



A Comparative Analysis of Online Content Regulation in EU and UK

Jorgo Çipa¹ 
Kozeta Sevrani² 

Received: April 20, 2024 / Revised: June 27, 2025 / Accepted: June 30, 2025

© Association of Economists and Managers of the Balkans, 2025

Abstract: *An important aspect of daily activity occurs in cyberspace, where individuals access numerous online platforms and benefit from the various services offered. The amount of online content is growing exponentially, and at the same time, it has increased the possibility that users face illegal and harmful content on different online platforms. Relevant organizations and governing bodies indicate that individual reports of illegal and harmful content have increased every year. This shows the inadequacy of actions by online platforms in tackling illegal and harmful online content and the need to change from a self-regulation approach to a more strict governmental regulatory approach. This paper provides an overview of online content regulation applied within the European Union, Germany and the United Kingdom and through a comparative analysis of these acts, similarities and differences are identified.*

Keywords: *Online Content, Regulation, Online platforms, Illegal content, Digital services act, Network enforcement act, Online safety act.*

JEL Classification: K23 · K38 · L86 · L51

 jorgo.cipa@unitir.edu.al

¹ University of Tirana, Faculty of Economy, Department of Statistics and Applied Informatics, Rruga Arben Broci 1, 1001, Tirana, Albania

² University of Tirana, Faculty of Economy, Department of Statistics and Applied Informatics, Rruga Arben Broci 1, 1001, Tirana, Albania



1. INTRODUCTION

Cyberspace ecosystem consists of many online platforms that offer a multitude of services. According to the [International Telecommunication Union \(2023\)](#), approximately 67% of the world's population or 5.4 billion people, are connected to the Internet. Especially in Europe, this percentage reaches 91% of the population. As a result, online content is increasing every minute, and internet users interact with new content at every moment. Based on information gathered by LocaliQ ([Marino, 2023](#)), in an internet minute in 2023, 66,000 photos and videos are shared on Instagram, 350,000 tweets are sent in X, 625 million videos are watched on TikTok and 6.3 million searches are done in Google. So, user-generated content constitutes a significant component of online content.

But, unfortunately, a lot of illegal and harmful content is placed on the internet and makes more and more people vulnerable to accessing or being accessed by this content, especially children. Almost 80% of people aged between 15 and 24 use the Internet ([International Telecommunication Union, 2023](#)). According to Internet Watch Foundation ([IWF, 2023](#)), 375,230 reports were assessed in 2022, which marks a 4% increase from 2021. The environment hosting illegal and harmful content has become highly varied. Beyond websites as the earliest traditional way, illegal and harmful content is created and hosted in different online platforms such as social networks, video-sharing platforms, search engines, online marketplaces, discussion forums, etc. At the same time, the range of illegal content has become wider, including not only copyright infringement, online child sexual abuse, but also terrorist content, hate speech, disinformation, etc.

Therefore, online content regulation is very crucial to protect individuals from illegal content and harm. This is actually not something new, but the approach to regulating online content has changed. In this context, there is a wide-ranging global debate about whether and how illegal or harmful online content should be addressed through regulation ([Ofcom, 2018; Price & Verhulst, 2000](#)).

In the beginning of platforms, self-regulation has been seen as the best solution, but now recent figures have shown that government bodies' intervention or regulation is required in order to establish a common approach to the responsibilities of online providers to deal with illegal and harmful online content. The current "platform governance" status quo is rapidly moving away from an industry self-regulatory model and towards increased government intervention ([Helberger et al., 2018, 2021](#)). Recent publications emphasize the transition from self-regulation governed by platforms to co-regulation and the expanded application of automated moderation systems ([Suzor, 2021; Kettemann, 2020; Gorwa, 2022](#)). Although such systems represent positive progress in tackling illegal and harmful content, several studies also point to the risks of over-blocking, over-removal, and bias in algorithmic decision-making, thus highlighting concerns about procedural fairness, transparency and user rights ([Kaye, 2021; Mac Síthigh & O'Dell, 2021](#)).

