# Online Intermediaries and Sustainable Market Regulation – a Smart Mix of Liability and Exemptions

by

Katarzyna Klafkowska-Waśniowska* and Katja Weckström**

**CONTENTS**



* Katarzyna Klafkowska-Waśniowska, Prof. UAM dr. hab., Faculty of Law and Administration of the Adam Mickiewicz University in Poznań (Poland); e-mail: kwasn@amu.edu.pl; ORCID: https://orcid.org/0000-0003-4164-979X.

** Katja Weckström, Prof. docent, UEF Law School, University of Eastern Finland (Finland); e-mail: katja.weckstrom@uef.fi; Research Gate: https://www.researchgate.net/profile/Katja-Weckstrom/research.

This paper was written as part of the FORK-project funded by the Academy of Finland and the University of Eastern Finland.

Edition of that article was financed under Agreement Nr RCN/SP/0324/2021/1 with funds from the Ministry of Education and Science, allocated to the "Rozwoj czasopism naukowych" programme.

Article received: 3 October 2023, accepted: 14 November 2023.

## *Abstract*

The Commission has advanced sustainable and responsible behaviour of business operators in the digital environment since the adoption of the Strategy for the Digital Single Market of 2015. The question remains, how can we reach the normative goal of ensuring a safe, secure and fair online environment, where fundamental rights are protected, and responsibilities of platforms, especially large players and gatekeepers, are well defined? A "smart mix" of mandatory and voluntary rules, in combination with industry self regulation, is applied to address business and fundamental rights. This paper asks how the Digital Services Act (DSA) answers the call for sustainable market regulation. Ideally, sustainable market regulation may respond to specific risks, and impose tailored duties for "diligent economic operators", without setting liability enhanced policy or enforcement targets for normal business activity.

The paper discusses what has changed in the approach adopted in the DSA; what is the role of intermediaries in the information flows online; and how this is linked to information and data, important from the perspective of energy consumption as a parallel sustainability goal. It analyses briefly the CJEU case law on balancing liability exemptions with fundamental rights, including the right to information and its impact on the interpretation of the DSA. The paper also considers how the DSA fosters the concept of diligence in the online environment, as well as consumer empowerment, as an important feature of sustainable market regulation.



## *Résumé*

Depuis l'adoption de la stratégie pour le marché unique numérique en 2015, la Commission encourage les opérateurs économiques à adopter un comportement durable et responsable dans l'environnement numérique. La question reste de savoir comment atteindre l'objectif normatif consistant à garantir un environnement en ligne sûr, sécurisé et équitable, où les droits fondamentaux sont protégés et où les responsabilités des plateformes, en particulier des grands acteurs et des gardiens, sont bien définies. Un «mélange intelligent» de règles obligatoires et volontaires, en combinaison avec l'autorégulation du secteur, est appliqué pour traiter la question des entreprises et des droits fondamentaux. Le présent article s'interroge sur la manière dont la loi sur les services numériques répond à l'appel en faveur d'une régulation durable du marché. Dans l'idéal, une réglementation durable du marché peut répondre à des risques spécifiques et imposer des obligations adaptées aux opérateurs économiques diligents, sans fixer d'objectifs de responsabilité, de politique ou de mise en œuvre renforcés pour l'activité commerciale normale. L'article examine ce qui a changé dans l'approche adoptée dans le DSA ; quel est le rôle des intermédiaires dans les flux d'informations en ligne ; et comment cela est lié à l'information et aux données, ce qui est important du point de vue de la consommation d'énergie en tant qu'objectif de durabilité parallèle. Il analyse brièvement la jurisprudence de la CJUE sur

l'équilibre entre les exemptions de responsabilité et les droits fondamentaux, y compris le droit à l'information, et son impact sur l'interprétation du DSA. Le document examine également la manière dont le DSA favorise le concept de diligence dans l'environnement en ligne, ainsi que l'autonomisation des consommateurs, en tant que caractéristique importante de la réglementation du marché durable.

**Key words:** digital single market; EU market regulation; online intermediaries; platform liability; liability exemptions; sustainability.

**JEL:** K2

## I. Introduction

The European Green Deal and Europe Fit for the Digital Age are leading EU priorities[1] that translate into autonomous EU legislative initiatives responding to UN sustainability goals.[2] The objectives of making Europe a carbon-neutral, modern and resource-efficient economy, alongside the preservation of the natural environment and achieving sustainability goals, dominate the discussion on sustainability. However, fostering innovation through digitalization should not be overlooked. The EU action plan for the digitalization of the energy sector is a prominent example of complementary actions under the two priorities.[3] Actions include empowering consumers, and increasing their control over energy consumption, as well as strengthening cybersecurity of digital energy services. The systemic risks are discussed in the context of digitalization and energy: cybersecurity, privacy, and the protection of fundamental rights and economic disruption.[4] Empowering consumers entails discussing sustainable market regulation, relating to the use of connected devices, the Internet of Things (hereinafter: IoT), sharing data, as well as developing algorithms advancing tailored energy consumption, such as in smart homes. It requires reflection on the rules governing online information flows.

[1] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Commission Work Programme 2020 A Union that strives for more, 29.01.2020, COM (2020) 37 final.

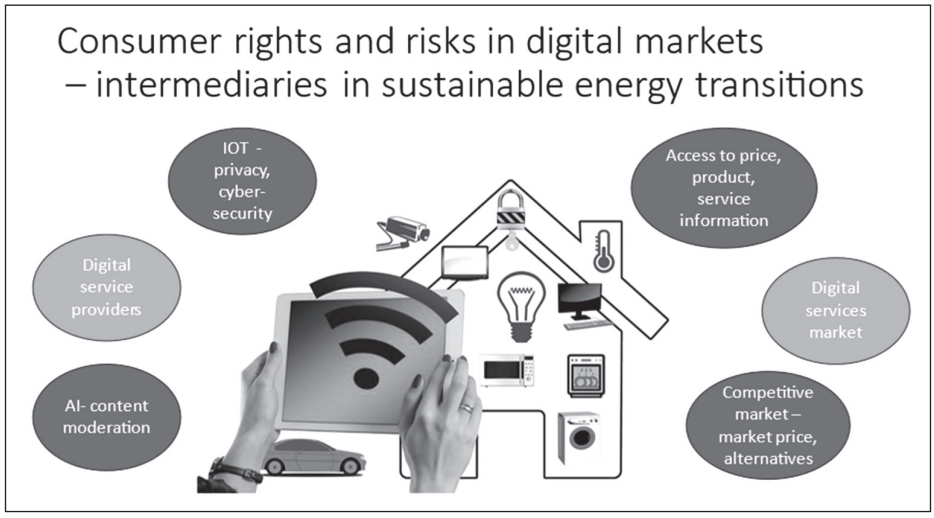
[2] UN General Assembly, Transforming our world: the 2030 Agenda for Sustainable Development, Resolution of General Assembly 25 September 2015 <https://documents-ddsny.un.org/doc/UNDOC/GEN/N15/291/89/PDF/N1529189.pdf?OpenElement> accessed 25 January 2024.

[3] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Digitalizing the energy system – EU action plan, 18.10.2022, COM (2022) 552 final.

[4] International Energy Agency, Digitalization and Energy (2017), 123 (hereinafter: Digitalization and energy).

