying as an information society service under the Media Services Act. The applicability of the relevant legislation will depend on the nature of the digital platform’s content. Specifically, it will be influenced by whether the platform’s operations are focused on transactional activities aimed at generating profit, or if they are more oriented towards the presentation and mediation of advertising, similar to social networks. In the latter case, the platform’s commercial purpose is driven not by the exchange of goods and services for monetary value, but by the financial value derived from advertising. In the first scenario, the digital platform operates as an intermediary that facilitates the meeting of supply and demand between business entities within specific economic sectors. Here, the actual transactions and legal activities are conducted through the platform’s internal mechanisms. The platform’s value lies in its ability to create a synergistic effect by linking a large number of participants with similar interests, thereby fostering the commercialization of their interactions. This dynamic leads to an ongoing expansion of these relationships and allows for the continuous entry of new participants (DaSilva & Trkman, 2013; Zuthsi et al., 2019). Consequently, the Electronic Commerce Act is expected to primarily govern the interactions between these entities.

In the second scenario, the digital platform assumes the role of an entity that offers a virtual space primarily for content creation. This platform is not mainly focused on facilitating the exchange of goods and services for financial gain. Instead, it provides a space where individuals can fulfil fundamental social needs, with a primary emphasis on personal expression and interaction (Cimpan et al., 2022; Parker et al., 2016). The primary added value of this virtual space lies in its broad accessibility to an unlimited number of users and the creation of synergistic interactions between them. Consequently, the commercial impact is achieved through the opportunities for content creation, often driven by advertising activities from specific users. While the use of the digital platform itself is typically free, making it accessible even to minors, the platform leverages these interactions and content to drive its commercial objectives. Therefore, the more engaging and varied the content on a digital platform is for its diverse user groups, the more likely users are to spend extended periods on the platform throughout the day. This increased engagement makes it easier to present new products and services to them, particularly when leveraging personalized content and algorithms to ensure that the right users see the most relevant offerings (Kangas et al., 2007; Strowel & Vergote, 2017).

⁶ Authors’ note: Compare the wording of Recital no. 12 of the Digital Services Act (*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)*, 2022).

A notable development driven by digital platforms is the use of content personalization combined with algorithms for displaying tailored content to individual users through profiling. Platforms like social networks and search engines collect various types of information – sometimes automatically – that may qualify as special categories of personal data under Article 9 of GDPR. They employ diverse methods for this, including analyzing frequently searched terms, users' hobbies and habits, and inviting participation in online surveys and contests. The information gathered and the connections made by computer algorithms are further leveraged through various operations, such as sharing this data with third parties who create advertising content displayed on digital platforms, or using it to conduct profiling, which allows for a higher degree of personalized content to be shown to users. Computer algorithms can process a vast array of diverse input parameters, identify connections that are imperceptible to human perception, and generate actionable results in a very short period. They can independently gather input data from multiple sources, particularly online, and evaluate human characteristics and behaviours without bias or emotion (Vojtko, 2017). When delivering personalized advertising that effectively targets the right users on a digital platform, there is a greater potential for valuing such activity, leading to higher revenue from advertisers compared to non-personalized ads aimed at a broader user group. In personalized advertising campaigns, the standard practice involves using recommendation algorithms that consider a specific customer's order history. These algorithms analyze the purchasing patterns of other customers to predict a range of products that might interest this particular customer. The algorithm works by scanning all shopping carts and identifying the products most frequently purchased by people who bought the same item as the original customer. In this way, personalized advertising has become an effective strategy for increasing brand awareness and engaging the target audience. Digital platforms serve as a bridge between promotional content and end users. The purpose of personalization is to boost consumer engagement and foster positive attitudes toward both the advertisements and the brand itself. This approach ensures that users are less likely to be annoyed by ads that do not interest them. To improve users' favourable attitudes toward advertising and the brand, advertisers utilize data collected from online monitoring of user activity (such as cookies) or purchase databases from third parties. This data helps them tailor ads to specific users based on their preferences, demographics, interests, or location. Research on the benefits of personalized advertising has shown that it captures greater attention from consumers than non-personalized ads, ultimately increasing the effectiveness of the advertisements (Kim et al., 2022).