For centuries, activists have struggled with the question of how and when governments should implement restrictions on free speech to safeguard individuals from content that may lead to harm ([Bickert, 2020](#)). This option is acknowledged as potentially the most invasive regulatory option, so its impact on individual freedoms has to be considered ([Parti & Marin, 2013](#)).

Regardless of the fact that there is a somewhat unified practice of what is considered illegal content, countries around the world have diverse interpretations of illegal online content and different models for regulating this content ([Mifsud Bonnici & de vey Mestdagh, 2005](#)). This paper provides an overview of different online content regulations applied in the European Union (EU), the

United Kingdom (UK), and Germany. By conducting a comparative analysis of these regulations, this paper aims to identify the strengths and weaknesses of each approach.

This paper is organized as follows. The methodology of this paper is described in Section 2. The third section of the paper explores EU regulation on tackling illegal online content. The next section examines Germany's approach on addressing illegal online content. The fifth section investigates how the United Kingdom regulates online content. In the following section, a comparative analysis of those regulations is undertaken. This analysis produces significant conclusions and findings for this paper in the last section.

2. METHODOLOGY

The authors perform a comparative analysis of regulatory frameworks addressing the issue of online content regulation in order to achieve the aim of this paper. The primary sources of data include the EU Digital Services Act, the German Network Enforcement Act and the UK Online Safety Act. Although there are other regulations on tackling illegal and harmful content, the research focuses only on the above 3 acts as they constitute the main jurisdictions based on their great impact on content regulation and the different approaches they offer within the European context, thereby providing a basis for their comparison, which is particularly relevant for countries like Albania aiming to align with EU digital policy frameworks. In order to highlight similarities and, especially, differences between these diverse jurisdictions' approaches towards online content regulation, the following research questions are identified:

RQ1. Which types of online platforms are regulated?

RQ2. Do these regulations define and categorize illegal online content?

RQ3. What obligations are imposed on online providers to enhance their accountability in content regulation?

3. EU REGULATION ON TACKLING ILLEGAL ONLINE CONTENT

EU Regulation 2022/2065 on a Single Market for Digital Services, known as the Digital Services Act (DSA), establishes a significant framework affecting European users who generate and disseminate online content as well as technology companies who serve as intermediaries on the internet. By amending the Directive 2000/31/EC on Electronic Commerce (E-Commerce Directive), DSA sets out the baseline regime applicable to all categories of intermediary services offered to recipients of the service that are located in the Union, irrespective of where the providers of those intermediary services have their place of establishment. Entry into force by 17 February 2024, the main goal of the DSA is to create a safer and more accountable digital space in which the fundamental rights of all users of digital services are protected (European Union, 2022).

It is important to mention that despite updating the EU E-Commerce Directive, DSA does not affect the application of this Directive, which continues to remain in force.

3.1. Categorization of Intermediary Service Providers (ISPs)

An important aspect related to illegal or harmful online content is the definition of the liabilities of the information society service providers, known as intermediary service providers (ISPs). The

DSA regulates the liability regime of ISPs. Based on this regulation, we have 3 (three) types of ISPs, whose liabilities are set out below:

Mere Conduit ISPs

Article 4 of the Digital Services Act, which explain “mere conduit”, defines that if the service provided by the ISP consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, the ISP is not liable for the information transmitted or accessed when it: (European Union, 2022)

- does not initiate the transmission;
- does not select the receiver of the transmission;
- does not select or modify the information contained in the transmission.

Caching ISPs

Article 5 of the Digital Services Act that defines “caching”, stipulates that if the service provided by the ISP consists of automatic, intermediate and temporary storage of information, in order to make the onward transmission of the information to the recipients of the service more efficient, the ISP is not liable on condition that: (European Union, 2022)

- does not modify the information;
- complies with conditions on access to the information;
- complies with rules regarding the updating of the information, specified in a manner widely recognized and used by industry;
- does not interfere with the lawful use of technology, widely recognized and used by industry, to obtain data on the use of the information;
- acts expeditiously to remove or to disable access to the stored information when information at the initial source has been removed or access has been disabled or when a judicial or an administrative authority has ordered such removal or disablement.

