What will be the economic impact of the Digital Services Act (DSA) on the business models of Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) in the EU?

Auteur : Brühl, Jeremy
Promoteur(s) : Grozdanovski, Ljupcho
Faculté : HEC-Ecole de gestion de l'Université de Liège
Diplôme : Master en sciences de gestion, à finalité spécialisée en droit
Année académique : 2024-2025
URI/URL : http://hdl.handle.net/2268.2/22960

WHAT WILL BE THE ECONOMIC IMPACT OF THE DIGITAL SERVICES ACT (DSA) ON THE BUSINESS MODELS OF VERY LARGE ONLINE PLATFORMS (VLOP) AND VERY LARGE ONLINE SEARCH ENGINES (VLOSE) IN THE EUROPEAN UNION?

Jury:
Supervisor:
Ljupcho GROZDANOVSKI
Reader:
Ashwin ITTOO

Master Thesis by
Jeremy BRÜHL
For a Master's degree in
Management-Law
Academic year 2024/2025

ACKNOWLEGDEMENT

First and foremost, I would like to express my sincere gratitude to Professor Grozdanovski for his invaluable guidance, constructive feedback, and support throughout the development of this thesis. His expertise and encouragement have been important in the shaping of my work. I would like to thank him for his constant support despite a difficult start. I am also thankful for Professor Ittoo for reviewing my master's thesis.

I would also like to thank the Public Policy Manager at Meta for taking the time to participate in the interview, which provided deep insights and greatly enriched the case study section of this thesis. I do not take his participation for granted, especially because I have received numerous rejections from others.

My sincere appreciation also goes to Pascal Arimont, deputy at the European Parliament, for his advice and suggestions during the early stages of my thesis. His support enabled me to establish contact with Meta and other *Very Large Online Platforms* (VLOPs), making this research possible.

Last but not least, I am deeply thankful to my friends and family for their constant encouragement, patience, and belief in me throughout this academic journey. A special thanks goes to Sebastian Zeimers for proofreading my work. He gave me helpful comments, which significantly improved the clarity and precision of my writing.

Thank you all for your support and contributions.

NOTE DE SYNTHESES

Avec l'introduction du Digital Services Act (DSA), l'Union européenne a réagi à l'environnement numérique en constante croissance et évolution. Le DSA est une législation européenne qui vise à protéger les utilisateurs des services en ligne en créant un environnement numérique de confiance et un cadre juridique harmonisé à l'échelle européenne.

Ce mémoire se concentre sur les Very Large Online Platforms (VLOPs) et les Very Large Search Engines (VLOSEs), car ce sont elles qui sont les plus concernées par le DSA, celui-ci leur imposant les obligations les plus lourdes.

La première partie, la revue de littérature, présente les résultats de la recherche existante en lien avec la question de recherche. En guise d'introduction, le DSA est d'abord présenté, en s'intéressant à sa portée temporelle, géographique et matérielle, c'est-à-dire les différents types de services intermédiaires concernés et les obligations qui leur incombent dans le cadre du DSA. Le principe de transparence est ensuite abordé, ainsi que son lien avec le DSA, à travers les obligations de transparence relatives à la modération des contenus, aux systèmes de recommandation, à l'évaluation des risques systémiques et à la publicité. Le régime d'exemption de responsabilité est ensuite expliqué, avant d'analyser le système de mise en œuvre du DSA et le rôle des différents acteurs impliqués : les coordinateurs des services numériques, la Commission européenne, les entités privées.

La partie empirique repose sur une étude de cas des VLOPs de Meta (Facebook et Instagram). Cette étude s'appuie sur les rapports officiels de transparence et d'évaluation des risques, ainsi que sur une interview d'expert réalisée avec le responsable des politiques publiques de Meta, et propose une vision concrète de la manière dont l'une des plus grandes plateformes mondiales répond aux exigences du DSA. Le mémoire met en lumière les défis de conformité, les adaptations nécessaires ainsi que les effets à long terme potentiels sur l'innovation, la compétitivité et les droits des utilisateurs dans l'écosystème numérique.

ABSTRACT

With the introduction of the Digital Services Act, the European Union has responded to the rapidly growing and constantly evolving digital environment. The DSA is an EU law that intends to protect users of online services by creating a trusted online environment and a harmonised legal framework in Europe.

This paper focusses on the *Very Large Online Platforms* (VLOPs) and the *Very Large Search Engines* (VLOSEs), because these are impacted the most by the DSA in terms of obligations laid on them.

The first part, the literature review, provides explanations of the findings of the literature relating to the research question. As an introduction, the thesis will firstly dive into the meaning of the DSA and its temporal, geographical and material scope, i.e., the different intermediary services and their obligations in relation to the DSA. Afterwards, the principle of transparency and its connection with the DSA is explained on the basis of the transparency obligations relating to content moderation, recommender systems, systemic risk assessment and advertising. The liability exemption system of the DSA is explained before finally turning to the analysis of the enforcement system of the DSA and its role of the different actors. These include the digital service coordinators, the European Commission and private entities.

The empirical section of the thesis is based on a case study of Meta's VLOPs (Facebook and Instagram). This case study is grounded in official transparency and risk assessment reports as well as an expert interview with Meta's Public Policy Manager and offers insights into how one of the world's largest VLOPs is responding to the demands of the DSA. The thesis highlights the compliance challenges and adaptations necessary to comply with the new regulatory framework. Additionally, the study discusses potential long-term effects on innovation, competitiveness, and user rights across the digital ecosystem.

Word count: 39. 987

TABLE OF CONTENT

GLOSSARY

Very Large Online Platform	VLOP
Very large Search Engine	VLOSE
Digital Services Act	DSA
Digital Markets Act	DMA
The European Commission	The Commission
The European Board for Digital Services	The Board
General Data Protection Regulation	GDPR
Digital Services Coordinator	DSC
European Union	EU
Consumer Rights Directive	CRD
Artificial Intelligence Act	AIA
Statement of Reasons	SoS
CJEU	Court of Justice of the European Union

LIST OF FIGURES

LIST OF TABLES

INTRODUCTION

Over the past few decades, the rapid progress and development of digital technologies has fundamentally transformed the way individuals, businesses, and governments interact with one another. The 21st century can be seen as the "digital decade", in which the internet and digital platforms have become an important aspect in nearly all aspects of social, economic, and political life (Turillazzi et al., 2023). From online shopping and social media engagement to news consumption and information search, digital services have become an integral part of daily life.

Among the most influential players in this digital ecosystem are Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs). These are defined under the DSA as platforms and search engines that reach at least 45 million active users per month within the EU[1]. Examples of VLOPs include Meta (Facebook, Instagram), TikTok, Amazon and Booking.com, while Google Search and Bing represent typical VLOSEs (European Commission, 2025). These entities provide core online services such as e-commerce, content sharing, video streaming, communication tools, and information search, while serving as intermediaries between businesses and users. This paper will mainly focus on social media platforms, whose primary offerings include content-hosting services and online advertising services**.** Content-hosting platforms, such as Facebook, Instagram, and TikTok, enable users to publish and interact with user-generated content. This places them at the centre of discussions about content moderation, illegal content removal, and fundamental rights protection. Closely linked with these services are advertising-based business models**,** which rely on the monetization of user data to deliver targeted ads and form a key revenue stream for platforms like Meta (Buiten, 2021).

VLOPs offer a wide range of benefits to users, businesses, and society as a whole. One of their most notable advantages is the convenience and accessibility they provide (European Commission, 2019). Platforms like Amazon, Facebook, and YouTube simplify everyday tasks, such as shopping, communication, and information consumption, making them essential tools in the everyday life of many people. Additionally, they make sure that the services are widely available to people across many different locations and living situations. From an economic standpoint, VLOPs create opportunities for businesses and individuals. VLOPs offers smaller companies the possibility of global visibility, targeted advertising, and direct access to the European market with the aim to create a fair competitive environment (Cohen, 2017; Moravcová, 2023; Turillazzi et al., 2023). Furthermore, online platforms make it possible for users to generate income based on activities on their platform such as the placement of advertising (Cohen, 2017). Furthermore, VLOPs enhance social connectivity, as they offer the possibility of real-time interaction and communication among users around the world (Van Dijck et al., 2018). Thanks to social media platforms in particular, it has become much easier to maintain personal relationships throughout the world while also offering a place for the exchange of opinions, political expressions and fostering public discourse in general (Van Dijck et al., 2018). Additionally, they offer a simple and easily accessible way of acquiring information and knowledge (Unesco, 2024). Platforms such as Google Search and YouTube provide immediate access to educational content, news, tutorials, and user-generated expertise, significantly simplifying the access to information. Finally, the rise of VLOPs can lead to technological advancement and innovation in artificial intelligence, algorithmic content moderation and other areas (Cohen, 2017). The result is a more personalized user experience, as recommendation systems adapt content and advertisements to the user preferences (European Commission, 2019; Kenney & Zysman, 2016).

Despite the many advantages, VLOPs also pose a range of significant challenges that attract the attention from regulators. According to the DSA, one of the most pressing concerns is the widespread

[1] Art. 33 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) *OJEU, L 277, 27.10.2022, p. 1–102* (hereafter abbreviated DSA)

dissemination of illegal or harmful content, such as hate speech, terrorist propaganda, or content concerning the sexual abuse of children (Turillazzi et al., 2023).[2] In addition to hosting illegal content, VLOPs can contribute to the violation of fundamental rights, including the rights to privacy, non-discrimination, and freedom of expression (Cohen, 2017; Turillazzi et al., 2023).[3] A major factor behind these risks is the lack of transparency and accountability regarding how platforms operate (Leerssen, 2023). Users often remain unaware of how decisions about content curation, moderation, or personalized advertising are made. Furthermore, the extensive collection of data can lead to serious privacy concerns (Cohen, 2017; Zuboff, 2023). Their economic power is very high, because VLOPs are very dominant in the digital market, which can lead to VLOPs creating an entry barrier for smaller competitors (Crémer et al., 2019). Lastly, users are in many cases left without effective appeal mechanisms, facing difficulties when contesting takedown decisions or attempting to understand why certain content is promoted or removed (Gillespie, 2018). These combined challenges highlight the growing need for robust regulation, such as the DSA, to ensure that platforms can be held accountable for their societal and economic impacts.

This complexity raises the question of to what extent these online platforms can be held responsible for the content they host or distribute. Historically, EU regulation was based on the E-Commerce Directive, which provided a liability exemption for hosting providers who were unaware of illegal content on their platforms (Buiten, 2021).[4] However, the Directive had become outdated as the digital landscape had evolved dramatically due to the exponential growth in digital services, the increasingly dominant role of platforms, and the higher social impact of online content (Turillazzi et al., 2023). In response, the European Union introduced the DSA as a part of a broader digital strategy, the “Europe Fit for the Digital Age” agenda. It aimed at shaping Europe’s digital future and is designed to ensure the protection of European values and rights in the digital space (European Council, 2022; Turillazzi et al., 2023). The DSA represents an update to the regulatory landscape, seeking to establish a uniform framework for digital services across the EU.[5] It imposes a set of due diligence obligations on digital service providers such as VLOPs and VLOSEs with the goal of enhancing user safety, promoting accountability, and protecting fundamental rights in the online environment.[6] Furthermore, the DSA aims to create a legal certainty for the service provider (European Commission, 2022). The DSA introduces several new tools for tackling systemic risks, including requirements for risk assessment, algorithmic auditing, and compliance reporting. Concerning the liability system, the DSA does not fundamentally change the liability exemption principle established by the E-Commerce Directive but introduces clearer responsibilities, especially for VLOPs (Buiten, 2021).

One of the cornerstone principles of the DSA is transparency. In the context of online platforms, transparency can be seen as the clarity and accessibility of information about how platforms operate, particularly regarding content moderation, algorithmic decision-making, and advertising systems (Ananny & Crawford, 2018). As digital platforms play an increasingly important role in shaping public discourse and economic activity, the calls for disclosure are getting louder in order to guarantee democratic accountability, user rights, and mitigate systemic risk (Gillespie, 2018). The DSA directly addresses these concerns by introducing robust transparency obligations for intermediary services, especially VLOPs and VLOSEs. Under the DSA, platforms are required to explain their content moderation policies, provide clear justifications for content removals or account restrictions, and offer users meaningful appeal mechanisms in order to ensure, that users are not subjected to arbitrary or

[2] Art 34 and others DSA

[3] Recital 81 DSA

[4] Art.12-15 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') OJEU, L 178, 17.7.2000, p. 1–16 (hereafter abbreviated E-commerce Directive

[5] Recital 4 DSA

[6] Art. 1 DSA

discriminatory decisions.[7] Moreover, the DSA mandates that VLOPs and VLOSEs conduct and publish annual risk assessments related to the dissemination of illegal content, threats to fundamental rights, and the manipulation of electoral processes or public health debates.[8] These assessments must be complemented by concrete mitigation strategies, ensuring that platforms take proactive steps to address the societal harms they may contribute to.[9] Transparency is also crucial in the area of online advertising, where users are often unaware of why specific ads are shown to them or how their personal data is used for targeting purposes.[10] The DSA requires platforms to clearly label advertising, identify the sponsor, and disclose key parameters used for targeting.[11] This empowers users to better understand and control their digital environment and to understand how their personal data is used. Finally, the DSA asks for independent auditing and public accountability. It grants regulators and researchers, access to platform data for the purpose of independent audits and impact assessments. This represents a significant step toward external oversight and shifts the balance of power away from platform self-regulation (Buiten, 2021). In sum, transparency within the DSA is not an end in itself but a way to govern online platforms to ensure a safer and more competitive digital economy (Flyverbom, 2015).

Therefore, these platforms needed to make some investments and adaptations to their systems in order to comply with the act. This thesis therefore focuses on the economic impact of the DSA on the business models of VLOPs and VLOSEs. In particular, it examines how compliance with transparency and accountability obligations affects platform operations and strategic decision-making. Through qualitative research, including a semi-structured interview with a public policy manager from META and an analysis of scientific literature and regulatory documents, this study seeks to answer the following research question:

What will be the economic impact of the Digital Services Act (DSA) on the business models of Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) in the EU?

The remainder of this thesis is structured as follows: The literature review covers in the first section a general overview over the DSA and its scope of application. Section 2 analyses the principal and the role of transparency within the DSA. Section 3 and 4 centre around the liability and the enforcement system of the DSA. Section 5 clarifies the methodology used for the case study in Section 6. Lastly, Section 7 makes the link between the literature and Meta case study.

[7] Art. 16,17 and others DSA
[8] Art. 34 DSA
[9] Art. 35 DSA
[10] Art. 26 DSA
[11] Art. 26 DSA

LITERATURE REVIEW

1. The Digital Services Act (DSA)

1.1 Definition

The DSA follows the E-Commerce Directive and is intended to create a legal framework suited to the challenges of the 'digital decade'(Savova et al., 2021; Turillazzi et al., 2023). The DSA is not pursuing a completely new approach to mastering the new challenges. Rather, it co-exists to a certain extent with the E-Commerce Directive (Savova et al., 2021). The DSA does not collide with the E-Commerce Directive and other European regulations but rather complements them (Moravcová, 2023). It helps to create a unified European digital market where the platforms are controlled by democratic entities (Chander, 2023; Erixon, 2021). The DSA uses a pyramidal approach (Andriychuk, 2021). This means that the obligations for service providers vary depending on different factors like the size, the role and the impact on the market in order to promote fair competition and to prevent large online platforms from abusing their position (Turillazzi et al., 2023). This is why intermediary services are less regulated than hosting services, hosting services are less regulated than online platforms, ... Critics claim that this approach does not eliminate harmful content but only pushes it to smaller platforms that are less strictly regulated (Erixon, 2021).

The DSA contains various rules to make life on the internet safer. Platforms have to take down inappropriate content without setting a regime of censorship (Erixon, 2021). The platforms have to find a balance between freedom of speech and the control of harmful content (Erixon, 2021). The DSA must strike a good compromise between transparency and the protection of privacy and intellectual property, which is hard to achieve (Edwards & Veale, 2017; Gorwa & Ash, 2020). Whether on social media, online marketplaces or other application areas, the DSA imposes rules on providers to make interaction on the internet more respectful and trusted. The DSA should ensure that users are protected from inappropriate and illegal content, fake news, but also from faulty or harmful products.[12] To achieve this goal, the service providers have to be proactive (Buiten, 2021; Moravcová, 2023). In addition, a lot of other stakeholders benefit from the DSA, such as the service providers due to legal certainty and harmonization of legislations across Europe (Moravcová, 2023).

Through its commitment to transparency, the DSA should both encourage competition and innovation and reinforce the trust in the service providers (Article 1 DSA).

1.2 Scope

The scope of application of the DSA spans over the temporal, the substantive and the geographical dimension.

1.2.1 Temporal scope

Intermediary services are subject to different dates or deadlines for some categories, because they are regulated differently. Since this paper focuses on VLOSE's and VLOP's, only dates and deadlines relevant to these platforms will be included in the analysis.

On the 15th of December 2020, the European Commission came up with the proposal to draft the DSA in order to adapt the European legislation to the challenges of the "Digital Decade" and to deliver an update to the obsolete E-commerce Directive (Turillazzi et al., 2023). Over the following months, the legislation was developed.

After the DSA was adopted by the European Parliament and the Council with a large majority, it was published in the Official Journal of the European Union on 27 October 2022. On February 17, 2024, the

[12] Recital 40 DSA

DSA came fully into effect, becoming legally binding for VLOPs and VLOSEs. Nonetheless, some articles relating to the VLOP'S already came into force earlier on 16 November 2022. These are listed in Article 93 DSA and contain some obligations that VLOPs were required to fulfil before 24 February 2024(European Parliament, 2022).

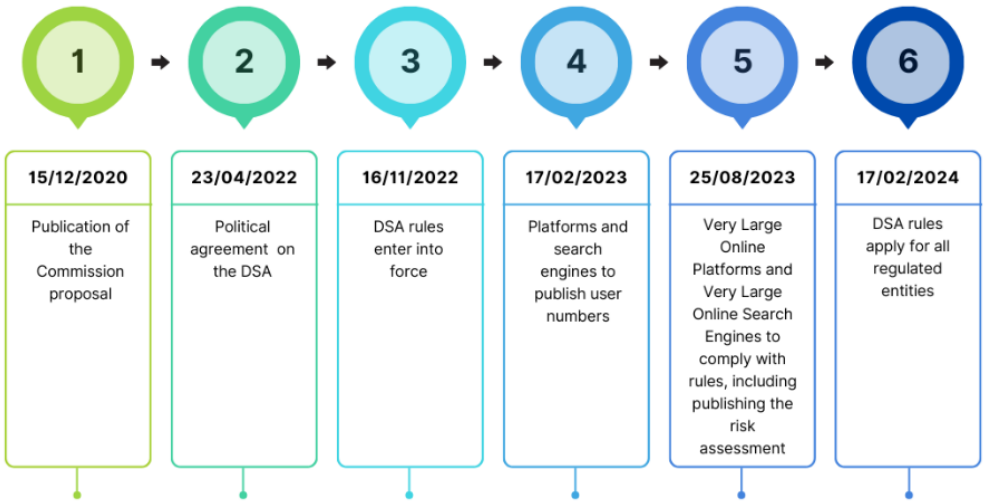
Article 93 of the DSA:[13]
"This Regulation shall apply from 17 February 2024.However, Article 24(2), (3) and (6), Article 33(3) to (6), Article 37(7), Article 40(13), Article 43 and Sections 4, 5 and 6 of Chapter IV shall apply from 16 November 2022."

The main purpose of these articles is to ensure that the DSA comes into force smoothly. To achieve this, certain transparency rules have already come into effect, such as the reporting obligation to publish the monthly active users of the platforms.[14] Based on these figures, the platforms that meet the threshold are designated as VLOP's or VLOSE's.[15] Furthermore, the requirement of independent auditing[16], data access provisions[17], supervisory fees[18], as well as Sections 4, 5 and 6 of Chapter IV concerning the enforcement and non-compliance penalties, also came into force earlier.

Since 16 November 2022, the European Commission has the authority to classify online platforms as VLOPs.[19] Once a platform is designated as VLOP, it must submit a transparency report to the Commission. This must be done within 4 months after designation or by 17 February 2023 at the latest. Within this period, the newly designated VLOP must comply with the obligations and rules that apply for these platforms. If those obligations are not fulfilled, the Commission can take action against the provider and possibly impose sanctions (European Parliament, 2022).

The Commission and the EU Member States should also take measures to guarantee the implementation, fulfilment and control of these obligations.

Figure 1: Timeline of the DSA (Cyber Expert, 2024)



[13] Art. 93 DSA
[14] Art. 24 DSA
[15] Art. 33 DSA
[16] Art. 37 DSA
[17] Art. 40 DSA
[18] Art. 43 DSA
[19] Art. 24 DSA

1.2.2 Geographical scope

Article 2.1 of the DSA:[20]
"This Regulation shall apply to intermediary services offered to recipients of the service that have their place of establishment or are located in the Union, irrespective of where the providers of those intermediary services have their place of establishment."

As indicated in Article 2.1, it is not important whether the service provider is based within the EU or not. The regulations apply as soon as the provider offers an intermediary service to users that are based within the EU. This can lead to a loss of attractivity of the European market(Turillazzi et al., 2023). The DSA has a large scope of application which helps to reduce the compliance costs for service providers and ensures a standardised legal framework among Member States (Turillazzi et al., 2023).

According to the DSA, the intermediary services have the obligation to determine a legal representative within the EU when the place of establishment is outside the Member States.[21]

Even if the DSA is only applicable in the EU Member States, a certain "Brussels Effect" is likely (Chander, 2023) and it would not be a novelty to EU regulations (Bradford, 2020). One speaks of the Brussels Effect when European legislation serves as inspiration for laws in other parts of the world. Previous regulations such as the "EU Code of Conduct against Illegal Hate Speech Online" created a similar effect (Nunziato, 2023). Despite its EU focus, it carries certain burdens that contribute a global influence (Nunziato, 2023). Since the DSA places more emphasis on protecting platform users from harmful content than on the absolute enforcement of freedom of expression, it can lead to conflicts with laws that take an opposite approach as in countries such as the United States (Nunziato, 2023). Furthermore, the DSA may require additional procedural requirements compared to other legislative frameworks around the world (Nunziato, 2023). Additionally, the definition of illegal content is not necessarily the same around the world. For instance, the denial of the Holocaust is a crime in Germany, while it is not prohibited in the USA (Piotr, 2022). Despite all these obstacles, it is highly likely that platforms will adapt their global content moderation practices and other procedural requirements to the European framework. This is especially due to the fact that the DSA could impose extremely high penalties and sanctions for non-compliance, which is why many platforms have an incentive to become compliant with the DSA and globalizing their content moderation approach (Chander, 2023; Nunziato, 2023). Through this strong legislation, the EU can thus influence how content moderation is handled worldwide(Nunziato, 2023).

The EU and its Member States are democratically governed and both the various constitutions and the 'Charter of Fundamental Rights of the European Union' provide a certain legal and democratic framework (Chander, 2023).[22] These are good prerequisites and therefore it is interesting for countries outside the EU to align their legislation with the European model because the objectives of the DSA are shared globally (Bradford, 2020; Chander, 2023). When talking about the potential global effect of the DSA, one must also consider that various guidelines of the DSA could be misappropriated or even used as a weapon to achieve an excessive governmental control of the internet. The DSA contains a number of precautions to prevent it from being misused by states, such as the independence of the Digital Services Coordinator, various conditions regarding trusted flaggers and risk mitigation measures (Chander, 2023).[23]

1.2.3 Material Scope: The different intermediary services and their due diligence obligations

The DSA's material scope of application is comparable to that of the E-Commerce Directive. However, the DSA imposes several additional due diligence obligations and there is a new subdivision of the

[20] Art 2 DSA
[21] Art. 13 DSA
[22] Charter of Fundamental Rights of the European Union, OJEU, C 326, 26.10.2012, p. 391–407 (hereafter abbreviated "Charter")
[23] Art. 22 DSA

service provider subcategories (Buiten, 2021; Savova et al., 2021). The DSA has a multi-level, pyramidal structure (Andriychuk, 2021; Buiten, 2021). The obligations that these online providers have increase with their importance and influence on the market (Strowel & De Meyere, 2023; Turillazzi et al., 2023). This pyramidal structure is divided into four levels. These different levels should guarantee fair competition, should ensure that the larger service providers do not abuse their market position and prevent legal barriers (Lomba & Evas, 2020). The due diligence obligations should balance the liability exemption framework and are not preconditional to the exemption (Husovec & Roche Laguna, 2022).

