

**STUDIA IURISPRUDENTIAE DOCTORANDORUM
MISKOLCIENSIVM**

**MISKOLCI DOKTORANDUSZOK
JOGTUDOMÁNYI TANULMÁNYAI**

23.



MISKOLCI EGYETEM
ÁLLAM-ÉS JOGTUDOMÁNYI KAR
DEÁK FERENC ÁLLAM-ÉS JOGTUDOMÁNYI DOKTORI ISKOLA

**STUDIA IURISPRUDENTIAE DOCTORANDORUM
MISKOLCIENSIMUM**

MISKOLCI DOKTORANDUSZOK JOGTUDOMÁNYI TANULMÁNYAI
2022. évi 1. szám

Tomus 23

Szerkesztő:
Prof. Dr. Róth Erika

Technikai szerkesztő:
Dr. Sági Edit

Kiadja:
Bíbor Kiadó Bt.
Felelős kiadó: dr. Borkuti Eszter

A kötet borítóján *Albrecht Dürer: Erasmus portréja* című metszet részlete szerepel

ISSN 1588-7901

A kötet kiadását az Igazságügyi Minisztérium jogászképzés színvonalának emelését célzó programja támogatta.

MISKOLC, 2022.

Előszó

A Miskolci Egyetem Deák Ferenc Állam- és Jogtudományi Doktori Iskolája gondozásában megjelenő *Studia Iurisprudentiae Doctorandorum Miskolciensium* 2022. évi első kötete ismét gazdag tartalommal kerül az olvasók kezébe.

Már megszokott, hogy a magyar nyelvű publikációkon kívül idegen nyelvű dolgozatokat is publikálnak a doktoranduszok, amely lehetőséget ad arra, hogy kilépjenek a nemzetközi szakmai közönség elé. Ebben a kötetben a tanulmányok fele angol nyelven jelenik meg. Öröndetes tendencia ez, hiszen a fiatal kutatók számára kiemelten fontos, hogy megismerjék őket és eredményeiket a hazai és a nemzetközi tudományos élet szereplői. Ebben az idegen nyelvű tudományos közleményen túl sokat segíthet az is, ha a témavezetővel közös publikációja jelenik meg a fiatal kollégáknak, amire szintén találunk példát a jelen kötetben.

Mindig megtisztelő számunkra, ha más doktori iskolák doktoranduszai írásaikat folyóiratunkban kívánják megjelentetni, de ritkán fordul elő, hogy a közölt tanulmányok többségét nem miskolci doktoranduszok jegyzik. E kötet esetében ezzel szembesültünk, a publikált huszonegy tanulmány közül tizenháromnak a szerzője nem a Miskolci Egyetemen folytatja doktori tanulmányait.

A feldolgozott témákat nehéz lenne csoportokba sorolni, a doktori kutatások sokszínűsége a publikációk változatosságában is tükröződik. Az európai uniós témák hosszú ideje változatlan aktualitása és népszerűsége mellett a magyar jogrendszer egyes területeit bemutató írások jelennek meg nagyobb súllyal, de olyan, jogtudományi szempontból hazánkban kevésbé kutatott országok jogintézményeiről is olvashatunk, mint Kazahsztán vagy Vietnám.

Jó szívvel ajánljuk folyóiratunk legújabb számát kedves olvasóink figyelmébe. Biztosak lehetünk benne, hogy a kötetben megjelent írások közül mindenki talál olyat, amely felkelti érdeklődését.

Ismételten köszönetet mondunk az Igazságügyi Minisztériumnak, hogy „A jogászképzés színvonalának emelését célzó programok” keretében lehetővé tette a kiadvány megjelenését.

Prof. Dr. Róth Erika
a Deák Ferenc Állam- és Jogtudományi Doktori Iskola Vezetője

Tartalomjegyzék

DR. IMRE MÁTYÁS - AIDA BEKTASHEVA

Correlation between International Investment Law and Rule of Law Constitutional characteristics of the Republic of Kazakhstan.....7

ASLI ALKIS

The impact of the Privacy Shield's invalidation on the EU-US dataflows.....23

BALOG IMOLA KLÁRA

Az ügyvédi reklámok, a hazai reklámjogi szabályozás tükrében.....41

DÁVID BÁNYAI

Foreign currency lending in Hungary61

BARTUSZEK LILLA JUDIT

Fenntartható Fejlődés az Európai Unióban - Az Európai Unió szerepe az ENSZ 2030-ra kitűzött Fenntartható Fejlődési Céljainak megvalósításában.....75

CZIBRIK ESZTER

Az Ákr. alapelveinek kapcsolatrendszere.....83

CZUCZINÉ KERESZTES ANITA

Higher education in public administration during the Covid-19 pandemic.....103

CSEH BALÁZS - KÁLMÁN BOTOND

Ki alkotja ma a jogot? – avagy a multinacionális cégek, a pénzvilág és a piac domináns szervezeteinek szerepe a jogalkotásban.....113

GARAMI MÁRIA

Jogviszonyváltás a változásmenedzsment tükrében.....137

GÁTI BALÁZS

Az adatvédelmi jog fejlődésének főbb állomásai.....153

HA VAN THAI*	
An exploration of current regulatory aspects of money laundering legislation in Vietnam.....	169
KISS REBEKA	
A törvények jogalkotói indokolása.....	185
KOTROUŠOVÁ DENISA	
Corporal Punishments as a Mean of Upbringing vs. Children’s Rights in the Czech Republic.....	211
MARIA MASŁOWIEC	
Achievements of the International Commission on Civil Status as a missed opportunity for the European Union.....	233
MÓRICZ ALIZ	
Biztosítási intézkedés a magyar végrehajtási eljárásban.....	249
PÁHI BARBARA	
A büntetőjogi felelősség alsó korhatára.....	267
RAED GHANEM	
Human Rights Between the Philosophy of Natural Law and Legal Positivism...	283
RITTERODESZ ZSUZSANNA	
Platform munkavégzés a munkajogi szabályozás perspektívájában – a COVID-19 hatása: magyar, finn, német és spanyol összehasonlításban.....	299
SCHMIDT LÁSZLÓ	
A hatályos magyar civilisztikai jogszabályok és a kánonjogi jogszabályok összehasonlítása, és az ezekhez kapcsolódó egyes hazai és nemzetközi bírósági döntések bemutatása.....	319
YASIN TOKAT	
Emergence of New Regulations for Digital Platforms in the EU.....	319
ZHANNA AMANBAYEVA	
Realization of the right of citizens to education in the Republic of Kazakhstan...	349

YASIN TOKAT*

Emergence of New Regulations for Digital Platforms in the EU

Abstract: Because of the internet's worldwide and complicated network, new challenges and debates concerning the use of technology in the best interests of nation states began to emerge. New ways are required to manage policy, influence behavior, and address all of the current concerns surrounding internet use. As the law tries to catch up with technology, new rules such as the European Digital Services Act, Germany's NetzDG, and the United Kingdom's Online Harms Bill have been introduced. The study will examine these regulations and assess their possible impact on the internet.

Keywords: Digital platform, European Union, Digital Service Act, Online Harms Bill

Absztrakt: Az internet világméretű és bonyolult hálózata miatt új kihívások és viták kezdődtek a technológia nemzeti államok érdekeit szolgáló felhasználásával kapcsolatban. Új módszerekre van szükség az irányelvek kezeléséhez, a viselkedés befolyásolásához és az internethasználattal kapcsolatos összes jelenlegi probléma megoldásához. Mivel a jogi szabályozás igyekszik felzárkózni a technológiához, olyan új szabályokat vezettek be, mint az európai digitális szolgáltatásokról szóló törvény, a német NetzDG és az Egyesült Királyság online károkról szóló törvénye. A tanulmány megvizsgálja ezeket a szabályozásokat, és felméri lehetséges hatásukat az internetre.

