Zoi Krokida is a lecturer in AI, Innovation, and Law at Brunel University of London. She is also an International Research Fellow at the Information Society Law Center of the University of Milan (2022–2025). She is a member of the Coordinating Board of the Scottish Law and Innovation Network (SCOTLIN) and the co-convenor of the Cyberlaw stream of the Society of Legal Scholars. She is the co-investigator of the research grant on the project "Social Media-Facilitated Trafficking of Children and Young People" by the ESRC Vulnerability & Policing Futures Research Centre. Her research interests include IP Law and New Technologies, ISPs' regulatory framework, online defamation, and responsible use of AI technology. She is the author of *Internet Service Provider Liability for Copyright and Trade Mark Infringement: Towards an EU Co-Regulatory Framework* (2022, Hart Publishing).
Contact: zoi.krokida@brunel.ac.uk

Soft Power
Revista euro-americana de teoría
e historia de la política y del derecho

Vol. 12(1). Enero-Junio 2025
ISSN (online): 2539/2239 ISSN (print): 2389-8232
https://doi.org/10.14718/SoftPower.2025.12.1.3

INSTITUTIONALISING ONLINE PLATFORMS UNDER THE EU DIGITAL SERVICES ACT: A PANACEA OR A RISK TO INNOVATION?*

Dr Zoi Krokida
Brunel University of London

INSTITUCIONALIZACIÓN DE LAS PLATAFORMAS VIRTUALES SEGÚN LA LEY DE SERVICIOS DIGITALES DE LA UE: ¿PANACEA O RIESGO PARA LA INNOVACIÓN?

Abstract
Online purchasing has been blooming in recent years, with 12 % of EU enterprises offering their goods for sale online. However, recent reports and a line of case law indicate an increasing number of trademark infringements within their networks. From a legislative perspective, at the European level, the regulatory framework governing online platforms' activities is based on the E-Commerce Directive, which has been updated by the Digital Services Act. This new framework came into force in 2022 and marks a shift from private ordering to the institutionalisation of online platforms' roles through a set of legal rules,

* Reception date: 11th february, 2025; acceptance date: 11th march, 2025. The essay is the result of research carried out within the Brunel Law School, Brunel University of London.

similar to those imposed on financial institutions. This article argues that the new legal framework envisaged in the Digital Services Act poses a serious risk to innovation within the EU Digital Single Market; hence, it puts forward a set of guiding principles based on a sector-specific legislative framework for the regulation of the liability of online platforms for trademark infringements that accrue within their networks.

Keywords
Digital Services Act; online platforms; innovation.

Resumen
Las compras en línea han experimentado un auge en los últimos años, con un 12 % de las empresas de la Unión Europea que ofrecen sus bienes en línea. Sin embargo, informes recientes y una línea jurisprudencial evidencian un aumento de infracciones de marcas dentro de sus redes. Desde una perspectiva legislativa, a nivel europeo, el marco regulatorio que rige las actividades de las plataformas en línea se basa en la Directiva sobre comercio electrónico, la cual ha sido actualizada por la Ley de Servicios Digitales. Este nuevo marco entró en vigencia en 2022 y marca un tránsito desde la autorregulación privada hacia la institucionalización del papel de las plataformas en línea mediante un conjunto de normas jurídicas, similares a las impuestas a las instituciones financieras. Este artículo sostiene que el nuevo marco jurídico previsto en la Ley de Servicios Digitales plantea un riesgo significativo para la innovación dentro del Mercado Único Digital de la UE. En consecuencia, propone una serie de principios orientadores basados en un marco legislativo sectorial para la regulación de la responsabilidad de las plataformas en línea por infracciones de marcas que se produzcan dentro de sus redes.

Palabras clave
Ley de Servicios Digitales; plataformas en línea; innovación.

Introduction

The growth of online purchasing has been rapid in recent years. In particular, it is estimated that during the COVID-19 pandemic, 12 % of EU enterprises began or increased their efforts to offer goods for sale via online marketplaces, apps, and websites (EUIPO, 2021, p. 1; Eurostat, 2022) Moreover, it is estimated that revenues for Amazon, Etsy, and eBay have reached more than one billion dollars in 2023 (Statista Research Department, 2024). However, recent reports indicate an increasing number of trademark infringements within their networks. For instance, a report commissioned by the European Parliament (2020) demonstrates that the internet is a facilitator for the circulation of copyright-protected content and counterfeit products online, and that Instagram has become a channel where intellectual property infringements take place (EUIPO, 2021, p. 1). Moreover, it has been reported that EU and domestic courts have become preoccupied with a number of lawsuits concerning trademark violations in the services of online platforms (Joined Cases C-148/21 and C-184/21).

