Daria Bulgakova

Visiting Scholar, Researcher

Uppsala University, Sweden

Sintija Deruma

Director of MBA on Cybersecurity management

BA School of Business and Finance, Latvia

THE LIABILITY OF ONLINE INTERMEDIARIES UNDER EUROPEAN UNION LAW

Abstract

This research explores the complex and multifaceted issue of online intermediary liability. It illuminates the challenges arising from the absence of uniform regulations and the need for a collaborative system between online intermediaries and rightsholders. Specifically, the article scrutinizes the liability of online intermediaries under European Union law for violations of legal interests in online content. It strives to balance intermediary liability frameworks and fair competition, drawing attention to the relationship between specific provisions and the concurrent regime outlined in the e-Commerce Directive. Moreover, the article evaluates the consistency of liability frameworks for online intermediaries and their compliance with market functioning rules under the Trade Secrets and the Unfair Commercial Practices Directives. Furthermore, the article consults the consequences of the EU Directive on Copyright in the Digital Single Market, which holds online user-generated content platforms directly responsible for infringing content. And, unlike the original draft, the final version of this directive does not impose general monitoring obligations. Nevertheless, online intermediaries may need to implement filtering measures to avoid liability for unauthorized communication of copyright-protected works to the public. The writing also considers the impact of a prior legal framework, and the Digital Service Act established to address the issue of online intermediaries being held liable for any illegal information disseminated through their platforms. The research underscores the innovative features of the Digital Services Act, acknowledging the challenges

of creating a practical legal framework striving to avoid conflicts with relevant laws. Therefore, this paper sheds light on the complex nature of online intermediary liability to the EU approach accordingly.

Key Words

Internet Service Providers, Illicit Content, Injunctions, Safe Harbour, Online Platforms

Research Issue

The spread of counterfeit goods on media and web platforms has become a significant concern for intellectual property lawyers and intermediaries about the balancing of legitimate interests such as competition with the need to address the proliferation of fake goods. The growing influence of online intermediaries (OIs) and the changing business models they operate under - have significant implications for the type of information they convey. This is because OIs allow users to upload content that can result in a wide range of infringements of third- party rights. The combat of illegal content online requires a holistic approach, as such content often migrates easily from one hosting service provider to another and tends to exploit the weakest links in the chain.[1] Therefore, the legal landscape around the liability of online intermediaries (LOIs) for spreading counterfeit content is rapidly changing, and a close examination of the various legal options and their costs are on the table.

It is crucial to recognize that LOIs have far-reaching legal implications, including increased accountability for OIs about copyright infringement. The sparked concern is about whether OIs should be held directly liable for such breaches rather than being subject to secondary liability. In contrast, trade secrets do not provide an exclusive intellectual property right, but they can extend indefinitely provided they are not involuntarily disclosed.[2] The EU Directive on Copyright[3] at first sight is with the intent of the Commission to codify the case law, at the same time, as the references to the active role of internet service providers (ISPs) and to the adoption of technologies for content recognition could suggest, however, the Commission seems to go beyond the mere codification of the European case law, as the notion

[1] Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online, C/2018/1177, *OJ L 63,* Recital 30, 6 March 2018.

[2] Niebel, R., de Martinis, L., & Clark, B. (2018). The EU Trade Secrets Directive: all change for trade secret protection in Europe? *Journal of Intellectual Property Law & Practice*, *13*(6) p. 447.

[3] Directive 2019/790/EU of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, OJ L130/92, 2019.

of the new ISPs' liability regime demonstrates.[4] In particular, it seems that the Commission intervenes in this way on the regulatory framework so to better protect right holders from the new challenges posed by digital technologies.[5] Likewise, there are two primary types of content recognition technologies: fingerprinting and watermarking.[6] Fingerprinting involves extracting easily recognizable features from certain types of content and using them to create a unique identification. These features are then compared to a reference database for identification purposes.[7] On the other hand, watermarking takes the opposite approach.[8] It involves embedding a unique digital watermark in the content, essentially 'tattooing' it in an invisible way. This watermarking operation makes each copy of the content unique, allowing for identification and tracking. Thus, while fingerprinting and watermarking both serve the purpose of content recognition, they use different approaches to achieve this goal. Fingerprinting extracts recognizable features from the content, while watermarking embeds a unique identifier into each copy. Watermarking technology, for example, would not necessarily qualify as searching material for specific purposes, as it looks for 'watermarks' and would result in the monitoring of all kinds of content, not just infringing content.[9] Furthermore, the e-Commerce Directive[10] offers liability limitations for specific activities or functions rather than for certain types of intermediaries or operators. These activities include transmitting data at a third party's request or providing access to a network, as well as caching high-demand material on a local server. Caching involves storing data on a temporary or longer-term basis, and it can help reduce the burden on the Internet infrastructure. However, it is important to remark that the liability limitations only apply to activities where the information is supplied by the end user and transmitted or stored at the request of end users. The Directive does not exempt on-line intermediaries from liability if they engage in activities such as selecting, modifying, or creating material themselves. Additionally, it is crucial to determinate that the liability limitations only apply to on-line intermediary activities and not to other on-line activities that

[4] Colangelo, G., & Maggiolino, M. (2018). ISPs' copyright liability in the EU digital single market strategy. *International Journal of Law and Information Technology*, *26*(2) p. 150.

[5] Ibid.

[6] Commission Impact Assessment on the Modernization of Copyright, SWD (2016) 301 final, part 3/3, Annex 12 A, pp. 164-165.

[7] For example, fingerprinting technology can identify a certain melody and match it to one in the database. YouTube's Content ID uses fingerprinting technology for this purpose.

[8] Watermarking is typically used in theatrical movie releases, as it enables the tracking of any illegal copies back to the original.

[9] Huhta, E. (2019). *Copyrights, Online Intermediaries and the EU: SaveYourInternet? : PlatformLiability in Light of Article 17 of the Directive of Copyright in Digital Single Market*. Uppsala universitet, Juridiska institutionen, p. 48.

[10] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, particularly electronic commerce, in the Internal Market ('Directive on electronic commerce'), *OJ L 178*, 2000.

may be considered 'intermediary activities'[11] but do not fall under the Directive's scope. For instance, if an on-line travel agency is sued for copyright infringement due to illegal copyright material posted on their website, it should be considered a content provider and subject to existing copyright liability laws.[12] Thus, the Directive's liability limitations apply to specific on-line intermediary activities but not to all on-line activities, and only if certain conditions are met, such as the end user providing the information and the intermediary simply transmitting or storing it. Nonetheless, trade secret protection is varying considerably from jurisdiction to jurisdiction, protecting know-how and industrial secrets and comprehensively infringement can be challenging for multinational companies.[13] Under the Trade Secrets Directive[14] remedies are available for third-party use of infringing goods. These goods are defined as products that significantly benefit from unlawfully acquired, used, or disclosed trade secrets, including their design, characteristics, functioning, production process, or marketing (as per Article 2(4)). This provision allows trade secret owners to prevent competitors from launching products that would infringe on their intellectual property, thereby safeguarding the competitive advantage they have gained from their innovative efforts. As a result, OIs are becoming involved in managing the information shared by third parties.[15]

The legal status of OIs in relation to liability for their users' commercial activities is nuanced issue. On the one hand, if OIs are classified as a trader, they may be subject to due diligence obligations under both the e-Commerce Directive and the Unfair Commercial Practices Directive (UCPs Directive),[16] potentially making them liable for the actions of their users. At the same time, the e- Commerce Directive may grant them immunity from liability, even for UCPs, creating tension between the two provisions of EU law. Thus, the balance between the interests of traders and intermediaries is a key consideration when assessing UCPs, and users' specific context of conduct should be taken into account. On the other hand, the question of whether OIs can rely on a claimant's notification to achieve immunity under the host for UCPs remains uncertain. This is because national courts' decisions can vary, resulting the negative impacts on those OIs operating in the EU's digital market. It needs to be

11 Julia-Barcelo, R. (2001). Liability for on-line intermediaries: comparing EU and US legal frameworks. In *E-commerce law and practice in Europe*. Woodhead Publishing Limited, Section 4: Intermediaries, p. 6.

12 *Ibid*.

13 *Ibid.*

14 Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use, and disclosure, *OJ L 157*, 2016.

15 Moscon, V. (2020). Free Circulation of Information and Online Intermediaries – Replacing One "Value Gap" with Another. *IIC - International Review of Intellectual Property and Competition Law*, *51*(8) p. 980.

16 Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC)

clarified how and when OIs should prevent future infringements after receiving a notification or court order. In the view of the research, these issues must be resolved uniformly. Hence, given the immense importance of online platforms and digital services, there is a need to introduce specific rules for the studied sector to improve online access to goods and services for consumers as well as to prohibit the dissemination of illegal content and products, and to facilitate innovation, competition and growth of the European digital ecosystem.[17] Respectfully, the novel Digital Services Act (DSA)[18] adopts a horizontal approach that complements existing EU legislative instruments and aiming to update the rules regarding the platforms of digital services through the revision of the legal regime formerly established by the e-Commerce Directive. For instance, the liability exemptions as contained in the e-Commerce Directive received comprehensive support from the stakeholders; but it cannot be denied that this exemption has also been subject to criticism, for example, in the event of online marketplaces consumers often rely on the brand image of the platform and even consider the platform as their contracting party rather than the party who uses the platform to commercialize its goods and services.[19] The DSA addresses this issue in Article 5(3) by stating that the exemption does not apply in cases where online platforms are held liable under consumer protection law for allowing consumers to enter into distance contracts with traders. This is because the online platform presents information or facilitates a transaction in a manner that would cause a reasonable and well- informed consumer believes that the platform itself or a service recipient acting under its control or authority. In the study's view, when the intermediary's actions are driven by profits and the harmed party is an individual, it seems reasonable to impose a liability regime where the intermediary is liable for the harm caused and can then seek redress against the infringer. This is particularly necessary as the intermediary is usually better equipped to bear litigation costs.[20]

Research Purpose

Hence, the research conveys key elements of intermediary liability that emerge, and recognition of these common will be crucial in developing consistent legal standards for LOIs. Thus, the study aims to determine whether European Union (EU) law adopts a consistent app-

2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), *OJ L 149*, 2005.

17 Chiarella, M. (2023). Digital markets act (dma) and digital services act (dsa): new rules for the eu digital environment. Athens Journal of Law (AJL), 9(1), 34; *See* Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe, 6 May 2015, COM (2015) 192 final.

18 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, *OJ L 277*, 2022.

19 Cauffman, C., & Goanta, C. (2021). A New Order: The Digital Services Act and Consumer Protection. *European Journal of Risk Regulation*, *12*(4) p. 766.

20 *Ibid,* p. 767.

roach to regulate content hosted by OIs and if liability safeguards the interests in the market in various scenarios. For example, in order to ensure transparency and fairness and to avoid the unintended removal of content (which is not illegal content), content providers should, as a matter of principle, be informed of the decision to remove or disable access to the content stored at their request and be given the possibility to contest the decision through a counter-notice, with a view to having that decision reversed where appropriate, regardless of whether that decision was taken on the basis of a notice or a referral or pursuant to proactive measures by the hosting service provider.[21]

Methods

To diagnose the underlying issue and work towards improvement, the research based on the 'black-letter law' method discerning European Union law and legal phenomena of online intermediaries' liability through analyzes, interpretation, and rationale juxtaposition of the e-Commerce Directive, Directive on Copyright in the Digital Single Market, Unfair Commercial Practices Directive, Enforcement Directive, Trade Secrets Directive, and Digital Services Act. The research believes to this extent, practical measures to address the online spread of counterfeit goods can only be implemented by developing uniform regulation.[22]

Analysis of Research Findings

The concept of LOI refers to the intermediaries, such as online platforms or ISPs, for the potential infringements committed by their users. Establishing standardized principles of LOIs is essential for effective cross-border enforcement in the online realm. In general, the liability for intermediaries can be categorized into direct infringement, accessory (secondary) liability, and intermediary liability: (a) direct or forthright infringement liability by the intermediary, (b) accessory liability or assisting another person in infringing, and (c) the intermediary liability of a subject to an injunction but not damages.[23] Direct infringement involves committing the infringing act and can result in an injunction and the payment of damages. Secondary liability, which is not among other things, directly applicable in the EU, involves assisting another person in committing the infringing act, resulting in injunction and damages. Intermediary liability only exposes to an injunction, not damages, and does not require the intermediary to be either a primary infringer or an accessory.