Kulcsszavak: digitális platform, Európai Unió, digitális szolgáltatásokról szóló törvény, online károkról szóló törvény

<https://doi.org/10.46942/SIDM.2022.1.319-347>

Introduction

There are several prerequisites for the existence of a free and democratic state. Freedom of expression, freedom of thought, and progressive ideas have risen to prominence in Western Civilization since times of the enlightenment, with the development of scientific thought, religious reforms, legal and political reforms. Today, democracy is an indispensable trait of the Western World where freedom of expression and the free exchange of information are absolute prerequisites of governance and policy making. Before the age of the internet, the rules of the

* Yasin Tokat, PhD student, University of Szeged, Faculty of Law and Political Sciences Doctoral School. Supervisors: Prof. Dr. Révész Béla full professor and Dr. habil. Merkovity Norbert associate professor.

games were more subtle with the established status quo where the government, the media, and the public each had clear roles and areas of operation. Nowadays, we are living in the information age and access to information takes place in an instant regardless of geographical location and time. This allows every user to access the information from any location at any time whenever they need it with the capacity to broadcast and share their knowledge and ideas with other people at a global reach. This development poses a direct challenge for the old establishments. However, the internet did not have this potential in its earlier days. It had rather humble beginnings, as an experiment to carry out simple conversations through data packages between the university campuses through a network of cables. Later, the visible potential of the internet widened its areas of operations with more and more functions.

Nowadays, it is almost impossible to imagine a world without the internet, smartphones, and computer technologies that depend on it to connect and operate smoothly. The chief function of the internet is to send and receive data and this makes it a vital part of the development of human civilization as we are separated from other animals because our linguistic capabilities serve as a conduit for human collective knowledge to pass over from generation to generation, from one geographic place to the other. If the internet is fastening this process thousands or millions of times, we should expect a leap in the development of our civilization. From this aspect, the internet seems like a true globalizing force and a hope for a better connected, peaceful co-existence.

While some governments are taking advantage of the internet by better aligning it with their national agendas, some states may find it difficult to move swiftly in this hyper-changing environment. The result is the domination of big technology firms from certain countries that influence and shape the online marketplace. This inequality and domination often leave some governments unprepared to handle international legal problems on the internet effectively. In Europe, particularly, the domination of big tech platforms over the internet and rising new challenges trigger a need to create safety mechanisms through frameworks and regulations. Moreover, some regulations and policies that seem fit for the current challenges on the internet, have the potential to create other issues concerning the basic rights of internet users and content producers. On the other hand, there is a great need of finding new approaches to manage policy, shape behavior, and handle all the prevailing issues about the use of the internet effectively without creating human rights issues and censorship. As the law is trying to catch up with technology, there are many blank spots concerning the enforceability of laws and policies in cyberspace. Currently, there are new developments within the European Union towards establishing some sort of control mechanisms for user-generated content over the social media platforms due to potential illegality, offensiveness, misinformation, and disinformation aspects. We can see new legal and regulatory measures in application such as Germany's NetzDG, the European Union's Digital Services Act, the United

Kingdom's Online Harm Bills, and other ones targeting online service providers that host and share user-generated content. In essence, these are the uncharted territories that governments try to navigate according to their concerns, interests, and national agendas.

The motive behind the creation of such legal measures might seem legitimate yet the extent, applicability in the real world, and the end result of those new measures cause some concerns and draw various criticisms from various experts and parties. When adopted recklessly and without diligence, some of these restrictive methods can severely compromise fundamental human rights with a direct impact on the future of the digital world. Furthermore, such measures can be an incentive for less democratic states to increase authoritarian practices, censorship, and pressure on their citizens. As the world is getting more and more connected, restrictive measures taken by one country might have a spillover effect on the other ones as well. It is especially the case for the leading countries when one developed European country drafts laws and regulations, other countries take it as an example to follow it with their own interpretations, interests, and designs. Several authoritarian states already put high pressure on the freedom of internet users through firewalls, censorship, and legal prosecution. This way, actions taken in one part of the globe can have various other echoes in the entire digital ecosystem, either in the positive or negative direction. This is how a restricted internet within hostile cyberspace can be a vicious cycle, triggering every country to take more and more draconian measures to tackle the frictions that take place on the internet. However, this is not how the internet was initially designed for. As the internet has become the primary platform where essential daily activities take place, putting a high emphasis on such issues also entails an open, free, and secure internet to make it meet with the ideals of a fair, connected, and united world.

Newly drafted regulations give big social media platforms and internet hosts the power to monitor the content which was produced by the internet users on behalf of the state institutions due to the vastness of user-generated content, missing technical and financial capacities to analyze such content at courts and formal state institutions. The internet platforms have to respond to the complaints in a timely manner and takedown offensive or illegal content within a short time period. If they do not meet these obligations, they have to face huge financial penalties. As a result, there is a high pressure on the social media platforms to take down content or media that received complaints and it can be more favorable for them to remove the content without risking a financial consequence by spending too much time on the analysis. In this case, it is the user that might pay the price which might as well lead to the violation of freedom of expression rights. Moreover, this issue is a highly complex one because the internet as an international platform cannot be governed by one country's legislation and governance. Consequently, if countries try to enforce locally designed laws, they cannot still govern the internet globally due to

this global and complex nature of the internet that exists in a politically and traditionally divided world with various countries and interests. Potentially, such regulation might divide the internet on the same line as the national frontiers, leading more towards digital nationalism. The European Union seems to be an ideal environment for more united and effective approaches towards the solution for some of the pressing issues regarding fake news, disinformation, misinformation, online manipulation, and security issues. Furthermore, internet laws need to be flexible enough to cover a wide range of theoretical areas with various probabilities that might have the chance to develop into a real case. Otherwise, the regulatory measures can become choke points by reducing internet users' capacity to express their ideas and opinions online, affecting their online experience in a downward direction.

The paper will analyze various legal measures crafted in the European Union and the UK towards combating those issues. Those regulations will be also compared and the necessity behind such regulations will be investigated. One of the goals of the paper is to reveal some of the positive aspects and negative impacts of such regulations on freedom of expression and the free exchange of information through digital platforms. Three main legal acts will be investigated, compared to one another, and contrasted including their aim and their critics. Firstly, the Digital Services Act Package of the European Union will be investigated. Then, Germany's Network Enforcement Act or NetzDG will follow. Lastly, the UK's Online Harms Bill will be considered. This analysis can reveal the common issues, concerns, and effectiveness associated with the enforcement of these regulations.

Research aim

The research aims to compare newly drafted EU and UK regulations concerning hosting and sharing of user-generated content, requirements for content removal or blockage, and the responsibilities of the internet intermediaries. Analyzing the nature of the unwanted or illegal content with their disruptive effects and investigating the possible negative effects of the suggested regulations such as censorship, freedom of expression, state surveillance, public-private cooperation against the internet users, and overall limitation to the free exchange of information.

Methodology

The legal frameworks and regulations will be analyzed along with various issues concerning illegal, legal but unwanted content, their share, hosting, and liability issues. Therefore, qualitative analysis will be carried out during this research. Comparative analysis will also be used to examine various regulatory acts in Germany, the EU, and the United Kingdom. In order to assess the effectiveness of these regulations expert opinions and critiques will also be included. A full and

accurate description of the events that took place recently will be incorporated as well. As a result, the research will be able to elucidate the links between the cause and effect of the events that have taken place.

Literature review

Joris van Hoboken, João Pedro Quintais, Joost Poort, and Nico van Eijk conducted a study for the European Commission in 2019 ¹. Their study, titled "Hosting intermediary services and illegal content online An analysis of the scope of article 14 of the Electronic Commerce Directive in light of developments in the online service landscape: final report" provides insight into the extent of content hosting, in the context of regulations relating to hosting and sharing of illegal content on the internet from the legal and practical reach of Article 14 of the Electronic Commerce Directive ² (2000/31/EC). Their research examines several possible income sources of various hosting intermediaries, as well as how these revenue streams may impact the incentives for services to address illegal or infringing third-party behavior. Finally, the research analyzes the most relevant legal problems surrounding the scope of Article 14 of the Electronic Commerce Directive, with an emphasis on case law from the European Court of Justice and other legal developments.