At the European level, the regulatory framework governing online platforms' activities is based on the provisions of the E-Commerce Directive (2000/31/EC), which has been updated by the Digital Services Act (Regulation (EU) 2022/2065). The new framework came into force in 2022 and has been described by Turillazzi et al. (2023) as "… a trade-off between the protection of users' Fundamental Rights and the ability to innovate and compete on online platforms" (p. 85). However, the new framework reveals a shift away from private ordering toward the institutionalisation of online platforms' roles. In particular, the new framework categorises online platforms differently and imposes new obligations on them, depending on their size, similar to those imposed by financial institutions. Crucially, while the shift from private ordering to the institutionalisation of online platforms may enhance brand owners' rights, it may also fail to accommodate online platforms' interests. Therefore, a risk may arise that jeopardises innovation within the Digital Single Market.

Against this background, this article argues that the new due diligence obligations in the Digital Services Act might subordinate the rights of online platforms, including the very large ones. To do so, the article first discusses the liability rules for online platforms under the E-Commerce Directive (ECD) and the EU Digital Services Act (DSA). In the second part, the article examines the shift from private ordering to the institutionalisation of online platforms and delves into a critical analysis of the relevant provisions from the DSA, drawing parallels with financial regulations. Following that, the discussion moves to the implications of imposing due diligence obligations on online platforms' interests and business models. Having discussed the relevant legal provisions

and their impact on online platforms' interests, the article offers a set of sector-specific recommendations to safeguard online platforms' rights and innovation across the Digital Single Market.

Liability of Online Platforms: From the E-Commerce Directive to the Digital Services Act

In 2001, the ECD came into force to regulate the activities of online platforms and their potential liability for trademark infringement. More specifically, Article 14(1) of the ECD offered the conditions under which online platforms were not liable for trademark infringements that took place within their networks and noted that online platforms were exonerated from liability if they did not have knowledge of the infringing material or illicit activity that took place within their networks, or when they expeditiously removed the infringing material upon receiving notification from the rights holders. Given that e-commerce was still in its infancy at the time, those immunity liability provisions were justified as a means of boosting innovation at the European level.

However, Article 14(1) of the ECD appears to be outdated. This was mainly because the article in question refrained from defining the liability of online platforms. Rather, it offered several defences to exonerate online platforms from liability. What is more, the national transposition of the provision across EU member states failed to provide a clear answer regarding the liability of online platforms. For instance, a report from the European Commission revealed that member states followed Article 14(1) of the ECD verbatim. They endorsed defences for ISPs that could be invoked to defend themselves against allegations of liability; meanwhile, there were variations in the interpretations of the terms amongst the member states. Finally, many courts turned to their national secondary tort liability rules to attribute liability to online platforms. Given the lack of harmonisation of secondary liability rules at the European level, each jurisdiction would apply its own national tort law to determine the appropriate tortious liability doctrines and thus define online platforms' liability (Krokida, 2022, p. 40).

Against this background, the EU policymakers introduced the DSA in 2022, described by scholars as "a major milestone in the history of platform regulation" (Keller, 2022, p. 299), while EU politicians applauded the new legislative instrument, with the Commissioner for the Internal Market Thierry Breton stating that

> With the DSA, the time of big online platforms behaving like they are "too big to care" is coming to an end. The DSA is setting clear, harmonised obligations for

> platforms—proportionate to size, impact, and risk. It entrusts the Commission with supervising very large platforms, including the possibility to impose effective and dissuasive sanctions of up to 6 % of global turnover or even a ban on operating in the EU single market in case of repeated serious breaches. EU institutions have worked hand in hand in record time, with determination and ambition to protect our citizens online. (European Commission, 2022)

Crucially, it seems that the DSA retains the key liability elements of the ECD by reinforcing the online platforms' liability regime, as set forth in Article 14(1) of the ECD. This means that, under Article 6 of the DSA, online platforms are not liable if they are unaware of the illegal activity or remove the illegal content expeditiously upon being notified. Indeed, Recital 16 notes that the liability framework set forth in the ECD is preserved in the DSA, while Recital 17 clearly states that the DSA does not provide a positive basis for liability of online platforms. Therefore, the flaws entailed in Article 14(1) of the ECD constitute a substantive part of the DSA.

However, apart from reinforcing the key liability features of the ECD, the DSA also provides clarifications regarding the active role of online platforms and their liability for illegal activities within their services. Indeed, unlike the ECD, the DSA introduces a quasi-Good Samaritan provision in Article 7, stating that online platforms are not deemed ineligible for immunity from liability if they undertake voluntary measures to detect illegal content online. This means that immunity liability defences will apply even if online platforms deploy measures to terminate or prevent the dissemination of content online. Furthermore, Recital 18 of the DSA describes the provision of services by online platforms as merely a technical, automatic processing of information and refrains from addressing the concept of the passive nature of online platforms as set forth in Recital 42 of the ECD.

