Acta Univ. Sapientiae, Legal Studies, **12**, 2 (2023) 19–35

DOI: 10.47745/AUSLEG.2023.12.2.02

The New Liability Forms of Online Platforms in the New European Digital Legal Framework from the Consumers' Perspective[1]

Zsolt HAJNAL

PhD, Associate Professor
University of Debrecen, Faculty of Law (Debrecen, Hungary)
János Bolyai Research Scholarship Holder
e-mail: hajnal.zsolt@law.unideb.hu

Abstract. The aim of the European legislator by the adoption of the Digital Services Act and Digital Markets Act was to ensure effective action to protect and improve the functioning of the internal market so that intermediary service providers address illegal content, online information, and other named societal risks with due diligence requirements. The aim of this study is to present the new rules on the liability of intermediary service providers under the DSA. I would like to illustrate the wide-ranging regulation of the liability of intermediary service providers and the case law of the ECJ and Member States through the example of online platforms and online marketplaces selected from a wide range of intermediary services, through the light and the expectation of a high level of consumer protection.

Keywords: consumer law, EU, digital services, illegal content, intermediary service provider

1. Introduction

In addition to the EU Treaties, the E-Commerce Directive, adopted in 2000,[2] formed the core of the regulatory framework for information society services, ensuring access to digital services in the internal market and laying down basic obligations for service providers. Since then, digitalization has also been a hallmark of

1 This study was made possible by the support of János Bolyai Researcher's Scholarship of the Hungarian Academy of Sciences.

2 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, OJ L 178, 17.7.2000, 1–16, transposed into Hungarian law through Act No. CVIII of 2001 on Certain Issues of Electronic Commerce Services and Information Society Services.

change in European and global trade and consumer society. Digitalization has become part of our everyday lives, changing our shopping habits, creating new forms of shopping, new types of products and, at the same time, posing new risks and new challenges for consumers, enforcers, and legislators alike. New innovative business models and services have enabled consumers to interact, share information, and engage in transactions with traders at a distance and across borders, using digital communication tools.

In response to market challenges, the European Commission was able to embark on a second review of the consumer acquis following the adoption of the Consumer Rights Directive and the rejection of the *Common European Sales Law* proposal.[3] The European Commission's 2015 Communication *A Digital Single Market Strategy for Europe* envisaged laying the foundations for the Digital Single Market.[4] In order for Member States to make better use of the opportunities offered by digitalization, it will be necessary to create Europe's digital single market.[5] The European Commission understands the Digital Single Market as a market in which the free movement of goods, persons, services, and capital is ensured and where individuals and businesses can go online without barriers, in full compliance with consumer and data protection rules and under conditions of fair competition. In its[6] strategy *Shaping Europe's Digital Future*, published in 2020,[7] the Commission aims to strengthen and modernize the rules applicable to digital services across the EU, clarify the role and responsibility of online platforms, and to fight the dissemination of illegal content. Finally, Regulation 2022/2065 of the European Parliament and of the Council on Digital Services (hereinafter referred as DSA) and Regulation 2022/1925 of the European Parliament and of the Council on Digital Markets (hereinafter referred as DMA) were adopted in autumn 2022 and have been applicable since 17 February 2024. The aim of the European legislator was to ensure coherent and effective action to protect and improve the functioning of the internal market so that providers of intermediary services address illegal content, online information, and other named societal risks with due diligence requirements. One of the fundamental objectives of the DSA is to ensure that what is illegal in the offline world is also considered illegal in the online world.

The aim of the study is to present the new rules on the liability of intermediary service providers under the DSA from the perspective of the consumer law. In the

3 European Commission 2011.

4 European Commission 2015.

5 According to the Commission, 'The Digital Single Market is a market where the free movement of goods, persons, services and capital is ensured and where individuals and businesses can go online without barriers, in full compliance with consumer and data protection rules and under conditions of fair competition. By completing the Digital Single Market, Europe can maintain its leading position in the digital economy, helping European businesses grow globally.' Digital Single Market Strategy. 1.