The pyramid's basis is formed by the providers of intermediary services which have the fewest obligations to fulfil and are the least strictly regulated. The second level includes the providers of hosting services. As Art. 3 (g) of the DSA statues:[24]

"'intermediary service' means one of the following information society services:
(i) a 'mere conduit' service, consisting of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network;

(ii) a 'caching' service, consisting of the transmission in a communication network of information provided by a recipient of the service, involving the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients upon their request;

(iii) a 'hosting' service, consisting of the storage of information provided by, and at the request of, a recipient of the service;"

These first two layers have the obligation to establish a single point of contact and if necessary, designate a legal representative.[25] Furthermore, they have to respect some criteria in their terms and conditions regarding content moderation[26] and are subject to several reporting obligations about content takedowns, content moderation and the number of complaints received.[27] There are a few additional obligations for the hosting services like the establishment of a notice and action mechanism which gives users the possibility to notify illegal content to the service provider.[28] In case of content takedowns or visibility restrictions, the hosting service provider has to deliver a statement of reason to the concerned person, in order to transparently explain their approach to the user.[29] Finally, hosting service providers have to report content that indicates a criminal offence to the competent authorities.[30]

The following two levels are composed of online platform providers, whereby an additional distinction is made between 'online platforms' (level 3) and 'very large online platforms' (level 4). As Article 3 (i) statues:[31]

„'online platform' means a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public, unless that activity is a minor and purely ancillary feature of another service or a minor functionality of the principal service and, for objective and technical reasons, cannot be used without that other service, and the integration of the feature or functionality into the other service is not a means to circumvent the applicability of this Regulation;"

[24] Art. 3 DSA
[25] Art. 11-13 DSA
[26] Art.14 DSA
[27] Art.15 DSA
[28] Art.16 DSA
[29] Art.17 DSA
[30] Art.18 DSA
[31] Art. 3 DSA

Additional to the aforementioned obligations, online platforms must meet other requirements such as the establishment of an internal complaint-handling mechanism[32] and offering users the possibility to access an out-of-court settlement.[33] Moreover, online platform providers give a priority to the notices provided by trusted flaggers.[34] Additional to the reporting obligations under Article 15 of the DSA, online platforms must report information about their monthly active users, the suspensions taken under Article 20 DSA and conflicts under out-of-court settlement bodies.[35] Moreover, there are some requirements considering advertising[36] as well as transparency requirements for recommender systems.[37]

1.2.3.1 VLOP's and their obligations

At the top of the pyramid are the VLOPs who have to fulfil most of the obligations. VLOPs are online platforms that are visited by an average of at least 45 million users within the EU. Article 33 of the DSA which is called "*Very large online platforms and very large online search engines"* defines them in the first section as follows[38]:

"This Section shall apply to online platforms and online search engines which have a number of average monthly active recipients of the service in the Union equal to or higher than 45 million, and which are designated as very large online platforms or very large online search engines pursuant to paragraph 4."

The DSA also shows that this threshold of 45 million users corresponds to around 10% of the population of the EU Member States. So, if the population of the EU changes significantly over the next few years, this value can be adjusted so that it can correspond to around 10% of the population. Critics argue that this threshold is set too high and that only the highly influential platforms are affected. They believe that various platforms that do not reach the threshold should also fulfil the same requirements as the VLOPs (Andriychuk, 2021). The platforms must report to the European Commission every 6 months on the number of their average users. If an online platform reaches the threshold of users, it will be categorised as VLOP or VLOSE by the European Commission and must adapt to the applicable rules within a period of 4 months.[39]

The additional obligations and requirements regarding VLOPs are rather requests for transparency towards the regulator than transparency towards the end users (Sanchez, 2024).

As VLOPs have a major impact on social life, the DSA imposes risk management obligations on them in order to reduce systemic risks (Strowel & De Meyere, 2023).[40] Further, VLOP'S should establish crisis response mechanisms to better manage upcoming crises[41] and independent audits should control the respect of due diligence obligations and codes of conducts.[42] The DSA requires VLOPs to make certain data available to the European Commission and the DSCs upon request so that they can verify compliance with the DSA.[43] Finally, the DSA imposes additional requirements regarding recommender

[32] Art. 20 DSA
[33] Art. 21 DSA
[34] Art. 22 DSA
[35] Art. 24 DSA
[36] Art.26 DSA
[37] Art.27 DSA
[38] Art. 33 DSA
[39] Art. 33 DSA
[40] Art. 34 and 35 DSA
[41] Art. 36 DSA
[42] Art. 37 DSA
[43] Art. 40 DSA

systems,[44] transparency in advertising[45] as well as additional reporting obligations.[46]The different obligations for the different service providers are illustrated at Figure 2.

Critics claim that these additional obligations for VLOPS are preventing some platforms from growing, as these requirements are also associated with additional costs and labour. They also fear that the stricter rules for VLOPs will shift illegal and harmful content to the smaller, less strictly regulated platforms. In other words, bad content could be off-shored to less regulated service providers (Erixon, 2021). On the positive side, the harmful content is shown to a smaller audience. On the negative side, it can lead to people becoming radicalised on smaller platforms, thereby becoming even more dangerous (Erixon, 2021).

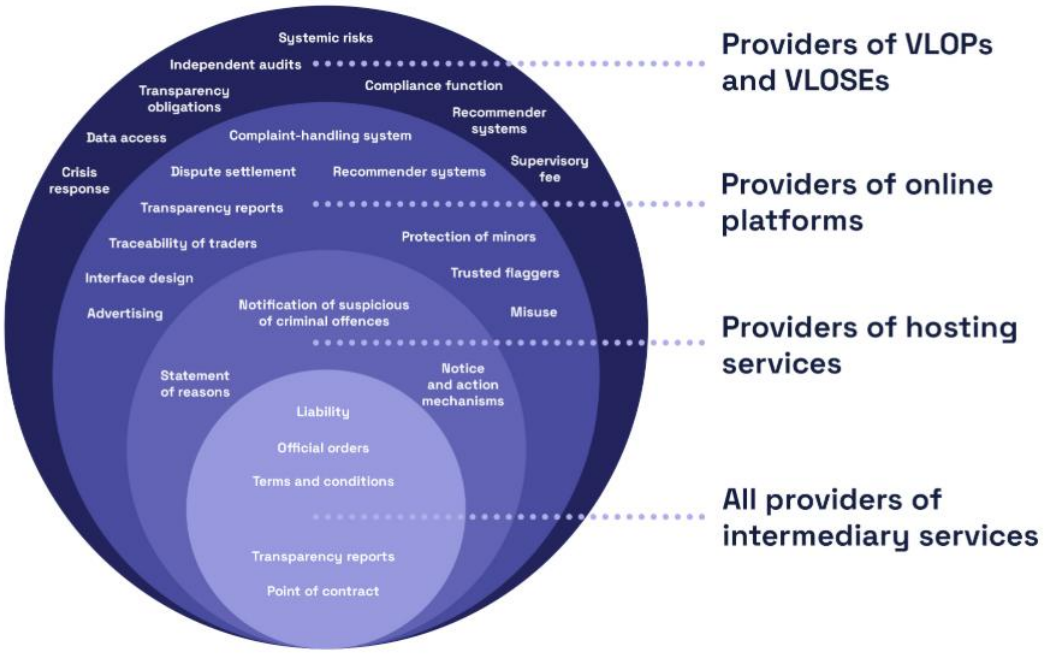


Figure 2: The different intermediary services and their obligations (Chatterjee, 2023)

1.2.3.2 Comparison with the designation of gatekeepers within the DMA

Both, the DSA and the DMA[47] are part of the digital agenda introduced by the EU and should work coherently. However, the legislators chose different approaches, leading to difficulties. Unlike the DSA's pyramidal approach, the DMA takes a binary approach to appoint gatekeepers, which strengthens inter-platform competition (Andriychuk, 2021). The pyramidal approach, on the other hand, makes it more difficult to scale up and penetrate the market because of its increasing obligations (Andriychuk, 2021).

Furthermore, the designation as a VLOP depends solely on reaching a numerical, quantitative threshold[48], whereas designation as a gatekeeper depends on both quantitative and qualitative factors. The qualitative requirements are listed at Article 3 (1) DMA as followed:[49]

[44] Art. 38 DSA
[45] Art. 39 DSA
[46] Art. 42 DSA
[47] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) *OJEU, L 265, 12.10.2022, p. 1–66* (hereafter abbreviated DMA)
[48] Art. 33 DSA
[49] Art. 3 DMA

"(a) it has a significant impact on the internal market; (b) it provides a core platform service which is an important gateway for business users to reach end users; and (c) it enjoys an entrenched and durable position, in its operations, or it is foreseeable that it will enjoy such a position in the near future."

The quantitative criteria to become a gatekeeper are more detailed and demanding than in the DSA. First, Article 3 (2) of the DMA requires "*an annual Union turnover equal to or above EUR 7,5 billion in each of the last three financial years".* Second, it is requested, that the platform has "*in the last financial year at least 45 million monthly active end users established or located in the Union and at least 10 000 yearly active business users established in the Union".* Finally, these thresholds must also be met over the last three financial years.[50]

As we can see, VLOPs in the DSA are a broader category of market operators than that of gatekeepers in the DMA. This means that platforms are first appointed as VLOPs even before they fulfil the conditions for gatekeepers. This in turn means that the other gatekeepers can prepare for the arrival of the new platform, as their growth is delayed by the additional obligations. The DSA is more focused on intra-platform competition whereas the DMA focuses on the inter-platform competition (Andriychuk, 2021).

2. Transparency

Transparency is one of the key concepts of the DSA and has become an important governance tool over the last years and a key element to increase the accountability of service providers (Braithwaite & Drahos, 2000; Waddock, 2004). Furthermore, it is a way for companies to showcase their commitment to social responsibility and ethical integrity to the public (Tapscott & Ticoll, 2003). Transparency is essential for the purpose of protecting the fundamental rights of users, strengthening their trust in platform providers and guaranteeing a secure online environment. However, the idea of transparency did not start with the DSA. Previous legislation, such as the E-Commerce Directive[51] or the Consumer Rights Directive (CRD)[52], also required service providers to disclose certain information in order to promote transparency. However, the DSA takes transparency a step further then these previous legislations. For instance, platforms must collect and verify information from traders who are active on their platforms. Under previous regulations, platforms were seen as passive intermediaries (Cauffman & Goanta, 2021).

Large online platforms like Google, Twitter and Facebook published voluntary "Transparency reports", further proving that transparency played a role in the digital ecosystem even before the DSA in the 2010's (Gorwa & Ash, 2020). In the field of advertising transparency, these platforms took voluntary action too, by introducing "paid for by" and "political advertising" notions (Gorwa & Ash, 2020; Walker, 2018). Critics argue that the voluntary transparency reports provided by the platforms often lacked clarity (Andriychuk, 2021; Myers West, 2018).

Transparency can be seen as an instrument in the fight against corruption and improving governance through open decision-making. Transparency can enhance efficiency and effectiveness, therefore leading to more accountable systems (Ananny & Crawford, 2018; Ball, 2009; Flyverbom, 2015). The feeling of uncertainty about the decision-making process scares many people. Transparency in the decision-making processes of platform providers gives users a certain amount of control, which helps them to understand various processes and gives them a sense of security (Ananny & Crawford, 2018; Phillips, 2011). However, publishing information only leads to a better understanding if users can make

[50] Art. 3 DMA

[51] Art. 5 and 6 E-commerce Directive

[52] 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 Text with EEA relevance, OJEU, L 304, 22.11.2011, p. 64–88

sense of the information that has been shared (David, 2018). Sometimes the information disclosed is too complex for the average person, so the transparency process only adds value for the user if he is able to understand and process the disclosed information (Ananny & Crawford, 2018; Christensen & Cheney, 2015). Thus, there are some critics who question the idea that more information always means better management of the systems (Albu & Flyverbom, 2019).

Transparency is not inherently neutral. The selection and dissemination of specific information can direct the focus of public attention toward particular content while minimizing or omitting attention toward other information. Consequently, by strongly emphasising and publishing various things, other matters are overshadowed and do not receive the attention that would actually be necessary. This could have an influence on the public perception and decision-making (François & Douek, 2021). Thus, transparency can serve as a mechanism for guiding behaviour and shaping discourse, making it a potential tool for political, social, or economic influence (Ananny & Crawford, 2018; Flyverbom, 2015; Gorwa & Ash, 2020).

There are various types of transparency. We cannot assign the DSA to a specific type because different articles of the DSA require different types of transparency (Ananny & Crawford, 2018).

First, it is essential to differentiate between "fuzzy" and "clear" transparency. Fuzzy transparency refers to the disclosure of information that, while formally accessible, lacks usefulness because it is incomplete, ambiguous or difficult to interpret (Christensen & Cheney, 2015; Fox, 2007). In the context of the DSA, critics argue that certain provisions and transparency obligations are not precise enough and call for a more stringent and clearly defined regulatory framework (Flyverbom, 2015). Conversely, clear transparency is characterized by the disclosure of specific, comprehensive, and practically useful information (Ananny & Crawford, 2018; Fox, 2007). An illustrative example of this within the DSA is Article 24, which mandates transparent reporting obligations, ensuring that the disclosed data is both structured and actionable. The information required in Art. 24 DSA is detailed, verifiable, standardized and their compliance can be monitored.[53]

A distinction can also be drawn between "hard" and "soft" transparency. Hard transparency is characterized by the existence of enforceable regulatory mechanisms, where non-compliance with disclosure obligations can result in sanctions, penalties, or other legal consequences. In the DSA, some articles call for legally binding penalties of up to 6% of the global annual turnover. In contrast, soft transparency requires the disclosure of information but operates under a weaker enforcement framework. It is based primarily on voluntary compliance, reputational incentives, or social pressures instead of formal penalties (Ananny & Crawford, 2018; Fox, 2007). Examples include the voluntary 'Codes of conducts[54], the crisis response mechanism[55] and the data access for researcher provision.[56]

Furthermore, transparency can be categorised according to its direction (Flyverbom, 2015). Online platforms are considered to have a high level of vertical transparency but to be rather untransparent in a horizontal way (Flyverbom, 2015). In this case, we speak of upward or downward transparency as well as inwards and outwards transparency (Ananny & Crawford, 2018; Flyverbom, 2015).

Upward transparency is the flow of information from subordinated entities or lower hierarchical levels (service providers) to higher authorities or regulatory bodies (European Commission or DSC). The information flows in this case from a lower to a higher level. This process facilitates oversight, decision-making, and regulatory compliance by enabling the regulatory bodies to monitor and assess the actions

[53] Art. 24 DSA
[54] Art. 45 DSA
[55] Art. 36 DSA
[56] Art. 40 DSA

and performance of the service providers (Ananny & Crawford, 2018; Heald, 2006). As an example, we can take the reporting obligations[57] or the risk assessment obligations.[58]

Downward transparency, by contrast, involves the flow of information from the top down the hierarchy, so from platforms to users (Ananny & Crawford, 2018; Heald, 2006). For instance, the DSA requires service providers to disclose who funded an advertisement, as well as the purpose behind its appearance, such as political advertising.[59] Furthermore, platforms have to explain the logic behind their recommender systems to users in a clear and simplified language, while also highlighting the key factors that influence recommendations.[60]

In the horizontal direction, transparency can be divided into inwards and outwards (Flyverbom, 2015).

With outwards transparency, information flows from within the platform to external stakeholders. The goal is to ensure that platforms allow users, regulators, and the public to understand their processes (Flyverbom, 2015; Heald, 2006; Reig et al., 2021). In the DSA, examples of outwards transparency include advertising disclosures[61], content moderation reports,[62] and recommender system explanations.[63]

Inwards transparency is the opposite, with information flowing from external sources into the platform. This allows externals to contribute knowledge that enhances decision-making and holds platforms more accountable (Ananny & Crawford, 2018; Flyverbom, 2015; Heald, 2006). Examples of the DSA include the independent audit procedure for VLOPs[64] and the option for platform users to report harmful content.

A further distinction exists between transparency as an event and transparency as a process. The first provides a snapshot of information at a specific moment. It focuses on the final outcome in order to identify the targets of transparency (Ananny & Crawford, 2018; Heald, 2006). The DSA imposes for example the obligation for platforms to deliver an explanation to the user if their content has been removed.[65] In contrast, transparency as a process focuses on ongoing procedures and continuous disclosure, with the primary aim of establishing visibility conditions. It is rather proactive than reactive (Ananny & Crawford, 2018; Heald, 2006). An example of this is the appeal mechanism for content removal, which is an ongoing process.[66]

The last distinction can be made between real-time transparency and retrospect (ex-post) transparency. The former is proactive whereas the latter is reactive (Ananny & Crawford, 2018; Heald, 2006).

However, transparency is not a cure-all medicine that immediately fixes every issue. It has its limitations and is not without its criticisms (Ananny & Crawford, 2018; Heald, 2006). To be valuable, several factors need to be considered. Some critics say that truth is not achieved by disclosure but rather through relationships and interactions (Ananny & Crawford, 2018). Thus, the human component should not be left out in the discussion (Crawford, 2016).

Transparency must go hand in hand with a certain power. It must be accompanied by the ability to analyse and understand the disclosed data in order to change something in a meaningful way (Heald,

[57] Art. 24 DSA
[58] Art. 34 DSA
[59] Art. 26 DSA
[60] Art. 27 DSA
[61] Art. 26 DSA
[62] Art. 15 DSA
[63] Art. 27 DSA
[64] Art. 37 DSA
[65] Art. 17 DSA
[66] Art. 17 DSA

2006). Action must be taken when misconduct is revealed. If there would not be consequences for wrongdoing despite the disclosure, transparency becomes meaningless and loses its value (Ananny & Crawford, 2018).

Total transparency can mean a significant invasion of privacy and could have an intimidating effect on some individuals (Ananny & Crawford, 2018). It could cause platforms to lose their competitive edge, particularly if they fully disclose sensitive information like their algorithms (Crain, 2018). Therefore, transparency should not be seen as a binary principle in which there is only a choice between total openness and total secrecy (Ananny & Crawford, 2018). Thus, significant attention should be given to what information must be made public and under what conditions so it still serves the public good (Fox, 2007).

Another issue is that when too much information is disclosed, the key details can get buried, potentially leading to opacity. On the one hand, this can happen unintentionally, but it might also be a strategic decision by the platforms to overwhelm external stakeholders with irrelevant information, making it difficult to find what truly matters (Stohl, 2016). Therefore, seeing information does not necessarily mean that you understand it. To fully understand how something works, it's essential to consider how the process, information, or system interacts with its environment and the impact it has on it (Ananny & Crawford, 2018; Resnick et al., 2000). To fully access the bigger picture, it is necessary to grasp both the individual components and how they work together (Resnick et al., 2000).

A significant technical challenge exists in achieving transparency, particularly with algorithms, as they continuously evolve, making them inherently complex and difficult to monitor over time (Crain, 2018; Diakopoulos, 2016).

2.1 Content moderation and shadow banning through the lens of transparency

Content moderation is a common practice used by platform providers to reduce the visibility of certain types of content on their platforms (Leerssen, 2023). It is often seen as necessary for platforms to function (Gillespie, 2018) and to ensure that the diffusion of socially harmful content is reduced (Katsaros et al., 2022) and community guidelines are respected (Drolsbach & Pröllochs, 2023; Horta Ribeiro et al., 2023). However, content moderation practices are not always as obvious to detect as, for example, deleting content or blocking accounts. Often, a less visible form of content modification, called 'shadow banning', is used (Gillespie, 2022; Leerssen, 2023). Shadow banning can be defined as "*a wide range of techniques that artificially limit the visibility of targeted users or user posts*" (Le Merrer et al., 2021). It can be interpreted as a secret sanction or as a choice of platform design (Leerssen, 2023). Yet, from a legal point of view hidden sanctions are viewed critically, as the person against whom the sanctions are directed has no chance to justify themselves or to contest these sanctions (Waldron, 2016).

Common practices in shadow banning are downranking, delisting and demonetization (Cotter, 2023; Jaidka et al., 2023; Leerssen, 2023). Using these practices, visibility is reduced without the user realizing it (Radsch, 2021). While the detection process is difficult and costly (Gillespie, 2022) ,their impact is also hard to determine, because the visibility of content on platforms is personalized and determined by complex algorithms (Jaidka et al., 2023; Le Merrer et al., 2021; Leerssen, 2020). In contrast to account suspension and content takedown, downranking is not a binary principle. It is therefore hard to draw a line and to define when content has been treated unfair (Gillespie, 2022). The fact, that it is hard to determine if and by how much an item is downranked, is a considerable problem of the DSA (Leerssen, 2023). A lack of transparency can lead to users not understanding why their uploaded content is being deleted or downranked which can quickly lead to mistrust and the platforms being accused of restricting freedom of expression (Gorwa et al., 2020; Leerssen, 2023; Suzor et al., 2019). It is often not clear whether the content has been moderated due to its classification (e.g. as harmful content) or because it is not relevant in the eyes of the platform providers (Thorson & Wells, 2016).

A lot of platforms use shadow banning because it is a more moderate way to reduce visibility. For instance, in order to remove disinformation or content that is "lawful but awful", the platform can just downrank it and thereby reduce its visibility (Leerssen, 2023). With this approach, the platforms avoid accusations of censorship and restrictions on freedom of expression, as the people concerned are unaware of shadow banning processes (Leerssen, 2023). The platforms can prevent the spread of disinformation without having to become "arbiters of truth" (Leerssen, 2023; Swisher, 2018). The responsibility goes from "no-publication" to "no-spread" of concerned content (Keller, 2021; Miller, 2021).

A further distinction can be made between content moderation based on behaviour or based on the actor (François & Douek, 2021).

2.1.1 Content moderation and shadow banning within the DSA

The fact that transparency is one of the key principles of DSA is also reflected in the content moderation rules. Before the introduction of the DSA, content moderation was largely based on self-regulation (Trujillo et al., 2024). The DSA establishes a notice and action mechanism,[67] which is not only applicable against illegal content but also against content that violates the Terms and Conditions of the platforms (Leerssen, 2023). The notice and action mechanism has a broad scope of application and Article 3(t) of the DSA defines content moderation in a similarly extensive way.[68] Content moderation under the DSA does not only refer to the removal of content but includes also shadow banning practices that reduce the visibility of content such as delisting and downranking. This represents an added value of DSA, because previous regulations took shadow banning procedures rarely into consideration (Leerssen, 2023). These visibility restrictions are defined at Recital 55 DSA as followed:[69]

"Restriction of visibility may consist in demotion in ranking or in recommender systems, as well as in limiting accessibility by one or more recipients of the service or blocking the user from an online community without the user being aware ('shadow banning')."

As already discussed in the previous section, transparency without understanding is not valuable (Ananny & Crawford, 2018; Christensen & Cheney, 2015). Therefore, the DSA imposes on the service providers to deliver in their Terms and Conditions "*information on any policies, procedures, measures and tools used for the purpose of content moderation, […], in clear, plain, intelligible, user-friendly and unambiguous language*".[70] The added value compared to previous regulations is that the DSA provides more clarity in the content moderation procedures by introducing a more systematic and understandable approach (Leerssen, 2023). Despite the newly created clarity in the Terms and Conditions, it is not always possible to predict content moderation decisions, as these are carried out on a large scale and not every decision can be controlled in its entirety. Many decisions are made completely automatically (Bloch-Wehba, 2020; Roberts, 2019). These machines do not have the same understanding as a human being and errors can occur (Roberts, 2019). It should therefore rather be used as a retroactive instrument to justify decision-making (Kaminski, 2020).

The statement of reason provides an additional tool to ensure transparency after the content moderation process.[71] The DSA obliges the service providers to draft a statement which contains a range of information and clarifications about the content moderation process. The statement of reason serves as a notification for the user, informing them of possible sanctions. It also serves as an explanation in order to be able to understand the content moderation process (Gorwa et al., 2020). These statements of reasons are then published in the DSA transparency database (Drolsbach &

[67] Art. 16 DSA
[68] Art. 3(t) DSA
[69] Recital 55 DSA
[70] Art. 14 DSA
[71] Art. 17 DSA

Pröllochs, 2023).[72] By analysing the Transparency Database provided by the European Union, it can be stated that there are significant differences between the platforms in terms of the number of moderation actions, the type of content moderated, the reasons for the moderation and the action taken to moderate the content (e.g. removed, demoted, account suspended). Moreover, there are differences in the use of automation with the moderation (Drolsbach & Pröllochs, 2023; Trujillo et al., 2024). The type of moderation depends largely on what type of content is offered on the platform (e.g. video, text, images). The main reasons why content is moderated are non-compliance with the Terms and Conditions of the platform (Art 17 §3 (e) DSA) or harmful and illegal content (Art 17 §3 (d) DSA). It is again worth noting, that differences remain between the platforms. Considering the automation with the content moderation process, almost 90% of moderated content was detected automatically without human intervention. For the vast majority of these, automation was also used to decide whether or not the content in question should be moderated. However, the Court of Justice of the European Union (CJEU) ruled in a Poland v Parliament and Council case, that "*...a filtering system that might not distinguish adequately between unlawful and lawful content, ...would be incompatible with the right to freedom of expression and information."*[73](Moravcová, 2023) Lastly, the actions taken to moderate the content also vary between the platforms. The most common action is the removal of content, followed by the demotion of content (Drolsbach & Pröllochs, 2023; Trujillo et al., 2024).

2.2 Recommender systems within the DSA

Recommender systems are a central part of the business models of many online platforms.[74] They have a huge impact on the content and the information presented to the platform user (Resnick et al., 2000; Schwemer, 2021). The recommender systems of YouTube and Netflix have influenced around 70-80% of the content shown on their platform (Schwemer, 2021).