Overall, one might conclude that the DSA provisions reinforce the ECD's liability rules and make a positive attempt to address the flaws identified in the ECD's immunity liability rules. Interestingly, apart from the liability provisions, the DSA envisions an additional set of procedural obligations for online platforms, adopting a tier-based approach. As Geese (2023) points out, "The DSA opens our eyes to the bigger picture in this respect. Whilst honouring the hosting liability exemption privilege of the E-Commerce Directive, it places the focus much more on the platforms' conduct through the regime of due diligence obligations" (Geese, 2023, p. 68). The following section provides a critical examination of the obligations to online platforms.

Obligations and Institutionalisation of Online Platforms

The legal framework envisaged in the DSA appears to signal a paradigm shift from private ordering to the institutionalisation of online platforms. This is because the DSA establishes, depending on their size, a foundation of obligations for online platforms by imposing procedural and compliance requirements. Crucially, as discussed below, such obligations seem to accentuate legal uncertainties and are subject to criticism.

Firstly, the DSA requires online platforms that attract less than 45 million users to adhere to a set of obligations. These obligations primarily focus on content moderation. More specifically, under Article 15, online platforms are required to publish transparency reports in a machine-readable format, in an easily accessible manner, and at least once a year on content moderation within their services. Moreover, as per Article 16, online platforms are also required to deploy a notice-and-takedown mechanism to prevent the dissemination of unlawful content within their services. The removal of content shall be followed by a statement of reasons that justify such removal. Finally, as per Article 20, online platforms are required to establish an internal complaints system and provide users with access to submit appeals against online platform decisions within a timeframe of at least six months following the decision.

However, it is worth noting that content moderation might not always be a panacea for consumer rights. There are several reasons for this. Firstly, there is a risk associated with issuing strategically structured transparency reports. More specifically, a recent BEUC report highlighted that transparency reports focusing on intellectual property infringements often provide limited information on product safety and consumer violations (BEUC, 2021). In addition, a scheme for internal handling of complaints might be subject to language or expertise barriers. For instance, decisions to remove content related to trademark infringement may require human staff with expertise in IP law or specific linguistic skills (Genç-Gelgeç, 2022, p. 48).

Secondly, the DSA imposes an overall risk management framework for very large online platforms, i.e., those platforms that attract more than 45 million users, subject to the European Commission's evaluation every six months. Interestingly, while the risk-based approach is a novelty in digital platform regulation, it is common in the regulation of financial markets (Efroni, 2021).

In particular, financial institutions are required to undertake enhanced due diligence measures in transactions exceeding €1,000 with high-net-worth individuals. For instance, the Anti-Money Laundering legislation requires financial institutions to verify the identity of their customers and the legitimacy of their transactions through client monitoring practices (AMLA). At the same time, electronic payment services are already covered by that

legislation and therefore are subject to due diligence obligations (Ullrich, 2017, p. 125). Amazon Payments Europe has been registered as an electronic money institution, while Google Payment Ltd has obtained an e-Money issuer license in Lithuania (Bloomberg, 2018). In the context of very large online platforms, as per Article 30 of the DSA, they are required to obtain identification information from traders who wish to use their services. More specifically, very large online platforms need to verify traders' contact details, identification documents, payment account details, and the trade register indicating where they are registered. This understanding has already been exemplified in Amazon's Brand Registry, which enables brand owners to register their trademarks (Amazon, 2024). Should a counterfeit product be displayed for purchase on the Amazon platform, the brand owner will be notified.

Furthermore, financial institutions are required to conduct a risk assessment as part of their business operations. For instance, the World Bank Group (2019) published a set of guidelines on credit scoring approaches and highlighted their use by banks to evaluate customer risks associated with individual business relationships. In this light, banks take into consideration a set of risk factors, such as the customer's reputation and/or known adverse information about the customer, the source, structure, and adequacy of information about the customer's wealth, the source of the customer's funds, expected activity on the account (types of transaction, volumes, amounts, the use of cash), the customer's profession/industry sector, and involvement in public contracts. For instance, the Financial Action Task Force sets out guidelines with regard to a risk-based approach in the banking sector and requires financial institutions to conduct risk assessments in order to assess how, and to what extent, the bank is vulnerable to money laundering cases, and to enable the banks to categorise the risk and determine the level of measures required to mitigate any risks of money laundering (FATF, 2014, p. 17).

In a similar fashion, in the context of online platforms, Article 34 requires them to analyse and assess any systemic risks in the Union stemming from the design or functioning of their service and its related systems, including algorithmic systems, or from the use made of their services. To do so, they need to consider a number of factors, such as the design of their recommender systems and content moderation systems, the applicable terms and conditions and their enforcement, the systems used for the selection and presentation of advertisements, and the data-related practices of the providers. Finally, Article 35 of the DSA envisages a set of measures in order to mitigate risks. For instance, very large platforms are required to undertake measures such as adapting the design features of their services or modifying their content moderation processes, as well as testing both algorithmic and recommender systems.