The Digital Services Act, in Article 1 in conjunction with Article 2, letter f), clearly defines social networks as digital platforms and categorizes their activities under the so-called “hosting” service. This classification establishes a legal basis that requires social networks to comply with the Act's provisions. The “hosting” service refers to the storage of information provided by the recipient of the service at their request. The primary obligation that arises for such entities is the duty to moderate the content within their internal infrastructure. Content moderation involves activities aimed at detecting and identifying illegal content, combating such content or information, and taking measures that impact the availability, visibility, and accessibility of this illegal content. These measures might include downgrading its position, restricting access, or removing it altogether (*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)*, 2022).⁷ This legal obligation for content moderation establishes a direct and binding responsibility for digital platforms, making them accountable for any violations related to this duty. It means that digital platforms are directly responsible for ensuring the legality of the content they publish, without the leniency or flexibility they previously had. This represents a relatively strong legal instrument, assigning responsibility not only to the content

⁷ See: Art. 2, letter p) of the Digital Services Act.

creator but also to the entity disseminating the content. As a result, it creates a quasi-joint liability relationship between these entities, with specific sanctions imposed on digital platforms for non-compliance⁸.

Article 5 of the Digital Services Act sets out strict and limited conditions under which a digital platform can be exempted from liability for the content it mediates. Digital platforms can avoid responsibility only if their service solely involves storing information provided by the user. Additionally, the platform must not have actual knowledge of illegal activities or content. If the platform does become aware of such illegal content, it must take swift action to remove it or disable access to it. Based on the above, it can be concluded that a digital platform operator will not be held liable for stored information if they are genuinely unaware of the illegal activity or content, or if they take appropriate steps to address it once they become aware. To qualify for this exemption from liability for hosting services, the platform must act promptly to remove or block access to illegal content as soon as it gains actual knowledge or awareness of it.

In this regard, digital platforms are expected to implement user-friendly reporting and action mechanisms that make it easy for users to flag content they believe to be illegal. Once reported, the platform must review the content to determine if it indeed violates regulations, and then decide whether to remove it or disable access⁹ (Geist, 2023).

5 Discussion

Profiling and automated processing are increasingly used as decision-support tools across various fields. However, these methods may overlook unique case-specific details, potentially leading to unfair or inaccurate outcomes. To address this, Article 22 of the GDPR and Section 28 of the Personal Data Protection Act (*Zákon č. 18/2018 Z. z. o ochrane osobných údajov, 2022*) give individuals the right to not be subject to decisions solely based on automated processing of personal data, including profiling, if such decisions significantly affect them or have legal implications. According to Article 4, par. 4 of the GDPR and Section 5, letter g) of the Personal Data Protection Act, profiling refers to any form of automated processing of personal data used to evaluate specific personal attributes or characteristics (Žulová, 2021). This includes analyzing or predicting aspects such as a person's health, preferences, interests, reliability, behaviour, location, or movement. The GDPR and the Personal Data Protection Act do not inherently prohibit profiling or automated decision-making; rather, these processes are subject to regulatory requirements and safeguards to protect individuals' rights.

If a digital platform uses an application or a specific algorithm to evaluate the information it collects, the automated decisions made can have a significant impact on the individuals involved and may even have legal consequences for them. Even if the input parameters used for these evaluations seem neutral at first glance, there is still a risk that, when combined, they could reveal characteristics that are protected under the principle of equal treatment and should not be considered. For example, if a platform's automated decision leads to blocking content or cancelling a user's account based on algorithmic analysis of posts and their specific words – without a deeper understanding or assessment of the content – it creates a serious issue.