6 Angyal 2020. 6.

7 European Commission 2020b (*Europe's Digital Future Strategy*).

course of the research, I would like to illustrate the wide-ranging regulation of the liability of intermediary service providers and the case law of the European Court of Justice and Member States through the example of online platforms and online marketplaces selected from a wide range of intermediary services.

2. The Personal Scope of the DSA: Various Types of Intermediary Service Providers

2.1. Intermediary Service Providers

The DSA applies to certain information society service providers that provide services for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. The DSA generally applies to intermediary service providers, which refers to a wide range of digital market players that are categorized by the DSA as providers of 'mere conduit' services (e.g. Internet service providers), 'caching' services (e.g. content distribution networks that store data for a limited period of time only), or hosting services (e.g. cloud or web hosting) according to the types of services they provide.

In addition to the above, within the category of hosting service providers, the DSA specifically mentions online platforms (such as social networks, online marketplaces, app stores, and online travel and accommodation websites), very large online platforms (with more than 45 million monthly active users in the EU and designated as such by the Commission) ('VLOPs'), and very large online search engines (with more than 45 million monthly active users in the EU and designated as such by the Commission) ('VLOSEs').

2.2. Online Platforms

Online platforms are therefore defined as hosting service providers, meaning that the information provided by recipients of the service is not only stored at the request of the recipients but is also publicly disseminated at the request of users.

According to point (24) of the DSA recital, a website may be classified as an online platform if it effectuates dissemination of information to the public not merely as a negligible minor ancillary function of the main service. Under the DSA, the storage of comments in the case of a social network should be considered to be an online platform service if it is clear that it is not a minor element of the service offered, while a cloud service or Internet hosting service should not be considered an online platform where the public dissemination of certain information constitutes a minor and ancillary element or a smaller functionality of such services. In its study, the European Parliamentary Research

Service defines online platforms as *entities that offer digital services to users, operate or can operate as business models in bilateral or multilateral markets, and allow for general facilitation of interaction between different market players, even if there is no direct interaction between them.*[8]

2.3. Online Marketplaces

The DSA has created a specific subcategory within online platforms for online platform providers that allow consumers to conclude distance contracts with traders. This definition corresponds to the concept of online marketplace in the Omnibus Directive[9] and to the category used *as an online marketplace* in the literature. The Omnibus Directive also included online marketplaces in its scope by amending the Consumer Rights Directive, defined as services that use software, including a website, part of a website, or an application, operated by or on behalf of a trader, which allows consumers to conclude distance contracts with other traders or consumers. The OECD defines online marketplaces as digital platforms that bring together buyers of consumer goods and third-party sellers and facilitate the performance of such contracts.[10]

3. The Colourful Regulatory Framework of Intermediary Service Providers

In addition to the DSA and DMA regulations, intermediary service providers and online platforms are also subject to several European and domestic laws, which are complemented by sectoral *soft law* rules, national and European court case law, agreements between market players and governments, and self-regulatory solutions. Due to the specificities of regulation, divergent national jurisprudence, and the nature of legislation requiring minimum harmonization, regulation had been characterized by fragmentation. As a consequence, operators were often forced to take into account the needs and expectations of several different legal systems when carrying out their cross-border activities covering several countries or regions, which constitute obstacles to the free movement of goods and services in the internal market.[11]

8 European Parliamentary Research Service 2021. 11.

9 Directive 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernization of Union consumer protection rules, OJ L 328, 18.12.2019, 7–28.

10 OECD 2022. 6.

11 European Commission 2020a. 23–25.

The current EU framework can be grouped mostly according to their substantial scope and the values to be protected:

Its legal regulation is based on the E-Commerce Directive, which regulates the basic conditions for the provision of all information society services, which established limited liability of the provider of information society services (*safe harbour rule*), as well as obligations to cooperate and take action, allowing the extension of online commerce. It also includes technology-specific rules for distance contracts concluded through webshops.

Media regulation is covered by provisions in the Audiovisual Media Services Directive (hereinafter referred as AVMSD).[12] Directive 2018/1808 amended and extended the Audiovisual Media Services Directive to video-sharing platforms as part of the Digital Single Market strategy and to audiovisual content shared through certain social media services. While the AVMSD includes video-sharing platforms in its scope, extending the scope of provisions ensuring the protection of minors and prohibiting content inciting hatred and violence, it also takes into account the limited ability of video-sharing platforms to monitor advertising that they do not sell or publish.