Our focus is on the regulation of intermediaries controlling market infrastructure that are capable of intercepting or releasing information provided by users, or technically altering and redirecting traffic flows online. We discuss these issues primarily in the context of the EU Regulation of 19 October 2022 on a Single Market For Digital Services – known as the Digital Services Act of 2022 (hereinafter: DSA), with its expressed ambition to create "a safe, predictable and trusted environment".[5] Starting from the Digital Single Market (hereinafter: DSM) Strategy of 2015[6], the European Commission advances sustainable and responsible behaviour of diligent business operators in the digital environment. The DSA aims to provide a "smart mix" of horizontal liability exemptions – essentially, exempting service providers from liability for the [illegal/unlawful] acts of the users of their services – and new "due diligence" obligations, subject to administrative liability. Furthermore, the "smart mix" we are discussing includes obligations directly imposed on service providers, that is, intermediaries, as well as incentives for them to take voluntary actions in the public interest.

**Figure 1.** Protecting rights and securing risks in smart home digital services




Source: Figure created by Katja Weckström.

[5] 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) (Text with EEA relevance) OJ L 277, 27.10.2022, p. 1–102.

[6] Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe, COM (2015) 192 final, 12.

Sustainable regulation for digital markets is directed at the objectives of fostering innovation (as a sustainability goal) as well as of the protection of "user rights", in the context of fundamental rights (privacy or freedom of expression) and consumer rights. Sustainable regulation needs to be clear and coherent to offer legal certainty to all market actors. At the same time, it needs to avoid over-regulation, yet be flexible enough to respond to evolving technologies and new practices that emerge on the market. The DSA fosters two complementary regulatory goals: i) preserving liability exemptions to offer space for the development of innovative services; and ii) engaging intermediaries in safeguarding user rights and preventing risks, by complex due diligence obligations specified within the DSA.

We, therefore, discuss what is new in the approach adopted in the DSA (Section I). In Section II, we discuss the role of intermediaries in information flows online and how is this role linked to information and data important from the perspective of energy consumption. We then move on to discuss the impact of CJEU case law on balancing liability exemptions with fundamental rights, including the right to information, and its impact on the interpretation of the DSA (Section III). As diligent behaviour of intermediaries is part of the goal of sustainable market regulation, subsequently the paper discusses the obligations imposed in the DSA, which aim to engage intermediaries in protecting user rights, without losing the protection of liability exemptions (Section IV).

## II. The EU Legal Framework for Liability Exemptions for Intermediaries

### 1. From the E-commerce Directive to the Digital Services Act

The E-commerce Directive (hereinafter: ECD) was adopted in the year 2000 and seeks to contribute to the proper functioning of the internal market by ensuring free movement of information society services between the Member States (Article 1). An information society service is defined as any service normally provided for remuneration, at a distance, by electronic means, and at the individual request of a recipient of such service.[7] It includes harmonizing

[7] Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the internal market (Directive on electronic commerce). For this purpose: "at a distance" means that the service is provided without the parties being simultaneously present; "by electronic means" means that the service is sent initially and received at its destination by means of electronic equipment for the processing and storage of data, and entirely transmitted, conveyed or received by wire, by radio, by optical means or by other electromagnetic means; "at the individual request of a recipient of services" means that the

provisions on the establishment of information society services, commercial communications, electronic contracts, the liability of intermediaries, codes of conduct, out-of-court dispute settlements and court actions, as well as cooperation between Member States. The ECD took important steps towards securing the freedom to provide services in the European Union, by introducing the country of origin principle (that is, point of first contact or home-country control). However, its practical impact was greatly affected by Article 1(3) ECD, which removed business-to-consumer (B2C) relationships from its sphere of harmonization. Thus, Member States were free to maintain national consumer laws at respective levels of protection.[8]

The EU position has since changed with the introduction of the Unfair Commercial Practices Directive of 2005 and the Consumer Rights Directive in 2011, as well as several subsequent measures that harmonize consumer protection across the EU.[9] Unlike the E-commerce Directive, the DSA has the form of an EU Regulation, and is, therefore, directly applicable in Member States. Hence, it can also be viewed as one arm of the general regulatory effort to improve online consumer protection across the EU. Although both the ECD and the DSA constitute market regulation and focus on the role of internet service providers as market actors, the hybrid feature of the DSA is novel.

---

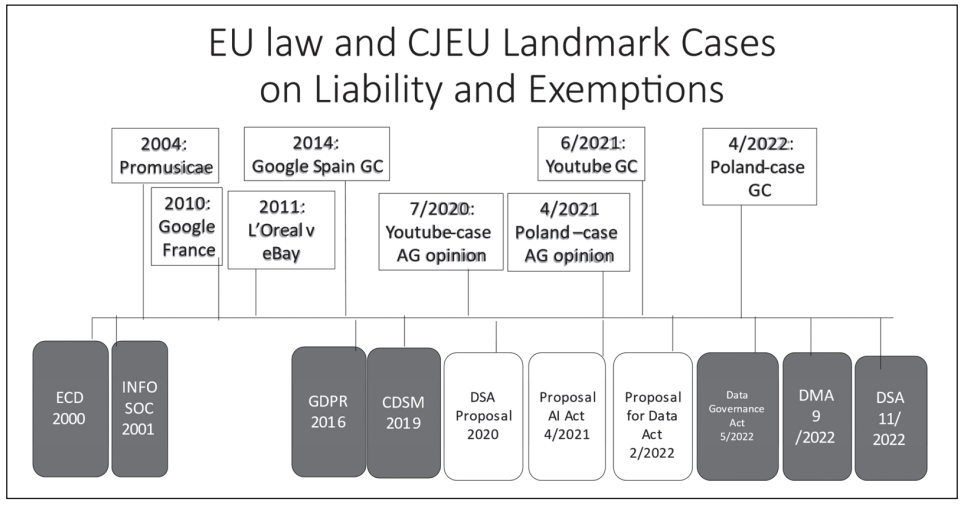
service is provided through the transmission of data on individual request. Art. 2(a) of the ECD refers to Art. 1(2) of the Directive 98/34/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations, OJ L 217/21, 5.8.1998. The definition provision remains unchanged in codifying Directive (EU) 2015/1535 of the European Parliament and Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification).

[8] Thus, the Directive applies to internet service providers in both business-to-business and business-to-consumer e-commerce, but national law may place additional obligations upon internet service providers based on national consumer law. First Commission report at 4. Likewise Art. 1(5) exempts taxation, cartel law and questions relating to personal data law from the sphere of application of the ECD. Art. 1(5(b)) explicitly exempts questions relating to information society services covered by Directives 95/46/EC and 97/66/EC, which regulate the right to privacy of personal data.

[9] Directive 2005/29/EC 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) (Text with EEA relevance) [2005] OJ L149/22. Directive 2011/83/EU 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 Text with EEA relevance [2011] OJ L304/64.

The European Union regulated the issue of liability of internet service providers from the perspective of e-commerce, as opposed to that of an infringement of a specific intellectual property right. Hence, the normative focus was not on defining specific illegal content, but on measures to remove clearly illegal content. The text of the ECD is, nevertheless, strongly influenced by copyright concerns, which were pressing at the time of the adoption of the ECD. The inter-relationship with copyright law was explicitly mentioned in the recitals of both the ECD and the Copyright and Information Society Services Directive (hereinafter: INFOSOC Directive).[10] As a consequence, the ECD applies to all types of illegal activity in a horizontal manner, that is, it covers civil, administrative and criminal liability for all types of illegal activities initiated by third parties online, including: copyright piracy, trademark counterfeiting, defamation, misleading advertising, unfair commercial practices, child pornography etc."[11]

**Figure 2.** Development of EU Law on Liability and Exemptions 2000–2022




Source: Figure created by Katja Weckström.