The DSA in Article 3 (s) defines recommender systems as follows[75]:

"*a fully or partially automated system used by an online platform to suggest in its online interface specific information to recipients of the service or prioritize that information, including as a result of a search initiated by the recipient of the service or otherwise determining the relative order or prominence of information displayed;"*

The DSA's new transparency obligations restrict this influence of the platform's recommender systems on the displayed content (Genç-Gelgeç, 2022). Article 27 of the DSA imposes an obligation on service providers to "*set out in their terms and conditions, in plain and intelligible language, the main parameters used in their recommender systems".* By analysing these parameters, the user can to a certain extent verify if their content has been downranked or demoted. The aim behind this article is to help the user understand why specific content is shown to them and increasing transparency.[76] The DSA aims to shed light on how recommender systems work, as they have been very opaque to this point (Schwemer, 2021). Critics say that the DSA does not go far enough, because it does not include a definition of the 'main parameter'. It therefore leaves the platform provider room for interpretation (Schwemer, 2021). Further critics raise concerns about the impact of recommender systems on privacy, diversity and public discourses (Helberger et al., 2021; Resnick et al., 2000; Schwemer, 2021). By analysing behavioural patterns, the decisions of users are manipulated and thus, recommender systems have a decisive influence on the digital economy (Andriychuk, 2021).

[72] Art. 24 (5) DSA

[73] CJEU, *Republic of Poland v European Parliament and Council of the European Union,* Judgment of the Court (Grand Chamber) of 26 April 2022, Case C-401/19.

[74] Recital 62 DSA

[75] Art. 3 (s) DSA

[76] Art. 27 DSA

The question also arises as to whether the recommender systems of the platforms fall under the definition of an 'AI system' provided by the Artificial Intelligence Act (AIA)[77], under which it is defined as follows[78]:

"AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments;"

Based on this broad definition, one can assume that recommender systems are considered 'AI systems' (Schwemer, 2021; Veale & Zuiderveen Borgesius, 2021). The AIA's risk-based approach divides AI systems into different risk categories (prohibited systems, high-risk systems, …). Prohibited AI systems are systems *"with the objective, or the effect of materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing them to take a decision that they would not have otherwise taken in a manner that causes or is reasonably likely to cause that person, another person or group of persons significant harm;".*[79] Recommender systems of online platforms do not fall within this category.

The high-risk level includes AI systems that are not prohibited but must fulfil additional obligations due to their high risk on fundamental rights, safety, or democratic processes.[80] The provider of those AI systems has to, among others, establish a risk management system[81], include human oversight[82], perform record-keeping[83] and needs the necessary transparency requirements[84]. The recommender systems used in online platforms may fall within the scope of these high-risk AIA systems. In this case, they must not only fulfil the requirements of the DSA but also additional requirements of the AIA (Schwemer, 2021).

2.3 Systemic risk assessments

Systemic risks play a crucial part in the obligations imposed on VLOPs, who changed the way information is handled (Halil et al., 2024; Swan, 2022). VLOPs have increased social influence due to their large number of users and therefore also offer a larger potential base for systemic risk (Eder, 2024). Prior the DSA, platforms pursued their own approaches to handling systemic risks, but these were often criticised and led to discussions (Darius et al., 2023). The DSA is innovative in terms of "systemic risks" (Halil et al., 2024) and imposes several obligations on VLOPs in order to detect, assess and mitigate these risks and make the process more transparent to the public.

Article 34 of the DSA, along with the Recitals 80-83, requires platforms to take an active role in identifying systemic risks and subdivide the systemic risks of VLOPs into the following four categories:[85]

1) Recital 80 DSA: "*Dissemination of illegal content, as the dissemination of child sexual abuse material or illegal hate speech or other types of misuse of their services for criminal offences,*

[77] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) *OJEU, L, 2024/1689, 12.7.2024* (hereafter abbreviated AIA)
[78] Art. 3 AIA
[79] Art. 5 AIA
[80] Art. 6 AIA
[81] Art. 9 AIA
[82] Art. 14 AIA
[83] Art. 12 AIA
[84] Art. 13 AIA
[85] Art. 34 DSA

and the conduct of illegal activities, such as the sale of products or services prohibited by Union or national law, including dangerous or counterfeit products, or illegally-traded animals" [86]

2) Recital 81 DSA: "*actual or foreseeable impact of the service on the exercise of fundamental rights, as protected by the Charter, including but not limited to human dignity, freedom of expression and of information, including media freedom and pluralism, the right to private life, data protection, the right to non-discrimination, the rights of the child and consumer protection."*[87]
3) Recital 82 DSA: "*actual or foreseeable negative effects on democratic processes, civic discourse and electoral processes, as well as public security."*[88]
4) Recital 83 DSA*: "negative effect on the protection of public health, minors and serious negative consequences to a person's physical and mental well-being, or on gender-based violence."*[89]

In addition to identifying these risks, the VLOPs must also take "*reasonable, proportionate and effective measures*" to minimize these risks. Therefore, they may have to adapt their recommender systems, their content moderation processes, their Terms and Conditions, their advertisement practices and increase the supervision.[90]

An additional tool to foster transparency are the "vetted researchers" (Engler, 2021). They have to fulfil a series of criteria mentioned in Article 40 (8) of the DSA and then be approved by the DSCs of the corresponding Member State. The DSC can accept or refuse this request with major differences in how this is handled across the various DSCs (Halil et al., 2024). The researchers have to be independent from commercial interest to ensure that their results are not influenced by commercial objectives (Leerssen, 2021). Furthermore, they are affiliated to a research organization and have a certain expertise in this field.[91] They can request access to data, that is not publicly available in order to analyse and to do research about systemic risks with the VLOP (Halil et al., 2024).

2.4 Advertising transparency

Advertisement practices are also regulated through the DSA because many platforms, like Meta or Google (Strowel & De Meyere, 2023) have an advertising-driven business model (Buiten, 2021). On the one hand, the monetization through advertising is an important revenue stream for platforms, but online advertising is also linked to a number of systemic risks like the dissemination of illegal or harmful content or discrimination between users.[92] Targeted advertising can be aimed specifically at the interests and weak points of the user and thus influence and manipulate their behaviour. This can lead to negative effects for the user and, in certain cases, even for the whole society.[93] Therefore, the articles 26 and 39 of the DSA impose a series of requirements in order to protect the user and to enhance the transparency and accountability in the online environment[94]. Article 26 obliges platform providers to clearly indicate that the presented content is an advertisement and the identity of the person who sponsored or paid for it. Additionally, they must specify the criteria used to display the content to the user, as well as the purpose behind presenting that specific content. Article 39 of the DSA contains additional obligations for VLOPs, which help users to understand why and by whom they are shown certain adverts ,aiming to reduce political and commercial influence while also putting an end to discriminatory targeting (Leerssen, 2020).[95] Furthermore, the legislator addresses increasing concerns about the lack of transparency in algorithmically targeted advertising, especially in politically

[86] Recital 80 DSA
[87] Art. 81 DSA
[88] Art. 82 DSA
[89] Art. 83 DSA
[90] Art. 35 DSA
[91] Art. 40 (8) DSA
[92] Recital 68 DSA
[93] Recital 69 DSA
[94] Art. 26 and 39 DSA
[95] Art. 39 DSA

or socially sensitive situations (Bayer et al., 2019). The advertising practices regulated within the DSA are linked to the European General Data Protection Regulation (GDPR)[96] and the European E-Privacy Directive[97]. They are not replaced by the DSA but fulfilled through its obligations. The DSA requires platforms to inform the user when an advertisement is targeted. The GDPR sets out a number of criteria that must be met to ensure that the use of personal data is lawful.[98] For instance, the user has to previously consent that his personal data is used for the purpose of targeted advertising. The E-Privacy Directive works in coherence with the DSA as it imposes some requirements concerning the storing and accessing of information through cookies. For instance, platforms have to ask for the user's consent before using cookies to track their behaviour.[99]

3. The DSA liability system

As stated in the first article of the regulation, the DSA establishes "*a framework for the conditional exemption from liability of providers of intermediary services".* However, this is not a reinvention of DSA, as previous legal texts already introduced such an approach in order to ensure that the internet remains neutral (Strowel & De Meyere, 2023). In Europe, the E-Commerce Directive introduced a liability exemption for content providers.[100] The rationale was that service providers can be regarded as impartial entities, because they typically do not modify or engage with the content transmitted through their networks. Article 6 of the DSA largely adopts the liability exemption, negligence-based system (Turillazzi et al., 2023) of the E-Commerce Directive[101] and adds a few additional features to cope with modern challenges like specific rules for distance contracts with traders[102](Cauffman & Goanta, 2021) or the Good Samaritan Clause (Cauffman & Goanta, 2021; Strowel & De Meyere, 2023; Wilman, 2022).[103]

Concerning the "Good Samaritan Clause", the DSA does not impose a general monitoring or active fact-finding obligations.[104] However, it allows platforms to carry out own-initiative voluntary investigations without the risk of being held liable for them.[105] These changes were necessary as the internet in the 1990s can also hardly be compared with today's internet, shifting from a decentralized and neutral position to a market, which is dominated by large platforms (Bennett & Livingston, 2020; Strowel & De Meyere, 2023). Legal certainty and increased compliance costs are reasons why the existing liability exemption system of the E-Commerce Directive have been adopted. However, unlike the earlier framework, the DSA introduces more extensive due diligence obligations (Buiten, 2021). This represents a shift away from self-regulation to a state where platforms are required to take active steps (Buiten, 2021; Strowel & De Meyere, 2023). As a result, even if platforms are exempt from liability, they have to fulfil the due diligence requirements (Husovec & Roche Laguna, 2022). At first glance, the liability exemptions of the E-Commerce Directive seems largely unchanged, but in practice

[96] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) *OJEU, L 119, 4.5.2016, p. 1–88* (hereafter abbreviated GDPR)

[97] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJEU, L 201, 31.7.2002, p. 37–47 (hereafter abbreviated E-privacy Directive)

[98] Art 6(1) GDPR

[99] Art. 5(3) E-Privacy Directive

[100] Art. 14 E-Commerce Directive

[101] Art. 12-15 E-Commerce Directive

[102] Art. 6(3) DSA

[103] Art. 7 DSA

[104] Art. 8 DSA

[105] Art. 7 DSA

it can be seen that the liability exemption approach has been indirectly changed by the increased due diligence obligations and higher penalties (Erixon, 2021).

3.1 Conditions for the liability exemption

The exemption from liability is not absolute. Various conditions must be met so that the service providers are not liable. To determine whether a platform qualifies for the liability exemption regime, the DSA adopts a binary approach by distinguishing between active and passive platforms. For example, they may not actively participate in the dissemination of false information and must remain neutral (Weck, 2024). Furthermore, providers cannot benefit from the exemption if they have actual knowledge of illegal content on their platforms.

3.1.1 Active role

The term "active platform" has been defined by the European Court of Justice in a large number of cases, such *Google France vs Louis Vuitton*[106] and *L'Oréal vs eBay*[107] (Buiten, 2021; Cauffman & Goanta, 2021). This binary distinction between active and passive platforms is being contested (Buiten, 2021). Critics argue that platforms today are more likely to be active co-creators of content (Rodríguez de las Heras Ballell, 2021). Especially since many platforms have an advertising-based business model where content moderation and downranking are common practices to increase revenue (Buiten, 2021). As a result, they actively influence the content that users are shown. The Impact Assessment also highlights that there is not a clear distinction between active and passive platforms. To determine whether a platform plays an active or a passive role, the Impact Assessment came up with the term of "predominant influence". There are several criteria listed within the Impact Assessment to define such a predominant influence such as: (European Commission, 2018)

a. *"The supplier-customer contract is concluded exclusively through facilities provided on the platform;*
b. *the platform operator withholds the identity of the supplier or contact details until after the conclusion of the supplier-customer contract;*
c. *the platform operator exclusively uses payment systems which enable the platform operator to withhold payments made by the customer to the supplier;*
d. *the terms of the supplier-customer contract are essentially determined by the platform operator;*
e. *the price to be paid by the customer is set by the platform operator;*
f. *the marketing is focused on the platform operator and not on suppliers; or*
g. *the platform operator promises to monitor the conduct of suppliers and to enforce compliance with its standards beyond what is required by law. "*

According to the European Court of Justice, an intermediary service provider is not neutral when he "*has provided assistance which entails, in particular, optimizing the presentation of the offers for sale in question or promoting those offers*".[108] Furthermore, the DSA states that the liability exemption shall also not apply if *"the provider of intermediary services plays an active role of such a kind as to give it knowledge of, or control over, that information*" and if the "*information is provided not by the recipient of the service but by the provider of the intermediary service itself, including where the information has been developed under the editorial responsibility of that provider*."[109]

[106] CJEU (grand chambre). *Google France SARL and Google Inc. v Louis Vuitton Malletier SA (C-236/08), Google France SARL v Viaticum SA and Luteciel SARL (C-237/08), and Google France SARL v CNRRH SARL and Others (C-238/08)*. 23 March 2010, Cases C-236/08 to C-238/08.
[107] CJEU, *L'Oréal SA and Others v eBay International AG and Others,* 12 July 2011, Case C-324/09
[108] CJEU, *L'Oréal SA and Others v eBay International AG and Others,* 12 July 2011, Case C-324/09
[109] Recital 18 DSA

3.1.2 "Knowledge"

In order to benefit from the liability exemption, platforms should "*not have actual knowledge of illegal activity or illegal content"* and "upon *obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the illegal content"*.[110] The service provider can gain actual knowledge "*through its own-initiative investigations or through notices submitted to it by individuals or entities in accordance with this Regulation in so far as such notices are sufficiently precise and adequately substantiated to allow a diligent economic operator to reasonably identify, assess and, where appropriate, act against the allegedly illegal content."*[111] A notion is defined as sufficiently precise when it *"contains sufficient information to enable a diligent provider of hosting services to identify, without a detailed legal examination, that it is clear that the content is illegal."*[112]

In conclusion, they cannot actively participate in any illegal actions and are also excluded once they become aware of illegal actions. Once the knowledge arises, they have to act (Weck, 2024). Critics argue that this approach may incentivize platforms to remove excessive amounts of content, potentially resulting in an excessive restriction of freedom of expression (Turillazzi et al., 2023).

The wording of the DSA is criticized, as it only lays down conditions for the liability exemption but leaves the conditions for liability to the individual Member States. As a result, it becomes increasingly difficult to create a consistent regulatory framework across the EU and raises concerns about the increasing legal fragmentation among the Member States (Cauffman & Goanta, 2021; Turillazzi et al., 2023).

4. The DSA Enforcement system

The DSA is a complex piece of legislation with different obligations for different types of service providers. However, the liability system and due diligence obligations are of no value if they cannot be monitored for compliance. Without a guarantee of implementation and enforcement, if necessary, through sanctions, the DSA cannot realize its goals and is therefore worthless. That is why the DSA has a whole chapter 5 dedicated to implementation, cooperation, enforcement and sanctions. As the DSA is an EU regulation, it is directly applicable in the Member States and does not need to be integrated into national legislation.

Next to the direct effect, the DSA is also horizontally applicable (Husovec & Roche Laguna, 2022). Compliance with the obligations imposed on service providers by the DSA is monitored jointly by national authorities, also known as DSCs, the European Commission and the European Board for Digital Services ("the Board"). Furthermore, private entities play a significant role in the enforcement of the DSA (Cauffman & Goanta, 2021). However, it is a novelty of the DSA that the European Commission has special responsibilities with regard to the control and the enforcement of the obligations imposed on VLOPs (Husovec & Roche Laguna, 2022). With the DMA, the European legislator has chosen a different, more centralized, enforcement approach. The implementation of the DMA is mainly supervised and enforced by the European Commission (Genç-Gelgeç, 2022). The Commission has been given a number of powers[113], which also enable it to initiate proceedings in the event of violations of the DMA and to impose if necessary (Genç-Gelgeç, 2022).[114] The DSA opted for a Commission-centralized approach for VLOPs and for a decentralized approach for non-VLOPs. The different enforcement approaches, especially for non-VLOP, could lead to difficulties concerning the coherence between the DSA and the DMA (Genç-Gelgeç, 2022).

[110] Art. 6 DSA
[111] Recital 22 DSA
[112] Recital 53 DSA
[113] Art. 15-21 DMA
[114] Art. 25 and 26 DMA

Regardless of national enforcement by the DSCs or enforcement at European level, effectiveness plays a crucial role. To ensure effective oversight of service providers, they must make a range of data available to the controlling authorities.[115] The European legislator has emphasized the importance of effectiveness outside the DSA, as this principle is also established, in Article 47 of the Charter,[116] and in the jurisprudence of the Court of Justice (Reyna, 2024). The lack of appropriate sanctions and penalties together with the lack of resources, investigation powers and enforcement powers can hinder compliance (Biard, 2024; Reyna, 2024). To ensure effective enforcement, not only the efforts of the DSCs and the Commission are required, but also other stakeholders (e.g. consumers, organizations, society groups, business users) and regulated entities, like the VLOPs or other service providers, have to participate (Reyna, 2024). The DSA introduced some obligations and instruments, like the Compliance Function for VLOPs to ensure and foster compliance and collaboration with the DSA (Moravcová, 2023).[117]

4.1 The Digital Services Coordinators (DSC)

In contrast to the E-Commerce Directive, the DSA explicitly defines and regulates the roles and responsibilities of national authorities tasked with enforcing its provisions (Buiten, 2021). Article 49 of the DSA states, that "*Member States shall designate one or more competent authorities to be responsible for the supervision of providers of intermediary services and enforcement of this Regulation ('competent authorities').*" [118]Out of these competent authorities, the Member State has to designate the DSC who is entrusted with the task to supervise and to coordinate the effective implementation and enforcement of the DSA obligations within this Member State (Yurukova, 2023). However, some critics ask for additional guidelines for the Member States on how they should coordinate the tasks between the different competent authorities within the state to avoid ambiguities (Cleynenbreugel & Mattioli, 2023).

To ensure a seamless implementation and faster enforcement of the DSA , the DSCs should cooperate with other competent authorities at national level as well as with the European Commission and the Board at European level (Berberich & Seip, 2021; Buiten, 2021).[119] This Member State-based approach allows Member States to report violations of the DSA, while the DSC of the respective Member State has "*exclusive powers to supervise and enforce this Regulation*"(Yurukova, 2023).[120] However, Article 56 (2) makes an exception to this exclusive right concerning the supervision and the enforcement of VLOPs. As will be argued further, this shall be the exclusive power of the European Commission. The fact that the DSA has chosen a Member State-based approach can lead to differences between the various Member States which hinders cooperation and results in discrepancies being abused (Ryan & Toner, 2020; Strowel & De Meyere, 2023).

The cooperation across borders was seen as a weakness of the GDPR and the same could become reality for the DSA's enforcement system (Savova et al., 2021; Strowel & De Meyere, 2023). In the past, it was common for the media sector to be controlled by different, separately managed authorities. This not only led to cross-border discrepancies but also to cross-sectoral discrepancies (Yurukova, 2023). The DSA seeks to enhance and accelerate the cross-border and the cross-sectoral cooperation and tries to reduce the discrepancies by a close exchange between the different DSCs and with the European Board of DSCs in order to exchange experiences.[121] Additionally the DSC serves as a single point of contact (Blázquez et al., 2021; Yurukova, 2023). One of the key elements of this coordination between the Member States is the European Board for Digital Services, primarily mentioned in Articles 61-63 of the DSA. The Board is an independent advisory group composed of the DSCs of the different

[115] Art. 40 DSA
[116] Art. 47 Charter
[117] Art. 41 DSA
[118] Art. 49 DSA
[119] Art. 49 DSA
[120] Art. 56 DSA
[121] Art. 58 DSA

Member States where each Member State, regardless of its size, is granted one vote and which is chaired by the Commission.[122] Essentially, the Board has the role of supporting and facilitating the coordination, issue opinions and advise the DSC and the European Commission.[123] Due to the above-mentioned discrepancies between the Member States, some are calling for an independent European-wide authority to regulate and supervise platforms (Strowel & De Meyere, 2023).

Another downside of this Member State-based system is that some DSCs have to handle much more work than others. For example, some countries end up with a large share of responsibilities because many major companies have their place of establishment in that respective country, largely due to their business-friendly tax laws (Strowel & De Meyere, 2023). Therefore, the legislator opted for a centralized approach at VLOP level.

The DSA requires, that the DSCs have the necessary structures and resources to carry out their task *"in an impartial, transparent and timely manner"* and independent from any external influence of other authorities like governments (Yurukova, 2023).[124] The Member States have the choice between creating a new authority or adapting an existing one (Yurukova, 2023). It is noticeable that the majority of Member States are opting for the appointment of existing authorities as their DSCs rather than setting up new organizations. This in turn can make cross-border cooperation more difficult, as nothing is standardized (Cleynenbreugel & Mattioli, 2023). To ensure that the DSC carries out its tasks independently, attention should be paid to the origin of the resources. Often the budget for the DSCs is provided by the state and could therefore be subject to a certain political influence (Irion et al., 2019; Yurukova, 2023). However, some countries may not have the necessary financial and human resources to implement the smooth enforcement of the DSA. In terms of human resources, a lack of experience, targeted training or education can hinder enforcement (Blázquez et al., 2021; Yurukova, 2023). However, it is crucial that well trained experts in the fields of data analytics and social behaviour exercise these tasks, which may pose some risks to the effectiveness of the DSA (Reyna, 2024).

The DSC has investigation powers like the power to require information from anyone *"that may reasonably be aware of information relating to a suspected infringement of this Regulation"* or the power to require help from judicial authorities to inspect places where information about infringements may be stored.[125] Furthermore, the DSCs have several enforcement powers listed at Article 51 (2) of the DSA.[126] This includes the power to impose fines, periodic penalty payments and interim measures as well as *"the power to order the cessation of infringements and, where appropriate, to impose remedies proportionate to the infringement".*

Even if some Recitals of the DSA demand an effective enforcement, this does not change the fact that the DSA gives the Member States a great amount of freedom in the appointment and design of the DSCs.[127] Therefore some critics ask for a clear guidance on a European level to ensure an effective and standardized enforcement (Cleynenbreugel & Mattioli, 2023).

4.2 The European Commission and the enforcement system for VLOP's

The enforcement system for VLOPs is to a large extent centralized in the hands of the European Commission (Buiten, 2021). The European Commission has exclusive powers on VLOPs and VLOSEs regarding the compliance, the supervision and the enforcement of the obligations mentioned at Section 5 of Chapter III in the DSA (Husovec & Roche Laguna, 2022).[128] This centralized approach was chosen, among other things, because some Member States could otherwise be overwhelmed. Applying

[122] Art. 60 and 61 DSA
[123] Art. 63 DSA
[124] Art. 50 DSA
[125] Art. 51.1 DSA
[126] Art. 51.2 DSA
[127] Recital 79 DSA
[128] Art. 56.2 DSA

the country-of-origin approach to VLOPs would place a disproportionate burden of Irish authorities for example, as many VLOPs are based there due to its favourable tax legislation (Buiten, 2021).

The Commission is also empowered to conduct investigations and inspections[129]. These include the ability to request information and carry out audits,[130] conduct interviews,[131] perform on-site inspections.[132] These tools are essential for assessing whether platforms are fulfilling their DSA duties. In the case of non-compliance, the Commission may impose penalties, including fines of up to 6% of the global annual turnover of the platform.[133] Additionally, Article 73 DSA allows the Commission to accept commitments from providers to address specific concerns, which then become legally binding.[134]

As the supervision, investigation, enforcement and monitoring of the obligations of VLOPs requires a certain infrastructure, trained specialists and financial resources, the European Commission is authorized to charge the VLOPs a supervision fee to cover the expenses involved in monitoring and supervising the compliance of the VLOPs.[135]

Even if the centralized approach eliminates some of the problems mentioned above, there are still points of criticism. Critics claim that the Commission is not entirely independent as it is influenced by political factors. An independent Europe-wide authority could be beneficial to counteract this problem (Buiten, 2021; Wagner, 2021).

4.3 The role of private entities in the enforcement of the DSA

When it comes to the enforcement and the supervision of the DSA, the European Commission relies to a certain extent on the assistance of private entities (Cauffman & Goanta, 2021). These private entities have to be seen as complementary to the public enforcement tools, like the DSCs and the Commission (Nagy, 2022; Sanchez, 2024). In the *Skanska case*, the CJEU also declared private entities to be part of the enforcement process.[136] Private entities have the role to support individuals in the enforcement of the DSA and to guarantee a fair process (Nagy, 2022; Tridimas, 2020). Among these private entities, *trusted flaggers* are designated organizations with proven expertise that are granted priority status when reporting illegal content to platforms.[137] *Independent out-of-court dispute settlement bodies* are recognized to handle conflicts between users and intermediary services in a fair, impartial, and efficient manner.[138]

The fact that independent out-of-court dispute settlement bodies allow parties to save a large share of high litigation costs makes their use more attractive (Cauffman & Goanta, 2021). The DSA also relies on *independent auditors* to assess whether VLOSEs comply with their obligations, particularly concerning risk assessments and mitigation measures.[139] Furthermore, *vetted researchers* can be granted access to platform data for the purpose of studying systemic risks, enhancing transparency and public accountability.[140]

Although it has become a trend in legislation to transfer some of the implementation and enforcement to private entities (Frosio, 2017). This privatization has also been the subject of some criticism

[129] Art. 67-72 DSA
[130] Art. 67 DSA
[131] Art. 68 DSA
[132] Art. 69 DSA
[133] Art. 74 DSA
[134] Art. 73 DSA
[135] Art. 43 DSA
[136] CJEU, *Vantaan kaupunki v Skanska Industrial Solutions Oy and Others*, 14 March 2019, Case C-724/17
[137] Art. 22 DSA
[138] Art. 21 DSA
[139] Art. 37 DSA
[140] Art. 40 DSA

(Cauffman & Goanta, 2021; Frosio, 2018). Concerns arise about the legitimacy of this privatization with regard to fundamental rights. First, to be legitimate, all the citizens have to be represented and protected (Senden, 2020). Second, the rules imposed by private entities have to fulfil the intended objectives (output legitimacy) (Cauffman & Goanta, 2021; Harlow, 2011).

