



WHETHER OPERATORS OF VIRTUAL ENVIRONMENTS CAN BE HELD LIABLE FOR ACTIONS WITHIN THOSE ENVIRONMENTS THAT VIOLATE HUMAN DIGNITY IN PARTICULARLY CONTEMPTUOUS AND DEGRADING BEHAVIOUR?

Gustė Kliunkaitė¹

DOI: <https://doi.org/10.7220/2029-4239.32.3>

SUMMARY

Rapid technological developments are shaping the everyday experience and introducing new regulatory concerns. Virtual environments, including virtual, augmented, and mixed realities, and the metaverse, create spaces where their users have highly immersive experiences that may interfere with their fundamental human rights, including human dignity. Since operators of virtual environments can control these environments, this article examines whether current regulatory frameworks establish liability of operators of virtual environments and whether those frameworks are effective in addressing behaviour within such an environment that is offensive to human dignity in contemptible and degrading behaviour.

To resolve the problem statement set out above, the article primarily focuses on an overview of risks posed by technological advancement, and corresponding legislative responses to the technological evolution. It further sets out the chosen methodology, systematic literature review, displays it step by step, and presents qualitative data. Consequently, it analyses academic discussions to evaluate the efficiency of current legislative frameworks addressing operators' liability for violations of human dignity in a contemptuous and degrading way and to provide recommendations.

Considering the systematic literature review findings, it may be concluded that the Digital Services Act addresses operators' liability for actions that violate human dignity in a contemptuous and degrading way; however, it is not capable of assigning liability to operators of smaller advanced environments. Therefore, it is recommended to complement it with a separate category applicable to operators of all virtual environments where proactive measures

¹ Author holds a master's degree in Law and is a graduate of the Faculty of Law at Vytautas Magnus University, Lithuania. This article is based on author's master's thesis.

would be enshrined, similar to the ones designed for bigger virtual environments, i.e. enhanced due diligence obligations and establishment of risk assessments whereby higher risks would be assigned to smaller and/or decentralised virtual environments.

KEY WORDS

Operators' liability, virtual environment, human dignity, contemptuous and degrading behaviour, Digital Services Act.

ABBREVIATIONS

AI – artificial intelligence;
DMA – Digital Markets Act;
DSA - Digital Services Act;
EC – European Commission;
ECD – E-Commerce Directive;
ECHR - European Convention on Human Rights;
ECtHR - European Court of Human Rights;
EU – European Union;
GDPR - General Data Protection Regulation;
SLR – systematic literature review;
VE – virtual environment;
VLOPs – very large online platforms;
VLOSEs – very large online search engines.

INTRODUCTION

Rapid technological development led to the introduction of smart technologies, including VE,² enabling interactions that resemble real-world experiences and demonstrating, as highlighted by the EC, a market estimated to grow from 27 billion EUR to 800 billion EUR by 2030.³ Predictably, it reflects the inevitable integration of it in everyday experiences, thereby increasing the risk of wrongdoings within such spaces. To support this claim, the European Union Cyber Security Agency identified potential crimes that could be carried out in VEs, such as fraud,

² J. M. David et al, "The Fourth Industrial Revolution: Opportunities and Challenges", *International Journal of Financial Research*, (2018 vol. 9(2)), p. 90-95.

³ European Commission, *Virtual Worlds* (2024 07 30); <<https://digital-strategy.ec.europa.eu/en/factpages/virtual-worlds>> [accessed April 26, 2025.]

identity theft, terrorist attacks, et cetera.⁴ Likewise, as VEs enable highly immersive forms of interaction, they pose a growing threat to fundamental human rights, including human dignity.

Human dignity is recognised as the basis for all fundamental rights due to its inherent and inviolable nature. Most severe prohibitions of human dignity intend to protect from torture, inhuman or degrading treatment or punishment.⁵ International legislative instruments, including the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment,⁶ Article 3 of ECHR⁷ and Article 4 of the Charter of Fundamental Rights of the EU⁸, directly prohibit these types of conduct. In particular, Article 4 of the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, obliges member states to criminalise every act of torture under their national law⁹, while the ECtHR obliges member states to put a legislative framework that protects from torture, degrading and inhuman behaviour.¹⁰ The extensive case-law of the ECtHR¹¹ demonstrates that violations of human dignity in degrading and contemptuous matter are highly relevant within the EU and there is a great risk of this type of crimes transition to VEs with technological advancements.

Considering the increasing influence of VEs and the increased risk of crimes, questions regarding the legal accountability of their operators, given their inevitable level of control, may be raised. Despite that, several legal instruments establish protection to human dignity, including but not limited to other legal acts: Article 21 of the Constitution of the Republic of Lithuania,¹² ECHR¹³, Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment.¹⁴ These norms are traditionally applied to real-world scenarios. Nevertheless, the EU invokes technological neutrality within existing legislative frameworks, which is the key principle in ensuring stability, as it assures its flexibility within technological development.¹⁵

⁴ A. Malatras et al, *Identifying emerging cyber security threats and challenges for 2030* (2023 03 29); < <https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030> > [accessed on 2024-06-05].

⁵ Case of the ECtHR: *Bouyid v. Belgium*, judgement of 28 Sep 2015, Application no. [23380/09](#).

⁶ United Nations, *Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment* (1984).

⁷ Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms*, as amended by Protocols Nos. 11 and 14, ETS No. 5 (Rome, 1950), Article 3.

⁸ European Union, *Charter of Fundamental Rights of the European Union* (2012), Article 4.

⁹ *Supra* note 6: *Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment*, Article 4.

¹⁰ Case of the ECtHR: *Hristozov and others v. Bulgaria*, judgement of 13 Nov 2012, Applications nos. [47039/11](#) and [358/12](#).

¹¹ In 2024, ECtHR data show 401 cases settled that fell under Article 3: 2 cases acknowledged acts of torture, 344 cases – inhuman and degrading behaviour, and the rest evaluated the effectiveness of investigations. See: Statistics on cases decided by the ECtHR in 2024, by ECHR Article and by country <[Statistics - ECHR - ECHR - ECHR / CEDH \(coe.int\)](#)> [accessed on 4 April 2025].

¹² Constitution of the Republic of Lithuania (1992), Article 21.

¹³ *Supra* note 7: *European Convention for the Protection of Human Rights and Fundamental Freedoms*, Article 3.

¹⁴ *Supra* note 6: *Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment*.

¹⁵ D. Helsinki et al, “Technology neutrality as a way to future-proof regulation: the case of the Artificial Intelligence Act”, Available at SSRN: <https://ssrn.com/abstract=5181085> (2025), p. 18.

This suggests fundamental rights, including human dignity, must be protected in both virtual and real-world environments, thereby raising the question whether such protection can be effectively ensured within the current legislative framework.

Moreover, it is noteworthy that the regulatory landscape within the EU remains fragmented, as there is no single legislative instrument that regulates the VE in its entirety. However, the EC has elaborated that these environments are regulated in the same way as other digital technologies and referred to myriad legislative frameworks like GDPR, DSA, DMA, et al.¹⁶ Nevertheless, these legislative acts apply to VEs to a certain extent. Given this, additional challenges arise regarding the determination and applicability of the liability of VE operators in practice.

Subsequently, academic discourse reflects this uncertainty. Eleonora Rosati¹⁷ and Ben Chester Cheong¹⁸ point out that current existing frameworks are inefficient because assigning liability to operators becomes complicated within advanced VEs like metaverses. Similarly, Amber Booth asserts that current regulations are ineffective in providing protection to individuals' rights in advanced VEs.¹⁹ In contrast, Rebecca K. Helm, Hitoshi Nasu²⁰, Giancarlo Frosio and Christophe Geiger²¹ disagree and emphasise that stricter liability obligations may unnecessarily limit free speech instead of protecting society.

Considering the expanding role of VEs in everyday life and the uncertainty of the existing legislative framework in the EU, this article aims to assess the effectiveness of current regulatory frameworks addressing operators of VEs' liability by reviewing regulatory frameworks within the EU and examining academic discourse using the SLR method, leading to recommendations aimed at strengthening the EU's regulatory approach.

¹⁶ European Commission, *An EU initiative on Web 4.0 and virtual worlds: a head start in the next technological transition* (2023 07 113); <<https://ec.europa.eu/newsroom/dae/redirection/document/97337>>, [accessed on 10 June, 2024], p. 4-5.

¹⁷ E. Rosati, "The localization of IP infringements in the online environment: from Web 2.0 to Web 3.0 and the Metaverse", *Journal of Intellectual Property Law & Practice* (2023, Vol. 18, No. 10), p. 724.

¹⁸ B. C. Cheong, "Avatars in the metaverse: potential legal issues and remedies", *International Cybersecurity Law Review*, (2022), p. 476.

¹⁹ A. Boothe, "The death and life of Jang Nayeon: a case for personality rights in the digital layers of reality", *International Journal of Law and Information Technology* (2022, 30), p. 416.

²⁰ R. K. Helm and H. Nasu, "Regulatory Responses to 'Fake News' and Freedom of Expression: Normative and Empirical Evaluation", *Human Rights Law Review* (2021, 21) p. 327.