[10] Recital 50 of the ECD and Recital 16 of the Directive 2001/29/EC on the harmonization of certain aspects of copyright and related rights in the information society [2001] OJ L167/10. See also Study on the Liability of Internet Intermediaries Markt/2006/09/E, 12.11.2007 12.

[11] However, the safe harbors do not apply to injunctions aiming at removal of illegal information or disabling access to it. Ulys, T.V. et al. Study on the Liability of Internet Intermediaries, Markt/2006/09/E, 12.11.2007, 4.

Figure 2 shows how EU law has developed relating to liability, and liability exemptions, for providing online services in the EU. It also gives a chronological reflection of central pieces of EU legislation and CJEU preliminary rulings, to re-create the context for the debate on liability and exemptions. While the text of the legal provisions is static, the substantive debates introduce reflections of technological development, and how innovative business models or services raise fundamental legal questions. It shows how the normative fabric becomes layered, when new legislation is introduced to co-exist with existing laws. Yet the interpretations of core provisions remain fairly consistent in CJEU case law.

## 2. A Dynamic Legal Context – the DSA Proposal

While confirming the principles set out in the ECD, the original DSA proposal[12] presented in 2020 made a clear effort to control the future actions of providers of digital services, and shift their role towards securing other societal interests, such as protecting fundamental rights of users and removing illegal content.[13] In essence, the DSA proposal targeted intermediaries because they have provided services that "chang[e] the daily lives of Union citizens and shap[e] and transform […] how they communicate, connect, consume and do business."[14]

> "The proposal defines clear responsibilities and accountability for providers of intermediary services, and in particular online platforms, such as social media and marketplaces. By setting out clear due-diligence obligations for certain intermediary services, including notice-and-action procedures for illegal content and the possibility to challenge the platforms' content moderation decisions, the proposal seeks to improve users' safety online across the entire Union and improve the protection of their fundamental rights."[15]

In addition, the proposal set clear responsibilities for Member States to ensure compliance of service providers in meeting EU imposed obligations, and to ensure swift and effective enforcement of citizen rights.[16] The most significant aspect of the proposal related to the deletion of Articles 12–15

[12] 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, 15.12.2020, COM (2020) 825 final (hereinafter: COM (2020) 825 final).

[13] COM (2020) 825 final, 1.

[14] Ibid.

[15] COM (2020) 825 final, 2.

[16] COM (2020) 825 final, 3.

of the ECD (liability exemptions for intermediaries), and their "reproduction" in the DSA. While the ECD and the principles underpinning it had remained in force, the DSA was meant to complement it. Moving Article 15 ECD, which includes a prohibition placed on Member States against imposing a duty on intermediaries to monitor content, from the ECD to the DSA, would have changed the balance of the principles underpinning the ECD – from general market regulation, towards the specific regulation of providers of services.[17] Normatively speaking, the 2020 DSA proposal sought to cement the role of digital service providers as agents of government instead of independent private actors in a free market economy. It would have constituted a clear shift in EU policy, of abstaining from regulation of e-commerce, towards the EU taking an active role in public regulation of the digital economy.

## 3. The Normative Context of Platform Liability in the Adopted Text of the DSA

In response to criticism, the Commission proposal was changed during the legislative process relating to the subject matter and the scope of the DSA. Three significant alterations were made that changed the interpretive framework. The wording and word order of the original proposal was modified in its final draft relating to the regulatory aims and its scope.

First, the order of Article 1(2) and 1(1) DSA was changed to set the general aim of contributing to the proper functioning of the internal market first, and the objective of laying down uniform rules second. The scope of the DSA thus upholds the general framework for EU e-commerce rules set in the ECD, despite shifting the text of Articles 12–15 of the ECD to the DSA.[18] Second, the addition of Article 2(3) DSA includes specific wording whereby the DSA does not affect the application of the ECD. This change sets the status of the DSA as co-existing with the ECD, rather than replace it. Third, a key addition lies in Article 1(1) DSA, where the wording "The aim of this Regulation is to contribute to the proper functioning of the internal market for intermediary services by setting out harmonised rules for a safe, predictable and trusted online environment that facilitates innovation and in which fundamental rights enshrined in the Charter, including the principle of consumer protection, are effectively protected" replaces the original draft's aim which was to "set out uniform rules for a safe, predictable and trusted online environment, where fundamental rights enshrined in the Charter are effectively protected".

[17] Ibid.
[18] Recital 16 DSA.

However, the DSA constitutes a measure of full EU harmonization, and so Member States may not maintain or introduce additional liability exemptions for intermediaries.[19] Although Article 3 of the ECD remains in effect (in relation to national regulation in other fields of law), EU rules relating to safe harbours for intermediaries are now harmonized. Under Article 3 ECD, national measures tasking intermediaries to act against illegal acts of users, or to provide information, are limited in scope, by necessity, and by the principle of proportionality.[20] Article 3 ECD limits measures setting obligations on specific intermediaries to the areas of: public policy (preventing serious crimes), public health, public security and consumer protection. Articles 9–10 DSA now set codified standards in relation to the field of application of such measures, which may apply, if there is a rational basis for such an order in any EU or national legislation.

The DSA was introduced together with EU Regulation of 14 September 2022 on contestable and fair markets in the digital sector – the Digital Market Act (hereinafter: DMA). Together, they constitute parts of the EU Digital Agenda with the aim of protecting users of digital services across the EU. The DMA identifies *core online platforms* as *gatekeepers* in the online market, and imposes duties designed to curb their market power to secure a fair environment for business operators and end users.[21] For our purposes, it is important to note that the DMA focuses on gatekeeper obligations that are designed to ensure market *access* on fair terms. In the context of competition law, actors that are in a dominant position are routinely subject to stricter standards and scrutiny of their actions that may have anti-competitive effects on future markets.[22] Gatekeepers can be understood as entities that have market power, that is, those that can manipulate market prices or demand and supply levels, without normal competition constraints. From a perspective of sustainability, we can assess whether the balance of regulation creates *systemic* risks while it attempts to remove *some* risks.

To illustrate the difference, modern state-owned enterprises (limited liability companies, LLCs), or private providers of essential services, are market actors that operate within a set regulatory framework. They do, however, operate *autonomously in terms of decisions* on future actions and investments, as long

[19] Recital 4 DSA.

[20] This is closely mirrored in how the CJEU approached the question in case C-401/19, *Republic of Poland v European Parliament and Council of the European Union* OJ C70/24 (hereinafter: Case C-401/19 *Poland)*. See infra.

[21] Art. 1 Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance) [2022] OJ L265/1.

[22] Art. 102 TFEU.

as they provide services on equal terms to all. If the role for digital service providers mirrors traditional publicly-controlled companies, which *must take account of public policy in operative decision-making,* rather than basing such decisions on supplying market demand, then this presents a sustainability risk for market regulation. Legal risk of liability affects decision-making on research, development and investments, that is, decisions to change or maintain the operations of the enterprise. Shifting the **status** of market-leader companies, to serve set public interests (securing fundamental rights of users), de-prioritizes serving unknown and undefined public interests, such as developing essential facilities for digital commerce, and propelling growth of the digital economy. A systemic reduction of free market-based R&D investments, slows down the platform economy. As a result, it impacts availability of new digital services that enable transitions towards more sustainable consumption habits. Change (innovation, market renewal, R&D investments) is needed to reach sustainability goals. Over-regulation, which in effect stagnates rather than fosters innovation, must be viewed as unsustainable market regulation.