Hosting ISPs

As defined by Article 6 of the Digital Services Act, hosting ISPs offer the service of the storage of information provided by a recipient of the service. The service provider is not liable for the information stored by service recipients when it: (European Union, 2022)

- does not have actual knowledge of illegal activity or illegal content;
- upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the illegal content.

So, the regulation gives explicit provisions on the conditions and circumstances under which the ISP will be responsible for user-generated content.

The E-Commerce Directive, also known as the safe harbour framework for internet intermediaries, has been a core pillar of internet regulation for the last two decades. Since 2000, when the Directive was adopted, the online services environment has been changed with the introduction of search engines, social media platforms, video-sharing platforms, the rise of mobile and cloud computing, etc. So Article 14 of the E-Commerce Directive applies to a greater number of services than was thought in 2000 (Van Hoboken et al., 2018). As a result, the Digital Services Act, compared to the Directive, brings a new categorization for the largest platforms, by introducing the terms of Very Large Online Platforms (VLOPs) and Very Large Online Search Engines

(VLOSEs). These are online platforms and online search engines that have a number of average monthly active users in the EU equal to or higher than 45 million. They are subject to stricter additional obligations based on their size and important role in the digital environment. The European Commission is the responsible entity to designate a platform as a VLOP or a search engine as a VLOSE based on user numbers provided by platforms and search engines by 17 February 2023. As of now, platforms such as AliExpress, Amazon Store, App Store, Pornhub, Booking.com, Google Play, Google Maps, Google Shopping, YouTube, LinkedIn, Facebook, Instagram, Pinterest, Snapchat, Stripchat, TikTok, X, Wikipedia, XVideos, and Zalando are categorized as Very Large Online Platforms (VLOPs). Additionally, Google Search and Bing have been designated as Very Large Online Search Engines (VLOSEs).

3.2. Obligations for Online Providers

The Digital Services Act (DSA) sets out a complete set of obligations on online providers to increase their transparency, security and accountability in the digital space. In the table below, the main obligations are listed and properly assigned to various categories of online providers. The DSA includes four major categories of online providers: intermediary services, hosting services, online platforms and very large online platforms and search engines. It is important to mention that in our analysis, other obligations specified in the DSA, which are not closely related to the issue of tackling illegal and harmful internet content, are excluded.

As shown in the table 1, online platforms, especially very large online platforms and very large online search engines, have the largest number of liabilities to be addressed and to be compliant with the DSA requirements. This proves their essential impact in the online ecosystem.

Table 1. A Taxonomy of regulatory obligations based on different types of online platforms

Obligations	Intermediary services	Hosting services	Online platforms	VLOPs/ VLOSEs
Act against illegal content upon the receipt of an order	x	x	x	x
Inform the recipient of the service affected regarding the reasons for removal and the possibilities for redress that exist	x	x	x	x
Provide specific information about one or more specific individual recipients of the service upon the receipt of an order	x	x	x	x
Designate a single point of contact for authorities	x	x	x	x
Establish a single point of contact for users of the service	x	x	x	x
Apply policies, measures and tools used for content moderation	x	x	x	x
Publish at least once a year, clear reports regarding content moderation performed	x	x	x	x
Put mechanisms in place to allow any individual or entity to notify them regarding potentially illegal content on their service		x	x	x
Provide a clear and specific statement of reasons to any affected recipients of the service for any restrictions related to illegal content		x	x	x
Inform the authorities of its suspicions of criminal offences		x	x	x

Provide users with access to an internal complaint-handling system			x	x
Inform recipients of the service about the possibility of an out-of-court dispute settlement			x	x
Give priority and process notices submitted by trusted flaggers			x	x
Suspend for a reasonable period of time the provision of their services to recipients that frequently provide manifestly illegal content			x	x
Put in place appropriate measures to ensure the online protection of minors on their service			x	x
Conduct a risk assessment related to the dissemination of illegal content through their services				x
Maintain a crisis response mechanism				x
Be subject, at their own expense and at least once a year, to independent audits				x
Establish a compliance function to monitor compliance with the DSA				x
Be charged annually a supervisory fee for each service				x