Under the study, the research formulates shared similarities in terms of intermediary and accessory liability because of a need for a mental element, or other words, knowledge. In

21 *Ibid,* at Recital 20

22 The best approach would be to develop further a law based on coordinated voluntary digital measures.

23 Mostert, F. (2020). Intermediary Liability and Online Trade Mark Infringement: Emerging International Common Approaches. In *Oxford Handbook of Online Intermediary Liability*. Oxford University Press, pp. 370–71.

this respect, several fundamental elements can be identified. Firstly, intermediaries are generally not held accountable for accessory liability if they were unaware of the infringing activity, except in cases of willful blindness. Secondly, intermediaries who do not promptly respond to notifications of infringing activity may lose their safe harbour protection,[24] which shields them from damages claims. The first opinion is based on the subsequent arguments: 1) Intermediaries are not held accountable for infringements if they were unaware of them but may face liability if they deliberately ignore it; 2) Intermediaries that do not take action after becoming aware of an infringement may lose their exemption from liability. To outline, OIs are only considered accessory liable for not taking necessary reasonable measures when offering their services online. This is because direct liability is typically unavailable, mainly when intermediaries use trademarks in their online advertising; 3) The most recent addition to LOIs is the jurisdiction to award injunctions against intermediaries to block internet access to prevent online copyright infringements.[25] Injunctions against intermediaries are becoming increasingly prevalent, requiring them to assist rightsholders in preventing and stopping further infringements. Injunctive relief is a remedy tool for combating illicit content shared through OIs services, as provisions of the e-Commerce Directive do not restrict the use of such measures. The notion of blocking injunctions Injunctions against intermediaries are becoming increasingly prevalent, requiring them to assist rightsholders in preventing and stopping further infringements. Injunctive relief is a remedy tool for combating illicit content shared through OIs services, as provisions of the e-Commerce Directive do not restrict the use of such measures. The notion of blocking injunctions against intermediaries, who are not directly involved in infringing activity but must assist in preventing it, is gaining widespread recognition.[26] Website-blocking orders come with certain requirements, such as the compasses of proportionality and necessity, and do not typically necessitate comprehensive monitoring by intermediaries. However, despite the general monitoring prohibition imposed by Article 15 of the e-Commerce Directive, intermediaries are required to comply with injunctions under Article 11 of the Enforcement Directive.[27] This provides a solid foundation

[24] *Supra* note 17.

[25] Lindsay, D. (2017). Website blocking injunctions to prevent copyright infringements: proportionality and effectiveness. University of New South Wales Law Journal, 40 (4) p. 1507.

[26] *See* CJEU, Case C-314/12, *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH*, ECLI:EU:C:2014:192, 27 March 2014. In this case, the CJEU recognized its approach towards injunctions requiring ISPs to block websites offering illegal information. Such an injunction is necessary to defend the copyright, which is a fundamental right deserving of the maximum protection possible. However, the Court acknowledged that no technique could completely stop infringements, and measures adopted by ISPs may not wholly halt ascertained violations. As such, the measures must be sufficiently compelling to genuinely protect copyright, either by preventing unauthorized access or making it difficult to achieve and seriously discouraging Internet users from accessing protected subject matter. Moreover, the contributory infringement of the ISP justifies the injunction, allowing them to avoid liability without bearing an unreasonable sacrifice.

[27] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, *OJ L195/16*, 2004.

for enforcement in the online environment where counterfeiting is prevalent. As a result, intermediaries are expected to take all necessary and appropriate steps to address infringement once notified.

The injunctions not only demand the removal of illicit content but also impose stay-down obligations, requiring intermediaries to prevent future uploads of similar content. The question of whether an obligation to search for infringing content online is compatible with Article 15 of the E-Commerce Directive depends on the interpretation of the concept of general monitoring, which is not clearly defined in the directive itself. Injunctions against OIs explicitly prescribed by Article 11 of the Enforcement Directive and Article 8 (3) of the Information Society Directive[28] requiring Member States to provide remedies for infringing activities. However, there is tension between the mentioned articles of the Enforcement Directive, the Information Society Directive, and the e-Commerce Directive Articles 12-15 because it raises the scope of injunctions and the extent to which Member States are required to provide them.[29] As a result, the national law of a particular Member-State[30] shall determine the legal basis for liability and whether that liability is for direct or secondary infringement.

To continue with a second point of view, yet, the e-Commerce Directive established safe harbours for ISPs engaged in mere conduit, caching, and hosting activities. Article 12 states that ISPs are not responsible for transmitted information if they neither initiate the transmission, choose the recipient, nor alter the content. Again, Article 13 provides immunity for automatic, intermediate, and temporary information storage as long as ISPs cannot modify the information, comply with access and updating requirements, and promptly remove or disable access to information that has been removed from the network or disabled by a court or administrative authority. Eventually, Article 14 outlines hosting providers' liability boundaries, stating that ISPs are not responsible for illegal information stored at a recipient's request if they lack actual knowledge of illegal activity or information and are unaware of circumstances from which such activity or information could be inferred, or if they promptly remove or disable access to the illegal information upon obtaining such knowledge or awareness. Alike, the e-Commerce Directive protects OIs from liability if third parties misuse their services for illegal activities by creating exemptions covering all forms of liability, including financial compensation for harm caused, civil and criminal penalties. Thus, Arts. 12-14 of the

28 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, *OJ L 167*, 2001.

29 COM (2017)708 Guidance on certain aspects of Directive 2004/48/EC of the European Parliament and of the Council on the enforcement of intellectual property rights of 29 November 2017.

30 Despite offering limited protection, the e-Commerce Directive aims to prevent fragmentation of intermediary liability within the EU.

e-Commerce Directive[31] protect passive and neutral service providers from liability for transmitting, caching, and hosting illegal information from third parties. To be exempt from liability, the service provider must limit their role to facilitating use by others and promptly remove or disable access to unlawful content once made aware of it. Importantly, Article 15 stipulates that ISPs operating within Articles 12 to 14 have no obligation to monitor their content actively.

On the other hand, in the Scarlet ruling,[32] the Court of Justice of the European Union (CJEU) found an obligation to monitor all content in order to prevent future infringements of intellectual property rights to be incompatible with the prohibition in Article 15 of the e-Commerce Directive. Practically, the main arguments are against blocking injunctions, described earlier, as a matter of policy and before the courts, that they are ineffective in that blocks being easily circumvented and do not reduce the overall level of infringements.[33] Under the study, an injunction can be commensurate even if it simply precludes a permit by a juvenility of users, and in order to issue it against an ISP it is proposed to meet four conditions: (i) the ISP must be considered an intermediary under Article 11 of the Enforcement Directive, and the users or operators of the website must be infringing the trademark; (ii) they must be using the ISP's services to do so; (iii) the actual must-have knowledge of the infringement; (iiii) IP address blocking can be considered proportionate if the proper procedures are followed, considering factors such as the importance of the rights involved, the availability of alternative measures, the efficacy of the blocking measures, and their impact on lawful internet users.[34]

Moreover, it is yet to be seen how the EU Directive on Copyright Article 17 influences the legal conditions outlined above. It familiarizes strict primary copyright infringement liability for online user-generated content platforms, which has significant consequences for platforms when the importance of specific knowledge of infringing content may change. This direct liability of platforms for infringing content places a heavy burden on them. It means the impor-

31 *See* Stalla-Bourdillon, S. (2017). Internet Intermediaries as Responsible Actors? Why It Is Time to Rethink the E-Commerce Directive as Well. In T*addeo, M., Floridi, L. (eds) The Responsibilities of Online Service Providers. Law, Governance and Technology Series, vol 31.* Springer, Cham, pp. 275- 293.

32 CJEU, Case C-70/10, *Scarlet Extended SA v SABAM*, ECLI:EU:C:2011:771, para 40, 24 November 2011.

33 *Supra* note 25, p. 1533.

34 Sir Richard David Arnold, styled the Rt Hon Lord Justice Arnold in the UK, has made significant contributions to the development of LOIs approach, mainly through orders that require ISPs to block access to infringing websites. He has successfully accommodated the diverse interests of intermediaries, internet users, and rightsholders by allowing adjustments to block requests and considering the potential impacts of IP address blocking on non-infringing users. In finding, the principle of reasonable measures and its flexible implementation highlights the benefits for adopting LOIs. Available from: https://www.fieldfisher.com/en/insights/it-s-another-website-blocking-injunction-but-not-as-we-know-it#:~:text=Mr%20Justice%20Arnold%20also%20considered%20seven%20principles%20proposed,rights%3B%20and%20%28vii%29%20the%20relief%20must%20be%20proportionate. [Accessed 11 February 2023]

tance of specific knowledge of infringing content may be less determinative. In contrast to EU law, the New Zealand copyright infringement system has been in place for a few years, targeting a specific issue of file-sharing. The New Zealand Copyright Tribunal manages the system, but appeals can be made to the High Court, although cases have yet to reach that level. The primary punishment is a monetary award, with the option for a court to suspend the infringer's internet account for six months. However, this provision has yet to be enforced. Unlike the copyright safe harbour mechanism, the New Zealand system includes a statutory counter- notice that allows users to respond to infringement notices. It obligates right- holders to provide evidence for the infringement claim. The system targets account holders instead of infringers, and copyright owners or agents can bring actions before the Tribunal, aiding coordination difficulties.[35] The service provider must keep records of subscribers who obtain infringement notices, but they cannot uncover their identity without a tribunal order.

Over the years ISPs executing orders have been adopting filtering systems and other tools to block access to infringers, though these measures challenge two important principles of Western legal orders: the freedom of expression and the freedom of engaging in business conduct.[36] That is why the use of these means have triggered a good amount of litigation.[37] Therefore, balancing the conflicting demands of rightsholders, ISPs, and internet users are crucial in determining what is considered reasonable. The ratio principle[38] requires ISPs to take not only reasonable but also proportionate measures to address an infringement once it has been brought to their attention. It provides clarity for ISPs in necessary actions preventing infringements by their users. In the view of the study, the ratio flexibility allows for its adaptation to the parties involved, including differences among platforms and ISPs. For example, a framework for commercial advertising networks may not be suitable for non-commercial products prioritizing free speech, and measures that work for a large ISP may not be feasible for a smaller provider with limited resources. In subsequent cases, such as Google France v Louis Vuitton[39] and L'Oreal v eBay,[40] the CJEU provided further guidance on interpre-

35 Dinwoodie, G.B. (2017). A Comparative Analysis of the Secondary Liability of Online Service Providers. In *Dinwoodie, G.B. (eds) Secondary Liability of Internet Service Providers. Ius Comparatum – Global Studies in Comparative Law, vol 25.* Springer, Cham, p. 49.

36 Colangelo, G., & Maggiolino, M. (2018). ISPs' copyright liability in the EU digital single market strategy. *International Journal of Law and Information Technology*, *26*(2) p. 145.

37 *Ibid*, pp. 142–159.

38 *See* Tuori, K. (2016). *Ratio and voluntas: the tension between reason and will in law*. Routledge.

39 ECLI:EU:C:2010:159, 23 March 2010. CJEU, Case C-236/08, *Google France v Louis Vuitton Malletier SA and others*,

40 CJEU, Case C-324/09, *L'Oreʹal SA and others v eBay International AG and others*, ECLI:EU:C:2011:474, 12 July 2011.

ting Article 14 of the e-Commerce Directive, which clarifies ISPs' liability boundaries. If an ISP's role in illegal activity by a third-party user is merely technical, automatic, and passive, the ISP is exempt from any form of liability. However, if the ISP is found to have control over the illegal information, it should be held liable for its active role.[41] For instance, an ISP that assists trademark infringers by optimizing or promoting their counterfeit products would be deemed to have played an active role.[42] Additionally, an ISP that has not played an active role could not benefit from the safe harbour under Article 14 of the e-Commerce Directive if it has been made aware of facts or circumstances that a diligent operator should have recognized as illegal conduct and failed to promptly prevent its recurrence by removing infringing materials or disabling access to users who have posted such materials online.

Regardless of the above discovered, the EU law does not address the liability of someone other than the direct infringer of the right if the right at issue is subject to EU law. In cases of primary infringement, a person is, subject to exceptions, liable when he or she performs one of the acts which are exclusively allocated to the right owner.[43] Neither knowledge nor a violation of a duty of care is required. But in cases involving intermediaries, the law must distinguish between socially acceptable activities and infringing acts.[44] Posting a hyperlink, operating a platform or a search engine are not illegal as such.[45] They can only constitute prima facie infringing communication to the public if additional factors are present.[46] And, whether the standard of secondary liability should be prescribed by EU law or left to the Member States,- a study relies upon the opinion of an Advocate General Szpunar: 'The European Commission, whose opinion appears to me to be shared by the United Kingdom of Great Britain and Northern Ireland, contends that liability for sites of this type is a matter of copyright application, which can be resolved not at the level of EU law but under the domestic legal systems of the Member States. Such an approach would, however, mean that liability, and ultimately the scope of the copyright holders' rights, would depend on the very divergent solutions adopted under the different national legal systems. That would undermine the objective of EU legislation in the relatively abundant field of copyright, which is precisely to harmonise the scope of the rights enjoyed by authors and other right holders within the single market. That is why the answer to the problems raised in the present case must, in my view,

41 C-236/08, (n 1) 114.

42 C-324/09, (n 2) 116.

43 Ohly, A. (2018). The broad concept of "communication to the public" in recent CJEU judgments and the liability of intermediaries: primary, secondary or unitary liability? *Journal of Intellectual Property Law & Practice*, *13*(8) p. 672.