A strong guiding principle of EU trade policy and law is towards market liberalization, and moving away from governments wielding significant policy power in a way that may disrupt markets. The key lies in developing the digital economy through *freedom of competition* and acquired market power, rather than using political power for economic gain. Ideally, sustainable market regulation may respond to specific risks and impose tailored duties for diligent economic operators, without setting liability enhanced policy, or enforcement targets for normal business activity.

## III. Information governance and content moderation

The goal of the DSA looks promising: creating a safe, predictable and trusted environment for digital services[23], with effective protection of fundamental rights. The concept of "digital services" potentially covers the whole digital market, yet the DSA targets not all information society services[24], but only those of intermediaries. Three categories of intermediaries are listed in the DSA: "mere conduit", "caching" and "hosting" services, following the categories of service providers potentially within the scope of liability exemptions regulated in Articles 12–14 ECD. All categories of service providers are subject to regulation, because of the role they play in the transmission and storage of

[23] Art. 1(1) DSA.

[24] As the services addressed by the ECD.

information.[25] "Online platforms" are hosting services but they not only store information, but also disseminate it to the public at the request of the service recipient.[26] This definition highlights the media aspect of online platforms, and integrates content moderation as an inherent feature of an "online platform" service.[27] Social media and online marketplaces are examples of popular platforms. As may be concluded from the DSA provisions, the "dissemination" of information, and the impact on platform users, raises the most problematic issues when it comes to regulating platforms. The regulatory answer is thus based on a graduated approach, depending on whether the core of the platform service is the transmission, the storage, or the storage and dissemination of information. In the latter case, another layer of regulation is imposed on so-called Very Large Online Platforms (hereinafter: VLOPs) and Very Large Online Search Engines (hereinafter: VLOSEs), based on the potential impact on users.[28]

Dealing with "information" is the basis for the categorization of services covered by the DSA. Along these definitions, the DSA recitals point to an increasingly complex ecosystem *for the transmission, "findability" and storage of data online*.[29] To make it even more complex, the discussion and analysis of the DSA focuses on "content" and its moderation, aiming at fighting "illegal content", and guarding the freedom of expression. None of these key terms: information, data or content is defined in the DSA itself. However, certain clues can be found, for example, in its definition of "content moderation", making it possible to identify typical types of content: posting text, photos, videos, sales offers or advertisements.[30] "Data", on the other hand, is defined for the purpose of the Data Governance Act as *any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording*[31].

---

[25] The definition of an "intermediary service" in Art. 3(g) DSA.

[26] Art. 3(i) DSA.

[27] Gillespie, T. 'Custodians of the Internet. Platforms, content moderation and the hidden decisions that shape social media' (2018) 21.

[28] Section 5 DSA imposing additional obligations on VLOPs and VLOSEs to manage systemic risks.

[29] Recital 28 DSA.

[30] Inferred from the definition of content moderation, and general examples of online platforms-Art. 3 t and rec. 13 DSA.

[31] Art. 2(1) Regulation (EU) 2022/868 on European data governance and amending Regulation (EU) 2018/1724 Regulation (Data Governance Act) [2022] OJ L152/1 (hereinafter: Data Governance Act). The same definition proposed in the draft for a Regulation of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act) COM (2022) 68 final (hereinafter: Data Act).

It is clear that the distinction between information, data and content is difficult to draw in the normative context. What amounts to "content" under the DSA, can at the same time be considered "data" in the data regulation context. An example can be found in the chart illustrating the impact of digitalization on energy demand in buildings.[32] Energy apps developed, among others by Google,[33] are key facilitators for smart homes and energy savings. The combination of apps (services) and connected devices (such as thermostats) is based on the exchange of data and information, though not necessarily made publicly available, as in the case of online platforms. Furthermore, some of the content/data is disseminated by the intermediaries at the request of the users (so a service provider performs the true role of an intermediary) and some, on its own initiative. Meta, for example, makes Electrical Distribution Grid Maps available to the public under the general Data for Good project.[34] This activity may test the limits of the term "content moderation", as distinct from "content publication", while its essence is to provide data for planning of infrastructure and community development projects.

The efforts to keep the regulation of content services, intermediaries and data services separate are obvious. For example, the Data Governance Act regulates the selected categories of data intermediaries: data intermediation services[35], and expressly excludes services that focus on the intermediation of copyright-protected content, as well as services, the main goal of which is to ensure the functionality of objects and devices connected to the Internet of Things (IoT).[36] The proposal for a Data Act, on the other hand, aims to harmonize rules on making data generated by the use of a product or related service available to the user of that product or service (IoT)[37]. It thus covers not only manufacturers, but also suppliers of related services, and users of the products and services in question. It also aims to reinforce user rights in relation to data processing service providers. The category of the data processing services encompasses "digital services", within the meaning

[32] Digitalization and Energy, 42–44.

[33] See Google Nest <https://play.google.com/store/apps/details?id=com.nest.android&hl=en_US>.

[34] Electrical Distribution Grid Map <https://dataforgood.facebook.com/dfg/tools/electrical-distribution-grid-maps>; an interesting example indicated in the doctoral dissertation of Adrianna Michałowicz Data Altruism in the European Union Law (2023), University of Łódź, unpublished.

[35] Art. 2(11) Data Governance Act *a service which aims to establish commercial relationships for the purposes of data sharing between an undetermined number of data subjects and data holders on the one hand and data users on the other, through technical, legal or other means, including for the purpose of exercising the rights of data subjects in relation to personal data*.

[36] Art. 2(11)(b) and (c) Data Governance Act.

[37] Art. 1(1) Data Act.

of the proposed Data Act.[38] The term expressly excludes online content services within the meaning of the Portability Regulation,[39] which focuses on audiovisual media services (AVMS) and providers of access to, and the use of, works and other protected subject matters such as broadcasts. These exclusions do not mean that "digital services" are not covered by the DSA, if they fall within the scope of regulated intermediaries.[40] Unlike the express mention of the relation of the DSA to the ECD in Article 2 DSA, there are no express references to the Data Governance Act,[41] or other data related legislation in the DSA.

The regulatory landscape for the digital market is thus dominated with EU laws addressing selected problems of multiple categories of online service providers. Although digital service providers often operate in several sectors, the regulatory choice may be justified by the attempt to avoid over-regulation, and leave space for innovation. Against this backdrop, the DSA appears to address the overarching problem of securing a safe environment and promoting due diligence of intermediaries. The clear objective of the DSA is to fight "illegal content", that is, any content not in compliance with EU law, or national law,[42] while, at the same time, preserving liability exemptions for intermediaries and fostering the responsible behaviour and diligence of intermediary service providers.

[38] Art. 2(12) Data Act: "data processing service" means a digital service other than an online content service as defined in Art. 2(5) of Regulation (EU) 2017/1128, provided to a customer, which enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources of a centralized, distributed or highly distributed nature; Art. 2(12) of the draft Data Act.