Basic rules on the liability of online content-sharing service providers to combat online piracy and infringements of copyright and intellectual property rights are included, inter alia, in the Directive on Copyright in the Digital Single Market,[13] which is accompanied by additional self-regulatory tools on the sale of counterfeit goods and online advertising and intellectual property.[14]

The Directive on combating the sexual abuse and exploitation of children and child pornography as regards the protection of children[15] imposes general obligations on Member States, without imposing specific obligations on online

12 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), OJ L 95, 15.4.2010, 1–24. It is transposed into Hungarian law through Act No. XXIV of 2020 among the provisions of the Act on Electronic Commerce.

13 Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending directives 96/9/EC and 2001/29/EC, OJ L 130, 17.5.2019, 92–125; Regulation (EU) 2017/1128 of the European Parliament and of the Council of 14 June 2017 on the cross-border portability of online content services in the internal market, OJ L 168, 30.6.2017, 1–11 ('The Portability Regulation'); Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society, OJ L 167, 22.6.2001, 10–19.

14 Memorandum of understanding on online advertising and intellectual property. https://ec.europa.eu/docsroom/documents/30226/attachments/1/translations/en/renditions/native (accessed: 15.11.2023); Memorandum of understanding on the sale of counterfeit goods on the Internet, https://ec.europa.eu/docsroom/documents/43321/attachments/2/translations/en/renditions/native (accessed: 15.11.2023).

15 Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, OJ L 335, 2011.12.17, 1–14.

platforms, whereas the AVMS Directive imposes such obligations on video-sharing platforms.

Council Framework Decision imposing obligations on Member States as a basis for tackling hate speech online,[16] and the Audiovisual Media Services Directive, which imposes specific obligations on online video-sharing platforms, complemented by a code of conduct.[17]

With regard to the new European product safety legislation, providers of online marketplaces have become obliged in the fight against unsafe products. If they can be considered the manufacturer or importer of a defective product (e.g. Amazon in connection with its own Kindle branded e-book reader), they can also claim damage caused by the defective product under the Product Liability Policy.[18] Although the EU Market Surveillance Regulation[19] did not previously contain explicit rules for online platforms, the new General Product Safety Regulation adopted on 10 May 2023[20] also establishes liability and obligations for businesses operating online marketplaces in relation to product safety in line with the DSA Regulation.

Regulation (EU) 2019/1150 of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services applies to platform-to-business contractual relationships (P2B),[21] which sets minimum standards to ensure that online platforms treat business users in a fair and transparent manner. The legislation is based on the recognition that in the future the SME sector will not conduct its online activities through webshops but through online marketplaces, so without minimum guarantee standards they would easily find themselves in a vulnerable and dependent situation.

Legal relations between consumers and businesses (B2C) are governed by the general European and national consumer protection private law and procedural

16 Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law, OJ L 328, 2008.12.6.

17 Code of conduct on countering illegal hate speech online. https://commission.europa.eu/document/download/551c44da-baae-4692-9e7d-52d20c04e0e2_hu (accessed: 15.11.2023).

18 Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products, OJ L 210, 7.8.1985, 29–33.

19 Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and regulations (EC) No. 765/2008 and (EU) No. 305/2011, OJ L 169, 25.6.2019, 1–44.

20 Regulation (EU) of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No. 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and of the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC, OJ L 135, 23.5.2023, 1–51.

21 OJ L 186, 2019.7.11, 57–79.

law. We apply the rules of the UCPD to commercial communications of businesses[22] to consumers and the Consumer Rights Directive and the E-Commerce Directive[23] to business-to-consumer contracts.

Legal relations between consumer and consumer (C2C) shall be governed by the private law rules of the Member State.