In addition, in the context of financial markets' regulation, supervisors are required to report any suspicious cases to the Financial Units. For example, as per Article 43 of the Anti-Money Laundering Directive ((EU) 2024/1640), supervisors must share information with the Financial Units on:

(a) the list of establishments operating in that Member State and of infrastructure under their supervision pursuant to Article 29a (1) of this Directive, and of any changes to those lists;
(b) any relevant findings indicating serious weaknesses of the reporting systems of obliged entities;
(c) the results of the risk assessments performed pursuant to Article 31, in aggregated form.

Similarly, in the DSA, Digital Services Coordinators have investigative powers. As per Article 51(1), such coordinators have:

(a) the power to require those providers, as well as any other persons acting for purposes related to their trade, business, craft or profession that may reasonably be aware of information relating to a suspected infringement of this Regulation, including organisations performing the audits referred to in Article 37 and Article 75(2), to provide such information without undue delay;
(b) the power to carry out, or to request a judicial authority in their Member State to order, inspections of any premises that those providers or those persons use for purposes related to their trade, business, craft or profession, or to request other public authorities to do so, in order to examine, seize, take or obtain copies of information relating to a suspected infringement in any form, irrespective of the storage medium;
(c) the power to ask any member of staff or representative of those providers or those persons to give explanations in respect of any information relating to a suspected infringement and to record the answers with their consent by any technical means.

Finally, the enforcement of obligations on financial institutions has been attributed to specific administrative bodies. In particular, under Article 50 of the Anti-Money Laundering Regulation, Financial Intelligence Units are required to have immediate and direct access to financial and tax information, as well as to information on funds and other assets subject to financial sanctions. In a similar vein, Article

49 of the DSA states that Digital Services Coordinators are assigned to supervise and enforce the DSA, while Article 51 lists the tasks they will carry out.

Overall, one might conclude that different obligations are imposed on online platforms based on their size. From content moderation to risk assessment obligations, a new institutional framework for online platforms emerges. Such a framework appears to raise legal uncertainties, yet shares commonalities with the regulatory framework of financial markets. In this vein, the following section examines the impact of the new framework on online platforms' rights and innovation within the Digital Single Market.

Implications

The set of due diligence obligations to online platforms, similar to financial institutions, might have a detrimental effect on their operation, the online platforms, violating their fundamental right to conduct business as per Article 16 of the EU Charter of Fundamental Rights, while at the same time posing risks for the prosperity of the Digital Single Market's environment.

Firstly, crafting a legal framework similar to that applied to financial institutions might conflict with the very nature of online platforms and the main rationale underpinning their business models. This is because online platforms are considered to be public squares where users can exchange information and views. Indeed, as Tourkochoriti (2023) points out, "Today, online platforms largely define the public sphere and the opportunities for citizens both to express themselves and access the views of others" (p. 133). Consider, for instance, the level of online engagement among users, which reveals that, as of June 2022, more than 500 hours of video were uploaded to YouTube every minute (Ceci, 2024). As a result, imposing a regulatory framework similar to that of financial markets might jeopardise their main aims.

In light of that, some users might migrate to other platforms or identify alternative avenues for exchanging information and views. This understanding has been illustrated in a number of media studies, where bans on specific political beliefs have led many internet users to move to other platforms that offer anonymity and confidentiality (Tourkochoriti, 2023, p. 144). For instance, a study of user migration across platforms reveals that the main reasons for migration may be poor service quality, negative interaction experiences, or attractive new features of newer platforms. Telling examples can be found on Reddit, where user migration from the platform resulted from amendments to its content moderation policy, and from X to Mastodon due to Twitter's change of ownership (Jeong et al., 2024).

Secondly, it appears that the DSA's provisions presuppose that all online platforms' business models, including those of very large platforms, operate like those of the Big

Tech Players. This is because several online platforms do not collect the information that the DSA assumes they collect. Indeed, Tushnet (2023) provides an example by citing the Organisation for Transformative Work, where they also work (p. 924). The scholar explains that the organisation is a volunteer-operated website for transformative, non-commercial works, and that, as of 2023, it has 4.7 million registered users who do not collect data or use practices through their recommender and advertising systems. As a result, the one-size-fits-all approach may create obstacles for businesses operating in the Digital Single Market and for new players seeking to enter it.

Thirdly, the imposition of procedural obligations might change the landscape of online platforms' business models. This is because very large online platforms already have the resources and know-how to develop measures to mitigate risks posed by the circulation of counterfeit goods online. Consider, for instance, that in the third quarter of 2023, YouTube's revenues reached $7.952 billion, while Meta's reached $32 billion (Statista Research Department, 2024). In addition, it appears that very large online platforms already have the resources to develop practices and demonstrate compliance with their obligations under the DSA. More specifically, Meta has already established an Ad Library where all advertisements targeting people in the EU are centralised and free to access by anyone (Facebook Ad Library). At the same time, Meta has developed two additional tools for researchers: the Meta Content Library and API. These tools include publicly available content from Pages, Posts, Groups, and Events on Facebook, as well as content made publicly available on Instagram. In this way, researchers can access the tools and therefore search and examine publicly available content through a graphical User Interface (UI) or a programmatic API. On the other hand, new players may not have the necessary assets to comply with their obligations and may be hesitant to enter the market. For instance, in the United States, after the attempted 2018 FOSTA-SESTA Law, which aimed to amend the intermediary liability framework under Section 230, investment in social media business models declined (Masnick, 2023). Therefore, the additional obligations might create a monopolistic market composed of Big Tech players that excludes SMEs.