4.4 Sanctions and penalties under the DSA

Without penalties in the event of an infringement, a law would have little power. The Member States have a certain framework within which they can set the penalties. Article 52 of the DSA states, that the penalties that the DSC can impose should be *"effective, proportionate and dissuasive"*. Regarding the level of the penalties, the DSA sets a maximum amount in Article 52 (3):

"Member States shall ensure that the maximum amount of fines that may be imposed for a failure to comply with an obligation laid down in this Regulation shall be 6 % of the annual worldwide turnover of the provider of intermediary services concerned in the preceding financial year. Member States shall ensure that the maximum amount of the fine that may be imposed for the supply of incorrect, incomplete or misleading information, failure to reply or rectify incorrect, incomplete or misleading information and failure to submit to an inspection shall be 1 % of the annual income or worldwide turnover of the provider of intermediary services or person concerned in the preceding financial year."[141]

Non-compliance with the DSA is therefore subject to severe penalties. However, violations of the obligations do not result in a loss of liability exemption (Buiten, 2021).

After analysing the role of transparency in the DSA and taking a closer look at its liability exemption and enforcement system, the research moves on to the empirical part of the thesis, where the literature is analysed in a case study of the company META.

[141] Art. 52 DSA

EMPIRICAL PART

5. Methodology

5.1 Introduction

This methodology section outlines the approach used to examine the economic impact of the DSA on the business models of VLOPs and VLOSEs in the EU. Given the nature of the research and the need to understand the perspectives of key stakeholders, a qualitative research design was employed. A semi-structured interview was conducted with a public policy manager from Meta, a leading VLOP, to gain insights into the implications of the DSA for their business model (Ruslin et al., 2022).

5.2 Research Design

This study employs a qualitative research design, chosen to provide an in-depth understanding of the experiences and strategies of business leaders in response to regulatory changes under the DSA (Jain, 2021). Qualitative research is particularly suitable for capturing the complexity of how the DSA impacts the business models of VLOPs. In a semi-structured interview, it is possible to get in-depth information due to its flexibility and it is more personal (Jain, 2021; Ruslin et al., 2022).

5.3 Sampling method

The sample for this research consists of a single participant, which is a public policy manager from Meta. Meta was selected because of its prominent role in the digital platform industry and its relevance to the research questions regarding the economic effects of the DSA.

While attempts were made to interview representatives from other VLOPs and VLOSEs, including reaching out to Zalando, Google, X and TikTok, those efforts did not result in additional interviews. Several platforms either declined or did not respond to the interview requests, which limits the diversity of perspectives in the sample. Nonetheless, the insights obtained from the interview with Meta provide valuable information about how a major platform adapts to the regulatory changes brought by the DSA.

The participant selected for this research was chosen based on his role and expertise in shaping Meta's policies and strategies related to the DSA. Due to his expertise in the field of the DSA, the participant was an ideal candidate for insights into how the DSA affects Meta's business model.

5.4 Data collection Methods

Data collection for this study was conducted through a semi-structured interview. The semi-structured format was chosen because it allows for a flexible but focused exploration of the participant's views. The method ensures that key topics related to the economic impact of the DSA are covered while also giving the interviewee the opportunity to provide in-depth responses (Jain, 2021; Ruslin et al., 2022).

- A semi-structured interview was conducted with a public policy manager from Meta. The interview focused on understanding how the DSA influences the company's business model, including operational adjustments, compliance costs, strategic responses and a potential Brussels Effect.

- The interview covered several topics based on the literature review in order to make a connection between the theoretical and the practical world (Hunziker & Blankenagel, 2021). Some topics included:
    - How the company is adapting its business model to comply with the new regulations.
    - The anticipated effect on revenue streams, including advertising models and content moderation practices.
    - Challenges and opportunities presented by the DSA in terms of regulatory compliance and market competition.
    - The enforcement and potential sanctions

The interview was conducted online via Teams and was recorded with the consent of the participant. The interview lasted approximately 90 minutes and provided rich, qualitative data for analysis.In addition to the interview, data was also collected through the analysis of scientific articles, policy papers, and relevant EU legislation. This secondary data provided a broader context for understanding the legal and economic framework surrounding the DSA and helped to support and validate the qualitative insights gathered from the interview. The literature reviewed included academic publications focusing on platform regulation, digital economics, and regulatory compliance. Furthermore, relevant legal texts such as the DSA, the General Data Protection Regulation (GDPR), the E-Commerce Directive and other previous EU regulatory frameworks were analyzed to understand the evolving regulatory landscape for VLOPs.

The study also made use of publicly available transparency, risk assessment, and compliance reports published by Meta. These documents offer valuable insights into how the company interprets and responds to the obligations imposed by the DSA, particularly in areas such as content moderation, systemic risk mitigation, and transparency in advertising. These reports served as a valuable tool for comparing interview and literature data providing a concrete basis for analysing the company's self-reported practices and compliance strategies.

5.5 Data Analysis Method

The data collected through the semi-structured interview were transcribed using a transcription software, called TurboScribe.ai. Prior to the interview, a questionnaire was prepared and sent to the interviewee so that he could prepare for the interview. While questions from the questionnaire were referred to throughout the interview, the conversation took the form of an open exchange, providing a deep understanding of the participant’s views on the economic implications of the DSA.

- The interview transcript was carefully reviewed, and themes related to the economic impacts of the DSA were identified.
- The analysis focused on the following core themes:
    - Regulatory compliance and its financial implications.
    - Strategic shifts in business operations due to the requirements of the DSA.
    - Perceived challenges and opportunities created by the DSA.

5.6 Ethical considerations

This study adhered to ethical guidelines to ensure that participants' rights were protected throughout the research process (Ruslin et al., 2022).

The participant was fully informed about the nature of the research, and their consent was obtained prior to the interview. The participant was assured that their responses would remain confidential and anonymized in the final thesis. Confidentiality was maintained throughout the study and identifying information about the interviewee and the company was excluded from the analysis to protect their

privacy. All interview data was stored securely and is only accessible to the research team. Participation in the interview was voluntary, and the participant was informed that they could withdraw from the study at any time without consequence.

5.7 Limitations

This research has several limitations that should be acknowledged:

- Sample size: The study relied on a single interview with one representative from Meta. As a result, the findings may not be fully representative of all VLOPs or VLOSEs in the EU. Future research could expand the sample size by interviewing representatives from additional platforms to provide a broader range of perspectives.
- Non-response bias: Attempts to interview representatives from other platforms were unsuccessful, which may limit the diversity of perspectives in this research. This single-source data may introduce some bias, as Meta's experience may not fully reflect the experiences of other VLOPs and VLOSEs.
- Limited data: The nature of the data collected in a single interview may not offer a comprehensive view of the economic impact of the DSA on business models. More interviews with industry professionals would help to enhance the depth and validity of the findings.

5.8 Summary

In conclusion, this methodology employs a qualitative approach to explore the economic impact of the DSA on the business models of VLOPs and VLOSEs in the EU. Through a semi-structured interview with a public policy manager from Meta, this study provides valuable insights into how the DSA affects the operational and economic strategies of a major platform. Despite the limitations related to the sample size, the findings from this research contribute to the understanding of the challenges and opportunities faced by digital platforms under the new regulatory framework.

6. Case Study Meta

6.1 Introduction

Meta, formerly Facebook, is one of the largest technology companies in the world and owns a variety of service providers such as Facebook, Instagram, Messenger, WhatsApp, and Threads. However, this case study will only focus on Facebook and Instagram, because these are the only platforms in the Meta portfolio that have reached the threshold of 45 million active monthly users, thus qualifying as VLOPs.[142] Each of these two platforms has around 260 million monthly active users within the European Union (Meta Transparency Report, 2023). In general, Meta and the other VLOPs support this threshold because it provides clear and appropriate benchmark. However, a more risk-based or qualitative approach, such as for the DMA, could capture smaller yet high-risk platforms like Telegram (Public Policy Manager META, personal communication, 2025). Next to the semi-structured interview, this case study analyses the transparency and risk assessment reports who were written by Meta and uploaded to their Transparency Centre. The aim of this case study is to provide a concrete example of how Meta implements the obligations required by the DSA with regard to transparency in content moderation, risk assessment processes and enforcement. Furthermore, the case study helps to clarify the extent to which compliance with DSA entails financial and structural adaptations of VLOPs. The Transparency Reports as well as the Systemic Risk Reports, referenced in this analysis, are published at the Meta Transparency Centre.

6.2 Meta's Position and Interpretation of the DSA (Interview-Based Insights)

6.2.1 Concerning the economic impact

Concerning META's revenue streams, the DSA does not fundamentally change Meta's advertising-driven business model. Although the DSA includes provisions around advertising, such as restrictions on targeting minors and the use of sensitive data, these areas were already regulated under GDPR or previously implemented by Meta. Therefore, the company has not seen significant disruptions in revenue generation. However, the DSA imposes substantial compliance costs. Instead of directly restricting revenue streams, the DSA affects the way Meta operates, especially in terms of compliance infrastructure and content governance. Meta had to significantly expand its internal compliance function (Public Policy Manager META, personal communication, 2025).

In order to comply with the DSA, META has built a team of more than 1000 people from the compliance, engineering and legal sectors. The compliance costs can therefore primarily be attributed to the wages of these employees. The platforms must ensure that mechanisms are not only in place for users to report problematic content, but also for regulators, trusted flaggers, and partner organizations. While some systems already existed beforehand, they had to be significantly strengthened, which requires financial and human resources. A key component of this practice involves human moderators working around the clock to handle escalations, so associated costs tend to be high. Although automation helps, the sensitive and smaller-scale nature of the content usually requires manual handling. Furthermore, these employees have been hired and trained which is also associated with costs. According to Meta's Public Policy Manager, *"when it comes to digital services, you don't have to buy things, you need to build them, so the way Meta measures its compliance cost is in engineering hours."* On the one hand, it is a law and non-compliance will cause sanctions, so they still have to commit despite these high expenses. However, Meta still wants to be able to innovate and to respond to user demands, which is why they built upon existing systems rather than creating entirely new ones from scratch (Public Policy Manager META, personal communication, 2025).

[142] Art. 33 DSA

6.2.2 Concerning an eventual global effect and the impact on competitiveness

According to the interview, Meta experienced several indirect effects of the DSA on innovation and competitiveness within the European Union. While the DSA does not directly hinder innovation because its rules do not specifically target product design or platform operations, it still contributes to significant delays in the launch of new digital services in the EU. One of the main reasons for this is the extensive documentation and risk assessment required prior to introducing a new product, creating a heavier compliance burden than in other regions such as the USA or the UK(Public Policy Manager META, personal communication, 2025).

A prominent example is the “Teen Accounts” feature, designed to adapt the platform experiences to minors. Although it was launched globally in September 2023, it only became available in the EU in January 2024 due to the added regulatory obligations under the DSA. Companies like Meta are cautious about launching new services in the EU without extensive pre-testing, due to the potential fines or investigations if a product appears to increase systemic risks, even during test stages. It is quite normal that various things do not work straight away during the test phase, which is why they are first tested and launched in a different market, as it would be too risky to directly enter Europe due to the high penalties of up to 6%. This has negative consequences for the VLOPs as well as for the users’ experience (Public Policy Manager META, personal communication, 2025).

This cautious approach leads to a recurring delay in product rollouts, placing the EU at a disadvantage compared to other digital markets. While regulations such as the DSA and GDPR aim to enhance user protection, particularly for vulnerable groups, they may also create unintended consequences by discouraging early innovation within the region. As a result, Europe risks becoming a secondary market for digital innovation, with new technologies and features tested and refined elsewhere before arriving in the EU (Public Policy Manager META, personal communication, 2025).

Concerning an eventual Brussels Effect, Meta’s representative was sceptic about the possibility of a global adoption of the DSA and thinks that the DSA is unlikely to trigger a strong "Brussels Effect" due to several reasons. Various regional differences in political systems, legal standards, and societal values regarding content moderation, make it challenging to introduce the DSA in other parts of the world. Content removal orders from public authorities may, for instance, work within the EU due to a strong democratic fundament, but implementing similar mechanisms in less democratic countries with less legal transparency could be problematic (Public Policy Manager META, personal communication, 2025).

Furthermore, the global interest for replicating EU digital legislation appears to be declining. For example, the European AI Act was not even replicated in the traditionally EU-aligned Switzerland. Even though Meta views the DSA as a region-specific framework, some provisions like certain transparency requirements may be adopted globally. However, other key components such as risk assessments are limited to the EU due to their high cost (Public Policy Manager META, personal communication, 2025).

6.2.3 Concerning the Enforcement system of the DSA

According to Meta’s Public Policy Manager, one of the main challenges with enforcing the DSA lies in the lack of harmonization across EU Member States. While the European Commission is in charge with the enforcement of VLOPs, key aspects like trusted flaggers, data access, and out-of-court dispute bodies are left to national DSCs whose levels of engagement and implementation vary widely across Member States. This leads to inconsistent implementations, creating operational difficulties for platforms who try to build compliant systems for countries with different approaches (Public Policy Manager META, personal communication, 2025).

Additionally, there is a legal uncertainty for the platforms, since there are no further specifications about compliance requirements. This lack of foreseeability disrupts the platforms’ ability of effective future planning and leaves them with uncertainty about human and financial resources needed. Furthermore, the risk of facing severe financial penalties, like the 6% of global turnover fines, increases

the pressure and concerns within companies. The risk of politicized enforcement amplifies these concerns, because the European Commission is a political organisation and may be influenced more heavily by external pressures than objective criteria. This approach undermines legal certainty, frustrates internal teams, and raises questions about the neutrality of the enforcement in areas such as content moderation and freedom of expression (Public Policy Manager META, personal communication, 2025).

6.3 Transparency Obligations: Response and Implications

The Meta Transparency Centre contains the transparency reports relating to the DSA, which can be sorted by date and platform. Since this work is limited to the VLOPs, the focus lies on the transparency reports of Facebook and Instagram.

It is notable that the reports from Facebook and Instagram are structured identically and that Meta follows the same approach for both platforms to comply with the transparency obligations under Article 15, 24 and 42 of the DSA. Logically, only the figures provided differ such as the number of content takedowns or the type of content removed. However, sometimes, even these figures are presented collectively. The reports are structured to first address the "*Transparency reporting obligations for providers of intermediary services*" mentioned in Article 15 (1) a)-e) DSA and then moves on to the transparency obligations of Article 42 regarding human resources and the transparency obligations regarding out-of-court dispute settlement bodies mentioned in Article 21 and 24 of the DSA (Meta Transparency Report, 2024). This structure has not changed over the course of the various transparency reports. Due to Meta's identical approach at Facebook and Instagram with regard to the transparency requirements of the DSA and due to the fact that this approach has not changed over time, this case study mainly refers to Facebook's most recent transparency report dated October 25, 2024 (Meta Transparency Report, 2024).[143]

Meta's approach on content moderation is based on different types of platform policies such as the Community Standards and the Advertising Standards. The Community Standards define which behaviour and content is permitted and tolerated on its platforms and which will be sanctioned. These standards serve to ensure that the services offered by Meta are not abused. Therefore, the platform provider reserves the right to remove content from the platform or reduce its visibility in order to guarantee a safe, humane and authentic environment on the platform that respects the privacy of users (META, n.d.). Furthermore, Meta counts on tools like the notice and action mechanism, required by Article 16 of the DSA so that users have the possibility to unfollow or block accounts that bother them (Meta Transparency Report, 2024).[144] As soon as META becomes aware of illegal or harmful content on its platforms, the platform provider takes action to address it. This requires a combination of human and automated resources as well as proactive and reactive measures (Meta Transparency Report, 2024).

6.3.1 Transparency in advertising

According to Meta, transparency was an essential aspect of its governance strategy, even before the DSA came into force. A key element of this strategy is the Ad Library, a publicly accessible archive that includes all ads run on Meta's platforms, including those that were removed from the platform for violating the policies. Initially, the Ad Library only included political ads, whose scope was expanded to all types of ads. Even though this move aligns with regulatory demands, it has drawn criticism from advertisers, who fear that their marketing strategies may become too visible to competitors. Despite these concerns, the overall advertising behaviour on the platform hasn't significantly changed, except for stricter rules regarding ads targeting minors, which Meta had already proactively adjusted for safety reasons. Therefore, Meta has no plans to change its advertising-based business model due to the DSA. The company keeps its belief that personalized advertising offers strong value, both

[143] Art. 15, 21, 24, 42 DSA
[144] Art. 16 DSA

economically for advertisers but also in terms of relevance for platform users. According to Meta's representative, personalization also contributes to user safety, since it helps to avoid that inappropriate content is exposed to certain groups of people, like minors. For Meta, personalization will therefore stay an important tool for the future of online business (Public Policy Manager META, personal communication, 2025).

According to the representative, the vast majority of harmful or misleading ads are intercepted before they appear on the platform. However, a small percentage may still be live for a short time (typically an hour or a day) before being removed. These ads still appear in the Ad Library, which supports transparency but can also create reputational risk. External observers may misinterpret the presence of these ads as a failure of moderation rather than a reflection of proactive transparency (Public Policy Manager META, personal communication, 2025).

Nonetheless, Meta has chosen to maintain this approach due to its belief that the more people understand how moderation works, the more trust can be built despite some arising criticism. This philosophy of proactive disclosure is seen as a fundamental component of the company's compliance with the DSA (Public Policy Manager META, personal communication, 2025).

6.3.2 Transparency in Recommender Systems

In response to the transparency obligations introduced by the DSA, Meta has implemented a range of measures aimed at explaining and giving users more control over how content is recommended on its platforms, such as Facebook and Instagram.

One of the central initiatives is the development of "system cards", which offer a general overview of how Meta's recommender systems work. They provide insights into the signals used to personalize content, helping users understand why certain posts, videos, or suggestions appear in their feeds.

Additionally, Meta has expanded its "Why am I seeing this?" feature (WAIST), which applies to both advertisements and organic content. This tool offers users explanations for why specific content is shown to them, such as following a particular account or because it is related to previous interests. However, the explanations are not in full detail to mitigate privacy and security concerns. To enhance user choice, Meta has also introduced alternative, non-personalized feed options. On Instagram, for example, users can choose between a personalized feed, a chronological "Following" feed, or a "Favourites" feed limited to selected accounts. Although features like Reels cannot be sorted chronologically, Meta provides options to view content based on general popularity rather than personal data. These measures were designed with the DSA in mind and reflect Meta's efforts to ensure that its recommender systems are transparent, understandable, and offer meaningful alternatives to users. At the same time, Meta emphasizes the need to maintain a balance between transparency and platform security to prevent that excessive disclosure of system logic could be exploited by malicious actors (Public Policy Manager META, personal communication, 2025).

6.3.3 Transparency requirements of Article 15 (1) a) of the DSA: Member State authorities orders

Article 15 (1) a) states:[145]

*"the number of **orders received from Member States' authorities** including orders issued in accordance with Articles 9 and 10, categorised by the type of illegal content concerned, the Member State issuing the order, and the median time needed to inform the authority issuing the order."*

First, the orders to act against illegal content, considered in Article 9 of the DSA[146] are addressed by Meta through a process where they first check whether the content in question violates their Community Standards or other policies. In the Case of a Community Standard violation, the concerned

[145] Art. 15(1) DSA
[146] Art. 9 DSA

content is removed from the corresponding platform. If that is not the case, it will be checked if the content is against the law in the corresponding Member State and would consequently be removed (Meta Transparency Report, 2024; Public Policy Manager META, personal communication, 2025). The difference between a Community Standard violation and a legal violation lies in the fact that content that goes against the Community Standards is removed globally on the platform. However, as the European Union is a very fragmented market with many differences among Member States, content violating a national law is only removed in this country. It still remains visible for users in other countries where this type of content is not prohibited, which is a process called geo-blocking. (Public Policy Manager META, personal communication, 2025). According to the representative, *"there is a big discrepancy between what you don't like, and what actually is illegal, or should not be on a platform, and that's an important aspect that not everyone has understood yet"* (Public Policy Manager META, personal communication, 2025). It is therefore important to understand that platforms are not required to comply with various requests to take down certain content simply because it is disliked or harmful to a particular individual. This would violate the fundamental right of free speech. In this case, the user has the obvious alternative of unfollowing the account (Public Policy Manager META, personal communication, 2025). Table 1 below provides an overview of the number of Authority Orders to act against illegal content by Member State for Facebook:

Table 1: Number of Authority Orders to act against illegal content by Member State for Facebook(Meta, 2023; META, 2024b, 2024a)

Transparency Report	Number of requests	Median response time
October 2023	0	///
April 2024	2089	20,5 hours
October 2024	679	25,8 hours

It should be emphasized that there is a large discrepancy between the requests received from the various Member States. For example, of the 2089 requests, 1562 came from Germany, 164 from the Czech Republic, 152 from France and 121 from Italy. The transparency report from October 2024 also shows that more than 500 of the 679 requests come from Germany and France.

The transparency reports list 14 different types of illegal content and a section called "others". The most frequent types of offences are "Account access", "Hate speech" and "Criminal organizations". However, most requests fall under the "Others" section, accounting for a large share with around 90% in the transparency report of April 2024 and around 63% in the transparency report of October 2024.

Furthermore, Member State authorities may request information about certain users.[147] In these cases, Meta checks whether the legal requirements are met so that the request is permissible. If the request is classified as valid, Meta delivers "*narrowly tailored user information in response to such orders, and only when we have a good faith belief that the response is required by law in that jurisdiction, affects users in that jurisdiction, and is consistent with internationally recognised standards."* (Meta Transparency Report, 2024). Table 1 below provides an overview of the number of Authority requests for information about users for Facebook and the linked Median response time

Transparency report	Number of requests	Median response time
October 2023	666	9,1 days
April 2024	7727	14,2 days
October 2024	3414	14,5 days

Table 2:Number of Authority Orders to provide information by Member State for Facebook in line with Article 10 DSA(Meta, 2023; META, 2024b, 2024a)

[147] Art. 10 DSA

The pattern of requests resembles that of those based on Article 9. Most of the requests come from Germany, followed by France. The report also lists a range of reasons for requests, including an additional "Other" section, which is used infrequently compared to the Article 9 DSA requests and the other reasons in the list. The most common report reasons in the Transparency report of October 2024 are Financial Fraud (634) followed by Child Safety (386) and Hate Speech (383).

6.3.4 Transparency requirements of Article 15 (1) b) of the DSA: notice and action mechanism

Article 15 (1) b) states:[148]

"for providers of hosting services, the number of notices submitted in accordance with Article 16, categorised by the type of alleged illegal content concerned, the number of notices submitted by trusted flaggers, any action taken pursuant to the notices by differentiating whether the action was taken on the basis of the law or the terms and conditions of the provider, the number of notices processed by using automated means and the median time needed for taking the action"

As requested by the DSA in its article 16, Meta has built a notice-and-action mechanism into its platforms which is easily accessible by clicking on the three small dots at the top of the post.[149] As soon as a piece of content has been reported, it undergoes the same review process as previously explained (Meta Transparency Report, 2024). However this notice and action mechanism isn't something completely new for Meta (Public Policy Manager META, personal communication, 2025). According to the Public Policy Manager, Meta already invested in the "integrity" of their platform services over the past 15 years to ensure user safety. Therefore, they did not have to start from zero and could build upon the already existing notice and action mechanism. Meta had to ensure that the existing notice-and-action mechanism complies with the DSA requirements like easy accessibility, delivering more informative statements of reasons and to guarantee these statements of reasons apply *"across the spectrum and not on a subset of issues"* (Public Policy Manager META, personal communication, 2025). Prior to the DSA, these informative Statements of reasons were not delivered to all users whose content was moderated. According to Meta's Public Policy Manager, this was not due to unwillingness from the company, but rather to not disclose the exact reason to the offender to minimize the risk that he tries to circumvent these criteria in the future (Public Policy Manager META, personal communication, 2025). Meta divides the received notices in the following four categories: Intellectual Property (IP), Defamation, Privacy and Other illegal content. Over the time of the 3 Transparency Reports, the number of submitted notices remains quite stable between 500 000 and 600 000. Around 20% of these notices lead to content removal, but the type of alleged illegal content varies over time. While in the first transparency report from October 2023, around 70% of incoming notifications were about Intellectual Property, this rate has fallen sharply. The percentage of IP notices fell drastically and the proportion of "other illegal content requests" rose from 12% to almost 50% on (Meta Transparency Report, 2024). The average time taken by Meta to respond to notifications has been reduced from 27.7 hours to 15.3 hours. However, Meta also states that notifications regarding defamation and harassment, for example, take more time on average. Although Article 22 of the DSA grants trusted flaggers priority in reporting, no such notifications had been submitted at the time of reporting (Meta Transparency Report, 2024).