4. Challenges Faced by Consumer Law before the DSA According to the Online Platforms

4.1. Qualification of the Parties

One of the characteristics of online platforms is that they can connect businesses and consumers in all possible relationships and facilitate their transactions, so we can talk about business-to-business (B2B), consumer-to-consumer (C2C), and consumer-to-business transactions as well. The consumer protection approach is only relevant in a consumer-to-business relationship, so the qualification of the parties is inevitable. The ECJ has elaborate case law on consumer qualification, many of which have examined attributes of consumers operating specifically online. In Case C-774/19 *Personal Exchange International Limited*,[24] the company sought to ensure that the professional knowledge of an online poker player earning regular income was not used to ensure that they could not be considered as a weaker party, a consumer. In its judgment,[25] the ECJ interpreted, in Article 15(1) of Regulation No 44/2001 (former Brussels I Regulation), that it is not the purpose of the regulation to determine the jurisdiction in relation to a poker game based on the invested money, which includes the chance of winning and the risk of losing. In its judgment C-498/16 *Schrems*,[26] the ECJ concluded that a private Facebook account user does not lose its status as a 'consumer' if it publishes and sells books, lectures – even for remuneration –, runs websites, collects donations, and helps consumers to enforce their rights and organize themselves. In the

22 Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No. 2006/2004 of the European Parliament and of the Council, OJ L 149, 11.6.2005, 22–39.

23 Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, OJ L 304, 22.11.2011, 64–88.

24 C-774/19. *A. B. and B. B. v Personal Exchange International Limited*, ECLI:EU:C:2020:1015.

25 Council Regulation (EC) No. 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, OJ L 12, 16.1.2001, 1–23.

26 C-498/16. *Maximilian Schrems v Facebook Ireland Limited*, ECLI:EU:C:2018:37.

Kamenova[27] case, moreover, in relation to the qualification as a trader of a user who simultaneously publishes eight advertisements on an online platform, the ECJ defined non-exhaustively the criteria that can be determined to be a trader on a case-by-case basis.

European jurisprudence abounds in relation to consumers, while there are fewer decisions on qualification as traders. The main problem in the digital market is that, for example, online marketplaces can connect all types of buyers and sellers, while classifying sellers as businesses is based on voluntary declarations without any other legal obligation. This also means, of course, that online marketplaces are suitable for sellers to run commercial economic activity without becoming entrepreneurs. All these transactions are thus falling out of the scope of consumer law. According to Article 6a(1) of the Omnibus Directive, online platforms are merely obliged to ensure that the quality of the seller can be identified, as well as information on the allocation of responsibilities between the platform and the trader and on the non-applicability of consumer protection rules if the seller is not acting in their capacity as trader, on the basis of voluntary information provided by third parties. However, they are not obliged to examine the entrepreneurial capacity of a seller registered as a consumer in the light of the number of products sold and their annual turnover.

The US legislature's INFORM Act could have served as a good example for the European legislator regarding the standardization of trader certification. Under the INFORM Consumer Act, online marketplaces are required to comply with the law's information collection and verification, data security, and reporting requirements for high-volume third party sellers on their platforms. High-volume third-party sellers are third-party sellers who have sold new or unused consumer goods in at least 200 separate transactions in any consecutive 12 months over throughout the previous 24 months and have generated a total gross proceeds of at least $5,000. The disclosure requirements of the Act apply only to high-volume third-party sellers who have at least $20,000 in annual gross revenue through the marketplace.

4.2. The Lack of Effective Consumer Redress

In addition to ensuring the full extent of consumers' substantive rights, the European Union protects consumers' rights by operating public and private enforcement systems that provide consumers with effective access to justice within the European Union. Thanks to digitalization, European consumers can conclude contracts with virtually any business in the world and, thanks to European private international rules, the non-derogating consumer protection provisions of the consumer's country of habitual residence and the jurisdiction

27 C-105/17. *Komisia za zashtita na potrebitelite v Evelina Kamenova*, ECLI:EU:C:2018:808.

of the court of the consumer's place of residence remain applicable despite the parties' differing provision, but this alone is still not sufficient to ensure effective legal protection. Consumers and national authorities cannot effectively deal with third-country businesses in the absence of European contact points, responsible persons to prosecute. Not to mention the strategically not negligible situation where data assets originating in Europe are not stored under European legislation, over which the European Union is keen to regain control.[28]

4.3. The Limits of the Liability of Intermediary Service Providers in the Case Law of the ECJ and National Courts

In addition to the practical difficulties of enforcing consumer rights, courts also had to confront the *safe harbour* principle,[29] which enshrines the relative absence of liability of intermediary service providers. Articles 14 to 15 of the E-Commerce Directive created an exemption from liability for intermediary service providers, which, however, is only available to undertakings that play a passive role. Over the past 20 years, national courts have increasingly sought to differentiate the safe harbour principle for online marketplaces, which exempts them from liability.