Joan Barata wrote an article in 2020, titled "Positive Intent Protections: Incorporating a Good Samaritan principle in the EU Digital Services Act" which was published by the Center for Democracy and Technology ³. His article discusses various aspects of hosting both illegal and lawful but undesirable content uploaded or posted by the users to be publically available through social media and web hosting services. Barata explains that the "Good Samaritan" concept spares internet intermediaries with some immunity for taking reasonable steps in good faith to protect unnecessary blockage and censorship while shielding their users from unlawful or legal but offensive content. According to Barata's analysis, the more the internet intermediaries monitor, the more likely they will come across potentially unlawful information. This can cause more strict control over the users uploaded content as the web hosts will progressively have to deal with more illegal content. This can increase the probability of neglecting a specific violation, which increases

¹ VAN HOBOKEN, J. - QUINTAIS, J. P. - POORT, J. - VAN EIJK, N.: *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: final report*. Publications Office of the European Union (29.01.2019) DOI 10.2759/284542

² Directive 2000/31/EC: Regulation Of The European Parliament And Of The Council on a Single Market For Digital Services (Digital Services Act). European Commission (15 December 2020).

³ BARATA, J.: *Positive Intent Protections: Incorporating a Good Samaritan principle in the EU Digital Services Act*. The Center for Democracy & Technology (29 July 2020). <https://cdt.org/wp-content/uploads/2020/07/2020-07-29-Positive-Intent-Protections-Good-Samaritan-principle-EU-Digital-Services-Act-FINAL.pdf> (date of download: 07/17/2021)

the danger of liability significantly. The paper makes a number of proposals for the Digital Platforms Act in order to incentivize an appropriate content moderation under the Good Samaritan concept, allowing intermediaries to address problematic but lawful material on their services. Barata suggests increasing the clarity about the scope and needs in notice-and-action systems while sparing the intermediaries from the duties to determine the legality of third-party content.

Another article was published by Barata in 2020 on the blog of the London School of Economics about content moderation ⁴. His article "Regulating content moderation in Europe beyond the AVMSD" discusses the possible effects of the EU Audiovisual Media Services Directive (AVMSD) which was adopted in 2018. Barata explains how AVMSD was created as a directive to create a more in-line framework in the digital era and reduce the divergent approach towards traditional television and emerging on-demand and video-sharing services. He points out significant challenges that the AVMSD will provide in managing a suitable separation between two sections. First, platform content moderation decisions are made in accordance with the law and are accompanied by a number of legal safeguards and protections for users against unfair treatment. Second, the actions were taken solely on the basis of their own terms of service, which are not legally binding. Furthermore, by using the country-of-origin concept, the responsibility for regulating the most major video-sharing sites is likely to be concentrated in the hands of local authorities. This means that no matter where in the Union the creator of the material and its intended audience are located, moderation of anything as domestically sensitive as hate speech or terrorist content will be largely determined by a single EU Member State. This generates a new regulatory environment that differs significantly from how the same idea is applied to traditional audio-visual material.

Dr. Barata has published another article about the Digital Services Act. His article "The Digital Services Act and its Impact on the Right to Freedom of Expression: Special Focus on Risk Mitigation Obligations" analyses the impact of the Digital Services Act on fundamental rights and freedoms ⁵. Barata proposes that due to its wide extent, Digital Services Act can be a beneficial instrument for assuring that fundamental rights are respected and protected by specifically crafted legislation fit for the sector-specific cases. Article 8 concerns service providers from relevant legal and administrative national authorities taking action against a specific unlawful or undesired content, according to Barata. The extent of these orders is

⁴ BARATA, J.: *Regulating content moderation in Europe beyond the AVMSD*. London School of Economics (25 February 2020). Available at: <https://blogs.lse.ac.uk/medialse/2020/02/25/regulating-content-moderation-in-europe-beyond-the-avmsd/> (date of download: 07/17/2021)

⁵ BARATA, J.: *The Digital Services Act and its Impact on the Right to Freedom of Expression: Special Focus on Risk Mitigation Obligations*. (27 July 2021). Available at: <https://libertadinformacion.cc/wp-content/uploads/2021/06/DSA-AND-ITS-IMPACT-ON-FREEDOM-OF-EXPRESSION-JOAN-BARATA-PDLI.pdf> (date of download: 08/04/2021)

determined by the competent authority, whereas national authorities are granted vast and nearly unrestricted jurisdiction to unilaterally impose a particular interpretation of international freedom of expression principles on other countries. Article 14 oversees notice and action processes. Barata mentioned that hosting providers conduct a good-faith judgment based on legality, necessity, and proportionality which creates a complicated structure as governmental entities at both the national and EU levels are also involved. As a result, appropriate adoption and application of principles and safeguards for the preservation of human rights such as freedom of speech become an inescapable requirement in such a situation.

In 2019, Daphne Keller published an article titled "Who Do You Sue?" on the Aegis Paper Series of Stanford University's Hoover Institute ⁶. In her article, Keller investigates the frictions of the free speech rights and content removal practices when platforms like Facebook, YouTube, or Twitter suppress the opinions and expressions of their users. The first section of the paper outlines rather a messy mixture of government and private influences behind various content removals that underpin numerous material deletions, as well as how this combination limits the ability of the users to oppose government action. The second section delves into the legal quagmire when users and lawmakers face asserting the right to communicate on major internet platforms. Keller further points out the issues created due to the inextricable link between the state and private power which might work against the right to the freedom of expression of the users. The government holds the power while the private sectors own the platforms and the innovative steps. If the balance is not maintained, the users can be the weakest link in this chain. For this reason, she further explains the necessity to comprehend and engage with both public and private powers to understand and safeguard the rights of internet users.

Jack M. Balkin's essay "Free Speech is a Triangle" was delivered at the Columbia Law Review's 2018 symposium "A First Amendment for All? Free Expression in an Age of Inequality," which was co-sponsored by the Knight First Amendment Institute and the Center for Constitutional Governance ⁷. The essay argues that the concept of free expression that dominated most of the twentieth century is no longer enough to safeguard it. He suggests that a dynamical or dualist model of speech control existed in the twentieth century, with two fundamental types of players: regional states on one side, and individuals on the other. According to Balkin, the model of the twenty-first century is quite diversified with numerous actors. He suggests seeing the basic structure like a triangle where the nation-states

⁶ KELLER, D.: Who Do You Sue? State And Platform Hybrid Power Over Online Speech. *Aegis Series Paper* No. 1902. Hoover Institution, Stanford University (29 January 2019). <https://www.hoover.org/research/who-do-you-sue> (date of download: 07/17/2021)

⁷ BALKIN, J. M.: Free Speech is a Triangle. *Columbia Law Review*. Yale Law School. Public Law Research Paper No. 640, (May 28, 2018). <https://ssrn.com/abstract=3186205> (date of download: 07/17/2021)

are at one corner, while privately held internet infrastructure firms, such as social media companies, search engines, broadband providers, and electronic payment systems, are on the other one. At the third corner, different types of individuals, established media, civil-society groups, cyber attackers, and trolls can be found. Balkin further argues that the capacity to have your voice heard in the digital age is affected by the power struggle between the forces such as the old-school, new-school, and private regulations focused on speakers while both nation-states and civil-society groups press digital service providers to regulate speech. Three issues arise as a result of this implementation. Firstly, nation-states utilize new-school speech control to exert pressure on digital firms, resulting in issues such as collateral censorship and digital prior restraint. Secondly, social media corporations establish complicated private governance and bureaucracies that regulate end users indiscriminately and without due process or enough clarity. Thirdly, end users are subject to monitoring and manipulation through digital means. The essay further continues with several suggestions on how nation-states should govern digital infrastructure in accordance with the ideals of free speech and the press.

Matthias Kettemann and Anna Sophia Tiedeke published their paper in 2019 at Leibniz Institute for Media Research, Hans-Bredow-Institut (HBI) with the title "Back up: Can Users Sue Platforms to Reinstate Deleted Content? A Comparative Study of US and German Jurisprudence on 'Must Carry'" ⁸. This paper also investigates the rising practice of private regulation of public communication through the service providers. It emphasizes the role of internet services in political communication which necessitates a careful examination of the issue from public interest and public law points of view. Kettemann and Tiedeke acknowledge that when users try to have their content back with a court decision, social network services must bear duties. Their research also examines this issue by investigating a number of US and German court cases involving account restoration and the republication of deleted posts, videos, and social media content. Lastly, the study demonstrates why private communication ordering should not be considered apart from public interest.