Source: Own processing

4. GERMANY'S APPROACH TO ADDRESSING ILLEGAL ONLINE CONTENT

Germany has adopted one of the most robust state-level regulatory frameworks regarding illegal online content, with a particular emphasis on combating hate speech. The German Network Enforcement Act (NetzDG) was adopted in June 2017 and entered into force on 1 October 2017.

4.1. Scope of the NetzDG

This act applies to all social networks that enable users to share any content with other users or to make such content available to the public, if the social network has more than two million registered users in the Federal Republic of Germany (Germany, 2017). This means that social networks or platforms that have fewer than two million registered users are outside the scope of this act. Also, online platforms intended for journalistic and editorial content and online platforms intended for the dissemination of specific content, such as online gaming platforms, professional social networks and online sales platforms, are exempt from the obligations of this act. In order to determine which illegal content is covered by this law, the NetzDG refers to 22 offences of the German Criminal Code, which include child sexual exploitation and abuse material, xenophobic, racist and other types of hate speech, terrorist content, content infringing intellectual property rights and online disinformation (De Streel et al., 2020).

4.2. Responsibilities of Online Platforms

With regard to reporting illegal online content, online platforms must ensure an effective and transparent procedure for handling complaints about unlawful content that needs to be easily recognisable, directly accessible and permanently available for users. After receiving the complaint, the online platform checks whether the content is illegal or not and whether blocking or removal procedures will be applied. The online platform has 7 (seven) days to remove or block access to the illegal content. This time limit is reduced to 24 hours in case of manifestly illegal content,

unless there is an agreement between the online platform and the competent law enforcement authority on a longer period for blocking or removal.

Another important obligation in this act is that the online platform must notify the complainant and the author of the content about its decision, while also providing them with the reasons on which this decision is based. In the case of removal, the online platform is obliged to retain the content as evidence and store it for this purpose for a period of ten weeks.

Online platforms are also obliged to appoint a representative in Germany to deal with requests or notices for information. Another special provision included in the act is that online platforms that receive more than 100 complaints per year about illegal content are obliged to produce reports every 6 (six) months on the handling of complaints regarding illegal content on their platforms.

4.3. Concerns Related to Freedom of Expression

Supporters see the act as a necessary tool in order to reduce or stop hate speech online and extremism. On the other hand, critics view it as a German “Censorship Law”, in the sense that forcing social media platforms to block or remove illegal content may sometimes result in a violation of free speech on these platforms. First, they argue that the law may lead to over-blocking as the sanctions are asymmetric; the online platforms are fined if they maintain illegal content, but not when they remove accidentally legal content (De Streel et al., 2020). Second, the main fear is that social media platforms might remove more content than necessary in order to avoid being fined (Heldt, 2019). Third, the NetzDG provides few mechanisms for the author of allegedly illegal content to complain, although the act imposes an obligation on online platforms to inform them regarding the decision. There are many reasons to criticise the NetzDG, but what it does, in the end, is increase intermediary liability for not reacting to user notices concerning unlawful content (Heldt, 2019).

5. REGULATING ONLINE CONTENT IN THE UNITED KINGDOM

In the UK, the Online Safety Bill establishes a new regulatory framework to tackle illegal and harmful online content. The Bill received Royal Assent on 26 October 2023 and is now known as the Online Safety Act. The Act defines that illegal content means any content consisting of certain words, images, speech or sounds that amounts to a relevant offence (terrorism offence, child sexual exploitation and abuse offence, offence that is specified in regulations made by the Secretary of State and offence of which the victim or intended victim is an individual). Also, it defines harmful content as the nature of the content where there is a material risk of the content having, or indirectly having, a significant adverse physical or psychological impact on a human of ordinary sensibilities (United Kingdom, 2023).