44 *Ibid.*

45 *Ibid.*

46 *Ibid.*

be sought rather in EU law.[47] In fact, the European legal framework regulates only a limited number of cases of indirect liability according to the subsequent CJEU case law, ISPs are only liable once they have become aware of illegal content. They are not generally required to monitor the information they transmit or store nor actively seek out facts or circumstances that might indicate illegal activity on their platforms.

Although achieving complete legal standardization poses challenges, the advocate's perspective could be developed and as a temporary solution, there is a need in the adoption of non-binding, voluntary guidelines across EU Member- States. In the interim, online intermediaries shall strengthen the internet area of operation by implementing security measures for ISPs activity control. An adaptable service workflow system can maintain and optimize its performance by monitoring and analyzing the significant variables in Service Level Agreements (SLA) such as response time, throughput, and utilization.[48] In a workflow composition scenario, SLA management needs to identify and control potential performance violation of workflow composition.[49] A SLA is a critical component of an IT outsourcing contract, which outlines the service standards that the service provider must meet. Typically, the SLA is included as a schedule or appendix within the framework agreement.[50] This agreement, along with all its schedules and appendices, including the SLA, may be referred to as the 'IT outsourcing contract,' the 'outsourcing contract,' the 'master services contract,' or the 'services contract.[51] Using a structured framework agreement with a separate schedule for the SLA provides several benefits. Firstly, it enables the separation of legal terms for the overall deal from the specific deliverables, technical details, and timetables that relate to the services outlined in the SLA. Secondly, it allows for greater clarity and precision in the definition of the services provided and the performance standards expected. Overall, a well-structured framework agreement with a clear SLA helps to ensure that the outsourcing contract meets the expectations of both parties and facilitates a successful partnership. This means that specific service details in the SLA are not mixed up, and are separated from, legal clauses, such as limitations of liability, indemnities, intellectual property, exclusion clauses and data protection clauses, etc. so there is a clear delineation between legal terms and practical details about services.[52]

47 Opinion of Advocate General Szpunar in case C-610/15, *Stichting Brein v Ziggo BV, XS4ALL Internet BV*, ECLI:EU:C:2017:99, para. 3, 14 June 2017.

48 Yong Sun, Wenan Tan, Ler Li, Guangzhen Lu, & Anqiong Tang. (2013). SLA detective control model for workflow composition of cloud services. *Proceedings of the 2013 IEEE 17th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, p. 165.

49 *Ibid,* p. 167.

50 Desai, J. (2010). *Service level agreements a legal and practical guide* (1st edition). IT Governance Pub, p. 18.

51 *Ibid.*

52 *Ibid,* p. 19.

Main Content

1. Trade Secret Infringement Through Online Intermediaries

Trade secrets provide protection for secret business information and may protect material such as confidential backend server processes and codes.[53] Trade secrets require no formal registration, but companies must take reasonable steps to keep them secret.[54] Globally, the preservation of unbeknownst know-how and business information is covered by Article 39 of The Agreement on Trade- Related Aspects of IPRs (TRIPS Agreement).[55] However, this provision must provide clear guidelines for implementing this legal protection at the national level or address its enforceability. As a result, the protection may have differing interpretations and implementations. In 2016, the European Union took steps to harmonize the protection of trade secrets with the Trade Secrets Directive. The foremost intent of this Directive is to address the fragmentation of laws protecting trade secrets, enhance cross-border innovation, and promote cooperation in research by providing rules to facilitate the information exchange. However, the Nordic countries have encountered challenges in determining the appropriate fora for trade secret cases. In Finland, such cases often involve criminal charges against employees, leading to the preference for local district courts, especially in situations where the employer and employee are situated in remote areas.[56] Conversely, cases on unfair commercial practices have traditionally been handled by the centralized Market Court in Helsinki for companies.[57] In Sweden, the Labour Court has primarily been responsible for hearing disputes between employers and employees or former employees.[58] In Denmark, specialized courts such as the Maritime and Commercial Court have jurisdiction over cases between companies with particular emphasis on cases involving the Danish Trade Secrets Act, industrial IP rights, including copyright in works of applied art and computer programs, as well as competition law.[59]

The simplified matter is that the Directive defines a notion of trade secrets with three key elements: secrecy, commercial value, and reasonable steps to preserve secrecy. Crucially, the nature of secret information is largely a matter of fact and degree.[60] Once a piece of infor-

53 Anon (2018) Creating an effective FinTech IP strategy. *Managing Intellectual Property*.

54 *Ibid.*

55 *See* more at: https://www.wto.org/english/docs_e/legal_e/31bis_trips_01_e.htm [Assessed 12 February 2023].

56 Schovsbo, J. and Bruun, N. (2020). The implementation of the Trade Secrets Directive in the Nordic countries. In *The harmonization and protection of trade secrets in the EU: an appraisal of the EU directive* (J. Schovsbo, T. Minssen, & T. Riis, Eds.). Edward Elgar Publishing, p. 99.

57 *Ibid.*

58 *Ibid.*

59 *Ibid.*

60 Trallero Ocaña, T. (5202). *The Notion of Secrecy A Balanced Approach in the Light of the Trade Secrets Directive*, 467.

mation becomes generally known, even in the event of misappropriation, it ceases to be protected.[61] The secrecy of information depends on the interpretation of the relative secrecy notion, which in turn depends on the platform's features and the target audience and refers to information that is not generally known or readily accessible to those who typically deal with it. In cases of commercial value where an intermediary is notified of trade secret infringement, whether the information was a trade secret at the time of the notice must first be determined. If the information was already publicly circulated online before the notice, it may have lost its character as a trade secret, and the OIs may not be held liable. The assessment of the preservation steps in specific cases depends on various factors, including the features of the platform it was shared and the target audience. The nature of published content is that its use lacks authorization, regardless of whether it has been placed into some database.

In the event of the disclosure of trade secrets through OIs, the study designs a potential scenario to consider in an instance where the claimant entrusts confidential information directly to an OI for safekeeping, such as in a cloud service where there is a risk of trade secret infringement on the part of the OI. Also, difficulties arise when a service provider facilitates or allows the disclosure of trade secrets through the actions of a third party. In such cases, there may be instances where an OIs actively induce or encourage disclosure. On the other hand, there may also be situations where OIs merely provide support by receiving, storing, and making the information accessible to the public. For example, in the event of global research collaboration between entities such as private companies, universities, and research institutions, there is a risk that confidential information may be disclosed without proper consent occurring in open repositories for research results, blogs, or even social media platforms.

Another dilemma is the interplay with exceptions to the protection of trade secrets, particularly regarding intermediaries and the freedom of expression and information. The right to trade secrets under trade secrets law is an information right under information law.[62] Viewing people’s trust as an information fiduciary in the present scenario may alleviate the problems associated with proving unauthorized use, as a mere breach of the fiduciary relationship does not require harm to create liability for damages.[63] On an intuitive level, it also seems sensible to assume that peoples trust has a fiduciary relationship with those who provided their data to it.[64] For example, the measures, procedures, and remedies provided in the Directive do not apply if the trade secret acquisition, use, or disclosure was made to exert

61 *Ibid.*

62 Udsen, H. et al. (2020). Trade secrets law as part of information law. In *The harmonization and protection of trade secrets in the EU: an appraisal of the EU directive* (J. Schovsbo, T. Minssen, & T. Riis, Eds.). Edward Elgar Publishing, p. 30.

63 Malone, M. (2021). On the (Data) Breach of Confidence. Alberta Law Review, 58(4) p. 954.

64 *Ibid.*

the freedom of expression and information, and media pluralism. The applicability of this exception is determined based on balancing the interests involved, considering the trade secret holder's interest and the public's right to access and circulate information.[65] The Trade Secrets Directive, unlike information law, does not contain any specific private use limitation, which raises the question of whether private use of trade secrets is allowed. While there may be a few situations where private use or sharing of trade secrets is necessary, it is important to consider whether the absence of a specific private use rule in the Trade Secrets Directive means that it is not possible to make private use of or share trade secrets. It may be argued that the private use rules accepted across all other information law disciplines should also apply to trade secrets law. The rationales behind the private use principle in information law include:

- the limited negative effect of private use on the right holder,
- the importance of private life considerations, and
- the difficulty of enforcing rules and investigating infringements

within the private sphere.

These rationales, in the view of the research, also apply to trade secrets suggesting that private use of trade secrets should be allowed to a certain extent. For example, can an employee tell their spouse about a forthcoming product launch or a business trip that reveals their company's acquisition plans?[66] When interpreting whether private use situations are unlawful under Article 4 or covered by the exemption for freedom of information under Article 5, it is important to consider the broad and open-ended rules in the Trade Secrets Directive[67] The number of people with whom the information is shared and the noncommercial purpose of the sharing should be taken into account when determining whether private use is acceptable. While sharing trade secrets may increase the risk that competitors will eventually know the information, sharing information between a wife and husband, for example, is not damaging the company's business opportunities. Therefore, the interpretation of the Trade Secrets Directive will depend on the specific circumstances and whether private use of trade secrets is deemed appropriate.

Therefore, remedies are needed. The Trade Secrets Directive provides comprehensive harmonization measures for remedies for illicit acquisition, use, or revelation of trade enigmas. Article 4 outlines the circumstances in which a third party may be liable for trade secret infringement, such as if they knew or ought to have comprehended that the trade secret was conveyed illegally. Accordingly, the following actions can be taken against the infringer: (1) a

[65] Moscon, V., & Hilty, R. M. (2020). Digital Markets, Rules of Conduct, and Liability of Online Intermediaries—Analysis of Two Case Studies: Unfair Commercial Practices and Trade Secrets Infringement. In *Oxford Handbook of Online Intermediary Liability*. Oxford University Press, p. 437.

[66] *Supra* note 62, p. 33.

[67] Ibid.

ban on the use or disclosure of the trade secret, and (2) a prohibition on producing, distributing, or using infringing goods,[68] as well as corrective measures for these goods. Besides, Recital 26 emphasizes the need to establish prompt, efficient, and easily accessible interim measures for the immediate cessation of the illicit acquisition, usage, or dissemination of a trade secret, even in instances where it is employed to render services. In addition, Recital 27 explicitly stresses the significance of implementing conclusive measures to prevent the unlawful exploitation or disclosure of a trade secret, including where it is used for the provision of services. As per Article 12, the judiciary can impose injunctions and corrective measures. Article 14 also specifies that an infringer may be liable to compensate the trade secret holder for the damage incurred. The applicability of the concepts might pose difficulties in relation to the relation to infringing goods. This is because the requirement that the illicit service has significantly benefited from unlawfully obtained, used, or disclosed trade secrets is not particularly informative.[69] Trade secrets can take on various forms and characteristics, making it challenging to determine what qualifies as infringing goods or infringing products (including services). For example, there may be instances where confidential customer information (a trade secret) is utilized to market lawful products to specific individuals.[70] In such cases, the distinction between infringing goods and products, services may become blurred.

Additionally, the legitimate interests of third parties must be taken into account meaning that (1) the level of responsibility of a third party may be lower than that of a direct infringer, and this can impact the type of remedy awarded, and (2) the judicial authority should consider the different circumstances of third parties who are aware of the trade secret's unlawful nature from the start and those who only become aware later on.[71] This allows for a more nuanced approach to determining the appropriate remedy in each case. The Trade Secrets Directive provides general regulations for the infringement of third-party trade secrets if it is known that the trade secret was illegally acquired. At the same time, the e- Commerce Directive exempts intermediaries from liability if they do not have actual knowledge. It also lacks specific rules for OIs, such as those in the Enforcement and Information Society Directive. Remedies, including precautionary and provisional measures, can only be applied to individuals who are liable or suspected of being liable for trade secret infringement. These remedies are available for third parties only if they meet the conditions outlined in Article 4(4), which requires knowledge that the trade secret was obtained illegally. Thus, the Trade Secrets Directive holds third parties liable. Given these inconsistencies, it is still being determined whether the Trade Secrets Directive can effectively resolve the LOIs.