6.3.5 Transparency requirements of Article 15 (1) c) of the DSA: Own initiative

Article 15 (1) c) states:[150]

*"for providers of intermediary services, meaningful and comprehensible information about the content moderation engaged in at the **providers' own initiative**, including the use of automated tools, the measures taken to provide training and assistance to persons in charge of content moderation, the number and type of measures taken that affect the availability, visibility and accessibility of information*

[148] Art. 15 (1), b
[149] Art. 16 DSA
[150] Art. 15 (1) c)

provided by the recipients of the service and the recipients' ability to provide information through the service, and other related restrictions of the service; the information reported shall be categorised by the type of illegal content or violation of the terms and conditions of the service provider, by the detection method and by the type of restriction applied;"

With the help of automated technology and a human review team, Meta removes millions of accounts and malicious posts, that violate its policies, every day. This is mainly automated, but in some cases certain serious violations are detected by technology and then submitted to a human review team for inspection. In accordance with Article 42 (2) a) and b) of the DSA and in order to comply with articles 16, 20 and 22 of the DSA, these team receive a special training based on the topics they review and are equipped with the necessary resources.[151] Furthermore, they are supported by vendor contractors in areas like work environment and psychological support. According to the transparency report, Meta's team responsible for platform security comprises around 40,000 people, of which around 15,000 are content reviewers. This team includes full-time employees as well as partner companies or external parties who review allegedly unauthorized content on the platforms around the clock in more than 70 languages. Meta's review system is programmed to focus on the content that is most likely to cause significant harm. Therefore, the platform uses rate limits, to discover bots' content, as well as matching technology that compares content to previously removed content. Furthermore, Meta uses AI in order to support the human review teams and to identify the content that should be submitted to the review teams. By allowing machines to learn from the decisions of human review teams, the technology is constantly being improved and the quality of automated decisions is enhanced. In accordance with Article 15 (1) e) of the DSA, these technologies are regularly tested for quality by taking random samples and having them checked by human reviewers, who compare it with Meta's expectations.[152] To quantify the accuracy of automation techniques, Meta introduced the Automation Overturn Rate in the April 2024 report. The automation overturn rate refers to the percentage of content initially removed through automated systems that is later reinstated, indicating cases where the automated decision was reversed. As this percentage drops from 8.4% to 7.47%, the automated technologies have become more efficient (Meta Transparency Report, 2024; Public Policy Manager META, personal communication, 2025).

Between April and September 2024, Facebook proactively removed almost 50 million pieces of content, with almost 95% of these being removed automatically. Approximately 7.4 million pieces of removed content were characterized as "Spam", 1.2 million as "Hate Speech" and 2.2 million as "Adult Nudity and sexual activity". Notably 35 million removals (around 70%) of fell under the category "Others". In the same period, Facebook took action against 88 million accounts of which around 90 % were automated (Meta Transparency Report, 2024).

Another tool used by Facebook to reduce the visibility of undesirable content is "demotion", also called downranking. Between April and September 2024, around 27 million pieces of content were automatically demoted. The majority of these were Fact-Checked Misinformation (70%), Violent and Graphic Content (21%) and Adult Nudity and Sexual Activity (4%) (Meta Transparency Report, 2024).

All ads on Meta are primarily reviewed through automated systems, to make sure they don't violate the Advertising Standards. Between April and September 2024, around 17 Million advertising and commerce content was removed, with around 80% removed automatically (Meta Transparency Report, 2024).

To avoid over-removal and to protect freedom of expression, Meta has recently shifted its content moderation strategy, because even if the margin of error of the automated technologies was very small, it sometimes led to content being wrongly removed from the platform. In response, Meta is now reducing proactive automation for less harmful content and replaces it more and more with a reactive

[151] Art. 42 (2) DSA
[152] Art. 15 (1) DSA

moderation. Therefore, they rely increasingly on user reports and human review. However, for severe violations like child sexual abuse, terrorism, or pornographic violence, automated systems remain essential, because the consequences of inaction are too serious. To balance safety and expression, Meta supports multiple reporting pathways: from users, trusted flaggers and official authorities. This dual approach helps to avoid unnecessary censorship while ensuring the removal of truly harmful content (Public Policy Manager META, personal communication, 2025).

6.3.6 Transparency requirements of Article 15 (1) d) of the DSA: Internal complaint-handling systems

Article 15 (1) d) states:[153]

„For providers of intermediary services, the number of complaints received through the internal complaint-handling systems in accordance with the provider's terms and conditions and additionally, for providers of online platforms, in accordance with Article 20, the basis for those complaints, decisions taken in respect of those complaints, the median time needed for taking those decisions and the number of instances where those decisions were reversed "

Meta offers users the opportunity to challenge the content moderation decisions made by Meta. This includes content removal decisions as well as demotion and account restriction decisions. Additionally, if Meta's decision does not change, the user still has the possibility to address an Out-of-court dispute settlement body. In accordance with Article 21 and 24 (1) a) of the DSA, Meta informs the affected users about this possibility.[154] [155]

Transparency report	Number of removal complaints	Restored after complaint
October 2023	1 745 355	575 248 (33%)
April 2024	2 340 515	667 357 (28,5%)
October 2024	3 509 362	871 759 (25%)

Table 3: number of removal complaints and the number of successful complaints on Facebook (Meta, 2023; META, 2024b, 2024a)

The number of removal complaints almost doubled, while the percentage of restored removal complaints sank from 33% to 25%. Most removal complaints fall in the category Adulty Nudity and sexual Activity as well as Bullying and Harassment. Still, nearly 60 % of removal complaints were classified as "Others" (Meta Transparency Report, 2024).

Most complaints about the demotion of content fall under the category of Violent and Graphic Content followed by Fact-checked Misinformation and Adult Nudity and Sexual Activity. Complaints against fact-checked misinformation are unsuccessful more than 95% of the time, whereas complaints against the other two are mostly successful (Meta Transparency Report, 2024).

In the October 2024 report, around 1.8 million complaints were submitted and around a third of these were successful. Regarding account restrictions, around 7.1 million complaints were submitted, with around a quarter being successful.

[153] Art. 15 (1) d) DSA
[154] Art. 21 DSA
[155] Art. 24 DSA

Transparency report	Time to take a decision	Time to act
October 2023	28.1 hours	0.2 hours
April 2024	0.2 hours	1.8 hours
October 2024	0.6 hours	11.8 hours

Table 4:average time it takes META to decide or to act on a complaint(Meta, 2023; META, 2024b, 2024a)

Demotion appeals represent a major challenge for Meta. While the company supports appeals for content removals, introducing these rights to demotions under the same legal framework led to operational and legal uncertainty. The issue lies in the ambiguity of how to distinguish between content demoted due to platform enforcement versus content that is naturally less prioritized due to personalization algorithms. It is therefore perfectly possible, that two users might see different content rankings for the same post due to personalization logic and not because of enforcement. The fact is that there is not a clear line poses a legal and technical challenge: it is unclear when a platform must issue a statement of reasons or offer an appeal mechanism for demotions that are not related to violations but rather to standard personalization practices. As a result, there is concern that regulations could unintentionally impose obligations that are difficult to implement or not in line with the original intent of protecting users against unfair enforcement actions (Public Policy Manager META, personal communication, 2025).

6.4 Risk Assessments and Mitigation Strategies

A significant part of the implementation of the DSA consists of the risk assessments and risk mitigation obligations for VLOPs, outlined in Article 34 and 35 of the DSA.[156] In accordance with Article 42 (4) DSA, Meta publishes a risk assessment report once a year, independent from Facebook and Instagram, in which it lists and analyses the various systemic risks and the associated problem areas on the platforms.[157] It also proposes solutions as to how the platforms intend to minimize these risks. Due to the fact that the DSA is still a relatively recent legislation, there is only one report covering the period of September 2023 to October 2024. As the risk assessment report of Facebook and Instagram are also almost identical, this paper will focus on the Facebook report.

6.4.1 Systemic risks on Facebook

The platform provider uses ISO 31000 to analyse and reduce the risks on Facebook with the aim to enhance security on the platform (META Risk assessment, 2024). ISO 31000 is an internationally known risk management tool for recognizing, assessing, addressing, monitoring, and sharing information about risks. It can be used in organizations of any size to improve strategic decision making, increase efficiency and improve stakeholders' confidence. By fostering the understanding of the risks, ISO 31000 helps Facebook take a proactive approach and anticipate the risks on the platform (ISO, 2018).

Meta has determined 8 systemic risk areas on its platform: Deceptive and Misleading, Civic Discourse and Elections, Public Health, Public Security, Gender-Based Violence, Protection of Minors, Fundamental Rights, Illegal Content. These systemic risks arise or are influenced by unauthorized user behavior and content, by the use of the platform in general or by algorithmic systems such as recommender systems (META Risk assessment, 2024). The Risk Assessment report contains a table that lists the 19 problem areas determined by Meta and indicats which systemic risk is linked to them. The factors who influence the systemic risks or the problem areas are listed in the Risk assessment report as follows: Recommender Systems, Content Moderation Systems, Terms of Service and their Enforcement, Ads Systems, Data Related Practices, Intentional Manipulation, Generative Artificial Intelligence (AI). For each of these factors, the report has clarified the approach taken during an

[156] Art. 34 and 35 DSA

[157] Art. 42 (4) DSA

assessment phase to understand how the respective factors influence the problem areas and the associated systemic risks. Furthermore, the report discloses what measures Meta has taken to address the identified risks. Finally, the report lists which points or procedures should be improved to minimize the risks.

Figure 3: META's Systemic Risk Landscape, link between Problem areas and systemic risks(META Risk assessment, 2024)

The problem areas and the linked risks are divided into 5 levels based on its potential negative impact and the probability that a harmful event will happen. In the following table, the risks are ranked from Tier 1 (extremely low risk) to Tier 5 (extremely high risk). The table shows the reduction of the inherent risks due to the measures taken by Meta and indicates, that the residual risks are all within the first two tiers (META Risk assessment, 2024).

Legend:

Inherent risk

Residual risk

Problem Area	Tier 1	Tier 2	Tier 3	Tier 4	Tier 5
Account Integrity & Authentic Identity		←			
Adult Sexual Exploitation & Adult Nudity			←		
Bullying & Harassment			←		
Child Sexual Exploitation, Abuse, & Nudity			←		
Coordinating Harm & Promoting Crime			←		
Dangerous Organizations & Individuals			←		
Discrimination / Discriminatory Actions			←		
Disinformation			←		
Fraud & Deception		←			
Hate Speech			←		
Human Exploitation			←		
Inauthentic Behavior		←			
IP Infringement					
Misinformation		←			
Privacy & Security		←			
Restricted Goods & Services			←		
Suicide & Self-Injury			←		
Violence & Incitement			←		
Voice & Free Expression		←			

Figure 4: Residual risk for the different problem Areas(META Risk assessment, 2024)

As all these problem areas are linked to a systemic risk, these systemic risks are also divided into different tiers. The following table indicates the Risk Tiers of the systemic risks.

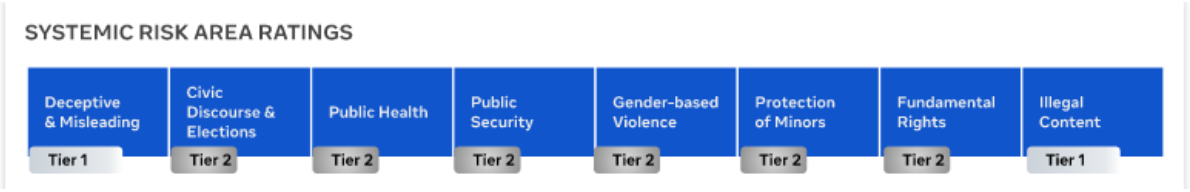


Figure 5: Systemic Risk Area Ratings(META Risk assessment, 2024)

According to Meta, the platform is trying to build systems that effectively identify and mitigate risks, which highlights the complexity of this task. The company has a large scale and not all internal processes are currently structured to meet regulatory standards and therefore, Meta is still improving and adapting its risk assessment approach. One challenge here is, that the DSA outlines what areas to assess but gives limited guidance on how to carry out the assessments in practice. This lack of clarity makes it challenging for the service provider to meet regulators' expectations. This ambiguity is especially problematic because the risk assessment process is highly structured, complex and resource intensive. It requires a thorough analysis of all risks outlined in the regulation, an evaluation of how the service may be affected and documentation of mitigation measures. While Meta conducts risk assessments not only for DSA compliance but also for other legal and operational purposes, like privacy and data protection, it's often unclear how much more is needed to satisfy the DSA requirements. This makes it challenging to know if current efforts are sufficient or if additional action is required. Furthermore, concerns have been raised about the fact that requirements may be influenced by external parties or used as a political tool. (Public Policy Manager META, personal communication, 2025)

In order to balance the risk mitigation with the respect of fundamental rights like the freedom of expression, Facebook relies on its Community Standards, feedback from users and experts in the field of human and civil rights as well as on proactive measures like training in human rights and other important areas. Furthermore, the company has a complaint system in place (META Risk assessment, 2024).

Lastly, the Assessment Report creates different control domains (shown in the figure below) and details how these different control domains help to understand how foundational control mechanism contribute to the control of the system risks.

Figure 6: Meta's Integrity Common Control Framework: Control Domain(META Risk assessment, 2024)

The Risk Assessment Report provides the main trends observed during the assessment for each of the above 19 problem areas , the core controls established to address the identified Problem Areas,and the key limitations encountered during the assessment period. An example for the problem area "Bullying and Harassment" can be found in Appendix 3.

7.Discussion

The aim of this research was to find out to what extent the DSA has an impact on the business model of VLOPs, through looking more closely at transparency, liabilities and the enforcement system of the DSA. An interview with a META public policy manager combined with their transparency and risk assessment reports provided information on the impact of the DSA on VLOPs.

The results suggest that the DSA does not fundamentally change META's advertising-based business model. META has built a team of more than 1000 people to comply with the DSA suggesting that the financial impact of the DSA is more likely to be reflected in increased engineering hours, i.e. the salary costs of the internal compliance function. According to *Turillazzi (2023)*, the DSA helps to reduce the compliance costs for service providers and ensures a standardised legal framework among Member States (Turillazzi et al., 2023). However, my findings suggest, that even if VLOPs do not start from scratch and the legal framework is standardised, compliance with the DSA represents a major cost burden (Public Policy Manager META, personal communication, 2025).

Objectives of the DSA include the encouragement of competition and innovation and the reinforcement of trust in the service providers.[158] However, the findings suggest, that the European Market will lose competitiveness even if the DSA does not directly hinder innovation because its rules do not specifically target product design or platform operations. However, a majority of product are launched later in the EU due to extensive documentation and risk assessment requirements. The high sanctions of up to 6 % of annual worldwide turnover discourage VLOPs to launch products in the European Market before testing them somewhere else. As an unintended consequence of the DSA, this can lead to a recurring delay in product rollouts, placing the EU at a disadvantage compared to other digital markets by discouraging early innovation within the region. As a result, Europe risks becoming a secondary market for digital innovation, with new technologies and features tested and refined elsewhere before arriving in the EU (Public Policy Manager META, personal communication, 2025). The high sanctions align with the literature who claims, that if there are no consequences for wrongdoing, transparency becomes meaningless and loses its value (Ananny & Crawford, 2018).

Furthermore, contradictory to Chander (2023), this study reveals that an extensive Brussels Effect is unlikely (Chander, 2023; Public Policy Manager META, personal communication, 2025). Regional differences in political systems, legal standards, and societal values regarding content moderation, make it challenging to expand the DSA to other parts of the world (Nunziato, 2023; Piotr, 2022). Although certain provisions like certain transparency requirements may be adopted globally, other components of the DSA such as risk assessments are likely to remain limited to the EU due to their high cost. Additionally, contradictory to Bradford (2020) and Chander (2023), this study reveals, that the global interest for replicating EU digital legislation appears to be declining as the example of Switzerland and the European AI Act show (Bradford, 2020; Chander, 2023; Public Policy Manager META, personal communication, 2025).

The case study demonstrated that, even if the European Commission oversees the enforcement of VLOPs, key aspects like trusted flaggers, data access, and out-of-court dispute bodies are left to national DSCs which leads to a lack of harmonization in enforcement systems across the EU Member States. This corresponds to Ryan & Toner (2020) as well as to Strowel & de Meyere (2023) who argue that the Member-State based enforcement approach of the DSA could result in the abuse of the discrepancies between the Member States (Ryan & Toner, 2020; Strowel & De Meyere, 2023). Even if the DSA tries to reduce these discrepancies by fostering close collaboration among the different DSCs and the European Board of DSCs[159], the level of engagement and implementation would vary widely across Member States. This leads to inconsistent implementations creating operational difficulties for platforms trying to build compliant systems. This can be attributed to differences in human resources,

[158] Art. 1 DSA

[159] Art. 58 DSA

a lack of experience, targeted training or education (Blázquez et al., 2021; Yurukova, 2023). An independent Europe-wide authority could be beneficial to address this issue (Buiten, 2021; Public Policy Manager META, personal communication, 2025; Wagner, 2021).

Furthermore, platforms criticize the legal uncertainty surrounding the clarity of requirements from the platforms and the Member States (Public Policy Manager META, personal communication, 2025). The critics about the lack of specification aligns with Cleynenbreugel & Mattioli (2023) who argue that a lack of guidelines could lead to an ambiguous enforcement across Member States (Cleynenbreugel & Mattioli, 2023).

Lastly, platforms fear a politicized enforcement as the European Commission is a political organisation (Public Policy Manager META, personal communication, 2025). This fear of an external political influence on the enforcement aligns with the literature who argue that the budget for the DSCs are often provided by the state and could therefore be subject to political influence (Irion et al., 2019; Yurukova, 2023). Furthermore, the literature claim that the Commission is not entirely independent as it is influenced by political factors. Here again, an independent Europe-wide authority could be beneficial to counteract this problem (Buiten, 2021; Wagner, 2021).

The case study reveals that the transparency requirements concerning advertisement do not have a significant influence on the business model of the VLOPs and on the users' behaviour. Meta keeps its belief that personalized advertising offers strong value, both economically for advertisers and in terms of relevance for end users (Public Policy Manager META, personal communication, 2025). This does not align with the literature, who claims, that advertising could be targeted to the users' interests and weaknesses and thus manipulate their behaviour leading to negative effects for the user and possibly even for society (Zuboff, 2019).[160] Corresponding to Gorwa & Ash (2020), who claimed that platforms already took voluntary transparency measures, META introduced the Ad Library to ensure transparency within the advertisement process prior to the introduction of the DSA (Gorwa & Ash, 2020). This aligns with Leerssen (2020), who claims that the DSA will reduce political and commercial influence and put an end to discriminatory targeting (Leerssen, 2020).[161]

Even though the Ad Library supports transparency, it could create reputational risk if external observers misinterpret the presence of these ads as a failure of moderation rather than a reflection of proactive transparency (Public Policy Manager META, personal communication, 2025). This aligns with the literature who states that publishing information only leads to a better understanding if the audience is able to interpret the information correctly, and that disclosure alone does not necessarily foster trust (Albu & Flyverbom, 2019; David, 2018).

Nonetheless, Meta has chosen to maintain this approach due to its belief in transparency (Public Policy Manager META, personal communication, 2025). This is confirmed in the literature, arguing that transparency fosters efficiency and effectiveness and therefore leads to more accountable systems (Ananny & Crawford, 2018; Ball, 2009; Flyverbom, 2015). Additionally, the literature claims that transparency is a way for companies to showcase their commitment to social responsibility and ethical integrity (Tapscott & Ticoll, 2003).

My findings reveal, that META has taken several initiatives like "system cards" and the "Why am I seeing this" feature to explain to users how the platform's recommender systems work (Public Policy Manager META, personal communication, 2025). This approach aligns with the aim of Article 27 DSA to act against opaque recommender systems (Schwemer, 2021).[162] Furthermore, the VLOP offers a non-personalized feed option. This aligns with Genç-Gelgeç (2020), who argues that the DSA aims to limit the influence of the platform's recommender systems on the displayed content (Genç-Gelgeç, 2022). At the same time, Meta emphasizes the need to maintain a balance between transparency and

[160] Recital 69 DSA
[161] Art. 39 DSA
[162] Art. 27 DSA

platform security noting that excessive disclosure could be exploited by malicious actors (Public Policy Manager META, personal communication, 2025). A significant technical challenge exists in achieving transparency, particularly with algorithms, as they continuously evolve, making them inherently complex and difficult to monitor over time (Crain, 2018; Diakopoulos, 2016).

The results indicate, that META first checks if the content requested for removal violates their Platforms Community Standards and if it should be removed globally. If that is not the case, the platform provider checks if the content violates national laws and as a response removes the content only in the affected Member State, which is called geo-blocking (Meta Transparency Report, 2024). This aligns with Leerssen (2023) and Article 3 DSA, who claims that the notice and action mechanism applies not only to illegal but also to harmful content (Leerssen, 2023).

Furthermore, *"there is a big discrepancy between what you don't like, and what actually is illegal, or should not be on a platform"* so platforms have to take care of fundamental rights but also avoid excessive removals (Public Policy Manager META, personal communication, 2025).

The study reveals, that the platforms did not have to start from scratch and could build upon the already existing notice and action mechanism to comply with article 16 of the DSA (Public Policy Manager META, personal communication, 2025).

The findings reveal, that META extends the Statement of reasons in accordance with Article 17 DSA in order to explain to the users why and what content is removed. This aligns with the literature who claims that transparency without understanding is not valuable (Ananny & Crawford, 2018; Christensen & Cheney, 2015). However, the company does not want to tell the offender exactly why the content was deleted, to limit the opportunity to circumvent these criteria the next time (Public Policy Manager META, personal communication, 2025). This aligns with the literature who claims that transparency should not be understood as a binary principle in which there is only a choice between total openness and total secrecy (Ananny & Crawford, 2018). It is important to carefully consider which information should be made public and under what conditions to ensure it serves the public good (Fox, 2007).

The study also reveals, that Meta relies significantly on the use of automation technology because it is essential when dealing with the large scale even if mistakes may occur. This aligns with the literature, who states that almost 90% of moderated content was detected automatically without human intervention (Drolsbach & Pröllochs, 2023). However, to ensure the quality of these automated decisions, these technologies are regularly tested for quality by taking random samples and having them checked by human reviewers comparing them with META's expectations. Moreover, META introduced the automation overturn rate to measure the success rate of these automation technologies (Meta Transparency Report, 2024; Public Policy Manager META, personal communication, 2025). This aligns with Roberts (2019) and Bloch-Wehba (2020) who claim that machines do not have the same understanding as a human being and errors can occur (Bloch-Wehba, 2020; Roberts, 2019). To avoid over-removal and to protect freedom of expression, Meta has recently shifted its content moderation strategy, because even if the margin of error of the automated technologies was very small, it sometimes led to content being wrongly removed from the platform. In response, Meta is now reducing proactive automation for less harmful content and replaces it increasingly with a reactive moderation, relying more on user reports and human review. However, for severe violations like child sexual abuse, terrorism, or pornographic violence, automated systems remain essential, despite the risk of over-removal, because the consequences of inaction are too serious (Public Policy Manager META, personal communication, 2025). This aligns with Kaminski (2020) who argue that automation technologies should be used more as a retroactive instrument to justify decision-making (Kaminski, 2020).

The transparency reports list the different types of moderated content, as required in the DSA, but a large share of the removed or demoted content was assigned to the "other" section. Thus, even if META fulfils the requirements of the DSA, the "other" section is a way to circumvent this requirement.

It should be understood that not every content removal can have its own category or be assigned to a category. However, it is questionable whether the transparency obligation is fulfilled if 60% to 70% of content moderations fall under the “other” section (Meta Transparency Report, 2024).

The study reveals that the demotion or downranking appeals represent a major challenge for META and has raised operational and legal uncertainties. The issue lies in the ambiguity of how to distinguish between content demoted due to platform enforcement versus content that is naturally less prioritized due to personalization algorithms (Public Policy Manager META, personal communication, 2025). This aligns with the literature who claims, that the detection process is difficult and costly (Gillespie, 2022). Furthermore the impact of demotion is hard to determine, because the visibility of content on platforms is personalized and determined by complex algorithms (Jaidka et al., 2023; Le Merrer et al., 2021; Leerssen, 2020). In contrast to account suspension and content takedown, downranking is not a binary principle. It is therefore hard to draw a line and to define when content has been treated unfair (Gillespie, 2022).