What is more, it seems that the additional obligations imposed on very large online platforms might prove tricky to comply with. In particular, very large online platforms might be struggling to implement measures in order to comply with their obligations. This understanding is exemplified by the number of procedural investigations initiated by the European Commission. Consider, for instance, that the Commission has already opened formal proceedings to assess whether TikTok and X may have breached the provisions of the Digital Services Act concerning the protection of minors, advertising transparency, data access for researchers, dark patterns, as well as the risk management of addictive design and harmful content (European Commission, 2023).

Fourthly, online platforms may be unsure how to incorporate the DSA's legal obligations into their policies and practices, and how to comply with them. This understanding has been exemplified in the Threads app developed by Meta. The app is a Twitter competitor and attracted over 100 million users across 100 countries within one week of its launch. However, Meta announced that users from EU member states cannot yet access the app due to 'regulatory uncertainty' stemming from the DSA's provisions (Kelly, 2023).

Finally, the new legal framework under the DSA might have a global effect. This could be achieved either through the digital platforms or the EU policymakers themselves. As for online platforms, tech companies are modifying their global policy practices to comply with new legal obligations. Indeed, Bradford (2019) argues that online platforms align their global practices with Brussels' legal mandates to enhance compliance efficiency (p. 232). On the other hand, EU policymakers can export parts of the DSA in other jurisdictions through free trade agreements (Chander, 2023, p. 5). This understanding has been exemplified in the General Data Protection Regulation, which came into force in 2018. The GDPR has been imitated in various jurisdictions, including Brazil, India, and Japan, as well as in US states such as California, thereby placing EU policymaking in the role of a global leader in regulating digital markets (FEPS, 2022). In the context of DSA, this might have negative implications for other legal systems. This is because problematic provisions of the DSA might also be exported to foreign jurisdictions, thereby triggering similar legal uncertainties and risks for global digital innovation.

Overall, one might conclude that the procedural obligations imposed on online platforms, particularly very large ones, may have a detrimental effect on innovation at the European level. Online platforms may struggle to comply with these obligations, while new players may be hesitant to enter the market. Furthermore, the legal provisions of the DSA may alter the business models of online platforms, particularly very large ones, transforming them from online spaces of free speech into profit-driven, capitalist infrastructures. In this context, the following section presents a set of novel recommendations to provide a balanced approach to regulating digital markets.

Towards a Sectoral-Based Legal Framework?

Regulatory Framework

The sector-based approach might offer an alternative to regulating digital platforms for trademark infringement and reduce innovation-related risks to some extent. This is because vertical legislation might offer flexibility in the law. For instance, the proposal for an AI Liability Directive envisaged a new liability regime to provide remedies to users who claim

damages from AI-enabled products and services. Indeed, with reference to sector-specific legislation, Kerber (2020) rightfully pointed out that,

> The most important advantage might be that with rules that are tailored to the specific economic and technological conditions of a sector, a much better balancing of the many trade-offs with regard to an optimal governance of data is possible. (p. 5)

This means that sectoral legislation can be adjusted to meet the industry's needs.

In light of that, a sectoral approach would enable policymakers to better decide which requirements need to be fulfilled and how they could be implemented in the specific sector. This is because a sector-specific approach often comes with ex-ante requirements that would enhance the efficiency of the legislation. Consider, for instance, the Copyright in the Digital Single Market Directive (DSMD). The European Commission noted that, under Article 17 of the DSMD, which regulates the liability of online content-sharing service providers, they may, where proportionate, possible, and practicable, conduct a rapid ex-ante human review of uploads that contain earmarked content identified by an automated content recognition tool. This understanding provides an ex-ante safeguard of users' fundamental rights, as an ex-ante human review can assess whether the video is lawful or unlawful. Otherwise, any removal of lawful content might jeopardise freedom of speech online.