GDPR already offered substantial protection to users against profiling and automated processing of personal data, even before the adoption of the Digital Services Act. This includes data collected by digital platforms, such as social networks. While GDPR and the Personal Data Protection Act do not outright ban decision-making based on profiling, they do provide

⁸ Authors' note: Discussed in more detail in Section 3.

⁹ Authors' note: In simple terms, digital platforms and search engines must provide a detailed annual report to the Commission on how their operations might pose systemic risks, like how their algorithms could spread misinformation or illegal content. They need to address these risks by, for example, changing their algorithms or flagging problematic content.

safeguards for individuals. Specifically, these regulations grant the right not to be subjected to a decision that is solely based on automated processing and has legal implications for the individual (as outlined in Article 22, par. 1 of the GDPR and Article 28, par. 1 of the Personal Data Protection Act) (Hudecová et al., 2020). The prohibition of automated decision-making, including profiling, applies only when the decision or profiling is entirely based on the automated processing of personal data. This means that the final decision is made without any human input or consideration of additional factors. The restriction on automated decision-making also applies if the decision has legal consequences for the individual or significantly impacts them in a similar manner. A decision has legal effects if it leads to the creation, modification, or termination of a person's rights or obligations, or if it prevents the person from exercising their rights. However, under Article 22, par. 2 of GDPR and Section 28, par. 2 of the Personal Data Protection Act, an individual does not have the right to opt out of automated decision-making if the automated processing is necessary for the conclusion or performance of a contract with the data subject, or if the processing is based on the individual's explicit consent. Consent is not considered a legally valid basis for processing if the data subject has no real choice, such as when consent to automated processing is a mandatory condition for receiving a service or when there is a power imbalance between the parties. For example, a digital platform that relies on consent as the legal basis for automated processing must be able to prove that individuals clearly understand what they are consenting to (Švec & Žullová, 2018).

Article 26 of the Digital Services Act aims to enhance the protection of digital platform users' rights, particularly concerning the platform's responsibility for mediated content, such as personalized advertising. It explicitly strengthens legal mechanisms that were initially introduced by Article 6 of the E-Commerce Directive (*Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')*, 2000).¹⁰ This enhancement also aligns with the legal interpretation of Article 22 of GDPR and incorporates findings from the Court of Justice of the European Union's decisions.¹¹ In this context, the nature of shared information – whether it's illegal or false – and its potential for widespread distribution are influenced by the cross-border or global operations of digital platforms. Vojtko notes that social networks enable the quick sharing of information stored by hosting providers among their users. He warns that there is a genuine risk that content flagged as illegal could be copied and reposted by another user on the same network. In legal proceedings, a competent court may order a digital platform to disable access to or remove stored information that is identical to content previously declared illegal, regardless of who originally uploaded it (Vojtko, 2017).

Given that advertising systems used by digital platforms (especially Very Large Online Platforms, or VLOPs) can pose significant risks, Article 26 of the Digital Services Act introduces additional protective measures beyond existing European legal frameworks. These risks can include financial contributions that support the spread of illegal or harmful content, as well as discriminatory advertising practices that undermine equal treatment. Digital platforms are therefore required to ensure that users clearly understand when and on whose behalf advertisements are shown. Additionally, users have the right to access information on how to adjust or disable the parameters used for ad personalization. This empowers users to “opt out”

¹⁰ Authors' note: For instance, Member States are required to ensure that commercial communications, such as advertisements, are clearly distinguishable. This requirement also extends to the labeling of promotional offers, contests, and games. See Article 6 of 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 Directive (*Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')*, 2000)

¹¹ Authors' note: Later cited point 36 and 37 of the decision of the Court of Justice of the European Union in the case of *Eva Glawischnig-Piesczek v. Facebook Ireland Limited* dated 3 October 2019, C-18/2018.