Meta applies the ISO 31000 framework to identify and manage systemic risks. In its Risk Assessment Report, Meta outlines eight key systemic risk areas, linked to 19 specific problem areas. These risks stem from user behaviour, platform use, and algorithmic systems such as recommender tools. The report also identifies seven influencing factors, such as content moderation, ads systems, and generative AI, and explains how each is assessed and mitigated. Risks are ranked on a five-tier scale, with all residual risks now in the lowest two tiers thanks to Meta’s mitigation efforts (META Risk assessment, 2024; Public Policy Manager META, personal communication, 2025).

Meta notes that the DSA’s vague guidance makes full compliance challenging, especially given the company's large scale. Risk assessments are resource-intensive and complicated further by potential external political influences. To balance safety and freedom of expression, Meta relies on Community Standards, expert feedback, and complaint systems. The report also introduces control domains within its Integrity Framework and provides detailed risk profiles for each problem area. Therefore, policymakers should make clearer guidelines for platforms (META Risk assessment, 2024; Public Policy Manager META, personal communication, 2025). This aligns with the literature who also calls for additional guidance(Cleynenbreugel & Mattioli, 2023).

Due to the fact, that this research was based on a single case study and one expert interview, the general applicability is limited. Future studies could compare multiple VLOPs or include perspectives from regulators.

CONCLUSION

This paper shows the impact of the DSA on the business model of VLOPs. The thesis reveals the economic and operational challenges that VLOPs have to overcome in order to comply with the DSA. When analysing these influences, a particular focus was placed on transparency, competitiveness, risk assessment procedures and the enforcement system within the DSA.

In summary, the advertising-driven business model of VLOPs has not changed fundamentally as a result of the introduction of the DSA. Platforms such as META continue to adhere to it, as the DSA has no major impact on revenue streams with regard to advertising. The main economic impact of the DSA lies in the very high compliance costs, which are calculated in engineering hours. Many platforms consider transparency to be important and have already undertaken their own transparency measures prior to the introduction of the DSA. As a result of the DSA, transparency measures are moving from self-regulation to a more regulatory approach. Platforms such as META welcome the transparency obligations, but also call for a healthy level so as not to threaten privacy, innovation and competitiveness. With regard to the competitiveness of the European market, it should be noted that the increased requirements regarding risk assessment and other documentation requirements mean that many products are coming onto the European market later because the platform providers do not want to risk penalties for violations of the DSA of up to 6% of their global annual turnover. However, the case study revealed, that platforms often do not know what exactly is required of them and therefore demand more guidance from the regulators. Concerning the enforcement system systems, META criticizes a possible politicization of enforcement by the European Commission and emphasizes that due to the fact that some important elements of enforcement are in the hands of the Member States, there are differences in enforcement between Member States. In future, therefore, care should be taken to ensure that enforcement is more uniform throughout Europe and perhaps an independent Europe-wide authority should be established for monitoring purposes.

The major limitation of this research is that it only focuses on META and the information comes from an interview with a META representative. This limits the generalizability of the research. Nevertheless, it provides valuable and interesting insights. Further research could make comparisons between several platforms or answer the question from a different perspective.

In the end, it remains to be seen how the implementation of DSA will progress in the future and what its long-term consequences are for VLOPS and the competitiveness of the European market.

APPENDIX

Appendix 1: interview questionnaire Meta

Interview Questions

For: Public Policy Manager Meta, in the context of Master's Thesis

By: Jeremy Brühl, Master's Student in Management-Law, University of Liège

Thesis Title: "Digital Services Act: The Economic Impact on the Business Models of Very Large Online Platforms (VLOPs) and Search Engines (VLOSEs) in the EU"

1. General Impact and Strategy

1. How has Meta internally responded to the introduction of the DSA?

2. Have there been noticeable shifts in business models, revenue allocation, or strategic priorities as a result of compliance requirements and does it affect Meta's long-term strategy in the European Market?

3. Has the DSA influenced Meta's competitive positioning in the EU digital market, compared to smaller platforms?
4. Do you see opportunities for innovation arising from DSA compliance?

2. Compliance and Operational Adjustments

1. What have been the biggest operational challenges in complying with the DSA?

2. How has Meta approached the implementation of obligations like risk assessments, algorithmic audits, or transparency reporting?

3. How has Meta adapted its internal compliance structures to meet the DSA's new obligations, especially as a VLOP? Has compliance required the development of entirely new internal roles/teams/departments?

4. Do you anticipate that DSA compliance costs will significantly impact Meta's operational budget in the EU?

2.A) Concerning the new Meta AI

1. What does Meta do to make the users understand how their personal data is used to train Meta's generative AI models, and what mechanisms are in place to ensure compliance with GDPR and DSA?

2. Meta offers an opt-out mechanism. What challenges have arisen in implementing it and what role plays the DSA?

3. What influence does the Meta AI have on the risk mitigation and transparency policy of Meta?

3. Content moderation procedures

1. To what extent has Meta adjusted its content moderation procedures in response to the DSA's requirements?

2. How is Meta approaching the risk of over-removal of content in light of concerns regarding freedom of expression under the DSA?

3. How do you ensure compliance with Article 14 and 15 regarding notice and action mechanisms and statements of reasons?

4. To what extent do you rely on automated tools for content moderation, and how do you ensure their accountability? Is there a large error margin?

5. How do you differentiate between illegal content and harmful but legal content in your moderation processes?

6. How do you ensure that the statements of reasons are clear and precise?

4. Algorithmic Systems and Recommender Transparency

1. How is Meta adapting its recommender systems to comply with the transparency requirements under Article 27 DSA?

2. What has been Meta's approach in offering users alternatives to profiling-based recommender systems?

5. Transparency and Advertising

1. How has Meta adapted to the DSA's obligations on advertisement transparency (Articles 26–28)? How did the DSA impacted Meta's approach ad delivery and targeted advertising?

3. Has Meta noticed any change in user or advertiser behaviour since implementing DSA-related changes?

4.Has the DSA led Meta to rethink or modify any aspects of its revenue model, especially with regard to targeted advertising?

6. Systemic Risks and Risk Management

1. Could you walk me through how Meta conducts its systemic risk assessments under Article 34 and 35 DSA? How do they identify, assesses, and mitigates systemic risks? What was the most challenging about it?

7. Independent Audits

1. How has Meta approached the new requirement for independent audits under Article 37 and what challenges have emerged?

8. Liability system

1.What do you think about the liability system of the DSA? Is it really a liability exemption system with all the due diligence obligations?

2. The DSA says that platforms have to take a neutral and passive role in order to benefit from the liability exemption. Are the terms "active platform" and "actual knowledge" clear enough?

9. Enforcement and Sanctions

1. How does Meta prepare for enforcement mechanisms under the DSA, particularly regarding the European Commission's supervisory powers over VLOPs?

2. What has been Meta's experience with Digital Services Coordinators (DSCs) so far and their coordination with the European Commission?

3. How is Meta managing the risk of non-compliance, given the potential fines of up to 6% of global turnover?

4. Are there concerns about inconsistent enforcement among EU Member States, and how does Meta mitigate that risk? Does Meta expect problems between the platforms and the regulators and how do you prepare for potential legal disputes?

5. Has Meta encountered challenges related to the cooperation mechanism between the Commission and national authorities?

10. The Brussels Effect

1. Do you see the DSA's requirements influencing Meta's operations in non-EU markets, where Meta adapts its global practices based on EU regulations? If so, which obligations are most likely to be extended globally?

2. How does Meta balance regulatory fragmentation, especially between EU, US, and other regions with differing digital regulations?

11. Others

1. Do you consider the threshold to designate VLOP's adequate and would you determine it on additional criteria like in the DMA?

Appendix 2: Interview Transcription

Interviewer: First of all, I would like to thank you for your time and I suggest you start by introducing your role at Meta.

META: I work in public policy, I worked very closely on the DSA, like it's one of the things I worked the most in the past years, I still work a little bit in it, but now once a law is passed it becomes a compliance kind of issue, which means I'm aware, most of the things you want to ask. I'm aware of our position, what we've done and so on, I don't know every little detail that you might have, but I'm sure this is not also what you're looking for either, so yes I'm not a lawyer, I'm not a compliance person, definitely an engineer, but you know I have more or less the answers and I think some of the questions are very interesting, because they touch upon some aspects that not so many people talk about, but I can go through it.

Interviewer: Can you give me a general overview of the global impact, the DSA has on Meta?

I mean I can give you a bit of a general sense, maybe first on the DSA, also because it's a very topical issue, especially now in the context of transatlantic relations. From a European perspective it's a law, we need to comply with this law, I think it's a law that was drafted in a quite forward-looking things, but as many legislation in Europe, the fact that you know we are a single market but very fragmented, that the enforcement is done very politically also with the European Commission, there are some risks of pushing the boundaries of what the law has adopted and the legislators have adopted a couple of years ago, that poses some risks not just in the debate on freedom of expression, but also in the issues around innovation and products that are built in Europe compared to the rest of the world, which is a very topical debate as well at the moment, so look we have worked quite intensely and probably in response to your first question, very intensely on complying with the DSA, I think over now probably a bit less, because you know the biggest chunk has been done, but we had a team of more than 1000 people that worked on compliance with the DSA, we did have I mean a mix of product people, compliance people, engineers, a legal policy as well that worked on basically determining what the solutions to comply with each of the provisions would have to look like, so it's a very costly exercise, maybe not in terms of like when it comes to digital services, you don't have to buy things, you need to build them, so the way we measure cost is in engineering hours, I don't have the number for that, but you know when you have like 1000 people working on it, it's a lot of hours spent on complying with the DSA, which is very costly and very expensive, but it's because we are committed to do it, we're committed of course within the boundaries of making sure that yes we protect the users online, in line with the law, but we're still able to innovate, to respond to user concerns and user demands as well on our platforms, which is not always a given and I'll tell you why a little bit later.

Interviewer: So 1000 people work on the compliance, I did not expect that

Meta: It's not just product people, but it's a group of people that were involved over the past two and a half, three years, and also before when the law was in the making to really build solutions, I mean it's a quite heavy legislation, again it's not necessarily legislation that touches upon specific product innovations, but it's a legislation that required a lot of work when needed, but the approach that we, I think you know a lot of people worked on it, but at the same time you had, I mean you know let's take Facebook and Instagram okay, because they are the two VLOPs, I mean we have other platforms, but they are the two very large platforms to date for Meta, it's two products, two services, where a lot of investments in what we call integrity, so everything that has to do with safety of users, a lot of investments were made over the past 15 years, so it's not something where we have to build from scratch a lot of things, but we needed to tweak a lot of stuff, so the approach that we've taken when we looked at compliance is, you know what do we have already, I can give you an example, you know notice and action, that is one of the questions that you have, it's something that already exists, like a reporting system for a user is something that already existed, whether it was for violations of our policies or for illegality of content, it's something that we already had, so we just needed to make it fit for what the law would require, meaning you know making it more easy to access, more informative

for users when you have statements of reasons, making sure that we have those across the spectrum and not on a subset of issues, which was the case for example before, for many different reasons, not because we don't want to provide a reason to a user, but because sometimes the reason might be linked to some legal cases, to some very dangerous types of violations, where you don't want to necessarily provide more information to the user that violated, in order to avoid that they can understand very clearly what the issue is and try to rob or ban the system the next time they want to try to violate our systems, so this is a kind of approach that generally we did and the focus has been on mostly a few, I mean as a priority a few things, one making sure that users are empowered on our platforms, so making sure that they understand the things they see, making sure they have a way to change things they see on the platform, I'll go a bit more detail later because you have some specific questions on transparency, you know this was the first big chunk which is something where the company has invested always a lot, I mean if you look also the comparison with other platforms, big platforms, Meta I think is the one that produces most of the reports externally, that publishes a lot of stuff, that has most of the programs for researchers as well, now needs to change with the DSA a little bit, but so it's something that the company has always invested as a priority, because there is a belief in the company that you know the more you explain to people, the easier it is for them to understand when things happen, as a policy person I can tell you, I'm not necessarily always in accordance with this, but sometimes being more transparent actually puts you in a spot where you are under much more pressure, I can give you an example, we have one of the main concerns that there is on the platforms is disinformation, so attacks from foreign actors and so on, and one of the ways this is done is through advertising, political advertising or not, we have historically, even before the DSA published in what we call ad library, published all the ads that have been running on a platform, including ads that were disabled, so if for example a Russian disinformation group uses ads, 99% of them would be captured at the beginning, so they would never appear on the platform altogether, but that 1% which is still relevant would still run, usually it runs for one hour, one day, a little bit, but it would still appear on this ad library, because we want to be transparent about it, when you see it from a third-party perspective, someone like a researcher or an NGO that looks at it, says actually there was disinformation on Meta's platforms, because we are transparent, but it doesn't say this was for one hour, this was a useless ad, so sometimes too much transparency also backlashes a little bit, but that's an approach that the company wants to keep and has always done, so that's one of the core aspects of compliance with the DSA. The second is making sure that we have systems to detect or to allow for this reporting of content, which is not just from the user, but also from the regulators, from the trusted flaggers, from other partnerships that we might have and so on, and this is something that existed already, but it was much, much more reinforced, and when you ask about the costs and so on, this is very costly, because this is humans, people that work 24-7, that have received escalations from trusted organizations, from regulators constantly, and it's all done in a human way, with some support of automation, but usually human, because it's a more limited amount of content. **And the last one** is to make sure that we try to endorse this risk-based approach that the DSA has put forward, with the risk assessment, with the auditability and stuff, I think that's probably most of the work nowadays goes into that, to make sure we have a system to detect and mitigate risks that is mapped out in a comprehensive way, because the company is big, we do a lot of stuff, but not necessarily everything is mapped out or fit for a regulatory kind of thing that you need to do, like the risk assessment, so that's a big chunk of work that is still ongoing, because it's an iterative stuff, also trying to understand what the regulator wants exactly from this risk assessment, which is not always easy, because the law doesn't really say much about it, it tells you the areas that you need to look at, but not what you exactly need to do.

So, this is a bit of an overview to respond to your question on what we've done in general and how we approach this internally, but it's a lot of work that has been going on, then some things will go bad or some things will not be perfect, that's always the case, but that's why we have also laws and regulators to look into it.

Interviewer: How does the DSA influence the business model and the revenue streams, especially concerning advertising?

I mean the DSA does not really target the revenue streams, what we call in terms of shifts is more what I just told you, like the cost of compliance, the cost of having operations in place constantly, new teams or expanded teams when it comes to content moderation, when it comes to doing transparency reports, when it comes to working with the auditors for the risk assessment, these are people that you need to hire and this fits in the whole cost of compliance.

Concerning the compliance function, we had to build the compliance function that started in the first days with something like five, six people, now I think it's a team of 30 people, so it's new teams, new workforce that you need to hire to do this kind of work. Of course, when it comes to the actual work on content moderation, this is not done specifically for the DSA, reinforced for the DSA, but we have teams that work globally as well and I think the latest numbers around our trust, what we call trust and safety personnel is like 35,000 to 40,000 people, they're not necessarily those that look at every content that comes on the platform, but they're those that develop the structure for this and that's investments that were done in the past 10 years, it's not because of DSA, you cannot hire 35,000 people for the DSA, but it's costs mostly related to the workforce, less about revenue stream because differently from the DMA, for example, the DMA touches upon business model issues and the DSA less, for us the business model is the advertising business model, the DSA does not hamper the way we do advertising online besides for sensitive data, which was already covered in any case by the GDPR and ads to minors, which is something that we had already done while the DSA was being negotiated, so it's not major differences in terms of revenue stream, but of course it's a lot of costs to comply with the law, that's for sure. I don't have the numbers, I don't think I could even share them, but the cost of compliance is quite relevant, it's quite big.

Interviewer: Do you see opportunities for innovation coming alongside the DSA? And what is the Impact of the DSA on the competitiveness of the European Market?

Okay, this is a good one, because I think the DSA has been built not to hamper innovation, definitely, there's no product-specific issues that undermine the way you run the daily operation of a platform or the innovation that you put forward. However, we have been facing, since the DSA has been in force, it's probably not just because of the DSA, but the DSA also is in the mix, that the DSA does have an impact on new products launched in the EU market, and for us that's a big innovation gap. And this is, you know, it's not to criticize the risk assessment framework, don't get me wrong, I think the risk assessment framework has its benefits, but because of that framework, because of this very heavily regulated kind of way of assessing and mitigating risks, which is normal, it's something that big companies do nonetheless, otherwise we wouldn't put a product in the market unless it's safe for the users, because otherwise nobody will use it or the experience would be bad on the platform.

But the risk assessment process has created a system where every product that we are launching globally, potentially, arrives to Europe late, and arrives to Europe late for different reasons. One, because we need to do due diligence, which is mostly about documentation that takes more time than if we would do it in other parts of the world. But also because oftentimes the way companies work in the tech industry, you do your own due diligence, let's say you take a new product, I mean Meta.ai is not a good example because the delay is due to GDPR.

I actually have a good example, Teen Accounts. So Teen Accounts is a product that we launched in Europe in January, which is basically a different experience for, a very specific experience for users below, for minors. So for people below 18, with a difference between whether you are between 13 and 16, and between 16 and 18, normally, because it's different kind of growth, or age groups.

Teen Accounts was launched in the US and globally in September of last year. In Europe, it was launched in January. And the reason why it was launched in January is partially because of this documentation, risk analysis that you need to document that you don't have to do in other parts.

But also because one thing that we do with this kind of products, at the moment they are ready to be launched. And they bring a positive benefit in this case, is that we need to test them. We need to test whether they work, we need to have rounds to understand whether there's some gaps and use that time to already in the market, try to see whether we need to change some stuff.

If we were to do it in Europe, we would risk fines. Because if something goes wrong, if something doesn't go as well as it should, when you're testing it, I mean, it's normal, it's a test, you need to try to see and potentially to read it. Your reason not being compliant, because it might be that something might be considered as violating or harming or diminishing, actually increasing the risks for, in this case, production of minors.

And you would risk investigations, enforcement fines and so on. So there's a lot of reluctance from the company, our company at the moment, but I'm sure it's the same in other companies, to actually go through with new products until they are heavily tested in other parts of the world. Things might go wrong in Europe, because Europe is different and the user base is different than in the US, for example.

But at least you can rely on an iteration that you've done and so on. But these six months are six months lost a little bit, six months of loss of production of minors in this case, something that you could have done before, you've done it later because you are too scared about the regulation. So it's not necessarily harming innovation in the sense of, we cannot bring product in Europe, but this delay is something that is now very normalized in companies that are investing in Europe, because the regulation and the burden of regulation and the risks related to potential non-perfect compliance with the regulation are quite high.

I mean, the 6% fine is quite high. So there is a little bit of, because here you asked about opportunities, I think opportunities don't depend necessarily on the DSA, because the innovation, especially when it comes to content moderation, it comes with a lot of variables, it's not because of regulation. But actually, there's a risk to innovation as well when it comes to making sure that some products can be in the market, things that are nice and cool, that have nothing to do with integrity, like it could be a meta-AI or something else, but also things that from an integrity perspective actually improve the experience for users is something that sometimes you don't necessarily have.

Interviewer: So would you consider that Europe or the European Union lose a bit of its competitiveness due to the DSA, because everything comes later to the EU?

Yes. I mean, again, it's not just the DSA. I want to be very clear about it, because I think it would be unfair to just blame the DSA for this. But the DSA contributes on some of these things.

It contributes because you need to factor in a few additional things that you don't have to do in the UK, or you don't have to do in the US, in Australia, in Korea, but these actually have an impact in terms of delay, in terms of potentially also safeguarding users more, and so on and so forth. Then it's not just the only one. I think GDPR in some circumstances is even worse than DSA, but this is one of the regulatory barriers that hamper competitiveness, yes, definitely, but also protection of users.

Because I mean, the Teen accounts has nothing to do with competitiveness. I mean, it's not a product where we make money out of. It's just a product that we have in the market to protect minors, to make sure that their experience is gated to the appropriate age group that they belong to.

But it's something that because of regulation is delayed in Europe. Now we have it, but you know, next iterations would have to go through the same kind of things. If we suddenly have to build a new product, we need to go through a critical risk assessment, it needs to go through discussions with the

regulator, you cannot test it in the meantime.So it's things that have an impact at the end of the day on the experience that there is for users in Europe.

Interviewer: A question concerning an eventual Brussels effect, do you see a way that countries around the world will adapt to European legislation? Furthermore, META have to adapt to European legislation due to high fines. Do you see a way that they will adapt to it globally?

So the answer, I mean, I don't know how it's going to go in the next years, but my feeling is that that is not going to happen for different reasons, not just because of the costs that can be wrong. I think there's different reasons.

I don't think you can export the DSA. I mean, the DSA, there's parts that maybe you can export because they're more about due diligence and stuff like that. But the core in terms of liability, in terms of what we call content law, content regulation belongs to a specific region as well.

I mean, for example, you can have a system of orders from authorities to remove content in the European Union because you have a democratic system that is accepted by all the states. You cannot export the same in Brazil. You cannot export the same in other countries where the boundaries between legal and political systems are a little bit more blurry.

So there is that aspect where I have the feeling that it will be difficult to export the DSA as it is in other countries. But also there's an aspect of values as well. There's different expectations on what platforms need to do or what constitutes a harmful or an illegal content in other parts of the world compared to Europe.

So I don't think it's going to happen. Maybe in some countries. I mean, in some countries, I think the debate was already there.

But I do have a feeling that there's not as much appetite as there was for GDPR, for example. I do feel there's not much appetite in general now to copy the EU for many reasons, mostly economic. I mean, look at the AI Act is something that, you know, another legislation flagship for the EU that everybody thought would be exported outside of the EU, and nobody's following the EU.

I mean, even countries like Switzerland that were historically just copy-pasting every legislation from Europe, they're just saying, no, thank you. That has to do with economic considerations that we didn't have at least last term here in Europe. But on the DSA, I do struggle to see a lot of uptake for similar kind of legislation, for the same type of legislation.

Do you see a way that META will adapt to the DSA globally?

That it becomes the global standard? That's not the case either, I think.

On some stuff, yes. Like, when it comes to making changes like the no-disconnection system, it's something that we have and we had a basis globally for it already. It's a system that already, and where needed, we have, you know, made sure that this was a global approach, but not everything.

We're not doing a risk assessment for the rest of the world. We're not planning to do certain aspects for the rest of the world. Some things are much more gated to Europe now than other parts of the world.

It's simply, you know, you know, it's costly to do it globally. And in some circumstances, we don't think necessarily it's the right approach to do it globally. So, we do it for regulation, but we don't necessarily do it for the rest of the world.

What party do you tend to do globally?

Basically, everything that is transparency oriented, we tend to do it globally. Everything that is not, we don't. That's the kind of, you know, very high-level kind of differentiation.

You have already said that you had some mechanisms like the notice and action mechanism, but what was the most difficult to implement, like risk assessment, algorithm audits, transparency reporting, statements of reasons you said you had already done before, but what was the most difficult to comply with?

One thing that we struggled a lot and we were quite concerned was related to, don't get me wrong, not user, I mean user appeals, not because we're against the user appeals, I think that's fine, but because the kind of way that you say was written, it covers removals of content, which is fine, I mean naturally so you need to have an appeal, but also things like demotions or reduction of distribution, which in a good chunk of circumstances is absolutely fair and normal, however it's very difficult to draw the line when it comes to platforms and the way personalized content works, it's very difficult to understand legally what's the line, what's the difference between a demotion that I do because you were just, I mean in the case for example of misinformation, we demote content to avoid that it becomes viral, so that's the type of thing and you say okay, if you're demoting me because you think it's misinformation, I should have the right to appeal that's totally fine, the same kind of action which is called demotion in the law or reduction of distribution, I can't remember now, applies just because of personalization of content, your feed will be different than mine, a content that I post on online, if I'm friend with you or with someone else might appear differently and might be demoted compared to other types of content simply because of your interests and preferences, so that's something we struggled quite a lot and we still struggle I think to understand what exactly the expectation is with this kind of content, because you can understand if I need to do a statement of reason and an appeal just because your content is less appealing than another one, I mean it misses probably the point of what this kind of regulation of this provision was about, but legally it's a little bit of a concern.

I think the other operational challenge is to understand a little bit more what the expectation is from the regulator on risk assessment, because risk assessment is a very structural work, I mean for a company, for a big company, you need to tackle it very structurally, you need to look at all the different risks that are identified in the DSA and understand whether your company is prone to that risk, which normally is yes, I think in all the circumstances and then we go a bit more granularly in terms of what kind of risk, what are the subset of risks and so on, but there is still not so much clarity on, basically you do that, you map out the risk and then you map out how your system works in absence of mitigations, if it's used by minors you are prone to risk of child abuse for example, it's not because of Facebook or Instagram inherently, but just because of the type of service that you're delivering and on top of that you map out all the mitigations that you have in place and then you have a final score, I mean I don't want to say it's mathematical, but you need to structure it and it's still a little bit difficult to understand what the expectation is, because this is one of the main parts of the DSA where a lot of attention outside of the platforms and the regulator is, NGOs, civil society, academics and so on, and there is an aspect of expectations externally that sometimes just don't fit the reality of how you need to comply with the law, so sometimes it's difficult to understand still what the expectation is, how you need to present it, how you need to do it and it's a lot of work done, I mean the risk assessment work is very heavy, it's every year, it starts the year before, it's very complicated and there's still little understanding of what the regulator really wants with this, if it's just a political tool, it's very difficult.