Moreover, sector-specific legislation may offer greater legal certainty to the parties involved. This is because the legislation will be more specific on the conditions, adoption of measures, enforcement, and oversight of the legal rules. The need for legal certainty has been outlined by Intergovernmental bodies and European Institutions. Consider, for instance, the European Commission's Impact Assessment report highlights the Council of Europe, which points out a number of recommendations for Member States with the need for aim of establishing legislation between cyberspace entities and public authorities that has "… a legislative clear legal basis and respects privacy regulations" (Committee of Ministers, 2007). This is warranted because the internet and all relevant digital technologies have high public service value and must promote the respect of human rights and other fundamental rights within the online environment. At the same time, the policymakers in the EU Cyber Forum declare that "legal certainty is key for a better international cooperation against cybercrime" (Council of Europe, 2020) while the Public Consultation on the evaluation and modernisation of the legal framework around the trustworthy use of

AI and states that such a framework aims to "ensuring legal certainty to facilitate investment and innovation in AI" (European Commission, 2021). The majority of respondents supported the introduction of specific requirements that would prevent the dissemination of unlawful content, along with a uniform level of enforcement of intellectual property rights at the European level. Such requirements could promote legal certainty among rights holders.

However, one might argue that a horizontal legislative framework would also enhance legal certainty. This could be achieved through standardisation and the application of future-proofed legal rules. In particular, with standardisation, uniform criteria will be developed and adopted across sectors. As Ranchordas and van t' Schip (2019) pointed out, "The proponents of future-proofing would then argue that a forward-looking approach to legislation can favour legal certainty as it allows the legislator to avoid scenarios of deeply ineffective and obsolete laws" (p. 21).

Yet, while this argument has its own merit, it should be noted that a horizontal framework may be broad enough to ensure applicability across sectors and accommodate adjustments driven by technological advancements. In this light, sector-specific legislation may offer greater legal certainty to the parties involved.

Having reflected on the regulatory considerations for developing sector-specific legislation on the liability of online platforms for trademark infringement, the narrative turns to the characteristics and conditions that could assist in developing the suggested legal rules.

Policy Suggestions

A legislative framework governing the liability of online platforms in the trademark context is not a novelty. Indeed, in the context of Intellectual Property Law, a sector-specific legislation is envisaged in the Copyright in the Digital Single Market Directive. The aim of the Directive is to provide appropriate remuneration for rights holders when their works are used and, therefore, close the value gap between rights holders and online platforms. In this light, Article 18 addresses appropriate and proportionate remuneration, Article 15 protects press publications in online use, and Article 17 addresses the use of protected content by online content-sharing service providers. What is more, the European Parliament's (2020) report for the European added value assessment of the Digital Services Act states that, in the online platform ecosystem, specific regulation is necessary to guarantee fair competition in the digital age (EU Parliament, 2020). In this way, asymmetries generated by market power would be reduced (Lomba & Evas, 2020, p. 29).

In terms of duties, online platforms should be held to a duty of care regarding the goods displayed on their services. This understanding is already exemplified in the relevant provisions of the DSA. More specifically, Article 30 introduces the know-your-customer requirement; as a result, providers of online platforms must obtain the contact details and verify the valid status of traders, while Article 32 requires providers of online platforms to inform consumers who have purchased an illegal product that the product or service is illegal, the identity of the trader, and any relevant means of redress.

Furthermore, several online platforms have already implemented measures to safeguard the circulation of lawful products within their networks. Amazon has introduced a Brand Registry scheme, which enables brand owners to register their trademarks. In this way, the Brand Registry comprises listings of products that use trademarks in their title but are not correlated with the brand the trademark represents, as well as images that include a logo that belongs to products that are not relevant to the brand; therefore, any unlawful use of a brand can be detected. In addition, several luxury brands have developed collaborations to protect their trademarks. A telling example is the Aura Blockchain consortium, which launched the Aura SaaS, a privately based blockchain platform initiated by LVMH, the Prada Group, and the Cartier Group (Aura Luxury Blockchain). The platform enables brands to register their products on the blockchain and issue digital certificates of ownership and authenticity.

The duty to develop a brand registry tool should be assigned to online platforms, taking into account their size and growth. Attributing responsibility to host ISPs based on their size is not a novel concept at the European level. Consider, for instance, Article 17(6) of the Copyright in the Digital Single Market Directive, which states that online content sharing service providers that have been in operation for less than three years and have an annual turnover below €10 million must demonstrate that they made their best efforts to obtain authorisation for the use of the works. Along similar lines, the compromised text from the EU Parliament excludes host ISPs with an annual turnover of less than €10M and fewer than 50 employees from the adoption of a filtering mechanism (Reda, 2019).

The suggested legislative framework would benefit from robust enforcement of rights. Indeed, Turillazzi et al. (2023) argue that the enforcement of the DSA is crucial (p. 83). This understanding is supported by the European Data Protection Supervisor (EDPS). More specifically, the EDPS Opinion notes that "any form of content moderation should take place in accordance with the rule of law" and stresses the need for the successful implementation of the DSA (EDPS, 2021). In addition, the importance of enforcing legal rules has already been illustrated in the context of data protection. A

report reveals that the Data Protection Authorities are not well equipped with technical resources or staff and states that, "The Committee fears that citizens' fundamental rights are in peril" (Committee of Justice, 2021). A telling example is the Irish Data Protection Authority, which has failed to resolve 98 % of 164 significant data protection complaints about privacy abuse, thus failing to comply with EU privacy laws and safeguard users' privacy rights (Matrix Security Watchdog, 2021).