or turn off ad personalization, significantly enhancing their control and protection. The new obligations for digital platforms build on existing user rights established by Article 22 of GDPR, such as the right to object to automated individual decision-making and the requirement to obtain consent before processing personal data for personalized advertising (Valentová et al., 2018). A notable change introduced by Article 26, par. 4 of the Digital Services Act is its explicit prohibition of profiling and the creation of personalized advertising based on special categories of personal data, as defined in Article 9, par. 1 of GDPR. This represents a significant shift from GDPR, which does not explicitly restrict profiling involving such sensitive data. Personalized advertising based on profiling can no longer use data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, or information related to health or sexual orientation.¹² This restriction on profiling is further intensified for minors. Article 28, par. 2 of the Digital Services Act explicitly prohibits digital platforms from displaying personalized ads based on profiling if they reasonably know that the user is a minor (*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, repealing Directive 95/46/EC (General Data Protection Regulation)*, 2018).¹³ In line with Regulation (EU) 2016/679, particularly the data minimization principle set out in Article 5, par. 1, letter c), this prohibition should not compel online platform providers to collect, store, or process additional personal data beyond what they already have to determine if a user is a minor. Therefore, providers should not be encouraged to gather age-related information from users solely to comply with this requirement. When evaluating risks to children's rights, digital platforms should consider factors such as how easily minors can understand the service and how the platform might expose them to content that could negatively impact their health, physical well-being, mental development, and moral growth (*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)*, 2022). Article 28 of the Digital Services Act clearly mandates that digital platforms implement effective and suitable measures to safeguard minors. While the specific measures are left to the platform's discretion, they could include designing online interfaces with enhanced privacy, security, and protection for minors, adopting internal policies focused on minor protection, or adhering to codes of conduct dedicated to safeguarding young users.¹⁴

¹² Authors' note: In addition to the measures mentioned, very large online platforms are required to support oversight and research into emerging risks from online advertising. This includes addressing issues such as illegal ads, manipulative techniques, and disinformation that could negatively impact public health, safety, civil discourse, political participation, and equality. They must also make archives of displayed advertisements publicly accessible. These archives should include ad content, advertiser information, and data related to ad delivery, particularly for personalized ads.

¹³ Authors' note: It's important to note that while the Digital Services Act doesn't specifically address the legal protection of minors, it does impose restrictions related to its scope. In practice, we must rely on Article 8, par. 1 of GDPR and Recital 38, which stipulate that minors are a vulnerable group, exposed to the negative impacts of social phenomena, including unauthorized and illegal intrusions into their private lives and that children require special protection for their personal data because they may not fully understand the risks, consequences, and safeguards related to data processing. This protection is especially important when their data is used for marketing, creating personal profiles, or when services are provided directly to them (*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, repealing Directive 95/46/EC (General Data Protection Regulation)*, 2018).

¹⁴ Authors' note: Concrete measures can also be found in the Commission's Communication of May 11, 2022, titled "A Digital Decade for Children and Youth: A New European Strategy for a Better Internet for Children" (COM(2022) 212 final).

6 Conclusion

It is challenging to predict the precise impact of the Digital Services Act on digital platforms, particularly social networks, or to gauge its effectiveness in enhancing user protection, especially for minors. However, drawing from the experience with GDPR since 2018, it is likely that the Digital Services Act will meet its objectives. This confidence stems from the robust structure of European supervisory authorities and the establishment of coordination points (digital service coordinators) in each member state, which suggests a high probability of achieving the regulation's goals. Early indications of the Digital Services Act's impact are already visible in the actions of major online platforms. For instance, TikTok and YouTube have responded by not only banning targeted ads for minors but also by automatically setting their profiles to private. This means that videos uploaded by minors can now only be viewed by users they approve, enhancing privacy and control for younger users. From the legal and professional perspective, it's clear that the Digital Services Act will introduce a substantial number of new obligations for digital platforms. These changes will significantly enhance users' ability to actively protect themselves if they believe their information or work is being shared illegally.