68 According to Trade Secrets Directive Article 2(4), infringing goods refer to 'goods whose design, characteristics, functioning, production process, or marketing significantly benefit from trade secrets that have been unlawfully acquired, used, or disclosed.'

69 *Supra* note 56, p. 95.

70 *Ibid.*

71 *Supra* note 65, p. 438.

Under the ideas described above, the legislator needs to consider the role of OIs in the digital environment and the potential overlap with the trade secret legislation. Moreover, in the case of Scarlet,[72] the CJEU established that EU legislation does not permit national authorities or courts to compel ISPs to implement filtering systems that monitor all electronic communications passing through their platforms, even in cases where these communications are conducted through peer-to-peer programs. The CJEU explained that for a filtering system to operate effectively, it would need to differentiate peer-to-peer traffic, identify illegal files, detect unlawful exchanges, and block them. This would necessitate active monitoring of all electronic communications conducted on the ISP's network, including the transmission of all information by all customers. Additionally, since filtering systems would be unlimited in time, they would apply to any future violations and be costly to implement and maintain. It is concluded [73] that such systems would impose undue burdens on ISPs, infringe on users' rights to protect their personal data, receive and impart information, and violate Article 3(1) of the Enforcement Directive, which mandates that IPR protection measures should not be unnecessarily complicated or costly.[74] As such, the Court found that filtering systems would not ensure a fair balance between IPR protection and the freedom to conduct business, transmit information, and protect personal data.[75] To highlight, the e-Commerce Directive may take precedence in cases where its conditions are met, exempting intermediaries from liability. It is still being determined whether Article 11 of the Enforcement Directive can be fully utilized in trade secret infringement cases.[76] Although the Trade Secrets Directive takes precedence in such situations, the issue of whether the Enforcement Directive can be used to address gaps in the Trade Secrets Directive still needs to be solved since the last one does not address the LOIs or provide secret trade holders with the option to seek injunctions against intermediaries who may be involved in trade secret infringement.[77]

Viewing through the lens of private international law, it is worth noting that if the safeguarding of trade secrets is considered an act of unfair competition, the applicable law would be governed by Article 6(2) (along with Article 4) of the Rome II Regulation, which stipu-

72 Case C-70/10.

73 Also, in the CJEU, Case C-360/10, *SABAM v Netlog NV*, ECLI:EU:C:2012:85, 16 February 2012, - following its ruling in Scarlet, the CJEU reiterated its position in the case of Netlog, where it was presented with a request to order a social network, acting as a hosting provider, to implement a filtering system for identifying digital copyright infringements. The court reaffirmed that the use of such a system could not achieve a fair balance between the competing interests involved in the case.

74 Case C-70/10, 36, 48.

75 Case C-70/10, 50, -where court refers to the violation of ISPs' users rights pursuant to Articles 8 and 11 of the Charter of Fundamental Rights of the European Union.

76 The use of the Enforcement Directive was discussed during the development of the Trade Secrets Directive, which ultimately led to the inclusion of Recital 39, which clarifies the specificity of the Trade Secrets Directive, stating that it takes precedence over the Enforcement Directive in cases where the two overlap.

77 An analogy could be made to apply the rules outlined in Article 11 of the Enforcement Directive.

lates that the regulation of the country where the damage occurs should be applied.[78] On the other hand, if trade secrets are deemed one of the categories of IPRs, Article 8(1) should be utilized, which specifies that the law of the country where protection is sought must be applied.[79] In line with the Commission's Proposal of July 2003,[80] industrial espionage, breach of contract, and divulgence of business secrets fall under the categories of bilateral unfair commercial practices outlined in Article 6(2) of the Rome II Regulation, which points to Article 4 of the same Regulation. As per the latter provision, the applicable law is that of the place where the damage occurred (lex loci damni) (Article 4(1)), however, if the parties share a common residence, the law of that country will apply (Article 4(2)), while Article 4(3) introduces an 'escape clause' to the preceding paragraphs and considers the law of the country that has a notably closer association with the misappropriation of confidential information.[81]

As more businesses start popping up, evolving the best partner is indispensable. This means cultivating a community and partnership strategy and how you are going to reward and engage users to keep them interested.[82] For this reason, and while the laws are chasing each other and competing with, it is proposed to follow technological progress in order to avoid trade secret infringements by establishing an independent institution to monitor them using artificial intelligence (AI) for information gathering.[83] However, the design and implementation of such an institution would require careful consideration of several factors, including the definition of monitoring criteria and the segregation of duties. To define the monitoring criteria, it is necessary to determine what activities would constitute trade secret infringements and how the AI system would identify them. This could involve developing a set of guidelines or rules that outline the types of behaviors or actions that are considered infringing and how they can be detected using AI. The guidelines could be developed in consultation with legal experts, industry representatives, and other stakeholders. Overall, designing and implementing an independent institution for monitoring trade secret infringements using AI would require careful consideration of various factors, including the definition of monitoring criteria and the segregation of duties.[84] In terms of the segregation of

78 *Supra* note 63, p. 121.

79 *Ibid.*

80 Proposal for a Regulation of the European Parliament and the Council on the law applicable to non-contractual obligations (ROME II) / COM/2003/0427 final - COD 2003/0168.

81 *Supra* note 63, p. 122.

82 *Supra* note 53.

83 *See* Ding, H. et al. (2020). State of AI-Based Monitoring in Smart Manufacturing and Introduction to Focused Section. *IEEE/ASME Transactions on Mechatronics*, *25*(5) pp. 2143–2154.

84 *See* Kobelsky, K. W. (2014) A conceptual model for segregation of duties: Integrating theory and practice for manual and IT-supported processes. *International journal of accounting information systems*, 15 (4) pp. 304–322.

duties, it would be consequential to confirm that the institution responsible for monitoring trade secret infringements is separate from any organizations or individuals involved in the creation or management of the trade secrets in question. This would minimize conflicts of interest and ensure the monitoring process is unbiased and impartial. However, with appropriate planning and oversight, such an institution could be an effective tool for protecting intellectual property and preventing trade secret theft.

2. Unfair Commercial Practice and Consumer Protection

The OIs, such as online marketplaces, social networks, rating portals, and other digital platforms, play a significant role in facilitating Unfair Commercial Practices (UCPs). The UCPs Directive sets out the rules for businesses engaged in consumer transactions and aims to prevent unfair practices that are misleading or aggressive. The Directive defines a UCP as unfair if it breaches the requirements of professional diligence and distorts the economic behavior of the average consumer. It contains a comprehensive list of actions and omissions and a general clause covering unfair practices that fall outside the definition of misleading or aggressive. Also, the general prohibition established by the Directive applies to UCPs outside of any contractual relationships between traders and consumers, bearing in mind that OIs can be considered subject to the Directive. The Directive raises the question of whether OIs can be held accountable for UCPs. However, two preliminary interpretative questions must be answered to determine the answer. The first question is whether OIs can be considered traders. If so, the second question is whether hosting third parties' activities is a commercial practice/activity.

Whether an OIs can be deemed a trader under the UCPs Directive is a matter of debate because the restrictive interpretation of the term trader has yet to be determined by the CJEU for categorization or not OIs as traders, and therefore, it is believed that the assessment is on a case-by-case basis. If an OI is not considered a trader, the UCPs Directive may indirectly affect the platform. The application of the UCPs Directive may depend on whether the OI facilitates the exchange of goods and services between consumers, such as rating portals, or supports traders' activities, for example, marketplaces. In the latter effect, the OI may be granted immunity under the e-Commerce Directive and only considered liable under certain conditions outlined in Article 14 of the e-Commerce Directive because the liability exemption regime of the e-Commerce Directive grants OIs legal certainty to provide digital services without exposing themselves to excessive liability from damages.[85] However, there is a growing trend to view transaction intermediaries and rating platforms as businesses that engage in commercial practices, evidently in the 2014 case brought by the Italian Association of Hotels

[85] Sagar, S., & Hoffmann, T. (2021). Intermediary Liability in the EU Digital Common Market – from the E-Commerce Directive to the Digital Services Act. *IDP: Revista de Internet, Derecho y Política*, 4.

against TripAdvisor,[86] examined by the Italian Competition Authority and the Administrative Court of Lazio. The objective of the case was to determine whether TripAdvisor's publication of unverified hotel and restaurant reviews written by users could be considered UCPs. The Italian Competition Authority classified TripAdvisor as a trader under the UCPs Directive as implemented in the Italian Consumer Code, citing that although TripAdvisor does not charge for its services directly, it generates revenue from targeted advertising. The Administrative Court of Lazio concurred with this outcome, affirming that TripAdvisor is engaged in commercial practices as a trader. Under the case study, the online platform is categorized as a trader and participates in commercial practices with users who are considered consumers under the UCPs Directive. In that case, its actions are considered commercial practices and may be held accountable for any UCPs. The court, however, arrived at a different conclusion regarding the negligence in the organization and supervision of TripAdvisor's review system and determined that consumers who engage with these reviews know they are subjective evaluations, not factual statements. Additionally, TripAdvisor has yet to announce the existence of a fact- checking system publicly. Therefore, the court concluded that TripAdvisor could not be considered misleading consumers.

Whether OIs can be held liable for the commercial practices of their users is a complex issue. On one way, if the intermediary is considered a trader, they may not be exempt from liability under the e-Commerce Directive and would be required to comply with the due diligence obligation outlined in Article 5 of the UCPs Directive.[87] In the view of the research, this would impose a duty to monitor or investigate. Conversely, being classified as a trader does not necessarily rule out the intermediary's status as a neutral platform. If the requirements for the e-Commerce Directive are met, the intermediary may still be exempt from liability, even for UCPs. This creates a conflict between two provisions in the EU's legal system and raises the question of how to balance the interests of traders and intermediaries. The assessment of UCPs requires a consideration of the specific context and conduct of the users. It remains to be seen whether the intermediary can rely on a notification from the claimant to achieve immunity under the host for UCPs. In cases where immunity is not applicable, the LOIs in a favorable manner remain a question that ought to be at a national deck of a particular Member-State, which can lead to uncertainty and negative impacts on the behavior of OIs in the EU's Digital Market. The issue of whether and under which conditions

86 Autorità Garante della Concorrenza e del Mercato (AGCM, Italian Competition Authority) on *TripAdvisor*, Decision PS9345, paras 87–9 (It.), 19 December 2014. This stake of the AGCM's decision was affirmed by the Tribunale Amministrativo Regionale (TAR) Lazio (Regional Administrative Tribunal of Lazio), Section I, Case no. 9355 (It.), 13 July 2015, in Diritto dell'Informazione e dell'Informatica 494 (It.); *See* also Kammergericht (Court of Appeal) Berlin, in MultiMedia und Recht 601 (Ger.), 8 April 2016.

87 For example, marketplaces such as eBay, Amazon, and other OIs may simultaneously be considered traders and hosting providers.

the intermediary should prevent future infringements after becoming aware of illicit content through a notification or court order is equally uncertain. These issues must be settled uniformly to clarify and reduce uncertainty in the online marketplace.

The discussion of the effectiveness of consumer protection in the online market and the consistency of the European legal system notes that while IPRs have remedies against intermediaries who facilitate infringement, the UCPs Directive does not provide similar remedies for consumers. Back in 2017, the European Commission imposed a fine on Google[88] for violating antitrust laws by leveraging its dominance in the search engine market to promote its comparison-shopping service, Google Shopping unfairly. This move was deemed an abuse of power, as it gave Google an unfair advantage over its competitors. This creates a regulatory misalignment. The study considers the possibility of filling this gap through the application of Article 11 of the Enforcement Directive but raises concerns about the scope of injunctions. Suppose the injunctions need to be more precise. In that case, they may delegate a discretionary assessment of the unfairness of commercial practice to the intermediary, potentially conflicting with the prohibition of imposing monitoring obligations. Regardless, Commissioner Margrethe Vestager said: 'Google has come up with many innovative products and services that have made a difference to our lives. That's a good thing. But Google's strategy for its comparison-shopping service wasn't just about attracting customers by making its product better than those of its rivals. Instead, Google abused its market dominance as a search engine by promoting its own comparison-shopping service in its search results and demoting those of competitors. What Google has done is illegal under EU antitrust rules. It denied other companies the chance to compete on the merits and to innovate. And most importantly, it denied European consumers a genuine choice of services and the full benefits of innovation.[89] The Commission found that Google's conduct potentially reduces consumers' ability to access the most relevant comparison shopping services.[90] Search users, the Commission found, tend to consider that search results ranked highly in generic search results on Google's general search results pages are the most relevant for their queries.[91] They click on them irrespective of whether other results would be more relevant to their queries.[92] The Commission noted that Google's information regarding differences in the underlying ranking mechanisms might only be comprehensible to the most knowledgeable users.[93] It is highly improbable that Google was not cognizant of the impact of search result rankings on its users, and it appeared to exploit a cognitive bias that consumers were prone to exhibit.