5.1. Categories of Regulated Online Services

This Act applies to providers of regulated services that have a significant number of users in the UK or that are capable of being used by individuals in the UK, more specifically:

- user-to-user services, which are services that allow users to generate, upload or share user-generated content or interact with other users, for example, social media services, video-sharing services, private messaging services, online marketplaces, dating services, review services, file and audio sharing services, discussion forums, information-sharing services and gaming services.

- search services, which are services that allow users to search particular content on the internet.
- video-sharing platforms, which are online services that allow users to upload and share videos with other people.
- services with pornographic content, which include online services that publish or display certain pornographic content in the form of videos, audio or images.

Services deemed to have a low risk of harm to users, or that are otherwise regulated, including emails, SMS and MMS messages, comments and reviews on provider content, one-to-one live audio communications, paid-for advertisements, and news publisher content, are exempt from the obligations.

5.2. Liabilities for Providers of Online Services

The Online Safety Act defines a set of obligations and duties to be met by regulated content providers to protect users from illegal and harmful online content. According to the Act, online platforms or providers need to take care of the following duties: (United Kingdom, 2023)

- to carry out an illegal content risk assessment and to keep it up to date;
- to minimise the presence and dissemination of priority illegal content;
- to minimise the length of time for which priority illegal content is present;
- where the provider is alerted by a person to the presence of any illegal content, or becomes aware of it in any other way, swiftly takes down such content;
- to produce an annual report regarding the handling of complaints about illegal and harmful online content on their platforms;
- to specify in the terms of the service how individuals are to be protected from illegal content. Those terms of service need to be clear, accessible and applied consistently.

Beyond the duties defined above, the Act puts particular duties for services likely to be accessed by children. They need to:

- prevent children of any age from encountering, by means of the service, primary priority content that is harmful to children;
- protect children in age groups judged to be at risk of harm from other content that is harmful to children.

6. Comparison of the EU Digital Services Act, Germany's NetzDG, and the UK Online Safety Act

These online content regulations are generally similar to each other as they impose strong obligations and duties on online platforms that are under their scope. The table below provides a comparative analysis of these three significant legislative acts based on several key criteria.

In terms of scope, the German NetzDG applies to a narrower range of online platforms compared to the other two regulations. By restricting to social networks only, this act excludes sales platforms and messenger services. In contrast, both the EU Digital Services Act and the UK Online Safety Act include these types of online services. The EU DSA and the UK OSA apply to a broader and almost identical range of online platforms. Another notable difference is that the German NetzDG and the EU DSA categorise online platforms based on the number of users in the territory where each regulation is applied, whereas the UK OSA does not have explicit categorisation criteria related to the number of users.

Table 2. Comparative Overview: EU Digital Services Act, German Network Enforcement Act, and the UK Online Safety Act

Criteria	EU	Germany	UK
	Digital Services Act	NetzDG	Online Safety Act
Categories of online platforms	<ul style="list-style-type: none"> intermediary services hosting services online platforms very large online platforms/very large online search engines 	Social networks with more than 2 million registered users in Germany	<ul style="list-style-type: none"> user-to-user services search services video-sharing platforms services with pornographic content
Definition and Type of Illegal content Obligations	Any information that, in itself or in relation to an activity, is not in compliance with Union law or the law of any Member State which is in compliance with Union law No categorisation of its types	No definition of what constitutes illegal content, and no categorisation of its types	Any content consisting of certain words, images, speech or sounds that amounts to a relevant offence (terrorism offence, child sexual exploitation and abuse offence, offence that is specified in regulations made by the Secretary of State and offence of which the victim or intended victim is an individual)
	<ul style="list-style-type: none"> Content moderation/removal Terms and conditions Provide information about specific users Designation of a single point of contact for authorities/users Transparency reporting obligations Mechanisms for users to notify about illegal content Statement of reasons Internal complaint-handling system/out-of-court dispute settlement Trusted Flaggers Suspension of users from service Protection of minors Risk Assessment Independent audits Compliance function 	<ul style="list-style-type: none"> Content removal Terms and conditions Provide information about specific users Designation of a representative in Germany Transparency reporting obligations Establishment of an effective procedure for reporting illegal content. Statement of reasons Complaint management system Storage of removed content as evidence for ten weeks 	<ul style="list-style-type: none"> Content moderation/removal Relevant Terms of Service /Terms of Use Provide information about specific users Transparency reporting obligations Mechanisms for users to notify about illegal/harmful content Transparent decision-making over actions taken in response to reports of harms Effective internal complaint mechanisms. Suspension of users from service Protection of children Risk Assessment Audits User Identity Verification
Reaction time	No specific time frames defined	<ul style="list-style-type: none"> Removal of manifestly illegal content within 24 hours. Removal of illegal content within seven days. 	No specific time frames defined
Penalties for non-compliance	Up to 6% of the provider's annual worldwide turnover	Up to €50 million	Up to £18 million or 10% of a provider's annual global revenue, whichever is highest