The rise of new regulations in Europe

The Digital Services Act Package of the European Union

As a region with high human development and economic wealth, the member countries of the European Union benefited greatly from the rapidly growing internet technologies and digital services which have long found their places at the

⁸ KETTEMANN, C. M. - TIEDEKE, A. S.: Back Up: Can Users Sue Platforms To Reinstate Deleted Content?. *Internet Policy Review*, 9(2). (2020). DOI: 10.14763/2020.2.1484

center of everyday life. People within the EU have the option to choose one option over another to connect with one another, purchase goods and services, and receive information instantly over the internet, and all of these means and technologies are continuously in a change where the EU has a strong influence. As a result of the adverse effects of this rapidly growing infrastructure, the EU countries have been working on some regulations to ensure that European law advances regarding the issues over the internet in tandem with these latest developments. The European Commission's Digital Services Act (DSA) is a legislative proposal that was introduced in the European Parliament and the European Council on December 15, 2020 ⁹. The Digital Services Act (DSA) is one of two concepts included in the Digital Services Act package. The other part of the package is the Digital Markets Act (DMA), which was also presented by the European Commission on the same day ¹⁰. Through the Digital Services Act, the European Union has been working over the past two years to develop feasible and long-term solutions for regulating online platforms and digital services. This crucial effort aims at regulating how fundamental rights are protected over the internet such as online privacy and freedom of speech. The ultimate objective of the DSA is to modernize the European Union's legislative framework, particularly the e-Commerce Directive, which was approved in 2000 ¹¹. In essence, this will entail additional laws on illegal material, deceitful advertising, and misinformation.

Let us briefly go over what those online services and markets are. Digital services are the services that are provided online such as websites, internet infrastructure services, and online platforms. There are also online intermediaries and platforms such as online marketplaces, application stores, social networks, digital media sharing platforms, and online travel and accommodation platforms. The Digital Markets Act also establishes guidelines for online gatekeeper platforms. Gatekeeper platforms are digital platforms that have a systemic role in the internal market, acting as bottlenecks for crucial digital services between the companies and users. Users and the overall market have benefited greatly from online platforms, which have also enhanced the efficiency in the internal market of the EU and contributed to the innovation. These platforms and their revolutionary approaches also made cross-border commerce easier both inside and outside the EU which has opened new horizons for the European firms and merchants by enabling them to expand into new markets. Besides these numerous advantages of the internet

⁹ Directive 2000/31/EC: Regulation Of The European Parliament And Of The Council on a Single Market For Digital Services (Digital Services Act). European Commission. 15 December 2020)

¹⁰ ESPINOZA, J. - HINDLEY, S.: *Brussels' plans to tackle digital 'gatekeepers' spark fevered debate*. *Financial Times* (December 16, 2020). Available at: <https://app.ft.com/content/22bda533-db74-4a3d-917b-75ac23c0f27f> (date of download: 07/05/2021)

¹¹ STOLTON, S.: *Digital agenda: Autumn/Winter Policy Briefing*. *Euroactiv*. (18 August, 2020). Available at: <https://www.euractiv.com/section/digital/news/digital-agenda-autumn-winter-policy-briefing/> (date of download: 07/05/2021)

platform, there have been certain issues and challenges that began to appear on the surface with significant consequences on society and the economy in general. For instance, online trade of illicit products or services, and exchange of illegal content can be given as some major sources of concern. Furthermore, the increasing use of Artificial Intelligence and algorithms with user interactions might cause some other problems. Manipulative algorithmic systems which are implemented within the online platforms have the potential to enhance the spread of disinformation and propaganda. These new issues, as well as how platforms respond to them, have a substantial influence on how fundamental rights are practiced and safeguarded online. Despite a variety of targeted, sector-specific measures at the EU level, major gaps and regulatory barriers have remained until the Digital Services Act came into existence.

The rapid digitalization of society and the economy has resulted in a situation in which a few big platforms control significant digital economy ecosystems. They have emerged as digital market gatekeepers with the authority to operate as private rule-makers which can restrict the market competitors through their executive and technical powers. These restrictions can lead to disadvantages for the business that use these platforms while lessening the available options for customers which can create undesirable market conditions. In light of these changes, Europe demands a contemporary legislative framework that protects user safety online, provides governance with basic rights protection at its core and preserves a fair and open online environment. Hence, the Digital Services Act (DSA) and Digital Markets Act (DMA) were created as a response to these developments. In many ways, the resolutions are complementary in terms of substance. They include a growing interest for the e-Commerce Directive's essential principles to be upheld and for fundamental rights to be protected in the digital environment, as well as online anonymity wherever technically feasible. They advocate for effective responsibilities to combat unlawful content over the internet, including transparency, information obligations, and responsibility for digital service providers. They also urge for public scrutiny at the EU and national levels, as well as cross-jurisdictional collaboration in upholding the law, particularly when dealing with cross-border issues ¹².

In Parliament, three initiative reports have been launched, from the Committee on the Internal Market and Consumer Protection, the Committee on Legal Affairs, and the Committee on Civil Liberties, Justice, and Home Affairs. The first report from the Committee on the Internal Market and Consumer Protection demands a comprehensive reform of the EU's current e-commerce legal framework while preserving the basic concepts of the liability system, the prohibition of extensive monitoring, and the internal market clause. The resolution, which reiterates the goals of the e-Commerce Directive, calls for measures that prioritize consumer safety and maintaining consumer trust in the digital economy while preserving the

¹² Ibid.9

fundamental rights of the users. The second report from the Committee on Legal Affairs, and the Committee on Civil Liberties urges drafting necessary legal codes to support a competitive digital environment in Europe, and the Digital Services Act is envisioned as a worldwide standard-setter in this regard. The third one from the Committee on Civil Liberties, Justice, and Home Affairs asks for more justice, openness, and accountability in the content moderation procedures of digital services, as well as the protection of basic rights and independent access to legal remedies¹³.

In addition to the DSA, the Commission aims to provide a fair play environment for competition across platforms. The EU digital commissioner Margrethe Vestager stated that the EU and the US must develop shared approaches to determine the best methods to govern competition in the platform economy¹⁴. The executive branch is considering several options aligned with this goal, including enforcement of increased competition, ex-ante regulation of digital platforms, and the creation of a new competition instrument. Vestager has proposed a number of alternatives for ex-ante regulation of digital gatekeeper platforms, including banning platforms from advertising their own downstream services more prominently than those of competitors. In terms of data regulation, there is a proposal to create a 'data silo' rule, in which conglomerate platforms are forbidden from using certain data sets for specific commercial objectives in order to prevent them from leveraging it unfairly.

In addition to the Digital Services Act, there are also proposals to require internet sites to delete reported terrorist information within one hour, as well as implementing certain preventative measures such as upload filters. While the Parliament opposes the inclusion of upload filters in the text, both the Council and the Commission favor their inclusion. Even though the Commission is keen to go on with this swiftly, given a slew of unresolved problems, such as cross-border removal orders and the role of platforms in identifying and deleting content, it is doubtful that discussions will come to a close very soon¹⁵.

Criticism

One of the issues related to the new regulation is defining what constitutes the legal but harmful content within precise borders. Indeed there is a lot of subjectivity associated with expressions considered harmful which might be perceived differently from person to person. Various individuals can have various tolerance levels for a particular speech to perceive it as harmful. It is often the case that this

¹³ Ibid.9

¹⁴ STOLTON, S.: *Vestager calls for EU-US 'common vision' on platform competition policy*. *Euroactiv* (30 July, 2020). Available at: <https://www.euractiv.com/section/digital/news/vestager-calls-for-eu-us-common-vision-on-platform-competition-policy/> (date of download: 07/05/2021)