Finally, the suggested legal rules should clarify the intersection with the legal rules enshrined in the Copyright in the Digital Single Market Directive. This is because there are online marketplaces that offer tangible and non-tangible goods. Tangible goods are understood as anything tangible, while intangible goods include eBooks, audio files, and online seminars, which can be viewed on YouTube. If a rights holder brings a lawsuit against the online marketplace for copyright or trademark infringement, one might wonder which principles should apply and under what conditions. Consider, for instance, following the *L'Oreal v Ebay* case, to attribute liability to the online marketplace, the Court shall examine whether the online marketplace is "aware of facts or circumstances on the basis of which a diligent economic operator should have identified the illegality in question and acted in accordance with Article 14(1)(b) of Directive 2000/31." Whether the principle of a diligent economic operator applies in cases where an online marketplace offers copyrighted content should be clarified.

Conclusion

This article has hitherto critically engaged with the new regulatory framework for online platforms, particularly very large ones. In particular, the new framework envisages a shift from private ordering to the institutionalisation of the role of online platforms, providing different categories of online platforms and ascribing to them new obligations, depending on their size, similar to those deployed by financial institutions.

The ascription of obligations for online platforms varies from content moderation to transparency reports, while very large online platforms are subject to a set of crisis management measures and operate under the supervision of the Digital Services Coordinators. Crucially, the attribution of obligations might have implications for innovation at the European level. This is because the provisions of the Digital Services Act presuppose that all online platforms' business models, including those of very large online platforms, operate similarly to those of the Big Tech Players. At the same time, a monopolistic market might be created, as very large online platforms already have the resources and know-how to develop measures to mitigate risks posed by the circulation of counterfeit goods online. Moreover, crafting a legal framework similar to that

of financial institutions might undermine the very nature of online platforms and the primary rationale underpinning their business models. Finally, online platforms may be uncertain about the application of the new rules; they may even struggle to implement measures in order to comply with their obligations. Finally, the new legal framework under the Digital Services Act may have a global impact and be transposed into other jurisdictions. A lack of clear legal rules may have a detrimental effect on the regulatory frameworks of online platforms worldwide.

In that vein, a set of sector-based considerations has been put forward. More specifically, this article argues that sector-specific legislation might offer an alternative to regulating digital platforms for trademark infringement and reduce innovation-related risks to a greater extent. This is because vertical legislation might offer flexibility in the law and enhance legal certainty for the parties involved. For instance, this could be achieved by imposing a duty of care on online platforms that display goods, taking into account the size and growth rate of these platforms. At the same time, the enforcement of legal rules across EU member states should also be of paramount importance. Otherwise, the lack of correct implementation of the rules might jeopardise innovation within the Digital Single Market.

References

Amazon. (2024). *Amazon Brand Registry: Protect and Build Your Brand in the UK*. https://sell.amazon.co.uk/brand-registry#:~:text=Find%20out%20more,adopter%20of%20Amazon%20Brand%20Registry

BEUC. (2021). *The Digital Services Act Proposal: BEUC position paper*. https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-032_the_digital_services_act_proposal.pdf

Bloomberg. (2018). *Google Payment expands with E-money license from Lithuania*. https://www.bloomberg.com/news/articles/2018-12-21/google-payment-expands-with-e-money-license-from-lithuania

Bradford, A. (2019). *The Brussels Effect: How the European Union Rules the World*. Oxford University Press. https://doi.org/10.1093/oso/9780190088583.001.0001

Ceci, L. (2024, January 23). YouTube Shorts: Daily views worldwide as of October 2023. Statista. https://www.statista.com/statistics/1364763/youtube-shorts-total-daily-views/

Chander, A. (2023). When the Digital Services Act Goes Global. *Berkeley Technology Law Review*, *38*(3), 1067–1088. https://scholarship.law.georgetown.edu/facpub/2548/

Committee of Justice. (2021). *Report on meeting on 27th April 2021 on the topic of GDPR*. https://data.oireachtas.ie/ie/oireachtas/committee/dail/33/joint_com-

mittee_on_justice/reports/2021/2021-07-22_report-on-meeting-on-27th-april-2021-on-the-topic-of-gdpr_en.pdf

Committee of Ministers. (2007). *Recommendation CM/Rec(2007)16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet*. COE.