88 Case AT.39740, *Google Search (Shopping)*, 27 June 2017.

89 European Commission, Press Release, Antitrust: Commission fines Google €2.42 billion for abusing dominance as a search engine by giving an illegal advantage to own comparison-shopping service, 27 June 2017.

90 Case AT.39740, para 597.

91 *Ibid*, para 598.

92 *Ibid.*

93 *Ibid,* para 599.

The distinction between search results and advertisements is apparent - advertisers are not obliged to include links to rival offers, rather they bid higher than their competition in an online ad auction to ensure that their ad is the only one displayed. However, ad auctions are akin to indexing and ranking search results as they dictate how consumers view their options in the market and the likelihood of their actions. When a small group of ad intermediaries towers the market and trade algorithmically inferred consumer profiles, it diminishes the visibility of options not based on those profiles, intensifying the exploitation of consumer irrationalities. The integration of market power analysis into consumer law prompts the query of whether every violation of EU competition law's abuse of a dominant position also constitutes a breach of the UCP Directive.[94] The UCP Directive explicitly safeguards fair competition and the misusage of domination under EU competition law could entail 'conduct which is directly exploitative of consumers,[95] making it necessary to examine whether the Directive has been violated in such cases. It is imperative to determine which entity is best equipped to regulate such behavior. It is worth noting that the UCP Directive extends to all online and offline markets, not only digital platforms. In non-digital settings, traders do not have the unprecedented control over the interaction with consumers that data- driven markets offer through personalized and systematized approaches.[96]

The Directive does not prohibit preventive content filtering outright, and many platforms have already implemented such technologies. It is important to note that the e-Commerce Directive is directed at Member States and not platforms themselves.[97] When it comes to the Directive on Copyright, the scope of monitoring obligations raises concerns. Some have argued that the difference between general and specific monitoring lies in the 'broadness of the object of the monitoring,' as Angelopoulos has suggested.[98] However, this interpretation has been challenged by Lucas-Schlotter[99] on the grounds that a measure that applies only to a portion of the content hosted by a platform is unlikely to be effective. Additionally, Lucas-Schlotter notes that the general nature of monitoring obligations does not stem from the number of works or subject matter monitored, but rather from the unspecified nature of the screening process. The general monitoring obligation should be understood as searching for

94 Directive 2005/29/EC, Recital 8.

95 European Commission, Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings, *O.J., C 45/7*, para 7, 2009.

96 Laux, J., Wachter, S., & Mittelstadt, B. (2021). Neutralizing online behavioural advertising: Algorithmic targeting with market power as an unfair commercial practice. *Common Market Law Review*, *58*(Issue 3) p. 737.

97 Angelopoulos, C. (2017). On Online Platforms and the Commission's New Proposal for a Directive on Copyright in the Digital Single Market, *SSRN*, p. 37.

98 *Ibid.*

99 Lucas-Schloetter, A. (2017). Transfer of Value Provisions of The Draft Copyright Directive (Recitals 38, 39 and article 13), p. 19.

all potentially illegal content. [100] Article 15 E-Commerce Directive prohibits monitoring of all content without a specified purpose.[101] Therefore, it can be argued that monitoring for the content which has already been identified by right holders as infringing is not general monitoring.[102] Lucas-Schlotter's position is formalistic, and if his interpretation of Article 15 of the E-Commerce Directive were adopted, it would result in arbitrary outcomes.[103]

Moreover, initially aimed at promoting the establishment of a fully integrated internal market, the EU's trademark policies have progressively shifted their focus towards addressing the security risks associated with the influx of illicit counterfeit goods - non-original physical goods manufactured without the consent of the Rights Owner which infringe IPR, pursuant to applicable Member State or EU law[104]- into the EU becoming increasingly concerned the internet service as a worth to streamline unfair commercial practice through the trade of illegal products. In addition, the online sale of counterfeit goods has implications for cybersecurity, potentially impacting network security, which is crucial to maintaining the competitiveness of the EU as an economic area. Under the CyberSecurity Strategy, - cybersecurity directs 'to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure'.[105] In particular, the Commission has sought to establish itself as a centre of expertise in this field, establishing the European Observatory on Infringements of Intellectual Property Rights (Observatory) as a means of identifying and sharing data on enforcement and best practices, as well as facilitating networks of private sector actors in proactively combatting the trade of counterfeit goods online.[106] By acting as a data gatherer, a point of contact for national bodies and private sector actors to share information on infringement practices, and then publishing reports on counterfeiting, the Observatory seeks to provide the EU with a repository for technical know-how and expertise that can then serve to reinforce the position of the EU as an actor in this field.[107] By establishing the Observatory as a point of contact, as well as facilitating soft mechanisms for voluntary regulation by networked actors operating on the Internet, the Commission has been further able to increase the effectiveness of online management of counterfeit sales, as well as expand

103 *Ibid.*

104 European Commission, The Memorandum of understanding (MoU) on the sale of counterfeit goods on the internet is a voluntary agreement facilitated by the European Commission to prevent offers of counterfeit goods from appearing in online marketplaces, Ares(2016)3934515, 21 June 2016.

105 European Commission, High Representative of the European Union for Foreign Affairs and Security Policy. Cybersecurity strategy of the European Union: An open, safe and secure cyberspace, No. JOIN (2013) 1. Brussels, 2013.

106 Farrand, B. (2018). Combatting physical threats posed via digital means: the European Commission's developing approach to the sale of counterfeit goods on the Internet. *European Politics and Society (Abingdon, England)*, *19*(3), p. 339.

107 *Ibid,* p. 346.

its competences as a cyber-security actor.[108] However, it became readily apparent that the Commission's legal actions in this field were not sufficient to manage the threat posed by the online sale of counterfeit items.[109] In this respect, it is vital to give a role to online intermediaries in identifying infringers and guaranteeing fair commercial practice, placing liability on online intermediaries to implement safeguards to protect the digital market by cyber vulnerability disclosure. It is because most of the vulnerability models implicitly assumed the independence of vulnerability disclosures, which overlooked market-drive incentives.[110] Responsible disclosure is a relatively new method for cyber vulnerability disclosure[111] aiming to 1) ensure that vulnerabilities can be identified and eliminated effectively and efficiently for all parties, 2) minimize the risk to customers from vulnerabilities that could allow damage to their systems, 3) provide customers with sufficient information for them to evaluate the level of security in vendors' products, 4) provide the security community with the information necessary to develop tools and methods for identifying, managing, and reducing the risks of vulnerabilities in information technology, 5) minimize the amount of time and resources required to manage vulnerability information, 6) facilitate long-term research and development of techniques, products, and processes for avoiding or mitigating vulnerabilities, 7) minimize the amount of antagonism that often exists between parties as a result of different assumptions and expectations, due to the lack of consistent and explicit disclosure practices.[112]

The stronger the link between external and internal market failures appears to be in a given market, the more consumer law benefits from considering the availability of non-personalized outside options.[113] Likewise, lowering the visibility of available outside options may already be enough to distort consumers' transactional decision-making in an unfair manner.[114] In this regard, the study proposes a set of common principles aligning with a call to establish a code of conduct for voluntary measures regarding counterfeit goods especially in the context of cross-national digital marketplaces in the EU.[115] First, intermediaries use notice and takedown policies, removing counterfeit listings upon receiving notification.

108 *Ibid,* p. 350.

109 *Ibid,* p. 348.

110 Tang, M., Alazab, M., & Luo, Y. (2019). Big Data for Cybersecurity: Vulnerability Disclosure Trends and Dependencies. *IEEE Transactions on Big Data*, *5*(3), p. 637.

111 Ķinis, U. (2018). From Responsible Disclosure Policy (RDP) towards State Regulated Responsible Vulnerability Disclosure Procedure (hereinafter – RVDP): The Latvian approach. *The Computer Law and Security Report*, *34*(3), p. 514.

112 Christey, S. (2002). Responsible Vulnerability Disclosure Process draft-christey-wysopal-vuln- disclosure-00.txt. *The Internet Society,* pp. 5-6.

113 *Supra* note 96, p. 736.

114 *Ibid.*

115 The measures taken are either initiated by OIs collaborating with rightsholders or supported by governments and their administrative bodies, leading to the creation of a set of common principles, known as ius gentium, to govern these voluntary measures.

Secondly, intermediaries have engaged in proactive monitoring, using keywords and other indicators to identify potential counterfeit products and flag them for review. Thirdly, implementing filtering systems that use algorithms to remove counterfeit listings from view automatically is desirable. Fourthly, intermediaries must adopt targeted payment processors for online traders selling counterfeit goods. Fifthly, voluntary registry systems allow rightsholders to control how product listings featuring their trademarks are displayed and limit them to pre-approved sellers. To tackle the rising issue of online sales of counterfeit products, OIs, and rightsholders have teamed up through voluntary cooperation, although it has yet to be a complete solution. Sixthly, advertising codes of practice shall be created to prevent the display of advertisements on fake websites, reducing the flow of advertising revenue to these sites. Lastly, intermediaries have educated users and businesses through educational campaigns and reminders during the upload process.[116]

3. The Liability of Online Content Sharing Service Providers

The Digital Service Act went into effect on 16 November 2022 and was enacted in response to the rapidly evolving digital world and the growth of new digital platform economies.[117] The DSA outlines clear accountability for LOIs providers by establishing due-diligence obligations and procedures for removing illegal and harmful content increasing obligations for risk assessment of automated filtering tools. The Act adopts a two-pronged approach to regulation. On the one hand, Chapter II outlines the LOIs of providers, which is, in the view of the study, a revised version of the existing liability exemption rules and restrictions on general monitoring, classifying functions into a mere conduit, caching, and hosting and introduces a 'Good Samaritan' rule in Article 6 and provisions for actions against illegal content and information requests. On the other hand, Chapter III establishes horizontal due diligence obligations for a secure and transparent online environment categorizing providers into four groups with asymmetric commitments, ranging from general to specific: (1) intermediary services, which is the broadest category and encompasses mere conduit, caching services, (2) hosting services consist of storing information at the recipient's request, (3) online platforms as providers that cache and broadcast dispatch to the masses unless it is a minor feature of another service, and (4) very large online platforms - subject to the highest level of obligations due to their systemic role in shaping information flows online and influencing public opinion.[118]

116 *Supra* note 23, pp. 376-377.

117 The DSA is built upon the principles established in the e-Commerce Directive aiming to create a harmonized legal framework that supports the provision of innovative digital services while safeguarding the rights of online users. The ultimate mission of the DSA is to create a safer and more secure online experience for users by establishing measures for fairness, transparency, and accountability in the moderation of online content. It requires implementing appropriate risk management and auditing systems to protect the integrity and transparency of online platforms against manipulative techniques.

118 Very large online platforms are with more than 45 million average monthly active users in the EU, representing 10% of the European population.

The liability exemption and due diligence obligations are separate, meaning that compliance with one does not affect the availability of the other.[119] The legal question is how the liability rules, and the asymmetric obligations apply to Online Content Sharing Service Providers (OCSSPs) as (very large) online platforms.[120] This analysis provides a model for examining the DSA's liability regime.

Articles 3, 4, and 5 of the DSA add significant innovations to the LOIs service providers by introducing a complex and detailed system of obligations. For example, the hosting safe harbour provision of Article 5 DSA was created to replace Article 14 of the e-Commerce Directive. However, the application of this provision is narrow in Article 17(3) of the EU Directive on Copyright only to the degree that the conditioning falls within the scope of Article 17. The liability directions outlined in the DSA are partially excluded for OCSSPs. Article 17(8) of the EU Directive on Copyright states that the application of this article should not result in any general monitoring obligation. This statement does not set aside the application of Article 15 of the e-Commerce Directive and can be seen as a mere declaration. Regarding hosting and online platforms, their notifications must comply with the mechanism outlined in Article 14 of the DSA, which also aims to clarify the ambiguity posed by Article 14 of the e-Commerce Directive. The DSA (Article 14(3)) clearly states that hosting services, including online platforms, can only be considered to have actual knowledge or awareness of Article 5 (regarding the obligation to remove illegal content or disable access) if the notices contain all of the elements outlined in paras 1 and 2. The last article left much room for interpretation regarding when providers have actual knowledge of illegal activity or illegal content.[121] The matter, - Article 14 of the DSA affects the scope and interpretation of Article 5, even though it duplicates the content of Article 14 of the e-Commerce Directive.