²¹ G. Frosio and C. Geiger, "Taking fundamental rights seriously in the Digital Services Act's platform liability regime", *European Law Journal* (2023, Vol. 29, Issue 1-2), p. 36.

THE VIRTUAL ENVIRONMENT TECHNOLOGY: POTENTIAL RISKS AND LEGISLATIVE RESPONSES

Potential risks of virtual environments

First, to contribute to a comprehensive view of this article, it is necessary to examine the potential risks posed by VEs. Accordingly, this subsection analyses the risks based on relevant literature review.

Primarily, several scholars raise concerns about mental health and arising security risks. Lin Sternlicht and Aaron Sternlicht worry that it can be highly addictive, which can lead to loneliness and worsen mental health.²² This argument could find evidence in the way social media platforms have caused addictive behaviour. Moreover, other academics outline that it causes myriad security threats, such as identity theft, data tampering attacks, privacy leaks.²³ They state that one of the main problems is that it lacks regulatory clarity, leaving greater discretion to criminals.²⁴ In addition, Diogo Pacheco Gomes and Paula Zambelli Salgado Brasil expand the list of potential crimes by pointing out instances like: cyberbullying and cyberstalking.²⁵ In their opinion, these acts are likely to occur because perpetrators are difficult to identify and regulatory instruments are ineffective to address liability issues.²⁶ In consideration of the fact that these cybercrimes are highly related to sensitive information, it is crucial to have clear rights and obligations of users, operators, and third parties to create a safe environment.

Furthermore, as technology develops, types of crimes are becoming more diverse. Lorena Arismendy Mengua outlines that VEs offer users increasingly sophisticated technology that may result in a more intense user experience.²⁷ She states that it could create space for misconduct that can directly target user in control of an avatar.²⁸ To support her statement, the author refers to increasing instances of sexual assault in VEs since the launch of the virtual reality game “Second Life”.²⁹ All things considered, it can be asserted that the progressive VEs bring forth an abundance of legal issues related to both regular cybercrimes and crimes that are typically conducted in real-life scenarios.

²² L. Sternlicht and A. Sternlicht, *A New Age of Digital Addiction - What The Metaverse Means for Mental Health and Digital Addiction* (2022); <<https://www.familyaddictionsspecialist.com/blog/a-new-age-of-digital-addiction-what-the-metaverse-means-for-mental-health-and-digital-addiction>> [accessed on 2024-11-14].

²³ M. Azmi et al, “The Social Impact of VR Technology on Society: A Systematic Literature review“, *Ultimatics Jurnal Teknik Informatika* (2022: 14(2)), p. 60.

²⁴ Id.

²⁵ D. P. Gomes and P. Z. S. Brasil, “The economic dimension of human rights in the digital world“, *Revista Foco* (2025, 18 (1)), p. 11.

²⁶ Id.

²⁷ L. A. Mengua, "Liability for Wrongful Behaviour in the Metaverse," *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* (2024, 15, no. 3), p. 240.

²⁸ Id.

²⁹ Id.

Additionally, other scholars emphasise issues related to human dignity violations. Marcus Duwell, in his research on human dignity and ethics within technology development, came to the conclusion that technological advancements shape the way people live, resulting in limitation of decisions they make at their own discretion.³⁰ Furthermore, Amber Boothe, in her research based on the story of Jang Nayeon, who was virtually resurrected after her sudden death in a VE,³¹ agrees that the issues of autonomy emerge within such environments.³² In conclusion, it can be implied that the risk of violating human dignity increases due to deprivation of autonomy.

Overall, VE technology raises several challenges. The potential risks of VE include legal issues, emerging mental health problems, and violations of both privacy and dignity. As this article concentrates on the question of operators' liability related to violations of human dignity, this research will proceed to an overview of current legislative frameworks within the EU to determine whether legislative acts address the liability of VE operators for dignity violations.

Overview of the existing EU legal framework

After conducting an analysis of risks posed by VE, the research will provide an overview of the current legal framework considering operators' liability in the EU, mainly focusing on EC insights in “[an] EU initiative on Web 4.0 and virtual worlds: a head start in the next technological transition”.³³

Primarily, for more than two decades, one of the main legal instruments regarding the liability of service providers was ECD.³⁴ However, the European Parliament has recognised that it was designed for an earlier phase of the internet and might no longer be effective to address advanced environments.³⁵ Consequently, EU introduced DSA³⁶ and DMA³⁷ to determine liability and obligations for advanced virtual platforms. The main difference between these two acts is that DSA focuses on ensuring customer protection and DMA aims to establish a fair digital economy.³⁸ More precisely, the DMA concentrates on establishing a competitive and fair digital market, while the DSA focuses on the elimination of fake news, hate speech, and the protection of fundamental human rights. The DMA primarily addresses companies with a significant

³⁰ M. Düwell, “Human Dignity and the Ethics and Regulation of Technology”, article in the book: Roger Brownsword, Eloise Scotford, and Karen Yeung eds., *The Oxford Handbook of Law, Regulation and Technology*, (Oxford: Oxford University Press, 2017), p. 192-193.

³¹ *Supra* note 19: A. Boothe, p. 389-399.

³² *Supra* note 19: A. Boothe, p. 406.

³³ *Supra* note 16: EC, An EU initiative on Web 4.0 and virtual worlds: a head start in the next technological transition, [accessed on 01 December 2024].

³⁴ Directive (EU) 2000/31/EC.

³⁵ A. de Streel and M. Husovec, *The e-Commerce Directive as the Cornerstone of the Internal Market: Assessment and Options for Reform*, Study for the Committee on Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, May 2020.

³⁶ Regulation (EU) 2022/2065.

³⁷ Regulation (EU) 2022/1925.

³⁸ European Parliament, *EU Digital Markets Act and Digital Services Act Explained* (2021 12 14); <<https://www.europarl.europa.eu/topics/en/article/20211209STO19124/eu-digital-markets-act-and-digital-services-act-explained>> [accessed on 2024-12-01].

influence on the market and currently has only six designated gatekeepers that fall under its requirements: Apple, Amazon, Alphabet, Meta, ByteDance, and Microsoft.³⁹ On the other hand, DSA takes a broader approach; however, its effectiveness to safeguard fundamental human rights within the VEs remains questionable in the academic environment.⁴⁰

Furthermore, the GDPR⁴¹ is the main act to protect individuals' privacy.⁴² EC describes this act as technologically neutral, meaning that it is fully applied to the processing of personal data in VE as in real-life scenarios.⁴³ However, Bailly Martin emphasises that the most recent wave of innovations may raise concerns related to GDPR efficacy.⁴⁴ He states that consent processes should be enhanced for virtual avatars as users increasingly engage directly through them.⁴⁵ In addition, he points out blockchain's immutable nature, which might be challenging to align with "right to be forgotten" indicated in Article 17 of GDPR.⁴⁶ However, the European Digital Identity Regulation,⁴⁷ obligates member states to EU Digital Identity Wallets within 24 months after the adoption of the regulation. Digital Identity Wallets are intended for Member states to ensure that citizens share their personal information to the extent they wish.⁴⁸ Meaning that this digital document can share only specific personal information, without revealing one's full identity or other personal details, helping to protect individuals' privacy and may solve the inadequacy of GDPR in VE.

Moreover, the AI Act concentrates on AI developers setting out requirements and obligations concerning the use of AI systems.⁴⁹ This act aims to develop the reliability of AI technology by ensuring that it does not violate individuals' fundamental rights and respects ethical norms.⁵⁰ The regulatory framework promotes this by creating a risk-based approach, meaning that AI systems are categorised based on risk by enforcing stricter rules for higher-risk applications. On the other hand, scholars raise questions regarding accountability for complex systems with several components.⁵¹ Therefore, this leads to the question of regulating VEs with

³⁹ European Commission, *Gatekeepers*; <https://digital-markets-act.ec.europa.eu/gatekeepers_en> [accessed on 2024-12-01].

⁴⁰ See i.e: E. Hine et al, "Safety and Privacy in Immersive Extended Reality: An Analysis and Policy Recommendations", *Digital Society* (2024, 3:3), p. 1-40 and G. Frosio and C. Geiger, "Taking fundamental rights seriously in the Digital Services Act's platform liability regime", *European Law Journal* (2023, Vol. 29, Issue 1-2), p. 74-75.

⁴¹ Regulation (EU) 2016/679.

⁴² Id, Article 1.

⁴³ *Supra* note 16: EC, *An EU initiative on Web 4.0 and virtual worlds: a head start in the next technological transition*, [accessed on 2024-12-01], p. 5.

⁴⁴ B. Martin, "Privacy in a programmed platform: how The General Data Protection Regulation applies to the metaverse", *Harvard Journal of Law & Technology* (2022: vol. 36, no. 1), p. 256-259

⁴⁵ Id, p. 257.

⁴⁶ *Supra* note 44: B. Martin, p. 258.

⁴⁷ Regulation (EU) 2024/1183.

⁴⁸ Id, Article 1.

⁴⁹ Regulation (EU) 2024/1689.