On 30 June 2008, the Commercial Court of Paris jointly ordered the American company eBay Inc. and its subsidiary eBay International AG to pay nearly EUR 40 million to the companies of the luxury group Moët Hennessy Louis Vuitton SA (LVMH Group) for failing to prevent the sale of counterfeit goods and for violating the applicants' selective distribution system.[30] Although the principle of exemption from liability of Internet hosting service providers is enshrined in the French legislation, which is in line with European rules, the Court clarified the role of eBay in the legal relationships and in the commercial chain. According to the ruling, eBay not only provided the hosting service but also actively participated in the transactions as an intermediary, facilitating them and collecting commissions on each sale. In view of this, the Court held that eBay companies can be regarded as intermediaries and cannot claim to be providers of special Internet hosting. In the *Louis Vuitton Malletier and Christian Dior Couture v eBay* cases, the Court held that activities on websites operated by eBay facilitated and intensified the marketing of illegal goods and, by allowing it, eBay failed to fulfil its obligations to trademark owners. The defendant's defence that it was not responsible for illegal content posted on others' pages was also not accepted by the Court because eBay did not exercise reasonable care and diligence in allowing the sale of goods advertised as 'false or counterfeit' in an easily identifiable manner.

28 Tóth 2011. 28.
29 Liber 2013. 12.
30 Commercial Court of Paris, General docket No: 200607799 (English translation).

The rulings stand in stark contrast to the New York Federal Court's ruling in *Tiffany v eBay*.[31] The Court dismissed the charges against eBay, finding that it had taken appropriate measures to prevent infringement and finding that the rightsholders were required to inspect their trademarks. According to its judgment, eBay admitted that it was generally aware that counterfeit Tiffany products were being listed and sold through its website, but that general knowledge was not sufficient to establish liability.

With regard to the active role of the online marketplace, the ECJ ruled in *Case C-324/09 L'Oréal SA v eBay International AG*[32] that that exemption applies to the operator of an online marketplace if the latter has not played an active role through which it knew or processed the stored data. An active role should be considered to occur where the operator of the online marketplace provides assistance consisting in particular in optimizing or facilitating the presentation of the offers for sale in question.[33]

With regard to the assignment of liability for online marketplaces, the L'Oréal case can be seen as a continuation of the ECJ jurisprudence of the C-148/21 and C-184/21 cases. In *Louboutin v Amazon Europe Core Sàrl and Others*,[34] an operator of an online marketplace was liable for selling counterfeit goods considering the identical character of the related goods from the point of view of a normally informed and reasonably observant user having regard to all the circumstances of the particular situation.

Although this is not a judgment specifically related to the liability of online marketplaces, we can see the possibility of extending the concept of seller to an intermediary in Case C-149/15 of the ECJ, *Sabrina Wathelet v Garage Bietheres & Fils SPRL*,[35] where the ECJ extended the concept of seller within the meaning of Article 1(2)(c) of Directive 1999/44/EC to include a seller or supplier acting as an intermediary in the name and on behalf of a private person who has not adequately informed the consumer-purchaser of the fact that the owner of the consumer goods sold is a private person.

31 *Tiffany v eBay Inc.*, 2010 WL 3733894.
32 C-324/09. *L'Oréal SA v eBay International AG*, ECLI:EU:C:2011:474.
33 Liber 2013. 25–26.
34 Joined Cases C-148/21, C-184/21. *Louboutin v Amazon Europe Core Sàrl*, ECLI:EU:C:2022:1016.
35 C-149/15. *Sabrina Wathelet v a Garage Bietheres & Fils SPRL*, ECLI:EU:C:2016:840.