Next, the applicability of Article 6 of DSA concerning OCSSPs is a complex issue since there may be valid arguments for not considering the unassuming the DSA's drawback exemptions as evidence of their non-applicability. According to Article 6 of the DSA, the aim is to detect and remove illegal content and comply with the Union's regulations. However, Articles 17(4) (b) and (c) of the EU Directive on Copyright already require OCSSPs to make every effort to prevent copyright-infringing content from being available. This can limit the ability of online platforms to engage in voluntary activities as required by Article 6 of the DSA. Voluntary measures taken by OCSSPs that go beyond what is needed could be allowed, but this is depen-

[119] Quintais, J. P., & Schwemer, S. F. (2022). The Interplay between the Digital Services Act and Sector Regulation: How Special Is Copyright? *European Journal of Risk Regulation*, *13* (2) pp. 204-205.

[120] Under Recital 53 of the DSA, '(...) it is necessary to impose specific obligations on the providers of those platforms, in addition to the obligations applicable to all online platforms. Due to their critical role in locating and making information retrievable online, it is also necessary to impose those obligations, to the extent they are applicable, on the providers of very large online search engines. Those additional obligations on providers of very large online platforms and of very large online search engines are necessary to address those public policy concerns, there being no alternative and less restrictive measures that would effectively achieve the same result.'

[121] Tommasi, S. (2021). The Liability of Internet Service Providers in the Proposed Digital Services Act. *European Review of Private Law*, *29*(Issue 6), 934.

dent on the implementation of Articles 17(7) to (9) of the EU Directive on Copyright. Meanwhile, the practical implications of the intersection between the DSA and the EU Directive on Copyright have significant consequences for the design of content-moderation systems used by platforms.

The rule in Article 6 DSA, which pertains to voluntary own-initiative investigations and legal compliance, must be more straightforward. Given the forthright relation to the liability immunities, its application is directly linked to the exact hosting safe harbour, which not accomplishes by OCSSPs as per Article 17(3) of the EU Directive on Copyright. In a narrow interpretation, this connection precludes the application of Article 6 DSA in the context of OCSSPs.[122] On the different arrow, the general monitoring ban in Article 7 DSA substitutes a similar prohibition in Article 15 of the e-Commerce Directive.[123] However, just because there is no obligation to monitor does not mean that providers have no obligation to prevent similar violations. The ruling in the case of Eva Glawischnig Piesczek v. Facebook Ireland Limited[124] highlights this point. Eva Glawischnig-Piesczek was a prominent member of the Austrian National Council, serving as the chair of the parliamentary party 'The Greens' and the federal spokesperson for the party. Facebook Ireland Limited, a subsidiary of Facebook Inc. based in Dublin, Ireland, operates an online social network platform accessible to users outside the US and Canada. In April 2016, a Facebook user shared an article from the Austrian news magazine oe24.at and added a disparaging comment about Glawischnig-Piesczek, indicting her as a 'lousy traitor of the people,' 'corrupt oaf,' and a member of a 'fascist party.' The content was visible to all Facebook users. After Facebook Ireland failed to remove the comment, Glawischnig-Piesczek brought an action against the company and requested an injunction to cease the publication and dissemination of the photographs and statements. The Commercial Court of Vienna granted the injunction, and the Higher Regional Court of Vienna upheld the order, except that it only applied to statements brought to the knowledge of Facebook Ireland. The Supreme Court of Austria considered the statements damaging Glawischnig- Piesczek's reputation, insulting, and defamatory. The referring court is tasked with determining whether a cease-and-desist order against the hosting provider of a social network with a large user base can be extended globally to statements with identical wording or content that the provider is unaware of. The Supreme Court of Austria has established in its case law that such an obligation must be deemed proportional if the service provider was already aware that the person's interests were harmed by a recipient's contribution, thus demonstrating the risk of further infringements. The EU law requires a hosting service provider to remove information they store if it is equivalent to previously declared illegal content or to block access to that content. This obligation is in line with the absence of a general monitoring requirement for in-

122 *Supra* note 119, p. 207.

123 It is preserved in the EU Directive on Copyright.

124 CJEU, Case C-18/18, *Eva Glawischnig Piesczek v. Facebook Ireland Limited*, ECLI:EU: C:2019:821, 3 October 2019.

termediaries. The equivalent information must have specific elements, such as the name of the person involved in the previous infringement, the circumstances surrounding that infringement, and content identical to what was declared illegal. This is so the hosting provider does not have to assess the content in question independently. In this case, the difference in wording between the equivalent content and the previously declared illegal content must not be substantial enough to require the hosting provider to conduct an independent evaluation.

Under the study, the rules outlined in Articles 8 and 9 of the DSA, which deal with orders against illegal content and the provision of information, may apply to OCSSPs. Article 8 offers a more detailed framework for OCSSPs than elsewhere. Article 8 introduces a novel requirement for providers of intermediary services to act against illegal content. Suppose they receive an order from national judicial or administrative authorities to act against one or more specific items of illegal content, in accordance with applicable Union or national law and in compliance with Union law. In that case, they are mandated to inform the issuing authority, or any other specified authority of the effect given to the order without undue delay. The provider must also specify whether and when the order was applied. This provision is a significant development in information law as it creates a clear obligation for intermediaries to report back to authorities regarding the enforcement of orders to remove illegal content. This is an important step towards improving transparency and accountability in the fight against illegal online content. While some might argue that Article 8(3) of the Information Society Directive provides specific rules for injunctions, this only applies to LOIs that do not stand directly answerable for the content they host. Article 9 grants the authority to issue an order to providers of intermediary services to provide information in compliance with EU law. Such orders must be provided with reasons and information on remedies available to the provider and the recipients of the service in question. The OCSSPs, on the other hand, are directly accountable for the liability[125] regardless of the content they host under the provisions of Article 17(1) of the EU Directive on Copyright. As a result, Article 8 of the DSA applies to OCSSPs but raises a question about the copyright enforcement of OIs.

The implementation and enforcement rules of the DSA should address all interests involved in a balanced, symmetrical way when the dilemma is that digital range confrontations contend the rights and interests of players when the notion of the recipient of the services is defined in Art. 2(b) DSA contains not just providers of content on hosting assistance but, furthermore, their readers instituting enforcement tools for victims, such as copyright holders, but also countermeasures for speakers, who can equally be copyright holders, and their readers as such:

1. Persons who post content online (content providers) are safeguarded under the recipients of the service designation, either individually through Articles 15, 17, and 18 or colle-

[125] In the CJEU, Joined Cases C-682/18 and C-683/18, *YouTube and Cyando*, ECLI:EU: C:2021:503, 22 June 2021, -it is found that if a platform does not alter as an OCSSP, it is subject to the pre-existing control.

ctively through Article 68 and, in some cases, Article 72 if they do not operate as a business. Besides, they may also be protected as copyright holders under relevant copyright legislation.

2. Readers who consult the content are also protected as recipients of the service collectively through article 68 and consumer associations if their rights are violated (per Article 72 of the DSA and Article 2(1) of the Representative Action Directive.[126]

3. Victims who are affected by the content posted (in the research context, it is copyright holders) are protected through the mechanisms outlined in the DSA, such as articles 14, 19, and others, as well as any related legislation, including copyright provisions for remedies against copyright infringement.[127]

While copyright holders have multiple avenues for enforcement, such as individually through Articles 14, 17, and 18, via trusted flaggers (as outlined in Article 19), and through representative entities (per Article 68), passive users (readers) and content providers have limited options for implementing and enforcing intermediaries' DSA obligations. Online platform providers must promptly inform complainants of decisions made regarding their complaints, provided that they were not made solely by automated means. They must also inform complainants about the possibility of settling disputes out-of-court and other available redress options following Article 18. Recipients of the service are allowed to select out-of-court dispute settlement bodies from any certified the Digital Services Coordinators where they are established, as long as they meet the conditions listed in paragraph 2 of Art. 18. Also, readers can only seek redress through qualified consumer organizations or public bodies under Article 72 of the DSA in conjunction with the Representative Action Directive. This type of collective enforcement is only available in cases where the DSA violations harm or may harm the collective interests of consumers. However, if content providers act commercially and in line with copyright law, - Article 72 of the DSA will not provide enforcement support. Content providers, on the other hand, do not always have individual claims that they can advance. Therefore, the remedies available for violations of DSA obligations should be fair and equitable, avoiding any advantage for one group at the expense of others.[128] There are also arguments for limiting enforcement to the provisions of the Act alone. Implementing unspecified non-DSA remedies based on national laws could disrupt the delicate balance between reducing illegal content and preserving the intervention with online freedom of expression, which the DSA seeks to maintain through its procedural approach to copyright and other substantive laws. In copyright law, where a comprehensive EU enforcement framework already exists, a restrictive policy would likely not result in significant enforcement gaps. The e-Commerce Directive lacks

[126] Directive (EU) (2020)/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC, *OJ L 409*, 2020.

[127] Peukert, A., et al. (2022). European Copyright Society – Comment on Copyright and the Digital Services Act Proposal. *IIC*, *53*(3) p. 371.

[128] Holcombe, R. (2015). Political Capitalism. Cato Journal, 35(1) p. 41.

enforcement rules, relying instead on cooperation between Member States and EU-level codes of conduct; while compatible, this approach has yet to improve enforcement uniformly.[129] To combat illegal content, the DSA acknowledges Trusted Flaggers, whose notices are processed and decided upon promptly. Enforcement powers are divided among several actors, including the Digital Services Coordinators and the European Commission, with the European Board of Digital Services serving as an advisory body. Under the study, the division of enforcement responsibilities and fostering collaboration among them are crucial steps to mitigate the potential drawbacks of centralized enforcement, such as prolonged delays. To ensure legal certainty, the DSA must address the issue of non-DSA enforcement measures. Allowing Member States to enforce these powers or permitting non-DSA actions to remain applicable would boost the practical effectiveness of the DSA's obligations and minimize reliance on resources allocated by the Commission and national Digital Services Coordinators. However, the DSA requires clarity on whether it has the sole authority to enforce OCSSPs' obligations or if violations can prompt private claims through additional legal avenues, such as tort and unfair competition law. This is especially crucial when considering copyright law, for instance, whether intermediaries can be held liable for compensating copyright holders for harm caused by an inefficient or absent notice-and-action process or whether uploaders can seek a remedy if a platform fails to promptly reverse an unjustified removal decision as outlined in Article 17(3) of the Act.

The research has shown, the DSA does not establish a level playing field for all parties involved but imposes additional obligations when online platforms must have an internal complaint-handling system that qualifies fusses to be nestled electronically and complimentary of charge for illegal content or content that goes against terms and conditions.[130] The DSA also sets out measures that online platforms must adopt against misuse by service recipients or complainants who frequently provide manifestly illegal content or submit unfounded notices or complaints, likewise, issuing a warning or suspending service provision for a reasonable period. In the view of the study, such voluntary remedies shall be based on the security measures especially using a defense-in-depth approach. The similar idea has also been implemented in the cybersecurity community to detect and prevent malicious intruders in a system.[131] A defense-in-depth approach, developed for a logic locked device, can defend the locking key value in an obscured system against any attack by deploying several independent protection layers and eventually raising the cost of all attacks to unacceptable levels.[132] Mul-

[129] Genç-Gelgeç, B. (2022). Regulating Digital Platforms: Will the DSA Correct Its Predecessor's Deficiencies? *Croatian Yearbook of European Law & Policy*, *18* (1) p. 54.

[130] Digital Service Act, Article 17.

[131] Rahman, M. T., Rahman, M. S., Wang, H., Tajik, S., Khalil, W., Farahmandi, F., Forte, D., Asadizanjani, N., & Tehranipoor, M. (2020). Defense-in-depth: A recipe for logic locking to prevail. *Integration (Amsterdam)*, *72*, p. 40.

[132] *Ibid.*

tiple defense layers are used for developing defense-in-depth for logic locking, the words 'defense-in-depth' and 'multi-layer defense' are used interchangeably.[134] This marks a significant shift towards of OCSSPs in assisting for better digital market workflow.