A major benefit of the new regulation is the enhanced ability for users to report illegal or inappropriate content on digital platforms. This improved reporting mechanism will strengthen users' legal standing by ensuring more effective content moderation. With the digital platform required to swiftly address and remove reported content – regardless of its global reach – affected individuals can expect prompt and efficient protection of their rights (Pacalajová & Kubinec, 2021). This approach ensures that any infringement on the fundamental rights and freedoms of individuals and entities can be promptly addressed, effectively preventing further harm. By implementing robust reporting procedures and providing mechanisms to challenge content moderation decisions, the Digital Services Act aims to protect affected parties and enhance overall user security. Highlighting this legal protection for very large online platforms will help counterbalance their economic dominance and improve their relationship with users. This is particularly achieved by empowering users with the right to understand and influence how their content is moderated, thanks to transparency regarding the algorithms and applications used by these platforms.

The actual impact of the Digital Services Act on the internal operations of digital platforms will become clear only through ongoing regulatory oversight and the enforcement of legal sanctions as outlined in Article 42 of the Act. Financial penalties for non-compliance can be substantial, ranging from 1% to 6% of the service provider's annual income or turnover, depending on the severity of the breach.

The enhanced protection of user anonymity and personal data on digital platforms will be further supported by Article 28 of the Digital Services Act, complemented by Article 22, par. 1 of GDPR. This combination will bolster safeguards against the over-personalization of advertising messages, reinforcing the privacy and data protection of digital platform users. Moreover, Article 26 of the Digital Services Act significantly strengthens protections for minors compared to previous regulations. It explicitly prohibits the use of profiling based on personal data collected from minors for online advertising, thereby enhancing their protection from targeted ads. When evaluating risks to children's rights, digital platforms must assess how well their services are understood by minors and consider whether the content accessible through their platforms could harm the health, physical, mental, and moral development of young users. This will significantly enhance the protection of vulnerable groups and safeguard users from harmful content.

Acknowledgement: The research was supported by the Scientific Grant Agency of the Ministry of Education, Science, Research and Sport of the Slovak Republic and the Slovak Academy of Sciences (VEGA, No. 1/0013/23) under the project entitled "Slovak Legislation's Response to European Labor Law and GDPR: A Study of Algorithmic Content Management in Employment Relationships".

Bibliography

- Botsman, R., & Rogers, R. (2010). *What's mine is yours: The rise of collaborative consumption*. Harper Business.
- Bulla, M. (2018). Nové formy regulácie ako odpoveď na meniaci sa svet práce. In M. Švec, & M. Bulla (Eds.), *Práca 4.0, digitálna spoločnosť a pracovné právo* (pp. 9-18). Friedrich Ebert Stiftung.
- Cîmpan, I., Crișan, E., Alanță, I., & Mihăilă, A. (2022). Digital platforms business models. *Review of International Comparative Management*, 23(5), 612-629. <https://www.rmci.ase.ro/no23vol5/04.pdf>
- DaSilva, C. M., & Trkman, P. (2014). Business model: What it is and what it is not. *Long Range Planning*, 46(1), 379-389. <https://doi.org/10.1016/j.lrp.2013.08.004>
- Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce") (2000). <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031>
- European Parliament. (n.d.). *Report on the European agenda for the collaborative economy*. <https://digital-strategy.ec.europa.eu/sk/policies/desi-slovakia>
- Felson, M., & Spaethem, J. L. (1978). Community structure and collaborative consumption: A routine activity approach. *American Behavioral Scientist*, 21(4), 614-620. <https://doi.org/10.1177/000276427802100411>
- Geist, R. (2023). Sociálne siete musia od dnes dodržiavať európske pravidlá. <https://euractiv.sk/section/digitalizacia/news/socialne-siete-musia-od-dnes-dodrziavat-europske-pravidla/>
- Hudecová, I., Cyprichová, A., Makatura, I., Pčolová, B., Jarottová Bujňáková, B., Mičura, J., & Mizák, V. (2020). *Nariadenie o ochrane fyzických osôb pri spracúvaní osobných údajov/ GDPR* (2nd ed.). Eurokódex.
- Kangas, P., Toivonen, S., & Bäck, A. (2007). "Ads by Google" and other social media business models. VTT Technical Research Centre of Finland. <https://publications.vtt.fi/pdf/tiedotteet/2007/T2384.pdf>
- Kim, J., Kim, T., Wojdyski, B., & Jun, H. (2022). Getting a little too personal? Positive and negative effects of personalized advertising on online multitaskers. *Telematics and Informatics*, 71, 101831. <https://doi.org/10.1016/j.tele.2022.101831>
- Laclavíková, M., & Olšovská, A. (2018). Človek a technika: Právno-historické východiská. In H. Barancová, & A. Olšovská (Eds.), *Priemysel 4.0 a pracovné podmienky* (pp. 84-98). Leges.
- Mendoza, C. (2022). The age of surveillance capitalism: The fight for a human future at the new frontier of power: by Shoshana Zuboff, New York, Public Affairs, 2019, 704 pp., €20.00, ISBN 978-1610395694. *Church, Communication and Culture*, 7(2), 452-455. <https://doi.org/10.1080/23753234.2022.2086891>
- ICF, Grimaldi Studio Legale, & 21c Consultancy. (2018). *Overview of the legal framework of notice-and-action procedures in member states SMART 2016/0039: Final report*. Publication office of the European Union. <https://op.europa.eu/en/publication-detail/-/publication/a56ceb47-2446-11e9-8d04-01aa75ed71a1>