¹⁵ Ibid.14

is in the eyes of the beholder. Likewise legal but offensive content is also relative to the person who is being exposed to the content. This dilemma creates issues around legal but harmful content. In order to avoid unnecessary censorship, the DSA demands online platforms to prepare reports and be transparent about the content that is being removed or blocked. The DSA makes online platforms liable to constantly monitoring the content that is uploaded or posted by the users. Those platforms have to create reports periodically with relevant details about the content that received complaints, the ones that are restricted, and the ones that are removed altogether. However, this creates a new set of issues due to the increased resources required to perform this activity. For major digital businesses, this responsibility may entail a lot of hassles and financial consequences. Naturally, they can try to avoid this by taking down content that does not have to be illegal or necessarily harmful. There are a lot of gray areas when it comes to political ideas or political expression. On the world wide web, one can come across certain political groups or activism that deem certain political expressions offensive. Those groups can unite to create pressure to block or remove that content. Moreover, certain risky posts or media can be removed as it is easier to do it than dedicate the sources to constantly investigate such content or risk being penalized financially by the authorities. Rationally, platforms will decrease those risks and burdens by removing or restricting access to content that is legal but creates risks for the platform. In a profit-oriented big tech world, this can create preferences for certain content creators, certain posts, or certain social media content to be given priority. Outside of such content, certain media or posts can get the red flag due to the risk they might bring in the industry's perception. As a result of this, certain users will be pushed away from the mainstream platforms and those users can come together to create more marginalizing sub-platforms. Extremists and others can build online ecosystems with a lot of content management issues and migrate their unpleasant content from popular platforms to less controlled ones. At their newfound home, those contents can become truly offensive or even illegal as there will be less control mechanism. In the end, more and more objectifiable content can end up on the darknet, drawing more users towards the anonymous platforms. Such segmentation of users or groups can create problems within society. Ideally, the thoughts and opinions should be countered with one another in a respectful manner through debates and discussions rather than being polarized further and further within enclosed political groups in a democratic society. If political views are becoming increasingly marginalized, supporters of such political opinions will be able to gather together and propagate their thoughts in a confined environment with like-minded individuals. This can pose a great danger to the Western way of thinking and ideas of progress.

Moreover, another problem area appears which can contradict the main purpose of DSA. There is the idea to give smaller internet platforms a voice and prevent the monopoly of the big tech companies in the digital environment. Thierry Breton,

the European Commission's Internal Market Commissioner, informed the European Parliament that some big tech companies act as if they are “too big to care” about legitimate complaints they receive and their roles in certain situations¹⁶. According to the EU Commission's impact assessment on future legislation, major online platforms have developed and gained gatekeeper status as a result of the platform economy's zero-sum dynamics. Gatekeepers are cited as a source of significant worry since they have the capacity to take part in detrimental business activities. These tactics have an impact on both the users and their competitors. Furthermore, the DSA has some counterintuitive elements to it as it is the big tech companies who have the resources to go over existing barriers and create their ways to deal with any regulation in the most optimal way. Expecting big companies to reduce their capabilities and size is rather a utopian concept as all companies are built for profit and chase constant growth. They will not take it as a sign to degrow and give others more space. Instead, they will optimize the process in the most smooth way while the smaller competitors can easily fail at doing so. As a result, this will be more cumbersome and arduous for small companies to deal with than the big tech companies. Naturally, this can lead to further growth and dominance of already well-established corporations on the demise of the smaller local competitors. For instance, with all international legal teams, research groups, contractors, and experts YouTube will mostly find ways to minimize the impact of DSA than other video hosting companies that are smaller in size with fewer resources. The question is what chance do the small video hosting companies have to benefit from such regulation in face of internet behemoths like Google, Amazon, Microsoft, Facebook, Twitter, and others.

Some of the issues arise from the current market conditions and position of the EU in the technology sector. The current state of the capital markets is insufficient to encourage expansion from the European Market. The EU states are struggling to stay up with venture capital investment for digital entrepreneurship, which is widening the gap between the European Union and the United States. Since 1995, it is estimated that the United States has spent 1.2 trillion dollars in venture capital for companies, compared to 200 billion dollars in Europe which makes a six-fold disparity between them¹⁷. The regulatory regime has a variety of effects on the scale-up phase. To begin with, European capital market regulation, particularly for big institutions, makes it more difficult to rapidly expand the pool of money

¹⁶ KAYALI, L.: *Brussels' plan to rein in Big Tech takes shape. Politico* (2020). Available at: <https://www.politico.eu/article/digital-services-act-brussels-plan-to-rein-in-big-tech-takes-shape-thierry-breton-margrethe-vestager/> (date of download: 07/20/2021)

¹⁷ ERIXON, F.: ‘Too Big to Care’ or ‘Too Big to Share’: The Digital Services Act and the Consequences of Reforming Intermediary Liability Rules. *European Centre For International Political Economy (ECIPE)* (April 2020). Available at: https://ecipe.org/publications/digital-services-act-reforming-intermediary-liability-rules/#_ftn4 (date of download: 04/20/2021)

available for late-stage venture capital investment. Another issue is related to market limitations, which are usually more stringent in Europe than in other industrialized economies.

Such limitations raise entrance barriers to the market. Importantly, the market rules that reduce competition have a significant influence on business turnover rates, which is one reason why growing and scaling up entrepreneurial initiatives and innovative business models in Europe is more challenging¹⁸. As a result, the US is much ahead in the competition regarding the internet and technology sectors which reduces the EU's position while the EU is embracing rather more market protectionist approaches. Unless the European competitors assert their position in the market and the EU leads the innovation, the European position will remain defensive towards the expanding American or Chinese markets and their influences.

Germany's Network Enforcement Act or NetzDG

The Network Enforcement Act or in German *Netzdurchsetzungsgesetz (NetzDG)* is a regulatory act that was passed by the German Bundestag in June 2017¹⁹. The long version of the act is "Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken" which can be translated as "Act to Improve Enforcement of the Law in Social Networks". As the name suggests, the law intends to counter agitation and fake news on social media by requiring hate speech and unlawful information on the internet to be removed from platforms like Facebook, Twitter, and Google. The NetzDG requires an online platform with more than two million users to develop more efficient and effective means to report and delete potentially unlawful information. Threats of violence and defamation must be removed within twenty-four hours of receiving a complaint, or within seven days if the matter is more legally complicated. Companies must also provide an annual report outlining how many postings were removed and the reasons behind the removal²⁰.

According to Article 1 of the NetzDG, the scope of the law includes online service providers and internet platforms that make a profit from the content by allowing users to share content with one another. Such content can be available to the general public via social networks. Platforms that provide journalistic or editorial material, or individual communication, are not considered social networks under

¹⁸ ANDERTON, R. - DI LUPIDIO, B. - JARMULSKA, B.: *Working Paper Series Product market regulation, business churning and productivity: evidence from the European Union countries*. European Central Bank. Paper No. 2332 (November 2019). <https://www.ecb.europa.eu/pub/pdf/scpwp/pscpwps/ecb.wp2332~53142f69bc.en.pdf> (date of download: 07/20/2021)

¹⁹ BÖTCHER, L.: *Network Enforcement Act (Netzdurchsetzungsgesetz, NetzDG)*. *German Law Achieve*, In section 'Media, Post, Information And Data' (26 January 2018). <https://germanlawarchive.iuscomp.org/?p=1245> (date of download: 07/06/2021)

²⁰ KNIGHT, B.: *Germany implements new internet hate speech crackdown*. *Deutsche Welle* (1 January 2018). <https://www.dw.com/en/germany-implements-new-internet-hate-speech-crackdown/a-41991590> (date of download: 07/06/2021)

this act since the service provider bears the obligation ²¹. Furthermore, Article 2 mentions that if the social network has less than two million registered members in Germany, it is exempt from the responsibilities. According to Article 1, social network providers who receive more than one hundred complaints per year must publish half-yearly reports on the treatment of complaints regarding unlawful content on their platforms, including the topics listed in the subsection. Article 2 obliges them to publish these reports in the Federal Gazette and on their website within one month of the end of the relevant half-year. The reports they post on their website must be readily identifiable, directly accessible, and available at all times.

The Act further mentions that a social network provider is responsible for establishing an effective and transparent system for dealing with complaints regarding illegal content. They should provide users with a readily identifiable, instantly accessible, and readily available mechanism for reporting illegal content ²². They are in charge of evaluating the complaint right away and determining if the alleged information is indeed illegal and should be removed. There is also the option of restricting access to the content. If the complaint is deemed improper, appropriate action should be conducted within twenty-four hours of receipt. If the social network and the relevant law enforcement entity have established an agreement, this period can be extended for difficult matters. A seven-day time limit may be exceeded if the decision regarding the unlawfulness of the content is based on the falsity of a factual allegation or is clearly based on other factual circumstances. In such cases, the social network can allow the user to respond to the complaint before the decision is made. Within the terms of Directives 2000/31/EC and 2010/13/EU ²³, the procedure must guarantee that each complaint, as well as the action taken to rectify the problem, is documented in detail. Section 4 obliges the management to monitor the treatment of complaints each month. Any organizational flaws in dealing with incoming complaints must be addressed straight away. The administration of the social network must provide training and support programs in the German language to those entrusted with handling complaints regularly. Companies that fail to meet the deadlines face fines of up to 50 million Euros, while individuals may report infractions to Germany's Federal Office of Justice, or Bundesministerium der Justiz und für Verbraucherschutz, using the online platform created for this purpose ²⁴.