Conclusions

The role of OIs is immense. These platforms facilitate the sharing of business information but also pose the challenge of liability due to the unauthorized transfer and distribution of the content. As such, both public and private entities must work together to address this multifaceted challenge and ensure the security and well-being of all individuals involved in an online arena. Rapid intervention is necessary to prevent adverse effects on the market. To create a legal algorithm, we should find a starting point, at which law should start recognizing discovery.[135] In the continental system, we do not have an explicit pre-emptive restraint doctrine, but we have a general clause that countries have the right to impose restrictions in order to protect legitimate interests.[136] In such situations, immediate protection that blocks the conduct may be more desirable. Essentially, any general content filtering obligation would be permissible, as long as the content being searched for is specifically defined. Although it may be true that searching for content that is already identified by rightsholders is not general monitoring, this argument is only valid if the technology used functions similarly to ContentID in YouTube which works by having right holders provide their works to a general database, which is then compared to the material uploaded by users.[137] However, an extensive obligation to monitor copyright-infringing content could potentially apply to content that has not yet been published in any media. The growth of digital markets will result in an increase in potential violations involving OIs and an increase in litigation. Relying solely on injunctive relief against OIs may have unintended consequences and may not be suitable for digital markets, which are inherently comprehensive. It is crucial to approach regulation and consider alternative mechanisms appropriate for digital markets. The debate on the Directive on Copyright highlights the need for a modern approach to regulating digital markets and the importance of considering new and traditional legal tools to ensure a functioning market. To clarify the CJEU's position, it held that EU fundamental rights do not prohibit national authorities or courts from issuing injunctions requiring ISPs to block their users' access to websites offering illegal content, as long as the measures taken do not unnecessarily deprive users of lawful access to information and effectively prevent or discourage unauthorized access to infringing materials. The EU law protects IPRs through provisions such as the Enforcement Directive Article 11 and the Information Society Directive Article 8 (3) for copyrights. Other areas of law, such as the Unfair Commercial Practices Directive and the Trade

135 *Supra* note 111, p. 519.

136 *Ibid*, p. 511.

137 Commission Impact Assessment includes an extensive analysis of how the Content ID works. See Commission Impact Assessment on the Modernization of Copyright, SWD (2016) 301 final part 3/3, Annex 12 A, p. 164ff.

Secrets Directive, need similar protection mechanisms. The EU law has attempted to regulate e-commerce through exemption rules for LOIs, but this has only complicated the legal framework. As a result, the intervention between the Unfair Commercial Practices Directive, the Trade Secrets Directive, and the e- Commerce Directive has led to problems of concurrent application, resulting in a lack of adequate protection for interests governed by these liability rules. Although market investigations have the potential to achieve all of these interventions, ensuring the necessary flexibility can pose a significant challenge. Therefore, an ex-ante regulatory framework may be better suited for designing and enforcing these interventions, providing market participants with greater clarity and predictability while also providing a stronger basis for ongoing oversight and enforcement by regulatory authorities.[138] By implementing such a framework, regulators can create a more stable and transparent environment that facilitates market efficiency, while also addressing the concerns that may arise from market power or other forms of market failure.

The new Digital Services Act aims to tackle this challenge and create a comprehensive framework for the LOIs. This new approach considers the size and reach of service providers and prioritizes their obligations in the online ecosystem. The DSA, in particular, Article 3, regulates the liability for mere conduit, which mirrors the well-established provisions outlined in Article 12 of the e-Commerce Directive. For online services that involve caching, Article 4 of the DSA reiterates the exemptions from liability established in Article 13 of the e-Commerce Directive. Service providers are exempt from liability for hosting activities, defined as the long-term storage of information provided by the service recipient, as outlined in Article 5 of the DSA. This exemption applies when the provider is unaware of the unlawfulness of the information and its circumstances, and if they become aware, they must act promptly to remove the information or disable access to it. Either of these conditions must be met for the provider to benefit from the exemption from liability resulting in the point of view that the DSA is not only a regulation that outlines what intermediaries must do to avoid liability but also includes unique and innovative elements, such as the liability regime for online service providers is reinforced by a closing provision that clarifies the absence of a general monitoring obligation. These elements set it apart from being a purely negative regulation.

Remarkable, -

1) The implementation of the EU Directive on Copyright Article 17 has led to a major transformation in the liability of online user-generated content platforms for primary copyright infringement. With platforms being held directly responsible for infringing content, this has created a significant burden for them. Also, the importance of specific knowledge of such content has become more critical, further complicating the matter.

[138] Fletcher, A. (2021) Market Investigations for Digital Platforms: Panacea or Complement? *Journal of European Competition Law & Practice, 12*(1), 55

2) The e-Commerce Directive, on the other hand, shields online intermediaries from the responsibility of monitoring the information and activities of third parties. Consequently, the legal framework for determining liability, as well as the type of infringement (direct or secondary), shall be based on the national law of the affected Member State.

3) To ensure the effective protection of trade secrets, it's crucial for the European legislator to carefully consider the position of online intermediaries and the overlap with trade secret legislation. This is because the ease of information sharing and access in the digital world can create challenges for safeguarding confidential information. Therefore, the legislator needs to assess how online intermediaries handle trade secret information and the measures they have in place to prevent its unauthorized disclosure or use. Additionally, it's essential to ensure that any new legislation or regulations do not inadvertently conflict with existing trade secret laws or create gaps in protection. Overall, a comprehensive approach is necessary to guarantee that trade secret protection remains effective in the digital age.

4) The authors determined a regulatory misalignment in consumer protection, where consumers have different remedies than intellectual property rights holders under the Unfair Commercial Practices Directive. The study recommends exploring the application of Article 11 of the Enforcement Directive to address this problem while raising concerns about the potential conflict between the scope of injunctions and the prohibition on imposing monitoring obligations.

5) The article recognizes the challenges that impede the creation of a coherent and effective legal framework for online intermediary liability. The Digital Services Act is not merely a regulatory framework that specifies the actions intermediaries of how to avoid liability. It also introduces unique and innovative features, such as a reinforced liability regime for online service providers, which is strengthened by a closing provision that explicitly clarifies the absence of a general monitoring obligation.

Recommendations, -

The OIs are generally not liable for infringing content uploaded or shared by their users, provided they act quickly to remove or disable access to that content when they become aware of it. However, to benefit from this liability exemption, online intermediaries must take distinguishing extents to prevent, detect, and respond to infringing content on their platforms. The study calls for more robust measures to be carried out to prevent and combat online infringement, including more decisive enforcement actions and greater cooperation between online intermediaries, rightsholders, and law enforcement agencies. These steps include implementing effective notice-and-takedown procedures for removing infringing content when notified of its presence and adopting measures to prevent future re- upload or dissemination of such content. Online intermediaries may also be required to implement tech-

nical measures, such as content filtering systems, to detect and prevent infringing content from being uploaded or shared on their platforms. The specific technical requirements for monitoring and reporting violations may vary depending on the type of online service being provided and the nature of the infringing content in question. However, online intermediaries are generally expected to take a proactive approach to monitor and report violations of intellectual property rights on their platforms and to work closely with rightsholders and law enforcement agencies to prevent and combat online infringement. It is worth noting that EU law needs to provide a comprehensive solution to the problem of online infringement.

Meanwhile, the subsequent measures recommended to be taken by OIs to mitigate their liability:

a) In terms of the liability of internet service providers, the research has shown that IP blocking can be an effective tool for preventing access to malicious sites or controlling the spread of malware. However, it can be bypassed or circumvented in some cases, mainly if the attacker operates a sophisticated technique. One possible alternative to IP blocking is the use of Service Level Agreements (SLAs) as a detective control. SLAs can define specific performance metrics or expectations for service providers or other third-party entities involved in providing online services or other resources. For example, an SLA could portray specific response times for addressing security incidents or require regular vulnerability assessments. By setting clear expectations and performance metrics for service providers, SLAs can help detect potential security issues and ensure that they are addressed promptly and effectively. However, a study records that SLAs are not a substitute for preventative controls such as IP blocking or other security measures. Rather, they are complementary control that can catch and react to security incidents that may have bypassed other controls. As such, SLAs should work together with other security measures to provide a comprehensive and effective security posture.

b) OIs to avoid trade secrets infringements shall apply monitoring by a completely independent institution using artificial intelligence for info-gathering purposes. It is a complex task requiring careful planning and execution. Here are some general steps that can be taken:

i. Clarification of the monitoring measures: The first step is to define the criteria for monitoring trade secrets infringements. This could include monitoring specific keywords, patterns of behavior, or types of information that are known to be sensitive. The criteria should be well-defined and based on clear legal and ethical principles.

ii. Invention of the monitoring system: The monitoring system should be designed to collect and analyze information relevant to the monitoring criteria. This could include AI tools to analyze data from various sources, such as social media, forums, and other online platforms. The system should be designed to be secure and protect the confidentiality of the collected information.

iii. Establishment of an independent institution: The monitoring system should be operated by an independent institution separate from the organization whose trade secrets are being monitored. This institution should be trusted and respected and have the necessary expertise and resources to operate the monitoring system effectively.

iv. Segregation of duties: It is paramount to establish a clear segregation of duties between the independent institution and the organization being monitored. This means that the independent institution should not have access to the organization's trade secrets or other confidential information and should not be involved in any activities that could compromise the confidentiality of that information.

v. Regular reviews and updates: The monitoring criteria and system should be reviewed and updated regularly to confirm they remain relevant and practical. This could involve conducting audits or assessments of the monitoring system or engaging with stakeholders to gather feedback and make improvements.

Comprehensively talking, the design and implementation of a monitoring system for trade secrets infringements using AI and an independent institution require careful planning and attention to detail. The monitoring criteria should be well-defined, the system should be secure and effective, and the roles and responsibilities of all stakeholders should be clearly established and communicated.

c) For fair commercial practice and consumer protection, the Responsible Disclosure Policy (RDP) approach is a voluntary framework solution that encourages online intermediaries to establish clear and transparent procedures for handling reports of security vulnerabilities and other issues on their platforms. The RDP approach promotes collaboration and responsible behavior among all stakeholders, including security researchers, online intermediaries, and end-users. In the context of the liability of online intermediaries, the RDP approach can be used to demonstrate that an intermediary has taken reasonable steps to prevent and mitigate security vulnerabilities and other issues on their platform. By establishing a clear and transparent RDP, online intermediaries can encourage security researchers and other stakeholders to report potential issues responsibly and cooperatively rather than engaging in unauthorized activities that could potentially harm the platform or its users. Notably, the RDP approach does not deliver a legal safe harbour or exemption from liability for online intermediaries. However, it can be employed to demonstrate that an intermediary has taken reasonable steps to prevent and mitigate potential issues on their platform, which may be taken into account by courts or other authorities when assessing liability in the event of a security breach or other issue.

Therefore, the RDP course can be a valuable tool for promoting responsible behavior and collaboration among all stakeholders in the online ecosystem and can help to prevent and mitigate security vulnerabilities and other issues on online platforms. However, it is essential

to document that the RDP approach is voluntary and may only be appropriate or feasible for some online intermediaries or situations.

d) Under the DSA, OCSSPs are required to implement a range of measures to prevent the dissemination of illegal content on their platforms. One technique that OCSSPs can use to meet these requirements is a defence-in-depth approach that involves implementing multiple layers of security controls to provide a comprehensive and effective security posture. This approach can be applied to various aspects of OCSSPs' operations, including:

i. A user authentication and access control: OCSSPs can use access control mechanisms to restrict user access to specific content or features based on their roles or permissions.

ii. Content filtering and moderation: OCSSPs can use a combination of automated and manual content filtering and moderation tools to identify and remove illegal content from their platforms. Automated tools such as machine algorithms can disseminate characteristics of illegal content, while human moderators can provide additional oversight and review.

iii. An incident response and reporting: OCSSPs should have well-defined incident response plans to identify and respond quickly. Additionally, they should be prepared to report security incidents to relevant authorities and affected users promptly and transparently.

Thus, by implementing a defense-in-depth approach, OCSSPs can create a layered security posture that effectively prevents the dissemination of illegal content on their platforms. However, a study remarks that only some security measures are foolproof, and OCSSPs should continuously monitor and assess their security posture to identify and address potential vulnerabilities or weaknesses.

Bibliography

1. Angelopoulos, C. (2017). On Online Platforms and the Commission's New Proposal for a Directive on Copyright in the Digital Single Market, *SSRN,* pp. 1-47. DOI: http://dx.doi.org/10.2139/ssrn.2947800

2. Anon(2018)CreatinganeffectiveFinTechIPstrategy.*ManagingIntellectual Property*.

3. Autorità Garante della Concorrenza e del Mercato (AGCM) on *TripAdvisory*, Decision PS9345, paras 87–9 (It.), 19 December 2014; Tribunale Amministrativo Regionale (TAR) Lazio, Section I, Case no. 9355 (It.), 13 July 2015 in Diritto dell'Informazione e dell'Informatica 494 (It.); Kammergericht (Court of Appeal) Berlin, in MultiMedia und Recht 601 (Ger.), 8 April 2016.

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

5. Christey, S. (2002). Responsible Vulnerability Disclosure Process draft- christey-wysopal-vuln-disclosure-00.txt. *The Internet Society. Retrieved* from: https://datatracker.ietf.org/doc/html/draft-christey-wysopal-vuln-disclosure- 00 [Accessed 25 February 2023].