[39] Regulation (EU) 2017/1128 on cross-border portability of online content services in the internal market [2017] OJ L168/1.

[40] M. Husovec points to the term "digital services" as not relevant in the DSA Regulation, and explains the applicability of DSA to hybrid platforms. See: Martin Husovec, 'The DSA's Scope Briefly Explained' (2023). Available at SSRN: <https://ssrn.com/abstract=4365029>, 4.

[41] Preceding the Digital Services Act, see Figure 2.

[42] Subject to the conformity with EU standards; Illegal content is defined in Art. 3(h) DSA and "content moderation" means the activities, whether automated or not, undertaken by providers of intermediary services, that are aimed, in particular, at detecting, identifying and addressing illegal content or information incompatible with their terms and conditions, provided by recipients of the service, including measures taken that affect the availability, visibility, and accessibility of that illegal content or that information, such as demotion, demonetization, disabling access to, or removal thereof, or that affect the ability of the recipients of the service to provide that information, such as the termination or suspension of a recipient's account Art. 3(t) DSA.

## IV. Liability exemptions in the DSA and CJEU case law

### 1. DSM policy proposals and Case C-401/19 *Poland vs Parliament and Council*

The DSA contains conditional exemptions from liability of intermediaries, for illegal actions of their users, with respect to the mere conduit of data (Article 4 DSA), for caching services (Article 5 DSA), and for hosting services (Article 6 DSA). Platforms that supply a variety of digital services generally fall within the category of hosting services, since they store information provided by the recipient of the service, that is, users of the service.

Chapter II of the DSA also contains limitations on the ability of Member States to impose further liability on intermediaries for the activities of their users, or third party content, on their sites. Importantly, according to Article 8 DSA, Member States may not impose upon intermediaries a general obligation to monitor the information, which providers of intermediary services transmit or store, nor to require intermediaries to actively seek facts or circumstances indicating the illegal activity of users. Article 7 DSA ensures that intermediaries may not lose the safe harbour protection granted to them under Articles 4–6 DSA for taking voluntary action to ensure compliance with legal obligations. In practice, the question of liability under Articles 4–6 DSA centres on whether intermediaries possess *actual knowledge* of illegal activity by their users. Thus, if intermediaries were to face full liability for gaining knowledge of such illegality through their own voluntary investigations, the legal framework would incentivize intermediaries to stay passive to prevent being found liable for the acts of others.[43] Such open-endedness and uncertainty relating to the liability for one's actions could qualify as a systemic risk arising from the regulation itself, and thus indicating the unsustainability of that regulation. Article 7 DSA removes such ambiguity, provides certainty, and creates an incentive for intermediaries to make voluntary efforts to fight illegality of user behaviours, that is, a "smart-mix" of sustainable market regulation.

[43] The 2011 decision in case C-324/09 *L'Oreal vs eBay* relating to the removal of counterfeit merchandise from eBay signaled that a duty to act could be triggered when intermediaries gain "actual knowledge" either via their own investigations, or when receiving a specific notification of infringing content by the right holder. Unlike copyright law, the trademark right does not contain exclusive rights to refer to the trademark in commerce, since it could create a barrier for a thriving secondary market in branded goods as well as comparative advertising by competitors (*Google France*). Subsequent case law relating to content that infringes copyright has emphasized that the duty to act to remove specific content requires a notification by the right holder. Art. 7 DSA clarifies that liability may not incur based on knowledge acquired during the exercise of best efforts to combat illegal activity on the platform.

Over two decades, the Court of Justice of the European Union (hereinafter: CJEU) has issued preliminary rulings on how to thread the line between platform liability and safe harbour exemptions in several cases relating to potentially infringing behaviour. The normative framework for the liability exemptions has developed over the last 20 years, since the introduction of the ECD. Table 1 shows the general categorizations of liability exemptions and links the past and future statutory placement of said provisions. It also links to CJEU case law where the interpretative context for the liability exemptions in EU law was developed.

In an action for annulment, Case C-401/19 *Poland vs the European Parliament and Council*[44], the CJEU was asked to assess liability imposed on online platforms in Article 17(4) of Directive 2019/790 on copyright and related rights in the digital single market (hereinafter: CDDSM) against fundamental rights protected in Articles 11 and 17(2) of the EU Charter of Fundamental Rights (hereinafter: EU Charter). The issue at hand was whether Article 17(4) CDDSM infringed user rights to freedom of expression and information, as guaranteed in Article 11 of the EU Charter. The concern arises, since online platforms, to avoid liability, are likely to use automatic filtering tools that can remove user access not only to illegal but also, albeit unintentionally, to legal expression. Over-regulation that impacts material covered by freedom of expression, indicates a systemic risk of unsustainable market regulation.

Prior to the introduction of Art 17(4) CDDSM, the exemption from liability for copyright infringements had been governed by Article 14 ECD (now Article 6 DSA), and the corresponding Article 3 of Directive 2001/29/EC of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (hereinafter: INFOSOC Directive).[45] At the time of the Opinion of the Advocate General Saugmandsgaard Øe of 15 July 2021, and CJEU Grand Chamber ruling on 26 April 2022, the DSA had been proposed, but not yet introduced as amended and passed.[46]

The CJEU reiterated its case law that links the interpretation of Article 11 of the EU Charter with that of the European Court of Human Rights' interpretation of Article 10 of the European Convention of Human Rights.[47] The guaranteed freedom of expression and information applies to both the

[44] Case C-401/19 *Poland*.

[45] Directive 2001/29/EC on the harmonization of certain aspects of copyright and related rights in the information society [2001] OJ L167/10.

[46] The DSA was published in the Official Journal as of 27 October 2022 and came into force on 16 November 2022.

[47] Case C-401/19 *Poland*, para. 46 citing ECtHR, *Cengiz and Others v. Turkey* App no 48226/10 and 14027/11 (ECtHR, 1 December 2015), § 52; and *Vladimir Kharitonov v. Russia* App no 10795/14 (ECtHR, 23 June 2020), § 33 and the case law cited.

**Table 1.** Liability safe harbor provisions for internet service providers in EU law

| General framework for liability exemptions in EU Law | | |
|---|---|---|
| **Provision in force** | **Previous provision or case law** | **Scope and subject matter** |
| ECD Art. 3<br>EU Fundamental Rights Charter<br>National constitutions | Case C-275/06 *Promusicae*,<br>Case C-401/19 *Poland* | general proportionality test for national measures placing obligations to secure rights on information society services |
| DSA Art. 4 | former ECD Art. 12 | liability exemption for mere conduit service providers |
| DSA Art. 5 | former ECD Art. 13 | liability exemption for caching service providers |
| DSA Art. 6 | former ECD Art. 14 interpreted in Cases C-268/08 & C-237/08 *Google France*; Cases C-282/18 & C-683/18 *Youtube*; Case C-401/19 *Poland* | liability exemption for hosting service providers (platforms) |
| DSA Art. 7 | new, overturning in part Case C-324/09 *L'Oreal vs eBay* | general exemption for diligent investigation into illegal activity |
| DSA Art. 8 | former ECD Art. 15 interpreted in Cases C-268/08 & C-237/08 *Google France*; Cases C-282/18 & C-683/18 *Youtube*; Case C-401/19 *Poland* | general prohibition on national measures imposing general monitoring obligations |
| CDSM Art. 17 | new, interpreted in Case C-401/19 *Poland* | specific liability regime for large online content moderation platforms |
| GDPR | codifying in part Case C-131/12 *Google Spain* | specific liability regime relating to the protection of personal data for all business activity |
| DMA | | due diligence obligations for gatekeepers to allow market access |

Source: Data assembled by Katja Weckström.

content of information and the means of its dissemination. Any restriction of the means of dissemination necessarily interferes with the guaranteed freedom of expression. The internet and online content-sharing platforms have become an important means for enhancing public access to news and public dissemination of free expression. It is both an important vehicle for exercising freedom of expression as well as gaining access to the expression of others.