5. Liability of Intermediary Service Providers under the DSA

5.1. The General System of Liability

The DSA lays down harmonized rules for the provision of intermediary services in the internal market, in particular the framework for the exemption from liability of intermediary service providers, due diligence obligations for providers of intermediary services, and rules on enforcement.

Chapter II of the DSA lays down rules on the liability of providers of intermediary services for content disseminated online by third parties. Prior to the DSA, the liability of online service providers was regulated at the EU level by articles 12–15 of the E-Commerce Directive, making the safe harbour principle of intermediary service providers an industry dogma. This regulatory principle agreed in this economic sector is maintained by the DSA, with only minor clarifications ensuring uniform application in all Member States.

The new duties of care are defined in Chapter III of the Regulation by specific types of intermediary service providers, with minimum obligations for providers of intermediary services, while online and large platforms' legal obligations enlarged. In section 1, obligations on all intermediaries, in section 2 obligations on hosting services, in section 3 obligations on online platforms, in section 4 rules on online platforms enabling the conclusion of distance contracts between consumers and traders, in section 5 rules on very large online platforms or very popular online search engines, and in section 6 other provisions on duties of care (e.g. Code of Conduct) can be found.

The minimum core of the obligation that should be guaranteed by all four nominated types of intermediary service providers are transparency reporting (Art 15 DSA), cooperation with Member State authorities (Art. 9–10), contact points or obligatory representative (Art. 11–13), and terms of services based on the respect of fundamental rights (Art. 14). Online platforms are required to ensure notice and action mechanisms, duties to inform consumers (Art 16–17), to report crimes (Art. 18), redress and ADR mechanisms (Art. 20–21), trusted flaggers (Art 22), anti-abuse measures and protection (Art. 23), protection of minors, and different kinds of transparency requirements that must be ensured (art-s 26–27).[36]

5.2. Escape from Liability and the Safe Harbour Principle

As before, the DSA does not exhaustively and positively define when service providers are liable for online content published by third parties but sets out

36 Grad–Gyenge 2023.

the conditions for exemption from liability adapted to different categories of intermediary service providers. Although there is no general monitoring obligation on providers of intermediary services, the DSA provides in addition detailed rules on notice-and-action mechanisms to be established by hosting service providers, which should be read in conjunction with liability exemptions (the 'Good Samaritan principle').

Like the E-Commerce Directive, the DSA exempts providers of intermediary services from liability for illegal content disseminated online.[37]

The new liability regime under the DSA maintains a distinction between mere transmission, caching and hosting service providers, which are subject to different liability exemptions:

Mere conduit service providers are not liable for the information transmitted or viewed under Article 4 of the DSA if the service provider does not initiate the transmission, select the recipient of the transmission, or choose or modify the information transmitted.[38]

A caching service provider is not liable under Article 5 of the DSA for the automatic, intermediate, or transient storage of information for the sole purpose of making the subsequent transmission of the information to other recipients of the service more efficient or secure at their request, provided that the provider does not modify the information. It also complies with the conditions relating to access to the information, with rules widely recognized and applied by industry for updating information, it does not prevent the lawful use of technology widely accepted and used in industry to obtain data on the use of information, and it takes immediate action to erase or disable access to stored information as soon as it becomes aware that information has been removed from the network or access to it has been disabled at the source of the transmission or that a judicial or administrative authority has ordered such erasure or disabling of access.[39]

According to the rules on the liability of hosting service providers set out in Article 6 of the DSA, service providers are only liable for illegal content hosted on their servers *if they have actual knowledge* of illegal activity or illegal content, or of facts or circumstances indicating manifest illegal activity or illegal content; or fail to take expeditious action to remove or transfer illegal content termination of access after becoming so aware. However, the fact that a service may generally be used to host illegal content should not be considered to be actually aware of illegal content by a hosting service provider. Furthermore, the mere indexing of information, the provision of a search function, or the recommendation of

37 Németh 2020. 188.
38 DSA recital (21).
39 Ibid.

information is not sufficient to assume that providers have 'specific' knowledge of illegal activities on their platforms or of illegal content hosted on them.[40]