6. Chiarella, M. (2023). Digital markets act (dma) and digital services act (dsa): new rules for the eu digital environment. *Athens Journal of Law (AJL)*, 9(1) pp. 33-58.

7. Colangelo, G., & Maggiolino, M. (2018). ISPs' copyright liability in the EU digital single market strategy. *International Journal of Law and Information Technology*, *26*(2) pp. 142–159. DOI: https://doi.org/10.1093/ijlit/eay005.

8. Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online, C/2018/1177, *OJ L 63,* 6 March 2018.

9. Court of Justice of the European Union, Case C-236/08, *Google France v Louis Vuitton Malletier SA and others*, ECLI:EU:C:2010:159, 23 March 2010.

10. Court of Justice of the European Union, Case C-324/09, *L'Oreˊal SA and others v eBay International AG and others*, ECLI:EU:C:2011:474, 12 July 2011.

11. Court of Justice of the European Union, Case C-70/10, *Scarlet Extended SA v SABAM*, ECLI:EU:C:2011:771, 24 November 2011.

12. Court of Justice of the European Union, Case C-360/10, *SABAM v Netlog NV*, ECLI:EU:C:2012:85, 16 February 2012.

13. Court of Justice of the European Union, Case C-314/12, *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH*, ECLI:EU:C:2014:192, 27 March 2014.

14. Court of Justice of the European Union, Case C-18/18, *Eva Glawischnig Piesczek v. Facebook Ireland Limited*, ECLI:EU: C:2019:821, 3 October 2019.

15. Court of Justice of the European Union, Joined Cases C-682/18 and C-683/18, *YouTube and Cyando*, ECLI:EU: C:2021:503, 22 June 2021.

16. Desai, J. (2010). *Service level agreements a legal and practical guide* (1st edition). IT Governance Pub.

17. Dinwoodie, G.B. (2017). A Comparative Analysis of the Secondary Liability of Online Service Providers. In *Dinwoodie, G.B. (eds) Secondary Liability of Internet Service Providers. Ius Comparatum – Global Studies in Comparative Law, vol 25.* Springer, Cham., pp. 1-72. DOI: https://doi- org.ezproxy.its.uu.se/10.1007/978-3-319-55030-5_1.

18. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, particularly electronic commerce, in the Internal Market ('Directive on electronic commerce'), *OJ L 178*, 2000.

19. Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, *OJ L 167*, 2001.

20. Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, *OJ L195/16*, 2004.

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

22. Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use, and disclosure, *OJ L 157*, 2016.

23. Directive 2019/790/EU of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, *OJ L130/92*, 2019.

24. Directive (EU) (2020)/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC, *OJ L 409*, 2020.

25. European Commission, Case AT.39740, *Google Search (Shopping)*, 27 June 2017.

26. European Commission, High Representative of the European Union for Foreign Affairs and Security Policy. Cybersecurity strategy of the European Union: An open, safe and secure cyberspace, No. JOIN (2013) 1. Brussels, 2013.

27. European Commission, The Memorandum of understanding (MoU) on the sale of counterfeit goods on the internet is a voluntary agreement facilitated by the European Commission to prevent offers of counterfeit goods from appearing in online marketplaces, Ares(2016)3934515, Brussels, 21 June 2016.

28. Farrand, B. (2018). Combatting physical threats posed via digital means: the European Commission's developing approach to the sale of counterfeit goods on the Internet. *European Politics and Society (Abingdon, England)*, *19*(3) pp. 338–354. DOI: https://doi.org/10.1080/23745118.2018.1430721

29. Fletcher, A. (2021). Market Investigations for Digital Platforms: Panacea or Complement? *Journal of European Competition Law & Practice*, *12*(1) pp. 44–55. DOI: https://doi.org/10.1093/jeclap/lpaa078.

30. Genç-Gelgeç, B. (2022). Regulating Digital Platforms: Will the DSA Correct Its Predecessor's Deficiencies?*Croatian Yearbook of European Law & Policy*, *18* (1) pp. 25–60. DOI: https://doi.org/10.3935/cyelp.18.2022.485.

31. Holcombe, R. (2015). Political Capitalism. *Cato Journal*, 35(1) p. 41.

32. Huhta, E. (2019).*Copyrights, Online Intermediaries and the EU: SaveYourInternet? : Platform Liability in Light of Article 17 of the Directive of Copyright in Digital Single Market*. Uppsala universitet, Juridiska institutionen, pp. 1-77.

33. Ķinis, U. (2018). From Responsible Disclosure Policy (RDP) towards State Regulated Responsible Vulnerability Disclosure Procedure (hereinafter – RVDP): The Latvian approach. *The Computer Law and Security Report*, *34*(3), pp. 508–522. DOI: https://doi.org/10.1016/j.clsr.2017.11.003.

34. Laux, J., Wachter, S., & Mittelstadt, B. (2021). Neutralizing online behavioural advertising: Algorithmic targeting with market power as an unfair commercial practice. *Common Market Law Review*, *58*(Issue 3) pp. 719–750. DOI: https://doi.org/10.54648/COLA2021048.

35. Lindsay, D. (2017). Website blocking injunctions to prevent copyright infringements: proportionality and effectiveness. University of New South Wales Law Journal, 40 (4) pp. 1507–1538.

36. Lucas-Schloetter, A. (2017). Transfer of Value Provisions of The Draft Copyright Directive (Recitals 38, 39 and article 13), pp. 1-22.

37. Matt Malone. (2021). On the (data) breach of confidence.*Alberta Law Review*, *58*(4) pp. 945–955.

38. Moscon, V. (2020). Free Circulation of Information and Online Intermediaries – Replacing One "Value Gap" with Another. *IIC - International Review of Intellectual Property and Competition Law*,*51*(8) pp. 977–982. DOI: https://doi.org/10.1007/s40319-020-00982-3.

39. Moscon, V., & Hilty, R. M. (2020). Digital Markets, Rules of Conduct, and Liability of Online Intermediaries—Analysis of Two Case Studies: Unfair Commercial Practices and Trade Secrets Infringement. In *Oxford Handbook of Online Intermediary Liability*. Oxford University Press, pp. 421–443. DOI: https://doi.org/10.1093/oxfordhb/9780198837138.013.22.

40. Mostert, F. (2020). Intermediary Liability and Online Trade Mark Infringement: Emerging International Common Approaches. In *Oxford Handbook of Online Intermediary Liability*. Oxford University Press, pp. 369– 380. DOI: https://doi.org/10.1093/oxfordhb/9780198837138.013.19.

41. Niebel, R., de Martinis, L., & Clark, B. (2018). The EU Trade Secrets Directive: all change for trade secret protection in Europe? *Journal of Intellectual Property Law & Practice*,*13*(6) pp. 445–457. DOI: https://doi.org/10.1093/jiplp/jpx227.

42. Ohly, A. (2018). The broad concept of "communication to the public" in recent CJEU judgments and the liability of intermediaries: primary, secondary or unitary liability? *Journal of Intellectual Property Law & Practice*, *13*(8), 664– 675. DOI: https://doi.org/10.1093/jiplp/jpy083.

43. Peukert, A., Husovec, M., Kretschmer, M., Mezei, P., & Quintais, J. (2022). European Copyright Society – Comment on Copyright and the Digital Services Act Proposal. *IIC*, *53*(3) pp. 358–376. DOI: https://doi.org/10.1007/s40319-022-01154-1.

44. Rahman, M. T., Rahman, M. S., Wang, H., Tajik, S., Khalil, W., Farahmandi, F., Forte, D., Asadizanjani, N., & Tehranipoor, M. (2020). Defense-in-depth: A recipe for logic locking to prevail. *Integration (Amsterdam)*, *72*, pp. 39–57. DOI: https://doi.org/10.1016/j.vlsi.2019.12.007.

45. 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, *OJ L 277*, 2022.

46. Sagar, S., & Hoffmann, T. (2021). Intermediary Liability in the EU Digital Common Market – from the E-Commerce Directive to the Digital Services Act. *IDP: Revista de Internet, Derecho y Política*, *34*. DOI: https://doi.org/10.7238/IDP.V0I34.387691.

47. Schovsbo, J., Minssen, T., & Riis, T. (2020).*The harmonization and protection of trade secrets in the EU: an appraisal of the EU directive* (J. Schovsbo, T. Minssen, & T. Riis, Eds.). Edward Elgar Publishing.

48. Stalla-Bourdillon, S. (2017). Internet Intermediaries as Responsible Actors? Why It Is Time to Rethink the E-Commerce Directive as Well. In T*addeo, M., Floridi, L. (eds) The Responsibilities of Online Service Providers. Law, Governance and Technology Series, vol 31.* Springer, Cham, pp. 275-293. DOI: https://doi.org/10.1007/978-3-319-47852-4_15.

49. Tang, M., Alazab, M., & Luo, Y. (2019). Big Data for Cybersecurity: Vulnerability Disclosure Trends and Dependencies. *IEEE Transactions on Big Data*, *5*(3), pp. 317–329. DOI: https://doi.org/10.1109/TBDATA.2017.2723570

50. Tommasi, S. (2021). The Liability of Internet Service Providers in the Proposed Digital Services Act. *European Review of Private Law*, *29*(Issue 6) pp. 925–944. DOI: https://doi.org/10.54648/ERPL2021048.

51. Trallero Ocaña, T. (2021). The Notion of Secrecy A Balanced Approach in the Light of the Trade Secrets Directive, pp. 5202.

52. Quintais, J. P., & Schwemer, S. F. (2022). The Interplay between the Digital Services Act and Sector Regulation: How Special Is Copyright? *European Journal of Risk Regulation*, *13* (2) pp. 191–217. DOI: https://doi.org/10.1017/err.2022.1.

53. Walden, I., & Hörnle, J. (2001). *E-commerce law and practice in Europe*. Woodhead Publishing Limited.

54. Yong Sun, Wenan Tan, Ler Li, Guangzhen Lu, & Anqiong Tang. (2013). SLA detective control model for workflow composition of cloud services. *Proceedings of the 2013 IEEE 17th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, pp. 165–171. DOI: https://doi.org/10.1109/CSCWD.2013.6580957.

Дар’я Булгакова

Доктор Філософії з Міжнародного Права, Запрошений Науковець, Дослідник

Уппсальський Університет, Департамент Права, Уппсала, Швеція

Синтія Дерума

Кандидат у Доктори Філософії (Менеджмент), Директор Освітньої Програми ‘Магістр Бізнес-Адміністрування: Управління Кібербезпекою’

Університет Банківської Справи, Факультет Бізнесу та Фінансів, Рига, Латвія

ВІДПОВІДАЛЬНІСТЬ ОНЛАЙН-ПОСЕРЕДНИКІВ У ПРАВІ ЄВРОПЕЙСЬКОГО СОЮЗУ

Це дослідження спрямоване на вивчення складної та багатогранної проблеми відповідальності онлайн-посередників, зокрема тієї, що виникає через відсутність єдиних правил. Саме тому, на думку авторів, є потреба в системі співпраці між онлайн- посередниками та власниками прав, інтереси яких порушені. Для досягнення вказаного, автори роботи прагнуть збалансувати систему відповідальності посередників і чесну конкуренцію, тим самим привертаючи увагу до взаємозв’язку між окремими положеннями та режимом викладеним у Директиві про електронну комерцію у праві Європейського Союзу (ЄС). Крім того, у статті оцінюється узгодженість систем відповідальності онлайн-посередників та їх відповідність правилам функціонування ринку ЄС згідно з Директивами про комерційну таємницю та про недобросовісну комерційну практику. У розрізі вказаного питання стаття також надає оцінку наслідкам Директиви ЄС щодо авторського права на єдиному цифровому ринку, яка накладає на платформи онлайн-контенту (створеного користувачами) відповідальність за порушення авторських прав такого контенту, однак яка й разом з вказаним не накладає загальних зобов’язань щодо моніторингу. Таким чином, онлайн-посередникам рекомендується впровадити заходи фільтрації з метою уникнення відповідальності за несанкціоноване оприлюднення творів захищених авторським правом. Окрім того, стаття враховує реформи у законодавстві ЄС, тому у статті також аналізується Акт про цифрові послуги для вирішення питання про притягнення онлайн-посередників до відповідальності за поширення незаконної інформації через їхні платформи. Враховуючи вищевказане, дослідження підкреслює інноваційні особливості даного закону, та радить курс на вдосконалення шляхом впровадження механізмів для його реалізації на практиці. Отже, ця стаття комплексно надає класифікацію складному характеру відповідальності онлайн-посередників відповідно до права ЄС.

Ключові слова

Інтернет-провайдери, незаконний контент, судові заборони, безпечна гавань, онлайн-платформи