⁵⁰ Id, Article 1.

⁵¹ H. Ruschmeier, "AI as a challenge for legal regulation – the scope of application of the artificial intelligence act proposal", *ERA Forum*, (2023: vol. 23), p. 372.

AI features. Evidently, AI is not an integral part of every VE; the obligations will not be applied to such environments.

Furthermore, it should be noted that users of VEs are also protected by the General Product Safety Regulation⁵² and Unfair Commercial Practices Directive⁵³ against misleading marketing practices, while intellectual property rights of operators and users in VE are protected by several EU legal instruments, including Copyright in the Digital Single Market,⁵⁴ the Protection of Trade Secrets⁵⁵ and the Regulation on the EU Trade Mark.⁵⁶

Overall, the overview of the relevant EU framework found that the DSA may be considered the main legal instrument to regulate liability regarding human dignity protection within VEs, as it has a significant impact on establishing accountability for violation of fundamental human rights. Since it is essential to evaluate its effectiveness within the academic environment, the research will proceed to the SLR, which will examine scholarly perspectives to identify strengths, limitations, and areas for potential improvement within the current regulatory framework.

RESEARCH METHODOLOGY: SYSTEMATIC LITERATURE REVIEW

As indicated above, the method chosen for this research is SLR, which will demonstrate transparent and replicable analysis of existing scholarly work on the matter of liability of VEs' operators.

Literature selection process

Developing and answering research questions from already existing literature is the essential component of extensive academic research.⁵⁷ One instance of such research methods is SLR. It can be defined as the identification, collection, and synthesis of prior academic literature on a particular topic.⁵⁸ This method will be used to answer the question of this article by identifying main regulatory aspects outlined by academics, categorizing them, subsequently, verifying the efficiency of the existing legal framework.

To identify the most assessed legal regulatory aspects, a qualitative content analysis is conducted to disclose knowledge on a particular topic. Qualitative content analysis is a social environment cognition method, which is used to interpret text-based data by systematically

⁵² Regulation (EU) 2023/988.

⁵³ Directive (EU) 2005/29/EC.

⁵⁴ Directive (EU) 2019/790.

⁵⁵ Directive (EU) 2016/943.

⁵⁶ Regulation (EU) 2017/1001.

⁵⁷ H. Snyder, "Literature review as a research methodology: An overview and guidelines", *Journal of Business Research* (2019, Vol. 104), p. 333.

⁵⁸ R. F. Baumeister and Mark R. Leary, "Writing Narrative Literature Reviews", *Review of General Psychology* (1997, Vol. 1, No. 3), p. 311.

analysing and classifying it.⁵⁹ The process of content analysis of legal research may be divided into following four stepwise stages: identifying and collecting the data needed for the analysis; coding the data; reporting; drawing conclusions and observations.⁶⁰

To fulfil the first step by identifying and collecting the data required for the analysis, a method of systematic literature selection was performed. The selection of academic literature is outlined in a step-by-step guide by Yannascoli et al. which includes a four-step procedure: identification, screening, eligibility, and inclusion.⁶¹

Prior to the identification stage, relevant terminology for the search was chosen through a pilot pre-screening of studies related to the research question on academic databases. Subsequently, chosen search terms were queried in every database used for the literature selection.

To perform a detailed SLR, it was essential to pre-screen literature on multiple information databases.⁶² In this case, the prior pre-screening was mainly concluded in the following electronic databases available in Vytautas Magnus University electronic library: EUR-Lex, Scopus, HeinOnline, Web of Science, and Oxford Journals Collection. Consequently, EUR-Lex, Oxford Journals Collection and Web of Science were chosen as literature sources due to their accuracy and quality of results, as well as greater convenience of search filters.

In the identification phase, the final literature selection for this research was conducted in February 2025. The search was performed using the following keywords: “*platform liability*”, “*intermediary liability*”, as well as “*dignity*” AND “*platform*” AND “*liability*”. An overall total of 4720 academic and 80 legal publications were found. However, since it was not practical to read all publications in depth, the following criteria were selected to decide what to include in the subsequent screening phase:

1. Date of publication. The scope of the review is limited to a selected set of academic articles and EU case-law from 2020 until the moment of research, considering the rapid development of technologies and the EC presentation of strategy “Shaping Europe’s Digital Future” where the most recent legislative framework regarding operators’ liability – DSA, was introduced.⁶³
2. Type of publication. The scope of the review is limited to academic articles in Oxford Journals Collection and Web of Science databases to ensure the use of credible and peer-reviewed publications. Furthermore, in EUR-Lex, preparatory documents were excluded, leaving only legal acts and case-law, since this review aims to compare them with academic publications.
3. Publication language. The scope of the review is limited to publications written in English language, to eliminate the risk of misinterpretation.

⁵⁹ V. Žydzūnaitė ir S. Sabaliauskas, *Kokybiniai tyrimai: principai ir metodai: vadovėlis socialinių mokslų studijų programų studentams* (Vilnius: Vaga, 2017), p. 57.

⁶⁰ P. Astromskis, *The Legal Regulation Framework for the Artificial General Intelligence* (doctoral thesis, Doctoral Programme in Law, Universitat Pompeu Fabra), p. 94.

⁶¹ S. M. Yannascoli et al., “How to Write a Systematic Review: A Step-by-Step Guide”, *University of Pennsylvania Orthopaedic Journal* (2013, Vol. 23), p. 66.

⁶² Id, p. 65.

⁶³ European Commission, *Shaping Europe’s Digital Future* (Luxembourg: Publications Office of the European Union, 2020).

4. Accessibility. The scope of the review is limited to academic articles that are open access.
5. Field of science. The scope of the inclusion is limited to academic articles from Oxford Journals Collection subject area – Social Sciences and Law, while Web of Science fields of Law and Information Science Library Science.

Screening by using the above-mentioned criteria excluded 4730 publications, leaving 63 academic articles and 7 legal documents for further eligibility assessment. At this stage of the selection, duplicates were removed, and abstracts, introductions, and conclusions were reviewed to identify and exclude irrelevant sources based on content. In addition, 7 strongly relevant publications were selected to achieve more accurate results. Consequently, a total of 27 publications were left for the inclusion of in-depth content analysis. The full process of literature selection is reflected below:

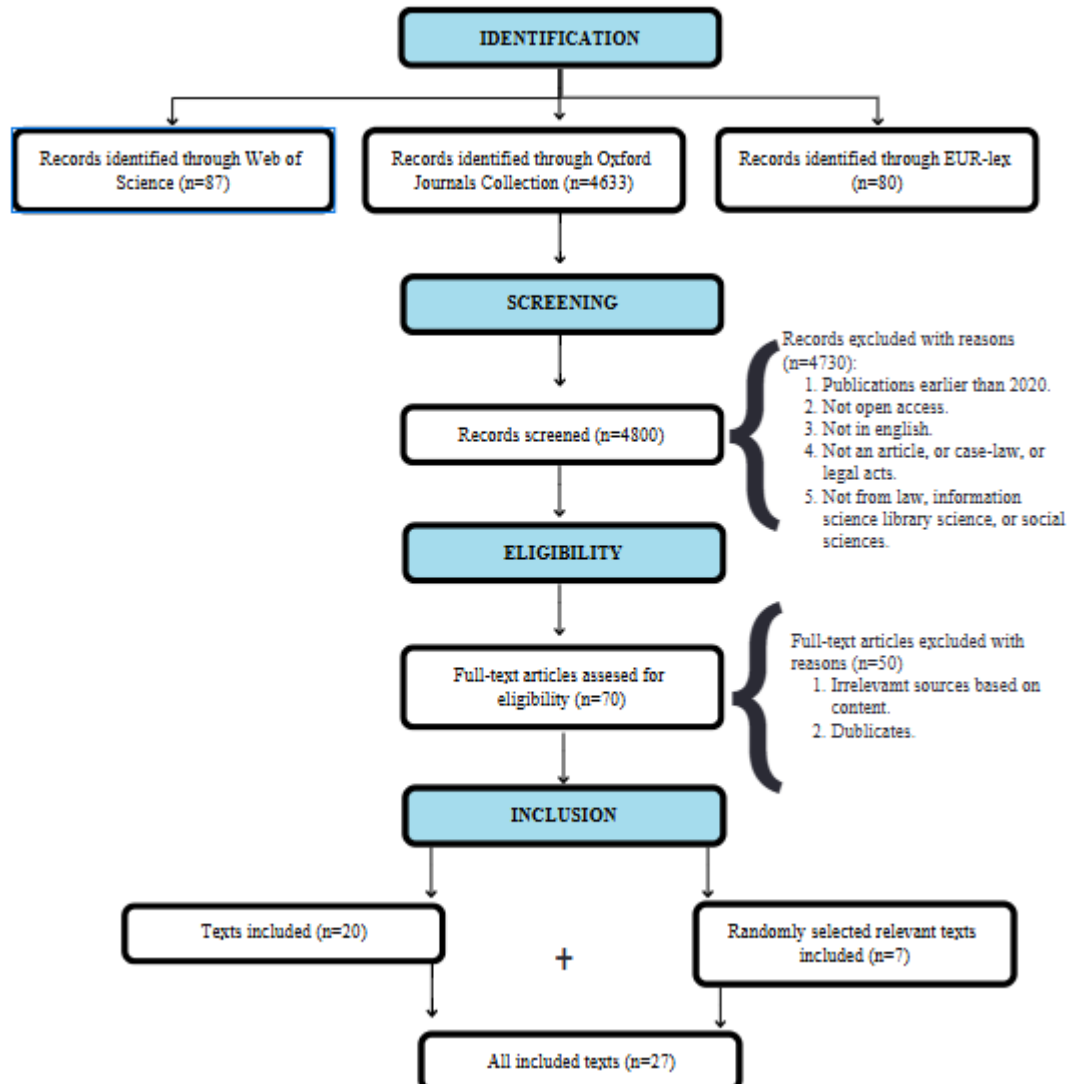


Figure 1. Literature search and inclusion for further analysis.