In line with the case law of the ECJ cited earlier,[41] the DSA provides for an exception to the liability exemption where an online platform acting as an intermediary misleadingly offers a product or service for sale in such a way that the average consumer may believe that the subject matter of the transaction is provided by the online platform itself or by a third party acting under the control of the provider.[42]

5.3. Illegal Content

Illegal content is defined in general framework in Article 2(h) of the DSA and recital (12) but refers to content considered illegal under other EU or Member State law. Against this background, the broad concept of illegality includes breaches of numerous information obligations stemming from EU and national consumer law, misleading information[43] about products or services,[44] fraudulent characterization of traders as consumers (to avoid consumers exercising their consumer rights),[45] and the sale of unsafe products. For example, the definition of illegal content includes hate speech or terrorist content or may be related to illegal activities such as sharing images of child pornography or infringing protected intellectual property rights.[46]

5.4. Notification and Action Mechanisms

The DSA has established a system with multiple levels of duty of care to ensure that action against illegal content in order to derogate the level of liability

40 DSA recital (22).

41 C-149/15. *Sabrina Wathelet v a Garage Bietheres & Fils SPRL*, ECLI:EU:C:2016:840.

42 DSA Article 6(3).

43 For example, information obligations under Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council ('Consumer Rights Directive'), OJ L 304, 22.11.2011, 64–88.

44 Misleading commercial practices within the meaning of Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC, and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), OJ L 149, 11.6.2005, pp. 22–39.

45 Under Article 6a(b) of the Consumer Rights Directive, when concluding a contract on an online marketplace, the marketplace's provider is obliged to inform the consumer whether their contractual partner qualifies as a trader.

46 Tóth 2022. 47.

immunity doctrine. One of the cornerstones of the system's operation is how the hosting service provider becomes aware of illegal content. Here are some possible ways to do this:

(1) carrying out voluntary monitoring;

(2) setting up reporting mechanisms;

(3) establishing a special status for trusted flaggers.

The DSA explicitly states that providers of intermediary services have no obligation to monitor the information transmitted or stored and that providers are not obliged to actively seek indications of illegal activity or take proactive measures in relation to illegal content. By regulating the *Good Samaritan principle*, DSA addresses the dilemma of losing liability immunity to hosting service providers who discover illegal content on their sites as a result of voluntary monitoring. Under Article 7 of the DSA, providers of intermediary services therefore do not lose their liability immunity when they voluntarily investigate on their own initiative or take other measures to detect, identify, and remove illegal content or disable access to it.

Article 16(1) of the DSA creates an obligation for hosting service providers (including online platforms, and thus online marketplaces) to provide notice. This should be understood as mechanisms that allow individuals and organizations to report content that they consider illegal. The obligations related to processing notices, informing the notifier, and classifying the content concerned by the notification as illegal are specified in detail in the DSA.

The DSA establishes a special status for trusted flaggers, which mainly consists in the fact that their referrals should be prioritized by hosting service providers and processed without undue delay.

According to the DSA, although there is no obligation for an online platform to monitor content automatically, as previously explained, there may still be cases where due diligence includes detecting illegal content on the platform. The new General Product Safety Regulation specifically regulates the liability of companies operating online marketplaces. According to § 22 (6) of the *Product Safety Regulation*, service providers operating online marketplaces must take into account the information on dangerous products communicated through the Safety Gate portal of the market surveillance authority in order to voluntarily implement measures. That obligation should apply not only to detecting, identifying, and removing illegal content but also to cooperating with market surveillance authorities through the system.

5.5. Consumer Information about Illegal Content

Action and notification mechanisms alone would not have the necessary effect without promptly informing consumers about illegal content. According to Article 32 of the DSA, where the provider of an online platform becomes aware

that an illegal product or service has been offered by a trader to consumers located in the EU through its services, it is obliged to inform consumers who purchased the product or used the service in the last six months that:

(1) the product or service is illegal,

(2) the identity of the trader, and

(3) any relevant means of redress.