²¹ Ibid.19

²² Ibid.19

²³ Ibid.9

²⁴ Ibid.20

As an example, we can briefly go over the report published by Google regarding the complaints and removal of the videos published on Youtube ²⁵. Firstly, Google explains the justification why they are subjected to NetzDG. They point out that their users within the Federal Republic of Germany are above the two million thresholds. Therefore, as an internet platform that publishes user-generated video content, they fulfill the initial two conditions mentioned in the article. This gives details about how they go about removing videos from YouTube based on the Law. They further explain general remarks on how Google deals with allegedly illegal content. The report gives the sum of all the reported videos, reported either by the users or by the agencies. Google separates each complaint reason separately also by providing analytical insight for each category. Among them are privacy complaints, defamation, insults, sexual content, harmful or dangerous acts, terrorist or unconstitutional content, violence, and hate speech or political extremism. They also mention removal volume, verified reporting agencies that work with Google. This way they obtain information from submitters and uploaders but also seek external advice on the concerned materials. Another important part of the report is the information provided about turnaround time, or how long it took for Google to remove the content as per the complaint reason. Finally, the publication provides overall methods employed in the making of the report, with the process used for evaluation.

Criticism

Germany's NetzDG raises some questions and evokes some concerns regarding the freedom of speech. This regulation has received several criticisms due to the possibility of using it to censor undesired opinions by categorizing them harmful or illegal. To mention a few of them, we can begin with the one criticism that came from Wenzel Michalski, director of Human Rights Watch Germany. Michalski mentions that there are legitimate concerns for governments and the public about the spread of unlawful or harmful content online, but the new German law has some fundamental problems ²⁶. For him, the NetzDG is largely an over-ambiguous, overbroad act that transforms private firms into overzealous expurgatory with the fear of receiving high fines, while leaving users with no judicial supervision or right of appeal. Two important parts of the bill, according to Human Rights Watch, contradict Germany's responsibility to safeguard freedom of speech and the free exchange of information. First, the legislation charges internet service providers that host user-generated third-party content with some heavy-duty tasks to determine whether the content is illegal, or illegal. This can set the initial setting that

²⁵ GOOGLE: Removals under the Network Enforcement Law. *Google Transparency Reports*. (2020). Available at: <https://transparencyreport.google.com/netzdg/overview?hl=en> (date of download: 07/06/2021)

²⁶ HUMAN RIGHTS WATCH: *Germany: Flawed Social Media Law*. New York, NY, the USA (14 February 2018). Available at: <https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law> (date of download: 07/06/2021)

incentivizes the suppression of seemingly legal speech. The fundamental issue is that it is difficult to decide what constitutes legal but harmful content and according to whom. In fact, such decisions can be difficult even for the courts to make since they involve a deep grasp of the context, the society, intentions, participants, and the environment. Moreover, since all of these take place in the open, public internet, initial conditions are too general to declare a legal speech offensive. Companies have little margin for error on deciding if a content receives too many complaints since there is a limited review period with the potential to receive high fines. This can lead to blocking or removal of the content rather than immediately going through the complicated mechanisms to prove that it may not with some high stakes. The second concern that is expressed by Michalski is that if a cautious corporate decision violates a person's freedom of expression or access to information, the current regulation fails to offer either judicial monitoring or a judicial remedy. The liability lies at the internet hosts and service providers and they are the private parties. Private company policy will decide the fate of the user's content should it receive complaints. Moreover, the government entrusts the internet hosts and service providers with the powers to monitor, block or remove content, which can also work on behalf of the government and cater to its need for surveillance with the private sector's innovative force. As a result, the major internet sites become the non-accountability territories, where government pressure to censor eludes court scrutiny²⁷.

This possible mechanism that the NetzDG creates can cause violations of the freedom of expression. As a fundamental right, free access to information and freedom of speech is part of the universal human right. Such a breach of the practice of this fundamental right can occur when the companies end up with over-removal acts due to legal and financial pressures. Technically, nothing can stop legal content from being removed or blocked when an internet hosting company has limited sources to dedicate to verify if the content is harmful or not. Google, Facebook, Twitter, and others are the target social media platforms. These companies are global by nature and complicated local legal matters can be too much for them to process. For instance, they need all the dedicated legal personnel with expertise in various areas depending on the case that is being dealt with and a good level of the German language to decide if the online speech or content is truly illegal. Combined with huge financial penalties and tight deadlines, these requirements are difficult to satisfy for each individual case in practice. Germany is the biggest country in the European Union in terms of population. It also has a robust economy and a good IT infrastructure. All these translate into numerous online users who both produce and consume content on the internet. This is why

²⁷ Ibid.26

it is much easier to simply remove or block the content that received complaints on complicated matters rather than dedicating all the resources for a post or a video.

The second point of concern is privatized enforcement of the law that deals with public matters. Before the age of the internet, public issues were dealt with at courts. Nevertheless, with the digitalization of communication, the courts were rather lagging behind in the fast-changing digital environment. This regulation suggested as a remedy for this issue bestows the private tech companies with the power to execute their decisions on the public users and content. Before content takedowns, the NetzDG process does not require a court order, and it does not provide a clear appeal option for individuals to seek impartial remedy. The content that is being hosted on online platforms is mostly profited by those companies. They have exclusive rights and power over them. With this law, digital service providers are empowered to decide the fate of a user's post. For instance, companies can have different priorities and ways of dealing with possible violations for content that is commercially profitable than content that does not generate enough money.

The third point of concern relates to what constitutes "unlawful" related to speech or opinion. When the tolerance is low, even seemingly normal content can become sensitive and can be the object of blasphemy, defamation, or hate speech. For instance, a group of people with a particular ideology, partisanship, or religion can constantly pressurize the platforms with constant complaints. Such multitude and persistence might make the content seem illegal. There are many opinions and dissident views. Before the age of the internet, they did not have that many chances to be heard by the wider public. So, the points of friction were fewer and such collisions occurred less frequently. Nowadays with the widespread use of the internet, anyone's opinions and ideas can be heard thanks to technology. This naturally increases the surface area for possible collisions of ideas, beliefs, disputes in the public sphere. If a popular opinion is harshly criticized, people can target the critic. Does this give enough ground to make the content illegal? Furthermore, even if the content is deemed illegal and banned from the host services of the social media, could those opinions stop and be destroyed in that way? Furthermore, this can evoke a counter move in return and get more radicalized through attracting more sinister groups into the underground platforms that are out of the sight of the public eye.

That being said, we might have another unintended consequence. This phenomenon is called the Streisand effect. It is a social phenomenon in which an attempt to conceal, delete or censor information has the unintended result of further exposing that information, typically via the Internet. This effect is named after the American actress Barbra Streisand, whose effort to hide the California Coastal Records Project's image of her Malibu home, taken to chronicle coastal

erosion in California, accidentally attracted further attention to it in 2003²⁸. The Streisand effect is an example of psychological resistance, in which people are much more motivated to acquire and share knowledge once they are aware that it is being hidden from them²⁹. There are several examples related to this phenomenon. For instance, in France, the deletion of the French-language Wikipedia entry on the military radio station of Pierre-sur-Haute by the French intelligence agency DCRI (Stands for General Directorate for Internal Security in English) resulted in the article momentarily becoming the most-viewed page on the French Wikipedia³⁰. Another particular case also involved Wikipedia in Greece. Theodore Katsanevas, a Greek politician and the son-in-law of the country's previous prime minister, filed a lawsuit accusing Dimitris Liourdis, a 23-year-old lawyer in training from Athens, of libel and defamation³¹. Liourdis is a Wikipedia contributor in the Greek language. As a result, the Wikimedia Foundation has stepped in defense of Liourdis. Katsanevas eventually brought more attention to the subject which might be inflicting even more damage to his own image by taking the matter to court without fully comprehending the online encyclopedia's distinctive culture. Members of the Greek Wikipedia community have attempted to bring the story to the attention of journalists in reaction to the lawsuit. They've also put banner advertising in the Greek edition of the online encyclopedia in defense of Liourdis. The debate has spawned a slew of new entries in a variety of languages on different Wikipedia editions.