Data extraction and coding

The second stage of analysis involved extracting quotes from the selected literature and coding this data. To carry this out inductive qualitative content coding technique was chosen.

This technique includes the following stages: open coding, material grouping, exclusion of sections and subsections, and abstraction.⁶⁴

Open coding consists of the extraction of quotes relevant to the research question. Primarily, every article was viewed, and quotes related to this article's topic were extracted. Subsequently, there were a total of 63 quotes were extracted and included for further analysis.

Accordingly, this material was grouped into 2 different sections: “Liability regimes of digital platforms and their influence on digital ecosystem” and “Regulatory issues and future development”, each containing the same number of citations.

Consequently, collected quotes were placed in specific subsections. The the first section was broken down into subsections: “Direct liability”, “Secondary liability”, “Platform behaviour”, while the second one into: “Assessment of legal effectiveness and societal impact” and “Future regulatory development to platform liability”. The highest percentage of extracted citations, to be more precise, 40.3%, fell under the subsection – “Assessment of legal effectiveness and societal impact”. This implies that aspects related to effectiveness and uncertainty of existing legal frameworks is examined the most within the academic environment. A graph reflecting the proportion of every subsection in percentages is presented below:

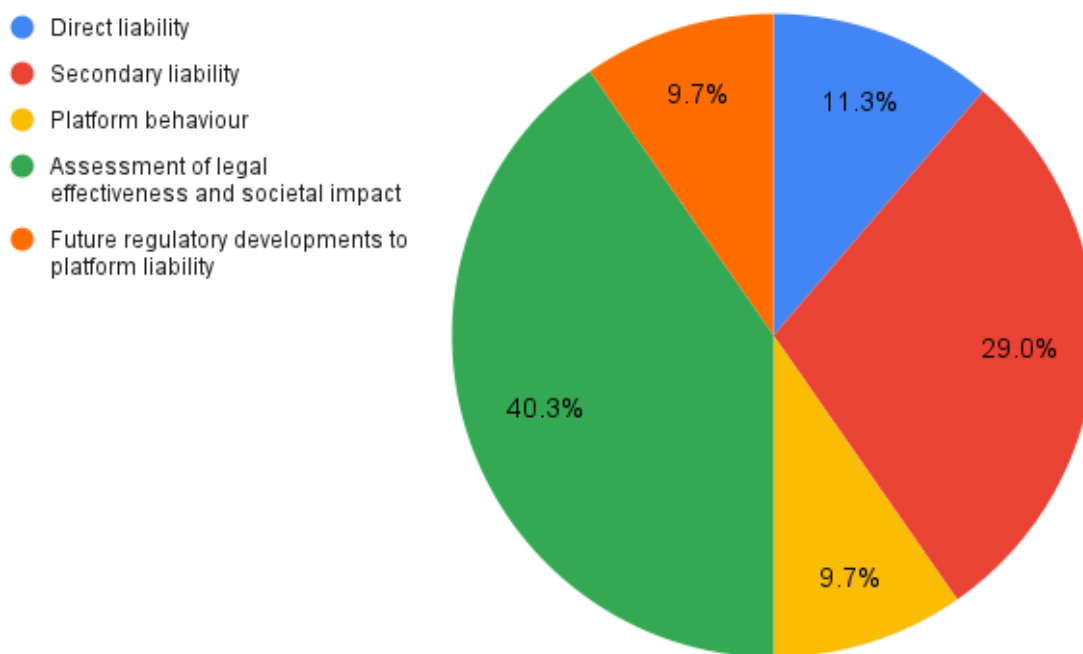


Figure 2. Proportion of each subsection.

⁶⁴ *Supra* note 59: V. Žydzūnaitė and S. Sabaliauskas, p. 70.

Methodical limitations

Primarily, the SLR was performed using subjectively chosen keywords and databases, therefore, there may be relevant literature available that is not included in this research. Nevertheless, the selected publications were efficient in solving the question of this research. Regardless, this limitation should be perceived as a suggestion for continued study by including different keywords, using other databases, et cetera.

Ultimately, due to the limited scope of this article, the research focuses solely on the liability of operators for actions within their created VE. As a result, the liability that end users face goes beyond the scope of this article. Nevertheless, this lays the groundwork for further research in the future.

OVERVIEW OF THE RESEARCH FINDINGS AND DISCUSSION

Considering systematically selected literature and data extracted from it, the research will proceed to analyse this data by organising it into thematic parts corresponding to the subsections established in the methodology part. Accordingly, the assessment of the current legislative framework's effectiveness and suggestions for regulatory enhancements regarding the accountability of VE operators for violations that offend human dignity in a contemptuous and degrading way will be addressed.

Direct liability

Direct liability is rarely imposed on digital platforms, although it is examined by some scholars. Within the legal framework, there is one definitive instance of direct liability established in the Directive on Copyright in the Digital Single Market.⁶⁵ To be more precise, Article 17 of it outlines that online sharing platforms can be held liable for copyright infringement if they display content uploaded by their users without the right-holder's permission.⁶⁶ The following subsection analyses the academic debate regarding this liability regime.

The plain idea of assigning direct liability to operators of VEs is perceived differently. Giancarlo Frosio explains that this regulatory approach enables linking non-professional users to professional service providers which may create liability-free space for the users.⁶⁷ This implies that operators are directly linked to users' behaviour who benefit from this liability regime because they are not held accountable for their actions. Additionally, he points out that imposing direct liability on digital platforms for their users' activity might stifle innovations because

⁶⁵ *Supra* note 54: Directive 2019/790.

⁶⁶ *Id.*, Article 17.

⁶⁷ G. Frosio, "It's all Linked: How Communication to the Public Affects Internet Architecture", *Computer Law & Security Review* (2020, 37, 105410), p. 21.

platforms may not be able to overview large amount of data.⁶⁸ Luis Roberto Barroso and Luna van Brussel build upon that by indicating that this regime may be destructive due to limited control of platforms within their created environments.⁶⁹ Overall, it can be concluded that data controlled by these platforms are extensive, therefore, it cannot be completely overlooked, which, subsequently, makes direct liability defective.

On the other hand, Directive on Copyright in the Digital Single Market provides an exemption from direct liability by encouraging online sharing platforms to make “best efforts” to obtain authorization.⁷⁰ This provision aims to encourage digital platforms to work with right holders of specific protected matter.⁷¹ However, within the academic environment, this is perceived more as an obligation than an exemption, since platforms are forced to take inevitable measures and filtering tools to ensure compliance and to avoid liability.⁷² Consequently, it is believed to unnecessarily limit free speech, as well as freedom of business and innovation.⁷³ In addition, Lucas Blackwell implies that platforms are entitled to take their own measures, which may not be effective at all, but they would be exempted from liability,⁷⁴ as the concept of “best efforts” is not outlined directly within the legal document and relevant case-law. Taking into account these concerns, the exemption arising from this legal act has two very clear drawbacks: first, it obliges platforms to filter users’ content which may result in stifle of innovations and freedom of speech limitations, second, online sharing platforms have considerable discretion in interpreting the exemption in question, which may eliminate the opportunity of assigning liability to operators of the online sharing platforms.

Overall, considering ideas enshrined in academic articles, the direct liability regime appears to contribute to users’ protection from liability. In contrast, a greater number of scholars in their publications tend to emphasise the negative aspects of it caused by the nature of digital environments and the inaccuracy of the existing legal framework, such as freedom of speech limitations, stifling of innovations, and excessive platform autonomy in deciding on their “best efforts” which ultimately undermines the effectiveness of this legal instrument.

Secondary liability

Mainly, digital platforms face secondary liability regarding users conducted activity. Therefore, this liability regime is analysed more broadly by academics due to its greater

⁶⁸ *Supra* note 67: G. Frosio, p. 21.

⁶⁹ L. R. Barroso and L. van B. Barroso, "Democracy, Social Media, and Freedom of Expression: Hate, Lies, and the Search for the Possible Truth", *Chicago Journal of International Law* (2023, 24, no. 1), p. 65.

⁷⁰ *Supra* note 54: Article 17, part 4.