- Pacalajová, N., & Kubinec, M. (2021). Statutory bar on the right to exercise a mortgage under the conditions applicable in the Slovak Republic and comparison with the legal regulation of the Czech Republic. *Danube: Law, Economics and Social Issues Review*, 12(3), 224-238. <https://doi.org/10.2478/danb-2021-0015>
- Parker, G. G., Van Alstyne, M. W., & Choudary, S. P. (2016). *Platform revolution: How networked markets are transforming the economy – and how to make them work for you*. Norton & Company.
- Rak, P., & Raková, K. (2021). Sociálne médiá a pracovisko. In *Sociální dilema 2021: Nové přístupy k managementu znalostí a ochraně na internetu* (pp. 7-14). Právní institut.
- 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, repealing directive 95/46/EC (General data protection regulation) (2018). <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>
- 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) (2022). <http://data.europa.eu/eli/reg/2022/2065/oj>
- Strowel, A., & Vergote, W. (2017). *Digital platforms: To regulate or not to regulate?* https://ec.europa.eu/information_society/newsroom/image/document/2016-7/uclouvain_et_universit_saint_louis_14044.pdf
- Švec, M., & Žul'ová, J. (2018). *GDPR a ochrana záujmov zamestnanca*. Friedrich Ebert Stiftung.
- Valentová, T., Birnstein, M., & Golais, J. (2018). *GDPR / Všeobecné nariadenie o ochrane osobných údajov. Zákon o ochrane osobných údajov*. Wolters Kluwer.
- Vojtko, J. (2017). Automatizované rozhodovanie a profilovanie v pracovnoprávných vzťahoch podľa Všeobecného nariadenia o ochrane údajov. *Časopis pro právní vědu a praxi*, 25(2), 255-274. <https://doi.org/10.5817/CPVP2017-2-5>
- Zákon č. 18/2018 Z. z. o ochrane osobných údajov (2022). <https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/18/>
- Zákon č. 22/2004 Z. z. o elektronickom obchode (2004). <https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2004/22/>
- Zákon č. 442/2012 Z. z. o medzinárodnej pomoci a spolupráci pri správe daní (2012). <https://www.slov-lex.sk/vyhľadavanie-pravnych-predpisov?text=442%2F2012>
- Zákon č. 264/2022 Z. z. o mediálnych službách (2022). <https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2022/264/20220801.html>
- Žul'ová, J. (2021). Používanie umelej inteligencie pri výbere zamestnancov z perspektívy GDPR. *Justičná revue : Časopis pre právnú teóriu a prax*, 73(1), 30-39.
- Zutshi, A., Rizvanović, B., & Nodehi, T. (2019). The evolution of digital platforms. In A. K. Shrivastava, S. Rana, A. K. Mohapatra, & M. Ram (Eds.), *Advances in management research* (pp. 47-57). Routledge.