The CJEU referenced its interpretation of the hosting exemption (at that time, Article 14 ECD) and clarified that the interpretation of any liability regimes needs to take account of the particular importance of the internet for the freedom of expression and information when implementing the regime.[48] In the context of this case, the CJEU noted also that the specific liability regime at issue in Article 17(4) CDDSM only applies to some large online-content sharing service providers whose main, or one of the main purposes is to store and give public access to a large amount of copyright protected works, or other protected subject matter uploaded by its users, which the provider organizes and promotes for profit-making purposes.[49]

The CJEU stated that the contested provision does not impact intermediaries in general, or the interpretation of the liability exemption for hosting services under Article 14 ECD (now Article 6 DSA), but is a specific liability regime designed for online-content sharing platforms with a particular purpose, and the particular problem of curbing end-user copyright infringements.[50] The CJEU further assessed the specific liability regime, its justifications, and the proportionality of the measure, against the requirement of service providers to exercise best efforts to remove unlawful content from their service, based on specific notifications by right holders.

The CJEU concluded that as such, Article 17(4) CDDSM requiring online content-sharing service providers to make best efforts to ensure the unavailability of specific protected content, constitutes a limitation on the fundamental right to the freedom of expression and information, because available means for employing best efforts (algorithmic enforcement), may also categorically remove lawful content from the service. Hence, any restrictive measure must be provided for by law and satisfy the proportionality test. Limitations may only be made if they are necessary, and genuinely meet objectives of general interest recognized by EU law, or the need to protect the rights and freedoms of others. In the event of a collision of rights, a fair balance must be struck between the interests at stake. Where there is a choice between alternative appropriate measures, the one that limits other rights the least must be chosen, and the disadvantages caused may not be disproportionate to the aims pursued.[51] The CJEU clarified also that, when assessing national measures implementing Article 17(4) CDDSM

[48] Case C-401/19 *Poland*, para. 47. Joined cases C-682/18 and C-683/18 *Frank Peterson v Google LLC and Others and Elsevier Inc. v Cyando AG* (hereinafter: *Youtube*) ECLI:EU:C:2021:503, paras 64, 65, 113.

[49] Case C-401/19 *Poland*, para. 30.

[50] Case C-401/19 *Poland*, paras 30–31. The Court notes tailoring measures in Art. 2(6) defining online sharing platforms and Art. 17(6) that limits these obligations only to intermediaries with an annual turnover larger than 10 million Euros.

[51] Case C-401/19 *Poland*, paras 63–68 and the ECtHR case law cited.

and other liability regimes, each EU Member State must make their own assessments in relation to the specific measures advanced.[52] Thus, the CJEU set strict criteria for tailoring measures in fundamental rights sensitive activities, in order to prevent practices that could lead to a systematic removal of lawful content from platforms.[53] It remains to be seen if Member States have headed the call to tailor-make safeguards when implementing Article 17 CDMSD.

## 2. Interpreting the DSA in Light of Landmark Preliminary Rulings

The reasoning in Case C-401/19 *Poland* is in line with established CJEU case law, since the *Promusicae* ruling from 2008[54], whereby Member States are responsible when implementing EU law to strike a fair balance between the various fundamental rights protected by the EU Charter. The factual risk of measures over-blocking lawful expression is recognized by the CJEU. In essence, online platforms are not obligated to produce a specific result (preventing illegal content being accessed via their service), but "the filtering measures which sharing providers are required to implement must comply with two cumulative obligations: They must seek to prevent the uploading of content which unlawfully reproduces the works identified by right holders while not preventing the making available of content which lawfully reproduces that subject matter. Hence, measures that systematically undermine the right of users to make use of protected works are not proportionate".[55] Hence, Member States may not systematically require blocking content that falls within the limitations of the Copyright Act, but must take account of the position of the intermediary to act diligently in relation to both right holders and end-users of their service.[56]

This leads us to CJEU case law indicating the bounds of Article 8 DSA (former Article 15 ECD), that prohibits Member States from imposing a general obligation on intermediaries for them to monitor content or data. The CJEU has introduced the concept of "diligent economic operator" to help define when the actions of an intermediary are sufficient in terms of

[52] Case C-401/19 *Poland*, paras 71 and 99. See to this effect also Communication from the Commission to the European Parliament and the Council, Guidance on Art. 17 of Directive 2019/790 on Copyright in the Digital Single Market, 4.06.2021, COM(2021)288 final at 2–3.

[53] Case C-401/19 *Poland*, para. 99.

[54] Case C-275/06 *Promusicae*, ECLI:EU:C:2008:54, para. 68.

[55] Case C-401/19 *Poland*, para. 85 citing Opinion of the Advocate General in paras 164, 165 and 191–193.

[56] Case C-401/19 *Poland*, Opinion of the Advocate General Saugmandsgaard Øe, paras 192–193.

remaining exempt from liability for the illegal activity of others online.[57] This concept distinguishes "no fault" – intermediaries, from platform operators that facilitate, or turn a blind eye to illegal activity online.[58] The mere fact that the operator knows, in a general sense, that some content is made available illegally on its platform, is not sufficient grounds to conclude that it acts with the purpose of giving internet users access to that content.[59] Liability cannot be inferred from the persistence of illegal activity, instead, intermediaries are exempt from liability, unless specific conditions for liability are in fact met.[60]

In the *Google France* case, relating to keyword advertising and the operation of the Google search engine, the CJEU faced the question whether trademark owners could prevent Google from displaying competitors' ads or search results, when consumers searched for a specific brand. The Court concluded that a service provider cannot be held liable for the data, which it stores at the request of an advertiser, unless, having obtained knowledge of the unlawful nature of those data or of that advertiser's activities, it failed to act expeditiously to remove or to disable access to the data concerned. A service provider remains exempt from liability if it has not played an active role of such a kind as to give it knowledge of, or control over, the data stored.[61]

Hence, the content and interpretation of safe harbours for intermediaries have not changed substantially with the incorporation of the provisions into Articles 4–6 DSA.[62] The *acquis* on Articles 12–14 ECD, on the limited liability of information society services for acts of its users, remains.[63] New technologies that allow increased consumer empowerment will continue to disrupt markets and propel digitalization. Smart regulation secures access to data and information to allow for competitive markets to develop, and give consumers price information. Less concentration (gatekeepers) in new markets allows consumers to make informed decisions and choose between quality digital services (high reward). The energy market has recently been liberalized, which

---

[57] Case C-324/09 *L'Oreal and Others*, ECLI:EU:C:2011:474, para. 120. While the concept remains valid, the DSA expressly overturns the conclusion (para. 122) in that case that intermediaries should be liable when acquiring knowledge when information is uncovered based on their own investigation into matters (DSA Art 7). Art. 7 DSA confirms and codifies CJEU preliminary rulings in subsequent case law e.g. *Youtube*, paras 84–86.