Source: Own processing

Regarding the definition and types of illegal content, the UK OSA provides in-depth specifications for defining what constitutes illegal content and its various types. On the other hand, the EU DSA and the German NetzDG lack clear in-text provisions for defining illegal content types. However, different categories of illegal content in the EU are regulated by other laws.

Additionally, the German NetzDG refers to the German Criminal Code for the categorization of illegal content and offenses. Another important difference to note is that the UK OSA is the only regulation that directly addresses harmful content.

As for the liabilities imposed on online platforms, the EU DSA and the UK OSA contain a broader and more rigorous set of obligations compared to the German NetzDG. An important distinction has to do with the approach to how these acts regulate illegal content. Both the EU DSA and the UK OSA mandate content moderation and removal, whereas the NetzDG only refers to the removal process and does not require any content moderation activity. Furthermore, the UK OSA requires platforms to proactively monitor and moderate all content to identify illegal and harmful content. Meanwhile, the EU DSA does not have a general obligation for providers to monitor content, as it operates based on a “notice and action” mechanism. In contrast to the EU DSA, the German NetzDG and the UK OSA do not provide redress rights for ordinary users, nor do they contain procedures to escalate complaints through out-of-court or in-court resolutions. While both the EU DSA and the UK OSA emphasise child protection, the UK’s OSA imposes a wider range of strict obligations related to measures for minors. It is also important to mention that the EU DSA uniquely implements a system of trusted flaggers, which are entities recognised for their particular expertise in detecting, identifying, and reporting illegal content.

Regarding reaction time, the German NetzDG has specific time frames defined, requiring the removal of illegal and harmful content within seven days and 24 hours in the case of manifestly illegal content. On the other hand, the EU DSA and the UK OSA do not have specific time frames and are limited to using terms such as ‘swiftly’ or ‘promptly’ related to illegal content removal, without defining what these terms precisely involve in terms of exact hours or days.

7. CONCLUSION

Online content regulation has gained high importance as reports of illegal and harmful content have increased. Deregulation and self-regulation proved insufficient and ineffective in addressing the various concerns of users, organizations, and authorities. Consequently, regulations implemented and enforced by governmental bodies have been seen as crucial in reshaping online safety, which is threatened by new types and forms of illegal content.

This paper examined three key regulations: the EU Digital Services Act, the German Network Enforcement Act, and the UK Online Safety Act. These acts jointly address the issue of illegal content and establish a clear regime of obligations for online platforms. Regardless of their common goal, they each have unique characteristics and differ from one another.

The EU Digital Services Act establishes a common approach across Member States by regulating a wide range of online platforms. The UK Online Safety Act is the only regulation that focuses on harmful content, particularly concerning children. While the EU Digital Services Act proposes a more reactive approach, the UK Online Safety Act imposes a more proactively approach. The German Network Enforcement Act places emphasis on content removal as it mainly targets hate speech on social networks.

These regulations have triggered concerns about their possible negative implications for the freedom of expression on online platforms. Therefore, it is imperative that content regulation processes must be transparent, trustworthy and reasonable to guarantee the right balance between online safety and free speech.