The other big challenge that we have, which is not necessarily on a specific vision, is the still lack of harmonisation of the DSA, I mean the DSA for us as VLOP is centralised to the Commission, however there's parts of the DSA which are not in the hands of the Commission, but in the hands of member states, like trusted flaggers, access to data, out of court bodies that can do adjudication or settlement, and the approach of every member state so far has been very different, which means for a company this is very complicated to scale and then it pisses off regulators, it annoys another one, it annoys an NGO, just because you build the system to make sure that you as fast as possible take decisions on specific content for example, but it runs counter to the way that other national regulators have thought

about how to implement this stuff, so sometimes it's a little bit complicated and it's one of the things we are still very actively working on, because when I have a country like Hungary that puts in place an out of court body that is a trusted flagger, that is a government sponsor, you still struggle on what do I do with it, how do I take decisions and so on, or I trust the flaggers that are usually big organisations and then you find that some countries want to have specific companies as trusted flaggers,

So it's all this kind of stuff that are still a work in progress in the DSA, it still creates a little bit of a vacuum, I mean I'll give you an example, data access is one of the most important articles I think in the DSA, because in terms of accountability we still don't have a delegated act on data access after two years and a half of legislation, and when you have to plan ahead for how you need to make sure that you comply with this law and you have zero visibility on what's going to happen potentially in a week or in a month or in six months, that has a lot of concerns operationally, because you hire people to do this kind of job, they don't have anything to do because this act is not there yet, so the law is not implemented yet on that, potentially you build systems in the meantime to adapt, but then the commission comes with the secondary legislation that runs counter to it, these are kind of things that create a lot of frictions and a lot of concerns when it comes to planning operationally, and there are big challenges that exist in the companies, the rest we do think that we put in place systems and products to comply with the DSA that are compliant with the DSA, whether they are challenging or not, yes, but we have to do it nonetheless, so that's not a big deal, but one thing that is challenging is the fact that the enforcement of the law is extremely political, again it has nothing to do with operational challenges, but it is an important point, because the commission, yes, it's a technical body, but it's also a political body, and in response to a political level, it responds to pressure from outside of the institutions, pressure from others, and sometimes this translates into incorrect or political enforcement of the law, which should be avoided as much as possible, especially on issues that are touching upon free expression, that are touching upon content of people, the way things are done online, like I can give you an example, we have, I mean, I cannot talk about the investigations, but the fact that there are investigations on us are public, there is an investigation on protection of minors, and one part of the investigation is on age verification of minors, which is an issue recognized by everyone as a challenge for the whole industry, and it's a challenge technically, it's a challenge legally, because you cannot just ask for a passport and collect it there, because of GDPR, you cannot really do this stuff, we and TikTok, just because, you know, we are the ones under more pressure politically when it comes to minors, because a lot of minors use, but we are the only two companies investigated on this issue, while the issue is a cross-industry challenge, I mean, if you go to Snapchat, or if you go to Booking, or if you go to Wikipedia, or if you go to whoever, or to Google and YouTube, Google less, because they're an operating system, but YouTube, or anyone else, they have exactly the same problem, which is, you're not going to do age verification perfectly, because you rely on systems that are not just, you give me the passport and I verify it, but these are kind of examples where, politically, there is an issue of enforcement, where, you know, right or wrong, I mean, you target certain companies because of the pressure that you receive externally, which, I get it, I mean, I work in this field, so I get it, but, you know, when you have a regulation, it really annoys people that don't work in policy, you know, they're the ones building products that are like, okay, but why us and not YouTube, or why me, so on, or because of reports from NGOs or news without even consulting the company, so this is a kind of thing, yeah.

Concerning Meta-AI: Was it difficult to introduce Meta-AI due to the transparency and risk mitigation obligations of the DSA? And the opt out mechanism you introduced in the Meta-AI, is it EU specific?

I believe it's EU-UK specific because of GDPR, yes, I mean, basically, I mean, the reason why Meta-AI has been delayed one year compared to the rest of the world, including the UK, is not because of DSA, it's because of GDPR, it's because, we rely on, GDPR has different ways to collect, like, you know, to, in this case, to train, to use personal data, even if they're public, I mean, in this case, we only use, we only train Meta-AI with publicly available data, but there are different legal bases that you can use,

and we rely on what is called legitimate interest, because, it's, or construction is, I don't know, one of these, I can't remember, I'm not a privacy expert, I'm sorry, but basically, what is required in that circumstance is to have a transparent, easy to use opt out for the user, which is different from consent, and the consent is not an appropriate legal basis when it comes to this kind of issue, because the moment that you train a model, you know, it's not that you're using a piece of data, and, you know, the output is exactly that data, it's just used for the purpose of training, so allowing for revoking consent at any time is an artificial construct that is not possible in this kind of stuff, but it took, like, one year for data protection authorities and the European Data Protection Authority to agree that this is the right way to do it, so that's the reason why it's delayed. When it comes to DSA, at the moment, it's not really an issue, because, I mean, again, we have done due diligence, we've done due diligence with the data protection authorities, also with the commission, but not because of the DSA, we've done it because we thought it was doing, because Meta.ai, at the moment, is on messaging services, which are not platforms, so it's not considered a platform in itself, because it's not a platform. So, basically, it is not an issue where the DSA comes in as a regulatory framework, it's something where the AI Act would come as a framework to do this kind of due diligence.

However, you know, they are likely to be, because they are in the rest of the world, if we get approval on GDPR to do it, that would fall into the platforms on Facebook and Instagram, and in that circumstance, we would have to do a risk assessment for the purpose of, you know, what is that. In general, you know, the Gen-AI products, like Meta.ai, like ShowGPT, like Gemini, they present the same risks that you would have on a platform. In some cases, a little bit more, in some cases, a little bit less, but they are the same risks.

Like, it's not that, you know, you have a different type of child protection concerns on Meta.ai or ShowGPT compared to what you have on Instagram. Actually, probably, it's even less, because it's a bilateral conversation with a machine, it's not a conversation where you are spreading in the whole world. So, the risk is not there.

And the risks, because probably what you refer is also, you know, for example, the use of AI-generated content or images that are then used on Facebook or Instagram to spread the misinformation, the scams, and all this stuff, that's already covered in the DSA as part of the content. The fact that it is AI-generated, the fact that it is done with the Meta.ai or something else, does not increase or decrease the risk of it. So, the DSA does not really play a key role here.

The AI act more, the GDPR much more, but when it comes to the assessment and mitigation of risks, it is not because of Meta.ai that we need to mitigate or assess the risks related to AI-generated content. It's because AI-generated content is on Facebook or Instagram, which is slightly different, because the rest is a bilateral conversation. Yes, there will be risks, but there will be ways to manage it within this kind of stuff.

The issue is when an AI-generated content, for example, scamming people there, but it's a risk that is inherent to Facebook and Instagram and needs to be mitigated on Facebook and Instagram, which is actually a good example as well, because of why regulation has been undermining sometimes this kind of work. Because, for example, on fraud and scams, you have a lot of scam ads that are done through AI. I mean, it's very basic AI.

It's just putting the face of usually a celebrity to scam someone. We have developed a product launched in the US in October, I believe, of last year, that is using facial recognition of celebrities with their consent to detect automatically whether there is an ad that uses their face. If it does, it is reviewed.

If it's a scam, it is removed. This product, because of legislation in the EU, could arrive only a few weeks ago. So this shows you, again, when laws have a great role, important to safeguard, to provide certainty, but sometimes they undermine innovation as well.

And innovation is not just innovation where Meta makes money out of it, or another company makes that. It's also innovation that makes it easier to detect problematic content that is online. But that's what it is.

That's where we live. And for now, it's difficult to change. But so when it comes to Meta.ai, it's not per se a platform, because it's an interpersonal kind of exchange.

And for the moment, it's only plugged in WhatsApp, which is not a platform either. So from a DSA regulatory kind of aspect, it doesn't really fit in the discussion. But the AI-generated content is very much front and center in the work that we do in the DSA risk assessment, mitigation and stuff.

In that case, I mean, we have a lot of stuff that we do on AI-generated content, but there's a lot of challenges also that are industry-driven. When it comes, for example, to labeling or watermarking this content, which is something that a lot of companies don't want to do. We do it, but a lot of companies don't want to do it, which means that if I'm on DeepSeek, I don't know what's called the actual product of DeepSeek, that doesn't watermark it and they don't care about it.

Recognizing that something is AI-generated on a platform is very complicated. Because you don't know what's the purpose. It's very blurry and sometimes it's easier, sometimes it's not.

And that's why you have a reliance on a lot of organizations that can flag these things, but they cannot check the whole platform content, which is massive. So that's something to keep in mind as well.

So now concerning to the content moderation procedures, how do you deal with over-removal and how do you ensure the freedom of expression, because you relay a lot of automatic tools?

Yes. So I guess you're familiar with the announcement and a lot of noise that came in January from the announcement of Mark Zuckerberg on content moderation. So, there's different parts of that announcement. One of them relates to the way we do content moderation.

In Europe, it's slowly changing, pending risk assessments and all this kind of stuff. But the reason why that announcement was made, which basically says that we are going to rely less on proactive automated detection and more on reactive kind of moderation, is exactly the response of this question.

The main reason is that, historically, we have built automated systems, which we call classifiers. Therefore, every specific violation of the policies that exist on a platform, we're automatically trying to proactively detect the content that is violating. However, they make mistakes.

Because even humans, to be honest, humans make more mistakes than machines, but they make mistakes. Those mistakes, even if they are 1% of the content, they are millions of pieces of content. And that's a risk.

But to change this approach a little bit, and go back to a place where we would still use automation, we would use it proactively for those very severe types of violations or illegality. For example, child sexual abuse, terrorist content, pornographic images, for this kind of stuff that are highly or extremely important societally. Because if you have a terrorist attack, if you make... Basically, what I'm trying to say is that we are going to keep using these in these circumstances, even if we know that they're going to make some mistakes.

Because the risk of not doing it is much higher than doing it. Because if there is child sexual abuse material online, and you just wait for someone to report it, you're not really doing something good, because it's going to have an impact in the real world in terms of violence. So these are very severe violations.

So we continue to run through automated systems, meaning you have a machine that proactively detects when something is posted, whether it is violating a certain policy. And then if it doesn't, or if it's not caught as violating, you will still rely on reporting of users. And when the user reports, you do a mix of automation and human reviews.

And then you have different ways to do it. But that's the kind of reason why we, in some cases, people say scale back a little bit. It's to make sure that for content that is not extremely harmful, that cannot lead to real world consequences and so on, we allow for more free speech, always with the possibility to report content and report content from a user, report content from a trusted organization, which in Europe is called trusted flagger.

In the US or in other parts, we call it trusted partners. It's like partner organizations that do this kind of work from authorities, from judges, from the police, from all the other things around that exist to report content to us. So that we balance this difficulty that we face in moderating too much versus safeguarding user experience and safety online.

So that's the kind of approach that we've taken. And it's exactly for this reason that you asked the question. It's to avoid over removal, because over removal leads to a lot of concerns for people about their speech, about what they say online and so on.

But still within the boundaries of making sure that, especially for the most severe violations, we continue to do what we do, which is important even if you make mistakes.

How do you differentiate between legal and harmful content?

This is important, because this is something that even the regulators struggle a lot with.

So there's... I mean, first of all, the DSA does not cover harmful but legal content. It does it in the context of the risk assessment, but it doesn't tell you you need to remove this. The risk assessment, to a certain extent, if you don't do it... But our company and every platform works in this way.

So you have what we call community standards, which is a set of rules that you need to follow on the platform. Not necessarily all these rules touch upon only legal content. Sometimes it's also about harmful content.

I can give you an example. A type of harmful misinformation that we remove is what we call voter fraud. It's one community standard.

Voter fraud is not illegal. I mean, I could say, guys, today there's elections, the ballots close at four o'clock, while in reality they close at midday. That's kind of misinformation.

And it's harmful because it affects an election. So we will remove that piece of content. Is it illegal to say something like that? Not really.

I mean, I can go in the street and say, guys, the ballot closes at four, and it's not true. In this case, it's to show you that our community standards don't necessarily align with the illegality of content. The illegality of content, there are some specific circumstances that are very national.

But in general, what is illegal in Europe or in the US aligns very much with one of the community standards, like terrorism, something around violence, or bullying and harassment is already there because not necessarily there's laws about it. But there's a lot of overlaps between the two. The way we do it operationally is that we will always check, even if you report content that's illegal, because we have two ways of reporting content.

They're all in the same thing. But one is reporting a community standard violation, which doesn't require a legal analysis. It requires an assessment of whether it goes against the policies of the platform.

And an illegal reporting system where you need to provide a legal basis because we need to verify the legality or illegality of this piece of content. Even if it is reported as illegal, companies will always look at it first from a policy of the company perspective. And the reason why it's done like that is because if the content violates the policy of the platform, it is removed globally, because it shouldn't be there, whether you are in Brussels or you are in Jakarta, it doesn't matter.

If it is not violating a community standard, but it's violating a law in Belgium, it would not be removed everywhere in the world, it would just be removed in Belgium. So if you are in Belgium, you cannot see this piece of content. But if you are in France, and in France this content is legal, you can see it.

There are some examples of, now it's not really the case because it's changing, but let's say if we didn't have a policy which is changing on nudity online, nudity sometimes might be legal in one country to depict nude images.

but let's say, if we didn't have a policy which is changing on nudity online, you know, nudity sometimes might be legal in one country to depict nude images, it might not violate our policies, we would, what we call it, geoblock it, so it's geoblocked in one country and then in the rest of the world it's available because it doesn't violate other laws, unless it violates other laws, in that case it would be geoblocked also there, otherwise it stays available on the platform. So that's, it's an important effect because not everybody understands it, but it's important to say that what is harmful but legal, you know, it's not illegal, so even if you don't like it, because sometimes, you know, we talk to regulators, especially the coordinators, when they were taking up this role, we talked about, you know, we had conversations about our content moderation, how we do it, our standards and so on, and a lot of times, you know, people, just because they don't like certain type of content, because it's harmful, but it's legal, you know, I mean, if I'm saying, if I'm making fun of someone, it might be harmful, but it's definitely illegal, I can do it in the street, I can do it in a park, I can do it in the stadium, I can do it everywhere, I can do it if I'm in the parliament, you know, like, as platforms, we cannot take action for things that people don't like, I mean, you have options as a user, so if you don't like a piece of content, you can just, you know, unfollow the person, you know, make sure that kind of post is not visible, if it is about a sensitive content, you can decide to not to see sensitive content altogether, but, you know, there is a big distinction to be made, and, you know, when we talk about, because we are in a transatlantic, a weird world, where the US government is very pushy on freedom of expression, what they care about is about, you know, the fact that, you know, sometimes in Europe, there is a big discrepancy between what you don't like, and what actually is illegal, or should not be on a platform, and that's an important aspect that not every regulator has seen yet, has understood yet, because we do face a lot of escalations from regulators, from the digital services coordinators, and a lot of times, these are about content that is perfectly legal, that is not in violation of our policies, it's just that they don't like it, someone doesn't like it, I mean, fair, but we need to be careful with free speech as well.

Concerning transparency in recommender systems, what did you do in relation with the DSA?

What we did for DSA is a system that we call system cards, we have taken all the surfaces that are recommender systems on our platforms to explain how they work, to give details on how it works, I mean, again, I cannot tell you how it works for one person compared to another, but it explains a little bit what are the signals that I recommend the system, depending on the surface it takes to determine what content you or me or someone else would see on the platform, so that's something that we've done, and on top of that, we have done it before the DSA, but, you know, it's still iterations that include also changes with the DSA, we have something called why am I seeing this, we call it waste, and basically on every piece of content that you see online, you have this kind of why am I seeing this,

which explains the reason why you're seeing this type of content, it applies also to ads, but also to content, it doesn't go super granularly, because, we need to also make sure we protect, you know, personal information and so on, but it explains, you know, you're seeing this because you're following this account, you're seeing this because this is related to interests that you have on this and that, so it's a way, and again, it's not up for DSA, we had it before, but, you know, we think it fits very well with the idea of transparency of recommended systems of the DSA, and it's something that it's been always appreciated, then again, you would always find critical voices saying that you need to be more specific, more granular and so on, but, you know, you need to be mindful of a lot of things as well in terms of security, in terms of, you know, not disclosing too much about how your systems work, because again, there are malicious actors as well that use this kind of information to override the system and create difficult stuff from a security perspective.

And the same is for alternative options, so this is something that we have done just before the DSA came in, with the DSA in mind, so basically if you go now on on Instagram or Facebook, you have, let's say Instagram as an example, you have the possibility to change the feed from, you know, personalized following, so basically chronological, or a third option which is, you know, you can select those that you want to see and you will just see those, and it's the same for Reels, like for Reels you can do it personalized or, I mean, you cannot do it chronological for Reels, but you can do it, what we do it is basically the most viewed stuff or something like that, I don't remember how it is, and I think it's the same for Explorer feed, like basically every service would have, that you have in the system cards transparently, would have an alternative option that is not personalized, but then, you know, what you can do, I mean, Reels you cannot really do them chronologically, but you can do them, you know, with no personal data involved or use.

Now about transparency in advertising?

Yeah, I mean, on the ads it's the same thing as the recommended system, you will be able to speak granularly why you're seeing a certain ad, but also every ad is even the ad library, so there, you know, this database of stuff, you know, it's called ad library for us, and it has all the, originally it was developed by Meta as a library of political ads, and now it is expanded to cover all ads, no matter whether it's political or commercial, and it includes various information about, you know, about the ad and the spending and so on, which is something,

What was the impact on advertiser behaviour?

The one thing that I remember that was heavily criticized by the advertisers was the changes that we have done to the ad library, because, you know, the DSA requires that we disclose certain types of information, that from our perspective it doesn't matter, you know, but from a perspective of an advertiser, of a company that is advertising, it reveals a little bit the strategy that they're doing in terms of marketing, so they're a bit concerned because they would, they fear that others would be able to see what they're doing and copy them or change them, and there was a lot of concern from that, but in general, you know, in terms of changes to behavior on the use of a platform, I don't think the DSA does that unless you're targeting minors, which, again, we don't allow in the same way that, I mean, for minors we don't allow to target on the basis of location and age, just because you need to, you know, otherwise you don't know whether someone is necessarily a minor, that's more of a safety reason.

Do you think this will lead Meta to rethinking their advertising-driven business model?

No, I mean, I don't think the DSA does anything, has anything to do with that more than DMA, but there's no intention from the company to rethink the business model, I mean, we do think that personalization in advertising is a value, it's a value for different reasons, it's a value for the users in terms of interest, and as they see, it's useful in terms of economic impact for advertisers, because they cost very little, and, you know, I think every euro that you spend on our platforms to advertise generates something like four euros in terms of sales for the companies, so it has big benefits, I mean,

there's a lot of entrepreneurs that scaled up thanks to advertising online, not just on Instagram and Facebook, but also on other platforms, so we see a big value in it, and personalization, which is something that nobody talks about, also allows for safety measures and stuff, if you can personalize experiences, you can make sure that, you know, you show it to appropriate people, that you don't show an ad that might be sensitive for someone, even if it doesn't use sensitive data, you know, that could be annoying for certain age groups, you know, it allows for also a level of safety that nobody talks about, because everybody cares more about the personal data aspect, but yeah, it's a value.

The DMA pushes the boundary of that, as you've seen, we have launched a **subscription model** as well in Europe, but we do think personalization still remains the biggest value that you have to do business online.

Concerning the systematic risk and risk management, you talked already about it, I don't know if you want to add something?

I mean, look, I don't have all the details in mind of how this works, but basically, you know, this is a scaled kind of process, where you map out, you know, different kind of risk areas that you need to look into, and then you map out the kind of tools, policies, products that you have in place to mitigate those risks, and then you try to see whether there's any left kind of options that you need to put in place at the moment. For the moment, I mean, for the way and things we have built our platforms, in terms of what we have shown, and it is confirmed also by the audit that is done externally, you know, what we have presented in terms of assessment of risk, and I think there is a version that is probably, or maybe it's the audit that is probably, that basically shows that we have a solid base of mitigations in place to fight the risks that are identified in the DSA, and it comes back to the point of before, like, sometimes it's difficult to understand what the expectation is from the regulator to go further than that, because, you know, in our perspective, you know, we do have mitigations in place for all the risk profiles, and when it's not, we have made tweaks to policies and so on, and we have done that globally, because we found there was, I mean, what I'm trying to say is that the idea of risk assessment is not something that is limited to the DSA, something that companies do nonetheless, and they do it for different reasons.

They do it for other regulations, they do it for privacy reasons and data protection reasons, so this idea, you know, of assessing risks when you launch product on your services is something that you do continuously, and the products that you build and you put in the market are also a response to that. Then, whether they are a response to DSA, it's very difficult to understand what the expectation is when it comes to this.

A Question about the liability system: Would you consider it still a system of liability exemption due to all the due diligence obligations?

I do, I mean, I am not the expert on this, but our legal teams are not concerned by this. I mean, the liability exemption is a big value for everybody, not just for the industry, and it is recognized by the DSA as, you know, still a cornerstone of how the internet works, and I think the DSA is quite clear on this. There are exemptions, I mean, when you do due diligence, is all the bars about transparency, about risk assessment and so on, it doesn't really touch upon the liability issues. I mean, I don't think the two aspects are complementary or not, you know, clashing with each other.

Like, the risk assessment doesn't tell you to over-remove, like, basically to be, that you have to be responsible for content even if you don't see it, or if you're not aware of it. The notice and action also is quite aligned with it, so I don't think there is an aspect or a challenge down to the liability system, which I think is taken very much from the e-commerce directive, kept more or less the same, and it's very similar to the safe harbor in the U.S. It's just something that is widely accepted as how the internet works. I mean, you know, the moment I become aware or have knowledge of a piece of content, I become liable of it, but also, you have this idea of voluntary detection, sort of voluntary measures in the DSA, and there is a protection on liability when you do this kind of activities as well. So, I do think

that it's not conflictual in the way that the two things are built. I never heard a concern from our lawyers, basically, on this point.

What do you think about the distinction between active and passive role and the term "actual Knowledge"? Are they precise enough?

I mean, I've never heard any concern on this, but I'm not a lawyer. Maybe, you know, there are a lot of litigations in this that I'm not aware of, but yeah, I mean, but I do think the liability system that is built clarifies the idea of what an active and passive role is, or neutral role is, and I think it's pretty straightforward where the responsibility lies on the individual and where the responsibility lies on the platform the moment they are aware of all this content.

What are the main issues concerning the enforcement system?

Yeah, I mean, the main issue with enforcement is the risk of politicization of the enforcement.

That's what we have seen so far. I mean, the investigations we've seen, I'm not saying they have no basis or they have a lot of basis, but they are politically motivated types. And we've seen examples.

I mean, I can give you an example. There's, you know, we have an investigation on disinformation in the context of elections, which, again, I mean, fine, which was done just before the European elections as a sort of, like, you know, we are watching you type of thing. And then, you know, if you look at the results of the European elections, in terms of results, what I mean, like, then what happened on the platforms and what you see from also analysis of organizations that monitor elections, Meta actually was the best performing one, but it's the only one with an investigation on disinformation in elections.

So it's sometimes it's a little bit, you know, you ask, I mean, in the company, you ask yourself whether this is politically motivated or actually based on sound, you know, evidence. But again, it's another topic. I don't think it's a topic for a thesis either.

What about the DSCs?

I mean, this is more a question that you need to ask the Commission. In our case, I mean, what I told you before, there is still a lack of harmonization on a lot of, there's a lot of fragmentation on some stuff. So that's not easy on some issues that need to be developed by DSCs compared to the Commission.

Our experience with digital service coordinators is quite okay. It depends on the coordinator. Some are very active, some are much less active.

We have engaged with all of them. I think, I mean, I think there's a couple of them that are still not officially appointed, but we have engaged always with them to explain how things work on a platform, to make sure that they have a direct channel of communication that is with the company and not with the person that they might know and an email they might get, so that it's streamlined. So it's quite good stuff.

Then it depends on the circumstances and what happens. I mean, a lot of cooperation has been done between DSCs, Commission and platforms, for example, on elections. On elections, there is a lot of work that goes on before the elections.

Partially, it's also, I mean, maybe it could have been mitigated a little bit if they would have done the same exercise that every other country has done over the past years, a couple of years. So that's how it is. But on that, the coordination is quite a positive example of the cooperation between platforms and regulators.

What's your opinion about the sanctions?

But we are very much aware of the 6% fine and that worries the company, of course.

Is inconsistent enforcement an issue?

I mean, that exists. I mean, for us, the enforcement is done at Commission level, so it's less inconsistent. That's more for non-beloved.

But legal disputes, I'm sure they would be, I mean, it's inevitable. I mean, with this kind of laws and stuff, it's inevitable. We actually do have a legal dispute.

Every company has a legal dispute, actually, with the Commission on the fee that we need to pay for their budget, for the supervision of platforms.

The threshold of envelopes with the 45 million active users. Do you think that this threshold is adequate? Do you think it's too high, too low? And do you think it needs additional criteria, like in the Digital Markets Act, where you have also qualitative criteria?