Council of Europe. (2020, September 16). *EU cyber forum: Legal certainty is key for a better international cooperation against cybercrime*. https://www.coe.int/en/web/cybercrime/glacyplusactivities/-/asset_publisher/DD9qKA5QlKhC/content/eu-cyber-forum-legal-certainty-is-key-for-a-better-international-cooperation-against-cybercrime

Efroni, Z. (2021, Nov 16). The Digital Services Act: risk-based regulation of online platforms. *Internet Policy Review*. https://policyreview.info/articles/news/digital-services-act-risk-based-regulation-online-platforms/1606

EUIPO. (2021). *Online advertising on IPR-Infringing Websites and Apps*. https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2022_Online_advertising_IPR_Infringing_Websites_and_Apps_2021/2022_Online_advertising_IPR_Infringing_Websites_and_Apps_2021_FullR_en.pdf

European Commission. (2021). *Impact Assessment report: Accompanying the Proposal for a Regulation of the European Parliament and of the Council, 1*.

European Commission. (2022). *Digital Services Act: Commission welcomes political agreement on rules ensuring a safe and accountable online environment*.

European Commission. (2023). *Commission opens formal proceedings against TikTok under the Digital Services Act*. https://digital-strategy.ec.europa.eu/en/news/commission-opens-formal-proceedings-against-tiktok-under-digital-services-act

European Data Protection Supervisor (EDPS). (2021). *Opinion 1/2021 on the Proposal for a Digital Services Act.* https://www.edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_services_act_en.pdf

European Parliament. (2020). *Digital services act: European added value assessment*. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/654180/EPRS_STU(2020)654180_EN.pdf

Eurostat. (2022). *Impact of COVID-19 on e-sales of enterprises.* Statistics Explained. https://ec.europa.eu/eurostat/statistics-explained/SEPDF/cache/105640.pdf

FATF. (2014). *Guidance for a risk- based approach: The Banking sector*.

FEPS. (2022). Beyond the Brussels effect. *Policy Brief*, 4.

Geese, A. (2023). Why the DSA Could Save Us From the Rise of Authoritarian Regimes. In J. van Hoboken, J. P. Quintais, N. Appelman, R. Fahy, I. Buri, & M. Straub (Eds.), *Putting the DSA into Practice on matters constitutional Enforcement, access to Justice and global implications* (pp. 63–75). Verfassungsbooks.

Genç-Gelgeç, B. (2022). Regulating Digital Platforms: Will the DSA Correct Its Predecessor's Deficiencies? *CYELP*, *18*, 25. https://doi.org/10.3935/cyelp.18.2022.485

Jeong, U., Nirmal, A., Jha, K., Tang, S. X., Bernard, H. R., & Liu, H. (2023). *User migration across multiple social media platforms*. arXiv. https://doi.org/10.48550/arXiv.2309.12613

Keller, D. (2022, November 7). *The EU's new Digital Services Act and the rest of the world*. Verfassungsblog. https://verfassungsblog.de/dsa-rest-of-world/

Kelly, M. (2023). *Here's why Threads is delayed in Europe*. https://www.theverge.com/23789754/threads-meta-twitter-eu-dma-digital-markets

Kerber, W. (2020). From (Horizontal and Sectoral) Data Access Solutions Towards Data Governance Systems. In *Data Access, Consumer Interests and Public Welfare* (pp. 439–476). http://doi.org/10.5771/9783748924999-439

Krokida, Z. (2022). *Internet service provider liability for copyright and trade mark infringements: Towards an EU Co-regulatory framework.* Hart Publishing. https://doi.org/10.5040/9781509948550

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

Masnick, M. (2023). The Unintended Consequences of Internet Regulation. *Copia*. https://copia.is/news/the-unintended-consequences-of-internet-regulation/

Matrix Security Watchdog. (2021). *Irish data regulator fails to resolve 98% of big tech GDPR cases*. https://www.securitywatchdog.org.uk/latest-news/irish-data-regulator-fails-to-resolve-98-of-big-tech-gdpr-cases/

Ranchordas, S., & van 't Schip, M. (2019). Future-Proofing Legislation for the Digital Age. In S. Ranchordas & Y. Roznai (Eds), *Time, Law, and Change* (pp. 7–28). Hart Publishing. https://doi.org/10.2139/ssrn.3466161

Reda, J. (2019). Article 13 is back on – and it got worse, not better. *Felix Reda.* https://juliareda.eu/2019/02/article-13-worse

Statista Research Department. (2024, February 14). *Amazon UK services: Turnover* (in million GBP). Statista. https://www.statista.com/statistics/1050066/amazon-uk-services-turnover/

Tourkochoriti, I. (2023). The Digital Services Act and the EU as the Global Regulator of the Internet. *Chicago Journal of International Law*, *24*, 129.

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

Tushnet, R. (2023). Three sizes fit home: why content regulation needs test suites. *Berkeley Technology Law Journal*, *38*, 921. https://btlj.org/wp-content/uploads/2024/01/0003_38-3_Tushnet.pdf

Ullrich, C. (2017). Standards for Duty of Care? Debating Intermediary Liability from a Sectoral Perspective. *JIPITEC*, *8*, 111. https://www.jipitec.eu/jipitec/article/view/197

World Bank Group. (2019). *Credit scoring approaches guidelines*.