[58] Case C-610/15, *Stichting Brein*, ECLI:EU:C:2017:456, paras 36, 45 and 48.

[59] *Youtube*, para 85.

[60] *Youtube*, para 87; distinguishing an interpretation of previous case law in case C-160/15, *GS Media*, ECLI:EU:C:2016:644.

[61] Case C-237/08, *Google France SARL and Google Inc. v Louis Vuitton Malletier SA* (C-236/08), *Google France SARL v Viaticum SA and Luteciel SARL*, ECLI:EU:C:2010:159 (hereinafter: *Google France*), para 120. See also Recital 22 DSA.

[62] Recital 19 DSA.

[63] Recital 16 DSA.

allows consumers greater choice between operators and prices. Smart home technologies rely on applications that collect, arrange and display information to consumers. Collection of data may occur inside consumer homes or outside, which immediately trigger both cybersecurity and privacy concerns (high risk). The key is to limit the risk without stifling the reward.

## V. Fostering responsible behaviour of diligent economic operators

DSA complements liability exemptions with a general framework enhancing responsibility of intermediaries, particularly online platforms. The focus in the DSA is on transparency in relations with service recipients, procedural safeguards in the case of content moderation, and holding service providers accountable for the decisions they make, as well as their activities in the area of advertising.

The Declaration of Digital Rights and Principles,[64] recently adopted by EU Institutions, stresses, in the context of safety, security and empowerment, "a high level of confidentiality, integrity, availability and authenticity of the information processed", and accessed by EU citizens. Platform services, including social media, are the main source of information, essential for informed and responsible choices in the context of sustainability and energy consumption[65]. The role of online intermediaries is discussed also as part of cybersecurity and Internet of Things (IoT); how to foster data flows and access to information with safety and ensuring the control of users. Energy consumption can be mitigated with the use of smart home appliances and connected devices, for example, in buildings.[66] This poses risks to cybersecurity that can be countered by the manufacturers or applications developers. Based on the large number of customers they serve, intermediaries are recognized to have power derived from their access to the contact details of their customers. This puts them in a position to inform users about infected IoT devices, which could prevent cyber attacks (especially Distributed Denial-of-Service, DDoS,

[64] European Declaration on Digital Rights and Principles, <https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles>.

[65] Sustainability Principle 24, European Declaration of Digital Rights and Principles; examples could include YouTube videos on how to save energy 5 amazing ways to save energy at home <https://www.youtube.com/watch?v=37kLS0uW16I>; or TikTok life-hacks on energy savings <https://studyfinds.org/tiktok-energy-saving-life-hacks/>; Instagram ideas for smart homes <https://www.instagram.com/explore/tags/smarthome/>; products offer at online marketplace allegro smart home <https://allegro.pl/kategoria/wyposazenie-inteligentny-dom-251242?string=smart%20home>.

[66] Digitalization and energy, 41–48.

and botnets). As noted, "intermediaries are not part of the IoT market, so they have low interest in detecting infected IoT devices via DNS and notifying users since they might incur in costs and personnel to deal with notifications." This poses questions on how to incentivize the intermediaries to engage in protecting their users.[67]

The DSA obliges intermediaries (service providers) to provide more information to their users (service recipients). All intermediary services must, in the terms and conditions of the service (ToS), inform users of any restrictions that the service provider imposes on the information that is provided by the users. It includes an obligation to explain the policies, procedures, measures and tools used for content moderation[68]. Service recipients should be made aware of the algorithmic decision-making and the human review process.[69] When actually restricting access to content deemed unlawful, users of hosting services, including platforms, should be presented with a statement by the service provider clarifying the reasons why the intermediary imposed an access restriction. This includes explaining what kind of a decision (removal or reduction of the visibility of content) was taken, whether there was a notice according to Article 6 DSA, or the decision was taken based on the service provider's voluntary investigation, if automated means were used and why the information was found to be illegal.[70] DSA provisions list in more detail not only what information should be provided to secure user rights, but how this information should be provided, apparently building on the experience with the application of information obligations in consumer related areas. Hence, required information should be provided to users in plain language, in easily comprehensible, clear and user-friendly manner.[71]

Due diligence obligations include establishing adequate means of redress for platform users. Redress mechanisms form an important pillar of the general framework for business responsibility in the area of human rights.[72] The DSA introduces certain mechanisms that business operators generally are

---

[67] E.lsa Rebeca Turcios Rodriguez' One thing after another. The role of users, manufacturers and Intermediaries in IoT Security' (2023) <https://doi.org/10.4233/uuid:64e15692-06d7-4e3a-9d51-97f4a07b403f>, Delft University of Technology, 17.

[68] See João Pedro Quintais, Naomi Appelman and Ronan Fahy, 'Using Terms and Conditions to Apply Fundamental Rights to Content Moderation' (2022), available at SSRN <https://ssrn.com/abstract=4286147> on the detailed analysis of the relations between ensuring freedom of expression and art. 14 DSA addressing the terms of service.

[69] Art. 14 DSA.

[70] Art. 17 DSA.

[71] Art. 14(1) and 17(4) DSA.

[72] UN, Guiding Principles for Business and Human Rights. Implementing the protect-respect-remedy framework, New York–Geneva 2011 <https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf>.

advised to provide and obliges online platforms to establish effective internal complaint-handling systems. Member States are also obliged to establish out-of-court dispute settlement mechanisms external to platforms.[73] It is clear that the service recipients addressed by a complaint are entitled to select any out-of-court dispute settlement certified according to the rules set in the DSA.[74]

The new oversight architecture for the platform environment includes administrative bodies, such as the Digital Services Coordinator, entities like "trusted flaggers" or academics requesting access to data[75], and the general public. The role of the Digital Services Coordinator in the certification process, as well as awarding the status of a "trusted flagger"[76] to selected entities and prioritizing internal review of the notices that trusted flaggers submit, aims to increase trust in balanced content moderation. Achieving balance is also guiding the provisions on the suspension of accounts of those who, on the one hand, frequently provide manifestly illegal content, and, on the other, frequently file notices that are manifestly unfounded.[77] Transparency and accountability are advanced with the obligations of reporting on **content moderation** that are made available to the public.[78].

Fighting illegal content and provision of illegal products and services is reinforced in the DSA in a number of ways. Special obligations are imposed on online marketplaces, that is, online platform services allowing consumers to conclude distance contracts with traders. The "know your business customer"[79] rule is encoded in Article 30 DSA, to allow for the pre-check of traders offering products and services in the EU. This, as well as rules that oblige platform service providers to inform consumers who purchased illegal products or use illegal services, about the illegality of that action, and about the identity of the trader engaged in illegal actions, as well as informing consumers of relevant means of redress, help prevent trade that is not in compliance with

[73] According to Art. 21(6) DSA, new mechanisms are not necessary: "Member States may establish out-of-court dispute settlement bodies for the purposes of paragraph 1 or support the activities of some or all out-of-court dispute settlement bodies that they have certified in accordance with paragraph 3".

[74] Art. 21 DSA.

[75] Recitals 92, 96–97 DSA, art. 40 DSA.

[76] Art. 22 DSA.

[77] Art. 23 DSA.

[78] Art. 15, 24 and 42 DSA addressing all intermediaries, online platforms and VLOPs respectively; Decisions and statements of reasons of online platforms shall be made available in the public database managed by the Commission Art. 24(5) DSA currently in the preparatory stage after the public consultations: https://digital-strategy.ec.europa.eu/en/news/digital-services-act-commission-launches-public-consultation-transparency-database-content.