The UK's Online Harms Bill

In the United Kingdom, there has also been a growing concern about harmful content and behavior which take place on the internet. The government of the United Kingdom wants to assure online safety and maintain optimum conditions of internet platforms for starting and growing digital businesses. According to paragraph one the digital economy urgently needs a new regulatory framework to protect the online safety of the citizens, as the internet also attracts unlawful and

²⁸ WISEMAN, T.: *What is the Streisand Effect?*. *Morris Law Center* (27 August 2020). Available at: https://morrislawcenter.com/what-is-the-streisand-effect/#_ftn2. (date of download: 07/11/2021)

²⁹ BURNETT, D.: *Why government censorship [in no way at all] carries greater risks than benefits*. *The Guardian*. London (May 22, 2015) <https://www.theguardian.com/science/brain-flapping/2015/may/22/government-censorship-psychology-theresa-may> (date of download: 07/11/2021)

³⁰ GEUSS, M.: *Wikipedia editor allegedly forced by French intelligence to delete "classified" entry*. *Arx Technica* (7 April 2013). <https://arstechnica.com/tech-policy/2013/04/wikipedia-editor-allegedly-forced-by-french-intelligence-to-delete-classified-entry/> (date of download: 07/11/2021)

³¹ SAMPSON, T.: *Greek politician who sued Wikipedia editor clearly never heard of the Streisand Effect*. *Daily Dot* (19 February, 2014). <https://www.dailydot.com/news/greek-politician-wikipedia-libel-lawsuit/> (date of download: 07/11/2021)

dangerous activities³². Over the internet, there are various types of illegal and undesirable types of activities, content, and behavior that concern the users in the United Kingdom. The UK government is aware of the growing issues that can take place over the internet as it becomes a vital part of the economy, education, communication as well as innovation. There are several particular harmful and illegal acts that the UK authorities try to deal with.

To begin with, online platforms may be used for cyber-bullying and harassment (para 2, 6)³³. People in vulnerable groups can be harassed, bullied, or intimidated via the internet. Young people or children may be exposed to physiologically harmful or distressing content related to self-mutilation, or suicide. These materials may have significant psychological and emotional consequences on vulnerable groups such as children and teenagers. Furthermore, child sex offenders utilize the internet to watch and distribute media depicting child sexual abuse, trick children on social platforms to abduct them, and even live stream children being sexually abused. Another point of concern is related to content that displays violence (para 3, 5)³⁴. Rival criminal gangs often utilize social media to instigate violence and promote gang culture. This, coupled with the illegal firearms trade over the internet, can be a major cause of inhumane violence on the streets which will severely threaten public safety. On the other hand, extremists and terrorist organizations utilize the internet to disseminate propaganda meant to radicalize susceptible people and to transmit material that aids or assists terrorist activities

Another point of concern is related to particular issues brought about by the rise of algorithms and machine learning. Today social platforms utilize automation algorithms and machine learning to make relevant suggestions to the users based on their activities, engagement, and search history. This might seem a great way to customize the user experience on digital platforms but there are several disadvantages associated with the use of algorithms for this purpose. One particular problem is that the users can be bombarded with single-sided information based on their previous search history and engagement, which will pick up more or less similar political interpretations and viewpoints. Instead of being exposed to a variety of opinions and perspectives, social media users might be entrapped within a bubble of similar opinions and engage with the people of the same beliefs and political ideologies as the big online platforms utilize algorithms that might provide a person with only one sort of information (para 4)³⁵. This can encourage misinformation by preventing readers from seeing the events from a different angle through critics and opposition views. Even in social sciences and humanities, multiple sources are

³² DCMS/Home Office: *Online Harms White Paper*, para 1, 2,3, 4, 5, 6, 12. (15 December 2020). Available at: <https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper> (date of download: 07/11/2021)

³³ Ibid.32

³⁴ Ibid.32

³⁵ Ibid.32

required in order to make data less subjective. Nevertheless, news and political discourses can be personalized with high subjectivity that can be expressed with a personal narrative. If users consume only one type of narrative regarding a sensitive topic, they will be exposed to only one subjective way of interpretation of the event. This can grow into a more serious issue that has the potential to impede democratic values and principles in society.

To tackle such issues the United Kingdom prepared an Online Harms Bill paper. With their Online Harms Bill White Paper, the government of the United Kingdom wants to establish a free, open, and safe digital environment in the UK where people may express themselves freely without being directed to harmful activities and content (para 12) ³⁶. Another need is an online environment in which businesses take effective measures to keep their customers secure, and where criminal, terrorist, and hostile foreign state activities are not allowed to poison the online platforms. This regulation is designed to counter prohibited destructive conduct over cyberspace. Another goal is to increase awareness among the citizens about the dangers of harmful activities that take place on the internet and assist them with ways to confront inappropriate behavior online. It is also expected that the victims know how to seek assistance if they receive harm on a digital platform. It is especially the case for children and teenagers as additional protection is given to them. An ideal case would be a worldwide alliance of nations working together to keep their populations safe online where the public faith in internet businesses and services has been restored (para 12) ³⁷.

It was first proposed in April 2019 by the government of Theresa May to be worked on. Like the German NetzDG and the European Digital Services Act regulations, the proposed legislation gave digital service providers the responsibility of filtering user-generated information in a way that protects users from being exposed to illegal or dangerous content online. The proposal has been hailed as a groundbreaking apparatus by the government, which promises it would usher in a new epoch of liability for tech companies and bring fairness and accountability to the online world ³⁸. Hence, the UK government has declared that social media firms, websites, applications, and services that contain user-generated content must delete and limit the spread of dangerous information, media and content or suffer from fines that might reach huge sums. When content is deemed lawful but might cause severe physical or psychological harm to the public, it will fall under the purview of a government regulator. The law endorses Ofcom as the regulator, giving it the authority to issue unprecedented fines of up to eighteen million UK pounds or ten

³⁶ Ibid.32

³⁷ Ibid.32

³⁸ LOMAS, N.: UK publishes draft Online Safety Bill. *Tech Crunch* (12 May 2021). <https://techcrunch.com/2021/05/12/uk-publishes-draft-online-safety-bill/> (date of download: 06/04/2021)

percent of its worldwide revenue. As a result, significant data breaches might result in a five billion pound penalty for a corporation like Facebook ³⁹.

Criticism

Despite its rationale to tackle the growing issues on the internet, the Online Harms Bill has triggered different criticisms with various arguments along the way. Critics argue that these plans will stifle freedom of speech by pushing platforms to censor content excessively, while also causing a huge legal and operational burden for digital firms, which will suffocate technological progress, especially by crippling the smaller competitive internet service providers. The regulator will also be given the authority to prohibit access to websites, implying the possibility of censoring whole platforms ⁴⁰. Yet, these all begs the questions of how to define what stands as "harms" and if the social media platforms or the web hosting services should be given the power to act as a police of speech and have the power to censor speech based on their convictions. According to the director of the Online Harms Foundation Adam Hadley, creating hefty monetary fines for internet firms simply encourages excessive content censorship, leading to the removal of lawful material and the migration of conspiracy theorists to self-owned underground platforms where their ideas are not readily challenged or controlled at all ⁴¹. The Open Rights Group, a UK-based digital campaigning organization established in 2005 for the protection of rights to privacy and free speech, posed their concerns related to the government's interception of the private messaging, wide definition of legal but harmful content, and dealing with journalistic material. In a 15 December 2020 blog post, they argue that on the assumptions of abusive or terrorist material, private communications may fall within the scope of the online harms framework and be scanned and intercepted⁴². The service providers can decode the encryption that is used to protect communications exchange and reveal the communication between the users. As a result, encryption and privacy are treated as privileges based on corporate policies rather than fundamental human rights. Another main point of their argument is concerning "legal but harmful" content. The content that is legal but considered harmful creates an obligation to evaluate the risk, the likelihood, and consequences of that particular case within subjective standards to achieve objective legal compliance. They argue what stands as harm is highly subjective. For them, the result will not be different from collateral censorship, in which service providers and administrators will think that they are compelled to remove what may be totally innocent and innocuous

³⁹ HERN, A.: Online harms bill: firms may face multibillion-pound fines for illegal content. *The Guardian*. The UK (5 Dec 2020). <https://www.theguardian.com/technology/2020/dec/15/online-harms-bill-firms-may-face-multibillion-pound-fines-for-content> (date of download: 06/04/2021)

⁴⁰ Ibid.38

⁴¹ Ibid.39

⁴² BURNS, H.: Online Harms: Freedom Of Expression Remains Under Threat. *Open Rights Group (ORG)*, London, the UK (15 December 2020) <https://www.openrightsgroup.org/blog/online-harms-freedom-of-expression-remains-under-threat/> (date of download: 06/04/2021)

content rather than the risk of getting under the microscopes of a regulatory inspection that can have huge financial and reputational consequences if they do not comply. From this aspect, the freedom of speech can be threatened with such poorly defined and subjectively measured norms of "harm". Another aspect of the bill is about the content related to journalism. To protect freedom of speech, the government has indicated that newspaper and journalistic content published on their own websites will be excluded from the legislation. Such comments made under those articles will be excluded as well. The Open Rights Group argues that it is hard to perceive how this will operate in practice without providing areas where people may share newspaper content without being subjected to platform terms and conditions.