Authors



Assoc. Prof. JUDr. Marek Švec, PhD., LL.M.

Matej Bel University in Banská Bystrica
Faculty of Law
Komenského 20,
974 01 Banská Bystrica
SLOVAK REPUBLIC
msvec@umb.sk
ORCID ID: 0000-0001-6483-0722

Marek Švec works as a university professor the Faculty of Law of the Matej Bel University in Banská Bystrica. He is the author and co-author of a large number of scientific papers in the field of labour law and personnel management, as well as personal data protection. He is a Secretary of the Scientific Board of Wolters Kluwer SR, s. r. o., for labour law. He is also the senior counsel of the labour issues portal www.pracovnepravo.sk. One of his functions is that of secretary of the Scientific Council of Wolters Kluwer publishing house in the field of labour law. He is a member of the Scientific Council of the School of Law of Matej Bel University in Banská Bystrica and the School of Mass Media Communication of UCM in Trnava. Mr. Švec is a lawyer and also holds a position of the Secretary General of the Board of the Labor Law Association.

PhDr. Adam Madleňák, PhD., MBA

University of Ss. Cyril and Methodius in Trnava
Faculty of Mass Media Communication
Námestie J. Herdu 2,
Trnava, 917 01,
SLOVAK REPUBLIC
adam.madlenak@ucm.sk
ORCID ID: 0000-0001-5634-7263



Adam Madleňák works as a lecturer at the Faculty of Mass Media Communication of the University of Ss. Cyril and Methodius in Trnava. In his scientific activities, he focuses mainly on the area of project and innovation management in small and medium-sized enterprises and human resources management, in particular the integration of communication tools to raise the awareness of products and services of business entities at the international level. He is a Vice President of the Occupational Safety and Health Independent Institute and Secretary of the Scientific Board of Wolters Kluwer for Marketing Communications.



PhDr. Vladimíra Hladíková, PhD., MBA

University of Ss. Cyril and Methodius in Trnava
Faculty of Mass Media Communication
Námestie J. Herdu 2,
Trnava, 917 01,
SLOVAK REPUBLIC
vladimira.hladikova@ucm.sk
ORCID ID: 0000-0001-6676-5450

Vladimíra Hladíková works as an Assistant Professor at the Faculty of Mass Media Communication at the University of Ss. Cyril and Methodius in Trnava. Within her scientific activities, she focuses her interest on the issue of new and digital media, especially the Internet and its impact on various areas of life, education, and human thinking, as well as cognitive changes and other processes brought about by the medium of the Internet. She also focuses on reflecting the impact and use of information and communication technologies in education or the information and education society. The author also examines the various aspects of the Internet, its benefits, and, in particular, the threats it poses and the opportunities for active protection against them. She is a member of the editorial board of the European Journal of Media, Art and Photography, Media Literacy and Academic Research Journal and she has also participated in several scientific projects in the field of digital communication and media.

Mgr. Peter Mészáros, PhD.

University of Trnava in Trnava
Faculty of Law
Hornopotočná 23,
918 43 Trnava
SLOVAK REPUBLIC
peter.meszaros@truni.sk
ORCID ID: 0000-0003-3870-4188



Peter Mészáros works as an assistant professor at the Department of Civil and Commercial Law of the Faculty of Law of the University of Trnava. He also obtained his PhD at this faculty, his dissertation being “Protection of the weaker party in private law” in the area of Private Law in 2014. In his pedagogical, scientific and lecturing activities, he primarily deals with private law – civil law, commercial law, consumer law, labour law, family law and partially also public law, in particular civil procedural law. He is a member of the editorial boards of several foreign periodicals. His research focuses on issues mentioned above at the national as well as international level.