References

- Bickert, M. (2020). *Charting a way forward Online Content Regulation*.
- De Streel, A., Defreyne, E., Jacquemin, H., Ledger, M., & Michel, A. (2020). *Online Platforms' Moderation of Illegal Content Online: Law, Practices and Options for Reform*. European Parliament.
- European Union. (2022). *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (L 277)*. Official Journal of the European Union. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065>
- Germany. (2017). *Netzwerkdurchsetzungsgesetz [Network Enforcement Act]*. Bundesgesetzblatt (BGBl.), Part I, No. 61, published on 7 October 2017. https://www.bundesjustizamt.de/SharedDocs/Downloads/DE/NetzDG/Leitlinien_Geldbussen_en.pdf?__blob=publicationFile&v=3
- Gorwa, R. (2022). Algorithmic content moderation: Technical and political challenges in the automation of platform governance. *Big Data & Society*, 9(1). <https://doi.org/10.1177/20539517221089300>
- Helberger, N., Pierson, J., & Poell, T. (2018). Governing online platforms: From contested to cooperative responsibility. *The Information Society*, 34(1), 1–14. <https://doi.org/10.1080/01972243.2017.1391913>
- Helberger, N., Pierson, J., & Poell, T. (2021). *Rethinking platform power: A research agenda for understanding platformization*. *Internet Policy Review*, 10(1). <https://doi.org/10.14763/2021.1.1552>
- Heldt, A. (2019). Reading between the lines and the numbers: an analysis of the first NetzDG reports. *Internet Policy Review*, 8(2). <https://doi.org/10.14763/2019.2.1398>
- International Telecommunication Union. (2023). *Measuring digital development: Facts and Figures 2023*. Retrieved from https://www.itu.int/hub/publication/d-ind-ict_mdd-2023-1/
- Internet Watch Foundation. (2023). *Annual Report 2022*. Retrieved from <https://annualreport2022.iwf.org.uk/>
- Kaye, D. (2021). *Speech police: The global struggle to govern the internet*. Columbia Global Reports.
- Kettemann, M. C. (2020). *The normative order of the internet: A theory of rule and regulation online*. Oxford University Press.
- Mac Síthigh, D., & O'Dell, E. (2021). Platform regulation and the UK Online Safety Bill: Legal challenges and policy opportunities. *International Journal of Law and Information Technology*, 29(2), 95–115. <https://doi.org/10.1093/ijlit/eaab025>
- Marino, S. (2023, December 4). What Happens in an Internet Minute? *LOCALiQ*. <https://localiq.com/blog/what-happens-in-an-internet-minute/>
- Mifsud Bonnici, J., & de vey Mestdag, C. (2005). Right Vision, Wrong Expectations: The European Union and Self-regulation of Harmful Internet Content. *Information & Communications Technology Law*, 14(2), 133–149. <https://doi.org/10.1080/13600830500042665>
- Ofcom. (2018). *Addressing harmful online content - A perspective from broadcasting and on-demand standards regulation*.
- Parti, K., & Marin, L. (2013). Ensuring freedoms and protecting rights in the governance of the internet: A comparative analysis on blocking measures and internet providers' removal of illegal internet content. <https://doi.org/10.30950/jcer.v9i1.455>
- Price, M., & Verhulst, S. (2000). *The Concept of Self-Regulation and the Internet*. Departmental Papers (ASC).
- Suzor, N. (2021). Governing the Internet through 'Self-Regulation': The shift toward coregulation in digital platforms. *Internet Policy Review*, 10(2). <https://doi.org/10.14763/2021.2.1565>
- United Kingdom.(2023). *Online Safety Act*. (c.50). https://www.legislation.gov.uk/ukpga/2023/50/pdfs/ukpga_20230050_en.pdf
- Van Hoboken, J., Quintais, J., Poort, J., & van Eijk, N. (2018). *Hosting Intermediary Services And Illegal Content Online: An analysis of the scope of article 14 ECD in light of developments in the online service landscape*