Failure to comply with this obligation may prevent the consumer from asserting their rights against the trader and may also cause harm and damage to consumers, which may also lead to liability for damages by the platform provider. According to *Rott*,[47] the consumer would have to prove not only misconduct but also that they could have obtained a remedy if they had been informed in accordance with Article 32 and that that opportunity was lost as a result of the lack or delay in providing information, for example because the trader had become insolvent or unavailable.

5.6. Relations with the European Commission and National Authorities

All intermediary service providers will be obliged to designate a single point of contact in order to establish effective, rapid, and direct communication among service providers, the European Commission, and national authorities. Similarly, they should designate a contact point enabling them to communicate effectively and directly with recipients of the service, including the selling trader as well as the consumer buyer. It is important that recipients of the service should be able to choose means of communication which are not based solely on automated means.

6. Concluding Remarks

With the Digital Markets Regulation, the legislator has set itself no less objective than to ensure that everything that is prohibited in an offline environment should also be prohibited in an online environment. The indisputable merit of the regulation is that it simultaneously leaves intact the liability principles that define digital markets and incorporates the European Court of Justice's interpretation of the law on digital markets, while at the same time imposing countless duties of care on intermediary service providers of different volumes. Although there is no progressive change of direction regarding the allocation of liability, the European legislator has developed a regulatory ecosystem with a sequential system of duty of care in which both public authorities and market participants can take effective action against illegal content placed and transmitted on the digital market.

47 Rott 2022. Sections 45–46.

References

ANGYAL, Z. 2020. Úton a digitalis egységes piac felé. *Miskolci Jogi Szemle* 15(3[Special Issue]): 5–13.

EUROPEAN COMMISSON 2011. *Proposal for a Regulation of the European Parliament and of the Council on a Common European Sales Law*. COM/2011/0635 Final – 2011/0284 (COD). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52011PC0635 (accessed: 15.11.2023).

2015. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Single Market Strategy for Europe*, COM(2015) 192 Final, 6.5.2015. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192 (accessed: 15.11.2023).

2020a. *Commission Staff Working Document Impact Assessment Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and Amending Directive 2000/31/EC*, SWD/2020/348 Final. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52020SC0348 (accessed: 15.11.2023).

2020b. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Shaping Europe's Digital Future*. COM(2020) 67 Final, 19.2.2020.

EUROPEAN PARLIAMENTARY RESEARCH SERVICE. 2021. *Liability of Online Platforms*. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/656318/EPRS_STU(2021)656318_EN.pdf (accessed: 15.11.2023).

GRAD-GYENGE, A. 2023. A tartalommegosztó platformszolgáltatók és más közvetítő szolgáltatók szerzői jogsértésekért való felelőssége a Digital Services Act tükrében. *In Medias Res* 2023/2: 25–44.

LIBER, Á. 2013. A közvetítő szolgáltatók felelőssége a szellemi tulajdon megsértéséért az Európai Unióban. *Iparjogvédelmi és Szerzői Jogi Szemle* 8[118](3): 5–42.

NÉMETH, Sz. 2020. *A közösségi oldalak szolgáltatóinak jogi felelőssége*. PhD dissertation. https://ajk.kre.hu/images/doc2021/doktori/Nemeth_Szabolcs_PhD_dolgozat_muhelyvitara_FINAL.pdf (accessed: 15.11.2023).

OECD 2022. The Role of Online Marketplaces in Protecting and Empowering Consumers. *Digital Economy Papers* 329: 1–52. https://doi.org/10.1787/9d8cc586-en.

ROTT, P. 2022. New Liability of Online Marketplaces Under the Digital Services Act? *European Review of Private Law* 2022/6: 1039–1058. https://doi.org/10.54648/erpl2022046.

SZALATKAY, J. 2023. Az online piacterek fogyasztóvédelmi felelőssége. In: *A hazai fogyasztóvédelmi jog áttekintése: alapok, kihívások, aktualitások*. Budapest.

TÓTH, A. 2011. The European Union's (Regulatory) Path towards Sovereignty in the Data-Based Economy. *European Review* 2011/2.

2022. Az online platformok európai szabályozása. *In Medias Res* 2022/2: 78–102.