⁷¹ C. Geiger and B. J. Jutte, "Copyright as an Access Right: Concretizing Positive Obligations for Rightholders to Ensure the Exercise of User Rights", *GRUR International* (2024, 73(11)), p. 1029.

⁷² Advocate General Saugmandsgaard Øe, Opinion of Advocate General Saugmandsgaard Øe, delivered on 16 July 2020, Joined Cases C-682/18 and C-683/18, Frank Peterson v Google LLC and Others; Elsevier Inc. v Cyando AG.

⁷³ *Supra* note 67: G. Frosio, p. 21.

⁷⁴ L. Blackwell, "The Death of Article 17: How the CJEU in Poland V. Parliament created a framework which prevents holding Youtube liable for copyright infringement under Directive (EU) 2019/790", *Southwestern Journal of International Law* (2024, 30, no. 1), p. 192.

relevance. It should be noted that intermediary liability discussed in academic articles is considered as a subset of secondary liability.

The first EU legal framework that introduced a regulatory approach to digital environments regarding their liability was ECD, which is critically assessed within the academic environment. The main discussed provision is Article 14 of ECD, which protects virtual platforms from liability in cases when they have no knowledge of the misconduct or when they remove illegal content immediately it appears on the network.⁷⁵ For instance, Henrik Saugmandsgaard Øe questions the effectiveness because, from his point of view, Article 14 of ECD ensures liability exemption in the majority of cases.⁷⁶ He states that the only definitive case when a platform operator does not have any knowledge is when they intentionally assist users in carrying out illegal activities.⁷⁷ In light of this, the clause makes it hard to prove that platforms were aware of users' wrongdoings; therefore, assigning liability to platforms becomes complicated.

In response to the inadequacies of the legal framework defined above, particularly given the pace of technological development, the EU introduced another legal framework – DSA. It integrated pre-existing liability rules from ECD and expanded them further. To elaborate upon this, Articles 4 and 5 of DSA were transferred from ECD regarding mere conduit and caching service providers.⁷⁸ However, liability obligations regarding hosting services were slightly changed. More precisely, Kinga Sorban outlines that it introduced two types of hosting services: ones that simply store users' content and others that enable user interaction.⁷⁹ Considering the nature of VEs, it can be concluded that it falls under hosting service providers.

Additionally, scholars emphasise that DSA takes a step further compared to the ECD. Primarily, DSA introduces a “*Good Samaritan*” clause, enshrined in Article 7, which provides legal certainty that digital platforms will not be liable for voluntary monitoring.⁸⁰ Given this, it can be asserted that DSA provides additional platform-friendly clauses. Furthermore, Baiyang Xiao,⁸¹ Joao Pedro Quintais and Sebastian Felix Schwemer⁸² state that DSA sets up a more detailed procedure on liability regime by imposing due diligence obligations in Chapter II of the DSA. Regarding the latter obligations, they vary based on the size and nature of the digital platform, for instance, VLOPs and VLOSEs face stricter rules that rely on risk assessments. These risk assessments are outlined by Xinyi Tu and Bruna de Castro e Silva as a key proactive measure to foresee negative effects on violations of fundamental human rights.⁸³ The authors add that

⁷⁵ *Supra* note 21: G. Frosio and C. Geiger, p. 38.

⁷⁶ *Supra* note 72: Advocate General Saugmandsgaard Øe.

⁷⁷ *Id.*

⁷⁸ See: Regulation (EU) 2022/2065, Articles 4,5, and Directive 2000/31/EC, Articles 12, 13.

⁷⁹ K. Sorban, “An elephant in the room—EU policy gaps in the regulation of moderating illegal sexual content on video-sharing platforms”, *International Journal of Law and Information Technology* (2023, 31), p. 174.

⁸⁰ C. Cauffman and C. Goanta, “A New Order: The Digital Services Act and Consumer Protection”, *European Journal of Risk Regulation* 12 (2021, no. 4), p. 774.

⁸¹ B. Xiao, “Making the private public: Regulating content moderation under Chinese law”, *Computer Law & Security Review* (2023, Vol. 51, 105893), p. 12.

⁸² J. P. Quintais and S. F. Schwemer, “The Interplay between the Digital Services Act and Sector Regulation: How Special Is Copyright?” *European Journal of Risk Regulation* (2022, 113), p. 201.

⁸³ X. Tu and B. de C. e Silva, “Are We Ready for the Metaverse? Implications, Legal Landscape, and Recommendations for Responsible Development”, *Digital Society* (2025, 4:9), p. 10-11.

human dignity is protected by DSA's Recital 67 and Article 25, where dark patterns are prohibited.⁸⁴ They define dark patterns as “*practices of deceiving or nudging users and distorting or impairing their autonomy, decision-making, or choice*”.⁸⁵ Given this, it can be asserted that operators' liability regarding violation of human dignity in particularly contemptuous and degrading behaviour within their environments is ensured.

Furthermore, scholars analyse the facets of VLOPs and VLOSEs in more detail. Thales Martini Bueno and Renan Gadoni Canaan add that governance within VLOPs will be ensured with independent coordinators who will implement the law at the national level with the opportunity to apply administrative sanctions.⁸⁶ To expand upon these obligations, Bram Duivenvoorde and Catalina Goanta specify that DSA imposes a duty to comply with every regulatory sector in relation with VE.⁸⁷ Meaning that content moderation obligations should be established broadly to prevent any wrongdoings within VEs. However, Recital 76 of DSA indicates that VLOPs and VLOSEs are considered platforms with a higher volume of societal impact, more precisely, having at least 45 million users.⁸⁸ This implies that risk assessments are not mandatory within smaller VEs; therefore, such platforms are not obliged to obtain proactive measures and are not held liable for human dignity misconducts unless it is removed after they are aware of it.

Overall, DSA can be considered the main legal framework in the EU that regulates operators' liability regarding human dignity violations. It should be noted that liability obligations were incorporated from ECD and supplemented with due diligence obligations, along with stricter rules for larger platforms. In addition, analysis found that DSA can be applied to assign liability to operators of VEs because these platforms fall under hosting services, however, proactive measures that are most effective to safeguard human dignity are only applied to bigger VEs, leaving smaller platforms aside.

Platform behaviour

Since the change in the legal framework undoubtedly affects the behaviour of operators, this aspect is analysed by scholars as well. Accordingly, the following subsection will outline the main ideas.

Primarily, scholars shed light on excessive content removal. Rebecca K. Helm and Hitoshi Nasu emphasise that the expansion of liabilities on intermediaries may encourage online platforms to censor more information to ensure efficient identification of illegal content, which may result in editorial behaviour of the platform.⁸⁹ Considering this, it can be implied that

⁸⁴ Id, p. 12.

⁸⁵ Id.

⁸⁶ T. M. Bueno and R. G. Canaan, "The Brussels Effect in Brazil: Analysing the impact of the EU digital services act on the discussion surrounding the fake news bill", *Telecommunications Policy* (2024, 48, 102757), p. 5.

⁸⁷ B. Duivenvoorde and C. Goanta, "The regulation of digital advertising under the DSA: A critical assessment", *Computer law & security review* 51 (2023, 105870), p. 6.

⁸⁸ *Supra* note 36: Regulation 2022/2065, Recital 76.

⁸⁹ *Supra* note 20: R. K. Helm and H. Nasu, p. 327.

platforms take on an additional role which arguably should be the concern of platforms. Additionally, Sarah Zarmsky adds that these liability obligations already caused adverse effects in platforms removing illegal content, which could have served as evidence for the prosecution.⁹⁰ This demonstrates a risky approach to digital evidence, which is a result of over-removal that platforms conduct to prevent accountability.

Furthermore, others distinguish the effect of stringent liability rules, causing economic consequences. Henrik Saugmandsgaard Øe asserts that holding operators liable for actions committed by their end users solely because they are aware of it may discourage innovation and its development.⁹¹ Yassine Lefouili and Leonardo Madio share a similar view and emphasise that the overall cost of platforms to provide their services will increase due to stricter liability obligations emerging with new legal frameworks, resulting in platforms stepping back from innovation implementation.⁹² In addition, they state that this could lead to higher business entry barriers, resulting in diminished competition.⁹³ Ultimately, considering that bigger platforms face more stringent liability, they assert that it may encourage transfer of illegal content to smaller platforms that are not regulated.⁹⁴ Therefore, it can be highlighted that stricter liability rules encourage platforms to stifle innovations, transfer illegal content to smaller platforms, and it may pressure smaller platforms to exit the business due to the high costs of obtaining compliance.

All things considered, a stringent liability regime may lead platforms to editorial behaviour, whereas this could result in the removal of the information that may be necessary for prosecution. Moreover, it is believed that stricter liability obligations on bigger platforms may transfer illegal content to smaller platforms. Ultimately, it may encourage operators of virtual platforms to stifle their innovation or even step back from the market due to the high costs of compliance.

Assessing legal effectiveness and societal impact

The increased attention to operators' liability within VEs led to debates among scholars regarding the effectiveness of current framework and its social outcomes. Therefore, scholarly perspectives regarding the above-mentioned matters will be reviewed below.