[79] KYBC explained <https://www.kybc.eu/>.

EU law.[80] This could potentially be linked to the ongoing efforts in advancing cybersecurity in ICT services and products.[81]

Social media, such as YouTube or TikTok, online marketplaces, such as AliBaba, AliExpress or Amazon Store, as well as search engines, like Google Search, are subject to a special set of obligations, if they fulfil the criteria for being qualified as a Very Large Online Platform (VLOP) or Very Large Search Engine (VLOSE).[82] Due to their impact on a substantial number of users,[83] VLOPs are required to actively track and mitigate systemic risks to public security, among others.[84] The concept of "systemic risk" has been thoroughly developed in the financial services sector. It is understood as a risk, which will result in such a significant materialization of imbalances, that it will spread on the scale impairing the functioning of (in this case) the financial system, and will adversely affect economic growth.[85] VLOPs are required to conduct risk assessments, including taking into account service structure and organization, design of its recommender and algorithmic systems, as well as data related practices of the provider.[86] Furthermore, the DSA establishes the general framework for crisis management, with the concept of a "crisis" as occurring *where extraordinary circumstances lead to a serious threat to public security or public health in the Union or in significant parts of it*.[87] Established for the case of an extraordinary situation, it may be applied in the case of military aggression, hybrid cybersecurity attacks, or terrorist attacks beyond borders.

[80] If we apply, *per analogiam*, the conditions from the definition of 'illegal content'.

[81] Developing cybersecurity certification is conducted with the effort of the European Agency on Cybersecurity, and includes initiatives such as ICT products certification scheme, Cyber resilience Act (Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending regulation (EU) 2019/1020, COM (2022) 454 final) or the AI Act (Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts, COM (2021) 206 final). <https://certification.enisa.europa.eu/>. Voluntary and compulsory certificates need, however, to be distinguished in this context. For example, not all products need a CE marking in the internal market. Decision No 768/2008/EC on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC [2008] OJ L2018/82.

[82] VLOPs/VLOSEs, designated according to Art. 33 DSA; the list was published in April 2023, <https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops>.

[83] 45 million active users per month.

[84] Art. 34 DSA; for the preliminary analysis see: Paddy Leerssen, 'Counting the days: what to expect from risk assessments and audits under the DSA- and when?' (2023) DSA Observatory <https://dsa-observatory.eu/2023/01/30/counting-the-days-what-to-expect-from-risk-assessments-and-audits-under-the-dsa-and-when/>.

[85] Paweł Smaga, 'The concept of systemic risk' (2014) SRC Special Paper No 5, 19.

[86] Four categories of systemic risks are listed in Art. 34 DSA, with more details on conducting risk management in Art. 34(2), and on the risk mitigation measures in Art. 35(1) DSA.

[87] Art. 36 DSA.

With the risk mitigation system in place, service providers should potentially be ready to offer a quick and adequate response, under the scrutiny of the European Commission.[88]

An overview of the DSA provisions associated most closely with safety and predictability in the online environment, shows that DSA pushes service providers not only to be active in content moderation, but also to organize their services in a transparent way, and to react adequately to orders or notices. Diligence is expected in both, fighting illegal content and services and protecting the right to receive and impart information, as well as consumer rights and other fundamental rights of users.

## VI. Conclusion

The purpose of EU Single Market law is to ensure free movement of, and access to markets for new products and services. Fostering innovation is a sustainability goal that should be promoted together with building resilient infrastructure, advancing sustainable cities and climate actions, as well as the digitalization of the energy sector. We have analyzed the features of sustainable market regulation that aims to achieve the abovementioned goals associated with the digital single market.

The DSA, for example, addresses a broad scope of intermediaries, and advances a novel approach to market regulation, bringing together the goals of free movement, facilitating innovation, and the effective protection of fundamental rights and consumers. The scope of services covered by the DSA has the potential to resonate throughout the digital market. They include, for example, services of collecting and publishing data related to the energy sector, informing consumers on energy saving options, or developing smart home applications. The text of the DSA reflects the long debate on diligent operation of digital infrastructure services. The discussion on the removal of unlawful content by intermediaries, featured prominently in CJEU case law, is reflected in the DSA and the normative framework for diligent intermediaries. Other regulations, for example, in the data sector, address specific risks, while the DSA provisions can be used to foster a general concept of diligence in EU law.

In the DSA, liability exemptions for intermediaries coexist with a more active role of intermediaries in organizing the safe, secure and predictable online environment. The aforementioned "smart-mix" of obligations and incentives for intermediaries, includes preserving existing liability exemptions, and reinforcing

[88] Art. 36(1) DSA.

the prohibition of a general monitoring obligation now codified in the DSA Regulation, which does not require implementation into national law.

At the same time, the DSA codifies established case law on sustaining the protection of fundamental rights, including the gist of the reasoning in Case C-401/19 *Poland*. Several future regulatory measures are associated with this right: safeguards for the freedom of expression inherently linked to the ability to inform others and getting informed, which depends on information provided to service recipients and consumers, and, if the process works, eventually, results in consumer empowerment. The ambition to sustainably regulate digital markets, and to enhance responsible business behaviour, is articulated in the DSA. It remains to be seen if the implementation of the DSA in practice maintains a balance that allows the set sustainability goals to be achieved.

## Literature

Commision, 'Communication from the Commission to the European Parliament and the Council, Guidance on Art. 17 of Directive 2019/790 on Copyright in the Digital Single Market' COM (2021) 288 final

Commision, 'Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe' COM (2015) 192 final

Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Commission Work Programme 2020 A Union that strives for more' COM (2020) 37 final

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Digitalizing the energy system – EU action plan, COM (2022) 552 final

Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Digitalizing the energy system – EU action plan' COM (2022) 552 final

Commision, 'Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe' COM (2015) 192 final

European Commission, 'European Declaration on Digital Rights and Principles' (*Shaping Europe's digital future*, 15 December 2022) <https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles> accessed 7 July 2023

Gillespie T, *Custodians of the Internet. Platforms, content moderation and the hidden decisions that shape social media* (Yale University Press 2018)

Husovec M, 'The DSA's Scope Briefly Explained' [2023] SSRN <https://ssrn.com/abstract=4365029> accessed 7 July 2023

Michałowicz A, 'Data Altruism in the European Union Law' (Abstract of the unpublished doctoral thesis, University of Łódź 2007)

Quintais JP, Appelman A and Fahy R, 'Using Terms and Conditions to Apply Fundamental Rights to Content Moderation' [2022] SSRN <https://ssrn.com/abstract=4286147> accessed 7 July 2023

Smaga P, 'The concept of systemic risk' (2014) SRC Special Paper No 5

Varbiest T, Spindler G andRiccio MG, 'Study on the Liability of Internet Intermediaries' [2007] SSRN <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2575069> accessed 5 May 2023

Turcios Rodriguez ER,' One thing after another. The role of users, manufacturers and Intermediaries in IoT Security' (Doctoral thesis, Delft University of Technology 2023)

UN General Assembly, 'Transforming our world: the 2030 Agenda for Sustainable Development' (25 September 2015) UN Doc A/RES/70/1

UN, 'Guiding Principles for Business and Human Rights. Implementing the protect-respect-remedy framework' (United Nations 2011)