From our perspective, this approach is fine. Because, again, other companies have been pushing for a more risk profile approach besides the numbers. I don't think that's the kind of objective that the Commission wanted to achieve with this. I mean, of course, everything is inherently about risks

I'm going to be wrong. But I mean, in some circumstances, yes, you could capture some platforms that are smaller, that have a high risk. I can imagine Telegram.

Telegram is a platform with quite a high risk, but it's not a below, or at least not yet. Nobody knows. I mean, there's very little transparency there.

In other circumstances, I think maybe something could be added potentially. But for us, it's pretty straightforward. We have never even considered what can we get differently in the deal of definition.

I mean, for us, it's pretty clear that we have two big platforms that are Instagram and Facebook, and they are very large. And they should be regulated this way. One thing that we would always want to avoid is a situation like the DMA, where you have de facto targeted only some companies on the basis of the country of origin, and not on the actual competition presence.

But otherwise, I think I would be surprised if any company that is designated, besides maybe Zalando, challenges the idea of the definition. Maybe some will try to be exempted, but one year you're smaller. Again, the competitive advantage of not being a VLOG is not as big as it would be on the DMA of not being a gatekeeper, for example.

So it's like being a VLOP or not doesn't bring you more revenue. It gives you sometimes more costs, but it's not costs that make you grow as a company and become bigger and scale up even more. So I don't think that's the case.

But let's see, they're going to review the VLOP definition chapter by November. Review doesn't mean that they revise it, that they change it, but they will evaluate it basically by mid-November. So let's see also what the experience of the commission is with this.

But for us, it's pretty straightforward. We will have other VLOPs, that's for sure, in a matter of months. But we're also not disputing that from a perspective of the definition.

Appendix 3: Bullying and Harassment: Example

What are we doing to try to prevent and mitigate these risks?

2024 Trends: During the assessment, we identified that bullying and harassment risks may disproportionately impact minors and thus could potentially increase the inherent risk exposure associated with this Problem Area. As a result, Meta has developed processes and tools specifically targeting minor protection, improved automated detection of content related to bullying and harassment, and bullying prevention resources. Additionally, it was identified that the high number of elections in the EU, including the EU Parliamentary Elections, could increase the risk of bullying and harassment against political public figures on the platform. As a result, Meta put in place dedicated election teams to combat the likely increase in adversarial behaviour.

Problem Area Mitigation Overview: As detailed in Section 6.2.1, we have an extensive ecosystem of controls that work together to manage these Problem Area risks on Facebook. Specifically for Bullying and Harassment, given the potential disproportionate impact on minors' and vulnerable users' well-being and mental health, we provide heightened protection for users under the age of 18, including protection from allegations about criminal or illegal behaviour and videos of physical bullying against minors, in addition to all other protections provided.

We have made strong investments in classifier performance through continuous improvement of our models, extensive experimental periods to test accuracy and stability, and settings to take automated enforcement actions. Additionally, we are continuing to build new features to improve detection of new content types, such as generative AI. This is exemplified by the fact that in the first quarter of 2024, globally, **we actioned 7.9 million pieces of bullying and harassment content on Facebook globally, with 85.6% detected proactively** before being reported by users.[85] Furthermore, we also include a link on nearly every piece of content for reporting abuse, bullying and harassment, and other issues and encourage self reporting as it helps us understand when a person feels bullied or harassed.[86]

We continue to provide many options for users to control their experiences on Facebook and limit unwanted interactions with other users to prevent bullying and harassment. These include blocking other users, restricting other users' ability to comment on their posts, and restricting visibility of posts and profile information for specific users.

There are also many teams at Meta, including the policy and safety teams, that routinely work with external parties to understand new trends and behaviours to help improve Meta's policies and resources. For example, **after working with over 400 women's safety organisations and experts, we established Meta's Global Women's Safety Expert Advisors to advance the safety of women online**. Additionally, we work with bullying prevention experts, such as the Diana Award Anti-Bullying Ambassador Programme, International Bullying Prevention Association, and Cyberbullying Research Centre to stay informed on bullying trends, and maintain our bullying prevention resources, such as Bullying Prevention Tips for Youth, Online Bullying Prevention Tips for Parents, and Managing Bullying and Harassment in Facebook Communities. We also engage with multiple governments during rollouts of EU hate speech tests, to collect feedback for improvements regarding perception of hostile speech mitigation measures on our platforms and services.

Limitations: Throughout our assessment, we identified areas for continued improvement as it relates to detection and enforcement. Bullying and harassment continues to evolve with the landscape of social interaction and digital connection. Threat actors continue to explore ways to circumvent detection and enforcement, such as using emojis, intentional misspellings or symbols. Additionally, with bullying and harassment being highly individualised and context-dependent, it often requires moderators to understand the relationship between users, the meaning behind content and behaviour, and the nuances of language and regional context to avoid over-enforcement of content moderation in benign scenarios. As cultural context changes and new generations emerge, new trends, terms and phrases that are not yet able to be flagged can emerge as well. Meta is continually keeping on top of culture shifts and adapting mechanisms to account for changing landscapes. Additionally, there are no automated detection or classifiers to detect bullying and harassment violations in ads. Therefore, we may rely more on user reporting and human review. However, new features are being built to improve detection of new types of content.

Figure 7: What META does to mitigate the risk of Bullying and Harassment(META Risk assessment, 2024)

REFERENCES

Scientific sources

Albu, O. B., & Flyverbom, M. (2019). Organizational Transparency: Conceptualizations, Conditions, and Consequences. *Business & Society*, *58*(2), 268–297. https://doi.org/10.1177/0007650316659851

Ananny, M., & Crawford, K. (2018). *Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability*.

Andriychuk, O. (2021). Shaping the New Modality of the Digital Markets: The Impact of the DSA/DMA Proposals on Inter-Platform Competition. *World Competition*, *44*(Issue 3), 261–286. https://doi.org/10.54648/WOCO2021017

Ball, C. (2009). What Is Transparency? *Public Integrity*, *11*(4), 293–308. https://doi.org/10.2753/PIN1099-9922110400

Bayer, J., Bitiukova, N., Bard, P., Szakács, J., Alemanno, A., & Uszkiewicz, E. (2019). Disinformation and propaganda–impact on the functioning of the rule of law in the EU and its Member States. *European Parliament, LIBE Committee, Policy Department for Citizens' Rights and Constitutional Affairs*.

Bennett, W., & Livingston, S. (2020). *The disinformation age*. Cambridge University Press.

Berberich, M., & Seip, F. (2021). Der Entwurf des digital services act. *Praxis Im Immaterialgüter-Und Wettbewerbsrecht (GRUR-Prax)*, *13*(1), 4–7.

Biard, A. (2024). The Age of Consumer Law Enforcement in the European Union: High Hopes or Wishful Thinking? *European Journal of Risk Regulation*, *15*(3), 625–636.

Blázquez, F. J. C., Denis, G., Machet, E., McNulty, B., & European Platform of Regulatory Authorities. (2021). *Media regulatory authorities and the challenges of cooperation*. European Audiovisual Observatory.

Bloch-Wehba, H. (2020). Automation in moderation. *Cornell Int'l LJ*, *53*, 41.

Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press.

Braithwaite, J., & Drahos, P. (2000). *Global business regulation*. Cambridge university press.

Buiten, M. C. (2021). The digital services act from intermediary liability to platform regulation. *J. Intell. Prop. Info. Tech. & Elec. Com. L.*, *12*, 361.

Cauffman, C., & Goanta, C. (2021). A New Order: The Digital Services Act and Consumer Protection. *European Journal of Risk Regulation*, *12*(4), 758–774. https://doi.org/10.1017/err.2021.8

Chander, A. (2023). *Front Matter – Volume 38, Issue 4*. https://doi.org/10.15779/Z38RX93F48

Chatterjee, S. (2023). https://www.holisticai.com/blog/rules-for-independent-audits-digital-services-act

Christensen, L. T., & Cheney, G. (2015). Peering into transparency: Challenging ideals, proxies, and organizational practices. *Communication Theory*, *25*(1), 70–90.

Cleynenbreugel, P. V., & Mattioli, P. (2023). Digital Services Coordinators and other competent authorities in the Digital Services Act: Streamlined enforcement coordination lost? *European Law Blog*. https://doi.org/10.21428/9885764c.f18f26b8

Cohen, J. E. (2017). Law for the platform economy. *UCdL Rev.*, *51*, 133.

Cotter, K. (2023). "Shadowbanning is not a thing": Black box gaslighting and the power to independently know and credibly critique algorithms. *Information, Communication & Society*, *26*(6), 1226–1243.

Crain, M. (2018). The limits of transparency: Data brokers and commodification. *New Media & Society*, *20*(1), 88–104. https://doi.org/10.1177/1461444816657096

Crawford, K. (2016). Can an algorithm be agonistic? Ten scenes from life in calculated publics. *Science, Technology, & Human Values*, *41*(1), 77–92.

Crémer, J., De Montjoye, Y.-A., & Schweitzer, H. (2019). *Competition policy for the digital era*. Publications Office of the European Union.

Cyber Expert. (2024, March). *The principle of the Digital Services Act*. https://blog.httpcs.com/en/digital-services-act-dsa-2/

Darius, P., Stockmann, D., Bryson, J., Cingolani, L., Griffin, R., Hammerschmid, G., Kupi, M., Mones, H., Munzert, S., & Riordan, R. (2023). *Implementing Data Access of the Digital Services Act: Collaboration of European Digital Service Coordinators and Researchers in Building Strong Oversight over Social Media Platforms*.

David, M. (2018). The correspondence theory of truth. *The Oxford Handbook of Truth*, *1*, 219–237.

Diakopoulos, N. (2016). Accountability in algorithmic decision making. *Communications of the ACM*, *59*(2), 56–62.

Drolsbach, C., & Pröllochs, N. (2023). *Content Moderation on Social Media in the EU: Insights From the DSA Transparency Database* (No. arXiv:2312.04431). arXiv. https://doi.org/10.48550/arXiv.2312.04431

Eder, N. (2024). Making systemic risk assessments work: How the DSA creates a virtuous loop to address the societal harms of content moderation. *German Law Journal*, *25*(7), 1197–1218.

Edwards, L., & Veale, M. (2017). Slave to the algorithm? Why a'right to an explanation'is probably not the remedy you are looking for. *Duke L. & Tech. Rev.*, *16*, 18.

Engler, A. (2021). *Platform data access is a lynchpin of the EUs Digital Services Act*.

Erixon, F. (2021a). *Too big to care or 'too big to share': The Digital Services Act and the consequences of reforming intermediary liability rules*.

Erixon, F. (2021b). *Too big to care or" too big to share": The Digital Services Act and the consequences of reforming intermediary liability rules*.

European Commission. (2018). *COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT REPORT ANNEXES Accompanying the document PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*. Publications Office. https://data.europa.eu/doi/10.2759/780040

European Commission. (2019). *How do online platforms shape our lives and businesses?* https://digital-strategy.ec.europa.eu/en/library/how-do-online-platforms-shape-our-lives-and-businesses-brochure#Benefits

European Commission. (2022). *The Digital Services Act: Ensuring a safe and accountable online environment*. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en

European Commission. (2025). *Supervision of the designated very large online platforms and search engines under DSA*. https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses

European Council. (2022). *'Path to the Digital Decade': Council adopts key policy programme for EU's digital transformation*. https://www.consilium.europa.eu/en/press/press-releases/2022/12/08/path-to-the-digital-decade-council-adopts-key-policy-programme-for-eu-s-digital-transformation/

European Parliament. (2022). *Digital Services Act: Application timeline*. https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2022)739227

Flyverbom, M. (2015). *Sunlight in cyberspace? On transparency as a form of ordering*.

Fox, J. (2007). The uncertain relationship between transparency and accountability. *Development in Practice*, *17*(4–5), 663–671. https://doi.org/10.1080/09614520701469955

François, C., & Douek, E. (2021). The Accidental Origins, Underappreciated Limits, and Enduring Promises of Platform Transparency Reporting about Information Operations. *Journal of Online Trust and Safety*, *1*(1). https://doi.org/10.54501/jots.v1i1.17

Frosio, G. F. (2017). Reforming intermediary liability in the platform economy: A European digital single market strategy. *Nw. UL Rev. Online*, *112*, 18.

Frosio, G. F. (2018). Why keep a dog and bark yourself? From intermediary liability to responsibility. *International Journal of Law and Information Technology*, *26*(1), 1–33.

Genç-Gelgeç, B. (2022). *REGULATING DIGITAL PLATFORMS: WOULD THE DSA AND THE DMA WORK COHERENTLY? 1*(3).

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

Gillespie, T. (2022). Do not recommend? Reduction as a form of content moderation. *Social Media+ Society*, *8*(3), 20563051221117552.

Gorwa, R., & Ash, T. G. (2020). *Democratic Transparency in the Platform Society*.

Gorwa, R., Binns, R., & Katzenbach, C. (2020). Algorithmic content moderation: Technical and political challenges in the automation of platform governance. *Big Data & Society*, *7*(1), 2053951719897945.

Halil, D., Kollnig, K., & Tamò-Larrieux, A. (2024). *Regulating pressing systemic risks – but not too soon?* Comparative Analysis of the Implementation of Data Access Requests to Platform Data under Article 40(4) of the EU Digital Services Act. SSRN. https://doi.org/10.2139/ssrn.4959049

Harlow, C. (2011). *Accountability as a value in global governance and for global administrative law*.

Heald, D. (2006). *Varieties of transparency* (Issue 135). Oxford University Press for The British Academy.

Helberger, N., Van Drunen, M., Vrijenhoek, S., & Möller, J. (2021). Regulation of news recommenders in the Digital Services Act: Empowering David against the very large online Goliath. *Internet Policy Review*, *26*(26 February).

Horta Ribeiro, M., Cheng, J., & West, R. (2023). *Automated content moderation increases adherence to community guidelines*. 2666–2676.

Hunziker, S., & Blankenagel, M. (2021). Research design in business and management. *Wiesbaden: SpringerGabler*, *1*.

Husovec, M., & Roche Laguna, I. (2022). Digital Services Act: A Short Primer. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4153796

Irion, K., Delinavelli, G., Coutinho, M. F., Fathaigh, R. Ó., Jusić, T., Klimkiewicz, B., Llorens, C., Rozgonyi, K., Svensson, S., & Smokvina, T. K. (2019). *The independence of media regulatory authorities in Europe*. European Audiovisual Observatory.

ISO. (2018). *ISO 31000:2018 Risk management—Guidelines*. https://www.iso.org/standard/65694.html

Jaidka, K., Mukerjee, S., & Lelkes, Y. (2023). Silenced on social media: The gatekeeping functions of shadowbans in the American Twitterverse. *Journal of Communication*, *73*(2), 163–178.

Jain, N. (2021). Survey versus interviews: Comparing data collection tools for exploratory research. *The Qualitative Report*, *26*(2), 541–554.

Kaminski, M. E. (2020). Understanding transparency in algorithmic accountability. *Forthcoming in Cambridge Handbook of the Law of Algorithms, Ed. Woodrow Barfield, Cambridge University Press (2020)., U of Colorado Law Legal Studies Research Paper*, *20–34*.

Katsaros, M., Yang, K., & Fratamico, L. (2022). *Reconsidering tweets: Intervening during tweet creation decreases offensive content*. *16*, 477–487.

Keller, D. (2021). Amplification and its discontents: Why regulating the reach of online content is hard. *J. Free Speech L.*, *1*, 227.

Kenney, M., & Zysman, J. (2016). The rise of the platform economy. *Issues in Science and Technology*, *32*(3), 61.

Le Merrer, E., Morgan, B., & Trédan, G. (2021). *Setting the record straighter on shadow banning*. 1–10.

Leerssen, P. (2020). The soap box as a black box: Regulating transparency in social media recommender systems. *European Journal of Law and Technology*, *11*(2).

Leerssen, P. (2021). *Platform research access in Article 31 of the Digital Services Act: Sword without a shield?*

Leerssen, P. (2023). An end to shadow banning? Transparency rights in the Digital Services Act between content moderation and curation. *Computer Law & Security Review*, *48*, 105790. https://doi.org/10.1016/j.clsr.2023.105790

Lomba, N., & Evas, T. (2020). *Digital Services Act: European added value assessment*. European Parliament.

META. (n.d.). *Community Standards*. https://transparency.meta.com/en-gb/policies/community-standards/

Meta. (2023). *Regulation (EU) 2022/2065 Digital Services Act Transparency Report for Facebook*.

META. (2024a). *Regulation (EU) 2022/2065 Digital Services Act Transparency Report for Facebook*.

META. (2024b). *Regulation (EU) 2022/2065 Digital Services Act Transparency Report for Facebook October*.

META Risk assessment. (2024). *Systemic Risk Assessment and Mitigation Report for Facebook*.

Meta Transparency Report. (2023). *Transparency Report Facebook* [Transparency Report].

Meta Transparency Report. (2024). *Regulation (EU) 2022/2065 Digital Services Act Transparency Report for Facebook*.

Miller, E. L. (2021). Amplified Speech. *Cardozo L. Rev.*, *43*, 1.

Moravcová, D. (2023). Impact of the DSA Regulation on Very Large Online Platforms. *Central European Journal of Comparative Law*, *4*(2), 163–176. https://doi.org/10.47078/2023.2.163-176

Myers West, S. (2018). Censored, suspended, shadowbanned: User interpretations of content moderation on social media platforms. *New Media & Society*, *20*(11), 4366–4383.

Nagy, C. I. (2022). What Role for Private Enforcement in EU Competition Law? *The Cambridge Handbook of Competition Law Sanctions*, 218.

Nunziato, D. C. (2023). The Digital Services Act and the Brussels Effect on Platform Content Moderation. *ChicagoJournalof InternationalLaw*, *24*(1).

Phillips, J. W. P. (2011). Secrecy and Transparency: An Interview with Samuel Weber. *Theory, Culture & Society*, *28*(7–8), 158–172. https://doi.org/10.1177/0263276411428339

Piotr, B. (2022). *Holocaust denial in criminal law: Legal frameworks in selected EU Member States*.

Public Policy Manager META. (2025). *Interview Meta* [Personal communication].

Radsch, C. (2021). Shadowban/shadow banning. *Teoksessa IGF Glossary of Platform Law and Policy Terms, Toimittaneet Luca Belli, Nicolo Zingales Ja Yasmin Curzi*, 295–296.

Reig, M., Gasco-Hernandez, M., & Esteve, M. (2021). Internal and External Transparency in Public-Private Partnerships—The Case of Barcelona's Water Provision. *Sustainability*, *13*(4), 1777. https://doi.org/10.3390/su13041777

Resnick, M., Berg, R., & Eisenberg, M. (2000). Beyond black boxes: Bringing transparency and aesthetics back to scientific investigation. *The Journal of the Learning Sciences*, *9*(1), 7–30.

Reyna, A. (2024). DMA and DSA *Effective* Enforcement—Key to Success. *Journal of Antitrust Enforcement*, *12*(2), 320–324. https://doi.org/10.1093/jaenfo/jnae018

Roberts, S. T. (2019). *Behind the screen*. Yale University Press.

Rodríguez de las Heras Ballell, T. (2021). *The background of the Digital Services Act: Looking towards a platform economy*. *22*(1), 75–86.

Ruslin, R., Mashuri, S., Rasak, M. S. A., Alhabsyi, F., & Syam, H. (2022). Semi-structured Interview: A methodological reflection on the development of a qualitative research instrument in educational studies. *IOSR Journal of Research & Method in Education (IOSR-JRME)*, *12*(1), 22–29.

Ryan, J., & Toner, A. (2020). *Europe's governments are failing the GDPR*.

Sanchez, M. D. M. (2024). The Devil Is in the Procedure: Private Enforcement in the DMA and the DSA. *U. Bologna L. Rev.*, *9*, 7.

Savova, D., Mikes, A., & Cannon, K. (2021). The Proposal for an EU Digital Services Act — A closer look from a European and three national perspectives: France, UK and Germany. *Computer Law Review International*, *22*(2), 38–45. https://doi.org/10.9785/cri-2021-220203

Schwemer, S. F. (2021). Recommender Systems in the EU: From Responsibility to Regulation. *Morals & Machines*, *1*(2), 60–69. https://doi.org/10.5771/2747-5174-2021-2-60

Senden, L. (2020). Towards a more holistic legitimacy approach to technical standardisation in the EU. In *The Legitimacy of Standardisation as a Regulatory Technique* (pp. 20–47). Edward Elgar Publishing.

Stohl, C. (n.d.). *Managing Opacity: Information Visibility and the Paradox of Transparency in the Digital Age*.

Strowel, A., & De Meyere, J. (2023). The Digital Services Act: Transparency as an efficient tool to curb the spread of disinformation on online platforms? *J. Intell. Prop. Info. Tech. & Elec. Com. L.*, *14*, 66.

Suzor, N. P., West, S. M., Quodling, A., & York, J. (2019). What do we mean when we talk about transparency? Toward meaningful transparency in commercial content moderation. *International Journal of Communication*, *13*, 18.

Swan, E. J. (2022). *Internet Law: A Concise Guide to Regulation Around the World*. Kluwer Law International BV.

Swisher, K. (2018). *Zuckerberg: The Recode Interview, Vox*.

Tapscott, D., & Ticoll, D. (2003). *The naked corporation: How the age of transparency will revolutionize business*. Simon and Schuster.

Thorson, K., & Wells, C. (2016). Curated flows: A framework for mapping media exposure in the digital age. *Communication Theory*, *26*(3), 309–328.

Tridimas, T. (2020). Financial regulation and private law remedies: An EU law perspective. In *Financial regulation and civil liability in European law* (pp. 47–72). Edward Elgar Publishing.

Trujillo, A., Fagni, T., & Cresci, S. (2024). *The DSA Transparency Database: Auditing Self-reported Moderation Actions by Social Media* (No. arXiv:2312.10269). arXiv. https://doi.org/10.48550/arXiv.2312.10269

Turillazzi, A., Taddeo, M., Floridi, L., & Casolari, F. (2023). The digital services act: An analysis of its ethical, legal, and social implications. *Law, Innovation and Technology*, *15*(1), 83–106. https://doi.org/10.1080/17579961.2023.2184136

Unesco. (2024). *What you need to know about digital learning and transformation of education*. https://www.unesco.org/en/digital-education/need-know?hub=84636

Van Dijck, J., Poell, T., & De Waal, M. (2018). *The platform society: Public values in a connective world*. Oxford university press.

Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the Draft EU Artificial Intelligence Act—Analysing the good, the bad, and the unclear elements of the proposed approach. *Computer Law Review International*, *22*(4), 97–112.

Waddock, S. (2004). Creating corporate accountability: Foundational principles to make corporate citizenship real. *Journal of Business Ethics*, *50*, 313–327.

Wagner, B. (2021). A first impression of regulatory powers in the Digital Services Act. *Verfassungsblog: On Matters Constitutional*.

Waldron, J. (2016). *The rule of law*.

Walker, K. (2018). Supporting election integrity through greater advertising transparency. *Public Policy*.

Weck, T. (2024). The DSA and Digital Violence: Entrepreneurial Freedom and Special Responsibility. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4667280

Wilman, F. (2022). Between preservation and clarification. *Verfassungsblog*.

Yurukova, M. (2023). *THE ROLE OF THE MEMBER STATES' DIGITAL SERVICES COORDINATOR FOR ENSURING COORDINATED AND CONSISTENT ENFORCEMENT OF THE DIGITAL SERVICES ACT*.

Zuboff, S. (2019). *Surveillance capitalism and the challenge of collective action*. *28*(1), 10–29.

Zuboff, S. (2023). The age of surveillance capitalism. In *Social theory re-wired* (pp. 203–213). Routledge.

Legal Sources

CASE LAW

CJEU*, Republic of Poland v European Parliament and Council of the European Union,* Judgment of the Court (Grand Chamber) of 26 April 2022, Case C-401/19

CJEU (grand chambre). *Google France SARL and Google Inc. v Louis Vuitton Malletier SA (C-236/08), Google France SARL v Viaticum SA and Luteciel SARL (C-237/08), and Google France SARL v CNRRH SARL and Others (C-238/08)*. 23 March 2010, Cases C-236/08 to C-238/08.

CJEU, *L'Oréal SA and Others v eBay International AG and Others,* 12 July 2011, Case C-324/09

CJEU, *Vantaan kaupunki v Skanska Industrial Solutions Oy and Others*, 14 March 2019, Case C-724/17

Legislation

Charter of Fundamental Rights of the European Union, OJEU, C 326, 26.10.2012, p. 391–407

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') OJEU, L 178, 17.7.2000, p. 1–16

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJEU, L 201, 31.7.2002, p. 37–47 (hereafter abbreviated E-privacy Directive)

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 Text with EEA relevance, OJEU, L 304, 22.11.2011, p. 64–88

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) *OJEU, L 119, 4.5.2016, p. 1–88*

Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) *OJEU, L 265, 12.10.2022, p. 1–66*

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) *OJEU, L 277, 27.10.2022, p. 1–102*

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) *OJEU, L, 2024/1689, 12.7.2024*