First, the majority of scholars emphasise the potential occurrence of unnecessary over-enforcement and freedom of speech limitations emerging with it. Scholars agree that imposing stricter liability rules may lead to over-filtering to avoid responsibility, which is likely to affect freedom of speech rather than the protection of society.⁹⁵ Moreover, Rebecca K. Helm and

⁹⁰ Sarah Zarmsky, "Is International Criminal Law Ready to Accommodate Online Harm?", *Journal of International Criminal Justice* (2024, 22), p. 180.

⁹¹ *Supra* note 72: Advocate General Saugmandsgaard Øe.

⁹² Y. Lefouili and L. Madio, "The economics of platform liability", *European Journal of Law and Economics* (2022, 53), p. 338.

⁹³ *Id.*, p. 339.

⁹⁴ *Id.*, p. 346.

⁹⁵ See: B. Sander, "Democratic Disruption in the Age of Social Media: Between Marketized and Structural Conceptions of Human Rights Law", *The European Journal of International Law* (2021, Vol. 32 no. 1), p. 170-171; *Supra* note 153: Advocate General Saugmandsgaard Øe.; Kebene Wodajo, "The user

Hitoshi Nasu are sceptical of content removal in cases where members of online platforms are aware of the suppressed information and outlined the term of “*Streisand effect*”.⁹⁶ This phenomenon occurs when content removal draws increased attention, potentially resulting in adverse consequences, i.e. society considering such actions as conspiracy.⁹⁷ Overall, the main issues emerging with the current legislative framework encouraging filtering are excessive limitation of freedom of speech, debates within VEs and unnecessary attention to removed content.

In addition, several scholars highlight the negative outcomes regarding economic development within a stricter liability regime. Giancarlo Frosio analyzes the algorithmic enforcement and concludes that legislative reforms imposing liabilities on digital platforms may result in digital architecture with less links, accesses, and innovations.⁹⁸ Lorena Arismendy Mengua agrees with this by emphasising the impact on internet access and expands on the latter perspective by pointing out that stricter obligations might favour larger intermediaries as they are more resourceful compared to the smaller competitors.⁹⁹ Ultimately, Caroline Cauffman’s and Catalina Goanta’s outline the general opinion on the diverse legislative reform: some find it daring, while others see it as too strict.¹⁰⁰ From their point it reflects the necessity to safeguard fundamental human rights in private spheres of technology and the importance of obtaining regulatory frameworks that nurture innovation and further economic development.¹⁰¹

Moreover, scholars examine whether existing legal frameworks are sufficient to regulate more advanced VEs. Primarily, Kinga Sorban states that the current legal framework focuses on balancing the interests of online platforms instead of prioritising assurance of victim protection and law enforcement.¹⁰² Meaning that protection of human dignity might be overlooked by the legislator. Moreover, Amber Boothe states that it is challenging to identify a liable party within VEs due to their immersive nature,¹⁰³ while Diogo Pacheco Gomes and Paula Zambelli Salgado Brasil build upon that by outlining that the existing legal framework cannot keep up with the technological development.¹⁰⁴ Ben Chester Cheong adds that the issue of assigning liability becomes even more challenging with decentralised VEs, as the identification of the operator is complicated.¹⁰⁵ To clarify his point, he illustrates his argument by noting that Satoshi Nakamoto, who is only a presumed creator of Bitcoin, cannot be sued for actions within the Bitcoin blockchain.¹⁰⁶ This implies that advanced VEs may be regulated by the existing legal instruments. However, not all violations will be adequately addressed because of their complex nature that blends with reality or operates in a decentralised system.

state: an alternative reading of the state role and duty in the age of platformized harm”, *International Journal of Law and Information Technology* (2023, 31) p. 10; *Supra* note 25: R. K. and H. Nasu, p. 327.

⁹⁶ *Supra* note 20: R. K. Helm and H. Nasu, p. 321.

⁹⁷ *Id.*

⁹⁸ *Supra* note 67: G. Frosio, p. 23.

⁹⁹ *Supra* note 27: L. A. Mengua, p. 238.

¹⁰⁰ *Supra* note 80: C. Cauffman and C. Goanta, p. 759.

¹⁰¹ *Id.*

¹⁰² *Supra* note 79: K. Sorban, p. 175.

¹⁰³ *Supra* note 19: A. Boothe, p. 407.

¹⁰⁴ *Supra* note 25: D. P. Gomes and P. Z. S. Brasil, p. 14.

¹⁰⁵ *Supra* note 18: B. C. Cheong, p. 476.

¹⁰⁶ *Id.*

It is also important to emphasise the uncertainty emerging with the setting of territorial jurisdiction for online harms. Eleonora Rosati outlines that challenges might arise regarding the determination of applicable jurisdiction, as the nature of VEs makes it difficult to connect a particular factor to a territory.¹⁰⁷ This view is also shared by Sarah Zarnsky, who emphasises that hate speech may be perpetrated from multiple states or even anonymous users using virtual private network services, resulting in difficulty in determining both territorial jurisdiction and legal basis for prosecution.¹⁰⁸ Nevertheless, this issue primarily concerns end-users' liability rather than operators'.

In conclusion, an overview of scholarly opinions reveals that existing liability regimes of digital environments are not efficient enough and bring forth an abundance of societal implications. The analysis of selected publications found that the main concerns emerging from the complex nature of VEs are related to the identification of operators in decentralised VEs and the determination of the jurisdiction of end users. In contrast, scholars argue that existing legal frameworks currently risk over-enforcement, which results in limitation of free speech, accessibility of technologies, stifle of innovations, and unfair competition between bigger and smaller entities.

Future regulatory developments on platform liability

In the prior subsection, researchers expressed their doubts on the effectiveness of the current legislative framework. Therefore, further analysis will move on to the overview of scholarly suggestions regarding the future developments of legal environments.

Scholars primarily provide recommendations regarding the safeguard of both freedom of expression and safety of VEs by emphasising the need for policymakers to stay open-minded within more advanced VEs like metaverses.¹⁰⁹ It can be asserted that these suggestions are broad in scope; therefore, can be considered negligible in enhancing the legislative environment. However, Giancarlo Frosio and Christophe Geiger propose the intervention of an independent regulatory authority, which would ensure both the protection of fundamental human rights and compliance.¹¹⁰ Nonetheless, the latter recommendation is insignificant as DSA enshrines an obligation for member states to designate a “Digital Services Coordinator” to ensure harmonization of this regulation.¹¹¹

Moreover, some attention is also devoted to jurisdictional concerns. As some scholars outline the issue of determining territorial jurisdiction, Eleonora Rosati suggests either extending the territorial competence of countries or imposing geo-blocking on online platforms to divide

¹⁰⁷ *Supra* note 17: E. Rosati, p. 722

¹⁰⁸ *Supra* note 90: S. Zarnsky, p. 176

¹⁰⁹ See: J. M. Ptaschunder, *Human Rights Online: Towards a New Generation of Human Rights in the Virtual World* (Columbia University, Graduate School of Arts and Sciences, 2024); *Supra* note 11: D. P. Gomes and P. Z. S. Brasil, p. 13; *Supra* note 10: X. Tu and B. de C. e Silva, p. 23.

¹¹⁰ *Supra* note 21: G. Frosio and C. Geiger, p. 36

¹¹¹ *Supra* note 36: Regulation 2022/2065, Article 49.

into territories.¹¹² However, DSA is implemented in every member state of the EU, meaning that jurisdiction issues are more relevant to parties that are not governed by this legal instrument.

Ultimately, it can be concluded that the ideas collected from the selected literature are not well-developed and lack substantial weight. Scholars primarily focus on outlining the balance of protecting free speech and preventing harmful activities; however, specific suggestions on how to change current EU frameworks are not specified. Nevertheless, the idea regarding territorial competence application of geo-blocking is more developed but remains irrelevant to operators as DSA aims to harmonise rules within EU borders that minimise jurisdictional risks.

CONCLUSION

The problem addressed in this article was whether the operators of VEs can be held liable for actions within those environments that are offensive to human dignity in contemptible and degrading behaviour. The chosen research methodology involved SLR, through which academic literature was collected and synthesised to identify regulatory aspects of operators' liability and verify the adequacy of current EU legislative frameworks, as well as to review scholars' views on future developments. After conducting the research using the described methodology, which aims to address the effectiveness of current legislative frameworks in the EU, the following conclusions were drawn:

1. Operators of VEs face direct liability for actions within these environments solely for copyright infringements. Considering scholars' opinions, this liability regime benefits users as it shifts the burden of responsibility to operators. This type of liability is unlikely to protect human dignity from illegal activities carried out in particularly contemptuous and degrading behaviour due to the high amount of data that VEs control, which may result in applications of algorithmic tools that would lead to over-enforcement rather than to the protection of fundamental human rights. In addition, a liability-free space environment for users may be assessed negatively because it could increase instances of violations conducted by users, subsequently, causing more harm to other users.
2. The main EU legislative framework addressing operators' liability regarding the protection of human dignity ought to be DSA, which enshrines intermediary liability to operators if individuals' rights are breached within their controlled environment. SLR revealed that academics mainly address the differences among DSA and ECD, from which liability rules were moved to and supplemented with due diligence obligations and stringent rules for bigger VEs. It was found that stringent liability rules that rely on proactive measures, such as risk assessments, are believed to be the most effective in preventing human dignity violations carried out in contemptuous and degrading behaviour. However, smaller VEs would not be obliged to take proactive measures, therefore, safeguarding human dignity there is likely to be ineffective.
3. A stringent liability regime might lead to editorial behaviour of virtual platforms and transfer of illegal activities to smaller platforms where liability obligations are not as strict. In addition, the current legislative framework is believed to diminish competition

¹¹² *Supra* note 17: E. Rosati, p. 722.

and reduce innovative solutions, which implies that stricter rules ensuring effective safeguard of human dignity would intensify these outcomes.

4. The analysis of views enshrined in the selected literature found that DSA brings forth an abundance of negative societal outcomes, however, it is inefficient to address more advanced VEs. On one hand, scholars distinguish that a stringent liability regime coming into force with the DSA may result in reduced accessibility of technologies, unfair competition between bigger and smaller platforms, and unnecessary limitation of free speech caused by over-enforcement, which may be applied by operators to prevent risks of facing liability. On the other hand, other scholars emphasise the complex nature of advanced VEs that brings forth issues of determining jurisdiction and identifying operators of decentralised VEs, which may result in failure to assign liability.
5. The SLR found that the suggestions of future development within the academic environment lack development or are irrelevant to regulating operators' liability. To be more precise, most recommendations rely on general observations, such as requiring a balance of free speech and harmful activities, and considerations of applying geo-blocking and extending territorial competence to resolve the issue with jurisdiction are mainly relevant to end users' accountability.

RECOMMENDATIONS

Considering the findings of the SLR, the legal landscape within the rapid technological development lacks certainty. Therefore, several regulatory gaps persist, specifically referring to more advanced VEs. Therefore, it is recommended:

1. To maintain focus on ensuring secondary liability to operators VEs, rather than imposing direct liability. The reason for this is that it is practically impossible for operators to control the extensive data that is stored within VEs, making this type of instrument inefficient and creating a liability-free space for users who could misuse it for adverse purposes.
2. To complement the main legislative framework, the DSA, with a separate category applicable to operators of VEs, where proactive measures would be outlined, similar to those designed for VLOPs and VLOSEs. This would create risk assessments for smaller platforms and pose higher risks to decentralised VEs as current regulatory frameworks cannot effectively impose liability obligations to operators of such environments.

LEGAL REFERENCES

Legislation

1. European Union. Charter of Fundamental Rights of the European Union. 2012.
2. Constitution of the Republic of Lithuania. 1992.

3. Council of Europe. European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14. ETS No. 5. Rome. 1950.
4. Directive (EU) 2000/31/EC.
5. Directive (EU) 2005/29/EC.
6. Directive (EU) 2016/943.
7. Directive (EU) 2019/790.
8. Regulation (EU) 2016/679.
9. Regulation (EU) 2017/1001.
10. Regulation (EU) 2022/1925.
11. Regulation (EU) 2022/2065.
12. Regulation (EU) 2023/988.
13. Regulation (EU) 2024/1183.
14. Regulation (EU) 2024/1689.
15. United Nations. Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment. 1984.

Special literature

16. Astromskis, Paulius. The Legal Regulation Framework for the Artificial General Intelligence. Doctoral thesis, Doctoral Programme in Law, Universitat Pompeu Fabra.
17. Barroso, Luis Roberto and Barroso, Luna van Brussel. "Democracy, Social Media, and Freedom of Expression: Hate, Lies, and the Search for the Possible Truth". Chicago Journal of International Law (2023, 24, no. 1).
18. Baumeister, Roy F., and Leary, Mark R.. "Writing Narrative Literature Reviews". Review of General Psychology (1997, Vol. 1, No. 3).
19. Blackwell, Lucas. "The Death of Article 17: How the CJEU in Poland V. Parliament created a framework which prevents holding Youtube liable for copyright infringement under Directive (EU) 2019/790". Southwestern Journal of International Law (2024, 30, no. 1).
20. Boothe, Amber. "The death and life of Jang Nayeon: a case for personality rights in the digital layers of reality". International Journal of Law and Information Technology (2022, 30).
21. Bueno, Thales Martini and Canaan, Renan Gadoni. "The Brussels Effect in Brazil: Analysing the impact of the EU digital services act on the discussion surrounding the fake news bill". Telecommunications Policy (2024, 48, 102757)..
22. Cauffman, Caroline and Goanta, Catalina. "A New Order: The Digital Services Act and Consumer Protection". European Journal of Risk Regulation 12 (2021, no. 4).
23. Duivenvoorde, Bram and Goanta, Catalina. "The regulation of digital advertising under the DSA: A critical assessment". Computer law & security review 51 (2023, 105870).

24. Düwell, Marcus. "Human Dignity and the Ethics and Regulation of Technology". Article in the book: Roger Brownsword, Eloise Scotford, and Karen Yeung eds., *The Oxford Handbook of Law, Regulation and Technology*. Oxford: Oxford University Press, 2017.
25. European Commission. *Shaping Europe's Digital Future*. Luxembourg: Publications Office of the European Union, 2020.
26. Frosio, Giancarlo and Geiger, Christophe. "Taking fundamental rights seriously in the Digital Services Act's platform liability regime". *European Law Journal* (2023, Vol. 29, Issue 1-2).
27. Frosio, Giancarlo. "It's all Linked: How Communication to the Public Affects Internet Architecture". *Computer Law & Security Review* (2020, 37, 105410).
28. Geiger, Christophe and Jutte, Bernd Justin. "Copyright as an Access Right: Concretizing Positive Obligations for Rightholders to Ensure the Exercise of User Rights". *GRUR International* (2024, 73(11)).
29. Gomes, Diogo Pacheco and Zambelli Salgado Brasil, Paula. "The economic dimension of human rights in the digital world". *Revista Foco* (2025, 18 (1)).
30. Helm, Rebecca K. and Nasu, Hitoshi. "Regulatory Responses to 'Fake News' and Freedom of Expression: Normative and Empirical Evaluation". *Human Rights Law Review* (2021, 21).
31. Hine, Emmie et al. "Safety and Privacy in Immersive Extended Reality: An Analysis and Policy Recommendations". *Digital Society* (2024, 3:3).
32. Jabar, Bakti Amirul, Azmi, Millia, Hernando, Graciél and others. *The Social Impact of VR Technology on Society: A Systematic Literature review*. *Ultimatics Jurnal Teknik Informatika* (2022: 14(2)).
33. Lefouili, Yassine and Madio, Leonardo. "The economics of platform liability". *European Journal of Law and Economics* (2022, 53).
34. Martin, Baily. "Privacy in a programmed platform: how The General Data Protection Regulation applies to the metaverse". *Harvard Journal of Law & Technology* (2022: Vol. 36, no. 1).
35. Mengua, Lorena Arismendy. "Liability for Wrongful Behaviour in the Metaverse". *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* (2024, 15, no. 3).
36. Ojanen, Atte, Helsinki, Demos and University of Turku. "Technology neutrality as a way to future-proof regulation: the case of the Artificial Intelligence Act". Available at SSRN: <https://ssrn.com/abstract=5181085> (2025).
37. Puaschunder, Julia M. *Human Rights Online: Towards a New Generation of Human Rights in the Virtual World*. Columbia University, Graduate School of Arts and Sciences. 2024.
38. Quintais, Joao Pedro and Schwemer, Sebastian Felix. "The Interplay between the Digital Services Act and Sector Regulation: How Special Is Copyright?" *European Journal of Risk Regulation* (2022, 113).
39. Rosati, Eleonora. "The localization of IP infringements in the online environment: from Web 2.0 to Web 3.0 and the Metaverse". *Journal of Intellectual Property Law & Practice* (2023, Vol. 18, No. 10).

40. Ruschemeier, Hannah. “AI as a challenge for legal regulation – the scope of application of the artificial intelligence act proposal”. ERA Forum, (2023: Vol. 23).
41. Sander, Barrie. “Democratic Disruption in the Age of Social Media: Between Marketized and Structural Conceptions of Human Rights Law”. The European Journal of International Law (2021, Vol. 32 no. 1)..
42. Snyder, Hannah. “Literature review as a research methodology: An overview and guidelines”. Journal of Business Research (2019, Vol. 104).
43. Sorban, Kinga. “An elephant in the room—EU policy gaps in the regulation of moderating illegal sexual content on video-sharing platforms”. International Journal of Law and Information Technology (2023, 31).
44. Streel Alexandre de, and Husovec Martin. The e-Commerce Directive as the Cornerstone of the Internal Market: Assessment and Options for Reform. Study for the Committee on Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies. European Parliament, May 2020.
45. Tu Xinyi and de Castro e Silva, Bruna. "Are We Ready for the Metaverse? Implications, Legal Landscape, and Recommendations for Responsible Development". Digital Society (2025, 4:9). p. 23
46. Wodajo, Kebene. “The user state: an alternative reading of the state role and duty in the age of platformized harm”. International Journal of Law and Information Technology (2023, 31).
47. Xiao, Baiyang. "Making the private public: Regulating content moderation under Chinese law". Computer Law & Security Review (2023, Vol. 51, 105893).
48. Xu, Min, David, Jeanne M. and Kim, Suk Hi. "The Fourth Industrial Revolution: Opportunities and Challenges". International Journal of Financial Research. (2018 Vol. 9(2)). p. 90-95.
49. Yannascoli, Sarah M. et al. “How to Write a Systematic Review: A Step-by-Step Guide”. University of Pennsylvania Orthopaedic Journal (2013, Vol. 23).
50. Zarnsky, Sarah. "Is International Criminal Law Ready to Accommodate Online Harm?". Journal of International Criminal Justice (2024, 22). p. 184.
51. Žydzūnaitė, Vilma, Sabaliauskas, Stanislav. Kokybiniai tyrimai: principai ir metodai: vadovėlis socialinių mokslų studijų programų studentams (Vilnius: Vaga, 2017).

Case-law

52. Advocate General Saugmandsgaard Øe. Opinion of Advocate General Saugmandsgaard Øe. Delivered July 16, 2020. In Joined Cases C-682/18 and C-683/18, Frank Peterson v. Google LLC and Others; Elsevier Inc. v. Cyando AG. Court of Justice of the European Union.
53. Case of the ECtHR: Bouyid v. Belgium. Judgement of 28 Sep 2015. Application no. 23380/09.

54. Case of the ECtHR: Hristozov and others v. Bulgaria. Judgement of 13 Nov 2012. Applications nos. 47039/11 and 358/12.

Internet sources

55. European Commission. An EU initiative on Web 4.0 and virtual worlds: a head start in the next technological transition (2023 07 113). <<https://ec.europa.eu/newsroom/dac/redirection/document/97337>> [accessed on 10 June 2024].
56. European Commission. Gatekeepers; <https://digital-markets-act.ec.europa.eu/gatekeepers_en> [accessed on 2024-12-01].
57. European Commission. Virtual Worlds (2024 07 30); <https://digital-strategy.ec.europa.eu/en/factpages/virtual-worlds> [accessed April 26, 2025].
58. European Parliament. EU Digital Markets Act and Digital Services Act Explained (2021 12 14); <<https://www.europarl.europa.eu/topics/en/article/20211209STO19124/eu-digital-markets-act-and-digital-services-act-explained>> [accessed on 2024-12-01].
59. Mattioli Rossella, Malatras Apostolos and others. Identifying emerging cyber security threats and challenges for 2030 (2023 03 29). <<https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030>> [accessed on 2024-06-05].
60. Statistics on cases decided by the ECtHR in 2024, by ECHR Article and by country <Statistics - ECHR - ECHR - ECHR / CEDH (coe.int)> [accessed on 4 April 2025].
61. Sternlicht, Lin and Sternlicht, Aaron. A New Age of Digital Addiction - What The Metaverse Means for Mental Health and Digital Addiction (2022); <<https://www.familyaddictionspecialist.com/blog/a-new-age-of-digital-addiction-what-the-metaverse-means-for-mental-health-and-digital-addiction>> [accessed on 2024-11-14].

In strict adherence to the principles of transparency and research integrity mandated by the European Research Area Forum, the author explicitly disclose the utilisation of generative artificial intelligence technologies during the commentary preparation process. Specifically, Grammarly (v1.2.220.1800) was utilised for the purpose of elimination of grammatical errors. It is imperative to emphasise that this tool functioned solely as an auxiliary mechanism. Accordingly, the author retain ultimate responsibility for the scientific accuracy, originality, and ethical integrity of the final output, ensuring full compliance with the normative standards established in the Living Guidelines on the Responsible Use of Generative AI in Research.

SANTRAUKA

AR VIRTUALIŲ APLINKŲ VALDYTOJAMS GALI KILTI TEISINĖ ATSAKOMYBĖ UŽ VEIKSMUS ŠIOSE APLINKOSE, KURIE ŽEIDŽIA ŽMOGAUS ORUMĄ, YPAČ NIEKINAMU IR ŽEMINAMU ELGESIU?

Spartus technologijų vystymasis ir vis didėjanti jų integracija į visuomenės gyvenimą iš esmės keičia kasdienybės dinamiką bei teisinio reguliavimo ypatumus. Virtualios aplinkos – apimančios virtualią, papildytą, išplėstinę realybę bei metaversatą – sukuria naujas erdves, kuriose asmenys patiria realias pasekmes, įskaitant ir žmogaus orumo pažeidimus, o šių valdytojai turi realią galimybę kontroliuoti naudotojų veiklą bei sustabdyti neteisėtus veiksmus. Nors Europos Sąjunga pristatė Skaitmeninių Paslaugų Aktą kaip priemonę, numatančią valdytojų atsakomybę už fundamentalių žmogaus teisių pažeidimus, moksliniame diskurse kyla reikšmingų diskusijų dėl reguliavimo veiksmingumo, dėl ko kyla būtinybė įvertinti, ar egzistuojantis reguliavimas Europos Sąjungoje yra visapusiškai pakankamas užtikrinti žmogaus orumo apsaugą virtualiose aplinkose, dėmesį skiriant sunkiausiai pažeidimų kategorijai dėl didesnės žalos rizikos. Pirmiausiai, straipsnyje yra pristatomos virtualios aplinkos technologijos keliamos rizikos, analizuojant aktualią akademinę literatūrą. Nustatoma, kad rizikos yra susijusios su psichikos sveikatos problemomis, privatumo ir žmogaus orumo pažeidimais bei teisinio reguliavimo iššūkiais, kuriuos lemia sparti technologinė pažanga. Taip pat, atsižvelgiant į keliamas rizikas, straipsnyje apžvelgiamas egzistuojantis virtualių aplinkų teisinis reguliavimas Europos Sąjungoje. Nustatoma, kad nėra vieno teisinio akto, kuris reguliuotų virtualias aplinkas iš esmės, tačiau, remiantis technologinio neutralumo principu, galima daryti išvadą, kad yra daugybė kitų teisės aktų, kurie atitinkama apimtimi reguliuoja virtualias aplinkas. Atkreipiamas dėmesys, kad pagrindinis teisės aktas, nustatantis valdytojų atsakomybę už žmogaus teisių pažeidimus jų valdomose aplinkose, yra Skaitmeninių Paslaugų Aktas.

Toliau išdėstoma tyrimo metodologija. Pirmiausiai, aprašomas tyrimui atlikti pasirinktas sisteminės literatūros analizės metodas nurodant jo įgyvendinimo eigą. Išaiškinama, kad šis metodas bus naudojamas siekiant atsakyti į šios tezės klausimą identifikuojant pagrindinius egzistuojančio reguliavimo Europos Sąjungoje ypatumus, susijusius su virtualių aplinkų valdytojų atsakomybe. Šiam tyrimui atrenkami 27 šaltiniai, iš kurių išskiriamos 63 citatos tolimesnei tyrimo analizei. Šios citatos skirstomos pagal tematiką į du skyrius: „Skaitmeninių platformų atsakomybės rūšys bei jų įtaka technologinei ekosistemai“ ir „Teisinio reguliavimo problemos ir tolimesnis reguliavimo tobulinimas“. Šie skyriai dar skaidomi į penkis poskyrius: „Tiesioginė atsakomybė“, „Netiesioginė atsakomybė“, „Skaitmeninių platformų elgesys“, „Teisinio reguliavimo veiksmingumo vertinimas ir socialinis poveikis“ bei „Tolimesnis reguliavimo tobulinimas skaitmeninių platformų atsakomybės atžvilgiu“. Galiausiai, tyrimo metodologijos sudarymo rezultatai ir išsamesni kokybiniai duomenys papildomai pateikiami vizualine išraiška.

Galiausiai, sisteminės literatūros analizės pagalba atliekamas teisinio reguliavimo Europos Sąjungoje, numatančio valdytojų atsakomybę, veiksmingumo tyrimas. Tyrime atskleista, jog Skaitmeninių Paslaugų Aktas numato valdytojų atsakomybę už veiksmus jų valdomose virtualiose aplinkose, kurie žeidžia žmogaus orumą, ypač niekinamą ir žeminamą elgesiu, tačiau šis teisės aktas neužtikrina valdytojų atsakomybės mažesnėse, labiau pažengusiose virtualiose aplinkose, kurios yra decentralizuotos. Dėl šių priežasčių rekomenduojama jį papildyti atskira kategorija virtualių aplinkų valdytojams, kurioje būtų numatyti reikalavimai taikyti pastiprintas tikrinimo priemones ir sudaryti rizikos vertinimą visų tipų virtualioms aplinkoms, įskaitant mažesnes, decentralizuotas.

RAKTINIAI ŽODŽIAI

Valdytojų atsakomybė, žmogaus orumas, virtuali aplinka, žeminamas ir niekinamas elgesys, Skaitmeninių Paslaugų Aktas.