In fact, the definition of "harm" seems to be cumbersome to make an objectively measurable parameter. The harmful content and behavior is defined by the government, specifically by the Department for Digital, Culture, Media, and Sport as anything that "has a reasonably foreseeable potential of having a major detrimental physical or psychological impact on persons" in paragraph 2.2 of their white paper under the title of "Harmful content and activity covered by the duty of care"⁴³. The term "adverse psychological impact," according to Graham Smith, can simply refer to being upset or unhappy in a broader sense; the less clear the meaning, the more discretion would be required to determine what constitutes harm and what types of content or activity are within the scope of the content providers' duty of care⁴⁴. He goes on to ask about the criterion for triggering the duty of care. He raises an important question by asking, how can we properly establish a threshold among tolerant users as well as the most easily disturbed ones if someone comes up with a claim of being affected by a particular content and receiving psychological damages as a result of the exposure? He wonders how you can objectively assess the likelihood of a negative psychological effect in this case to establish objective parameters.

Discussions

Through the vast network of billions of devices, the internet functions as a conduit for the most fundamental freedom, freedom of expression to be exercised through instant and global access today. As it was discussed in the previous chapters, beneath

⁴³ DCMS/Home Office: *Online Harms White Paper: Full government response to the consultation*, para 2.2. (15 December 2020). <https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response> (date of download: 06/04/2021)

⁴⁴ SMITH, G.: The Online Harms edifice takes shape. *Cyberlegal Blog* (17 December 2020). <https://www.cyberleagle.com/2020/12/the-online-harms-edifice-takes-shape.html> (date of download: 06/04/2021)

all the advantages that internet technologies have yielded so far, there has been a growing potential and concern about the malevolent use of internet platforms. Such a new set of issues create new contested areas between the private companies, governments, and users that have the potential to end up with more and more limitations on the practice of the free exchange of information and ideas openly and globally through the internet. These issues create urges to be taken care of while pushing the government to take actions towards regulating some aspects of the internet which are characteristically restrictive. In a sense, the law is trying to catch up with technology, while there are many blank spots concerning the enforceability of laws and policies in cyberspace with unknown downsides of such regulations on other user rights and benefits. Currently, the European Union seems to be taking more strict measures to monitor and block the unwanted contents which are uploaded by the user on social media platforms hosted by internet service providers or intermediaries. Moreover, some regulations and policies that seem fit for the current challenges on the internet, have the potential to collide with the basic rights of internet users and content producers. Furthermore, a borderless internet is attempted to be ruled according to local jurisdiction which brings other issues as a byproduct. From a different aspect, this issue might be the reflection of a clash between the modern and the traditional where the internet's globalizing power is challenged by traditional institutions, namely the states. Even though the internet might have created a cyberspace realm, the states as the traditional sovereign powers have no intention to leave cyberspace alone through their rather underdeveloped or immature tools. As a result, striking a balance on a global level where all countries, all businesses, and individuals participate and benefit from the fruits of digitalization fairly and peacefully becomes quite difficult in a world made off by different cultures, political ideas, religious thoughts, and various approaches to everyday life matters. Therefore, we cannot expect a one size fit for everyone. Consequently, the result of the real-world application of the new internet regulations is difficult to foresee in the digital environment which moves in the fast lane. Therefore, there are various concerns and criticisms from different experts and parties as seen.

New internet regulations make social media platforms and internet service providers liable to report and respond to complaints regarding illegal content or legal but undesired content. This approach creates a new practice of private governance which might be a solution but also lead to further problems. A major part of these issues arises from the contents which revolve around sensitive topics or in a gray area regarding political extremism and hate speech. Not every marginal idea has to be labelled as extremism or fundamentalism. Not every idea or speech can be anchored to the mainstream version of discourse and measured where they stand on the political spectrum. Another important issue is also about the executive powers given to the private companies in the removal or blocking of the content. By requiring corporations to censor content on behalf of the government, the bill sets a troubling precedent for other governments, especially the ones with

authoritarian inclinations, to try to monitor user activities and control expression online. If this practice becomes a widespread practice among the less democratic states, the internet once imagined as an open platform for the free flow of ideas and information in the democratization process can become a tool of undemocratic governance and modern means to monitor and suppress political opposition. If content restriction practices become more and more prevalent among various states, the Balkanization of the internet will be imminent with yet unknown consequences.

Another issue is concerning the difficulty of controlling or dictating how things ought to be for something as big and complex as the internet. Why should people let the government intervene with their communication with expectations of security while the government with their limited sources and technical capacity will outsource this task to third parties? This can further revoke philosophical and moral questions concerning security versus freedom. So, should people give up a portion of their freedoms to receive an apparently more secure online platform? If security is the primary concern above all, the ultimate safety will be to shut down the internet entirely and there will not be any more issues. However, just like a durable ship is not built to rust at the harbor, the fear of the change can not be the ground for keeping the society from expressing their opinions and interacting with one another without creating a culture of fragility and offensiveness. Another question can be asked whether the users to be considered violators of service terms by default until they are proven innocent? If constant monitoring mechanisms detect allegedly unwanted or illegal content, it is expected to be taken down within twenty-four hours. Nevertheless, offensive content is subjective, relative matter with widely defined terms. Furthermore, if it is deemed illegal, it is done so without a court order. All in all, these situations create dilemmas while private internet companies are expected to act on behalf of the governments to tackle such content issues. How well a privately-held company can safeguard user rights and their contents and where lies the checks and balances? This concern is nothing but a more contemporary version of an ancient dilemma. The problem has been revoked by Juvenal in his *Satires* in the second century BC in ancient Rome when he wrote: "Quis custodiet ipsos custodes ipsos".⁴⁵ It can be translated into English as "Who will guard the guardians themselves". The phrase was originally intended to allude to the challenge of guaranteeing marital faithfulness, but it is now more often used to refer to the problem of regulating the conduct of those in positions of authority, which Plato discusses in the *Republic*.⁴⁶ If we can think of the social media and digital environment as a realm, whom and how shall we give the authority to guard it, if it requires a guardian at all? It is especially the case for speech restrictions.

⁴⁵ JUVENALIS, D. - J.: *Satires. Satire VI*, lines 347–348 (2nd Century AD) <https://www.thelatinlibrary.com/juvenal/6.shtml> (date of download: 06/07/2021)

⁴⁶ HURWICZ, L.: But Who Will Guard the Guardians? *The American Economic Review*, 98(3), 577-58 (2008). <http://www.jstor.org/stable/29730087> (date of download: 06/07/2021)

On the other hand, when deemed offensive, possible censorship of unwanted content or extreme political opinions will not stop these ideas from spreading. With a too wide definition of offensive, unwanted or illegal speech over the internet, countries can ultimately increase censorship which can even lead to the domination of popular opinion and the radicalization of the dissident voices. This brings us to the opposite side of the movement that gave birth to Western democracy and tolerance. In the dawn of the 20th century, the freedom of speech was echoed in the following words of Evelyn Beatrice Hall, in her book ‘the Friends of Voltaire’: “I disapprove of what you say, but I will defend to the death your right to say it”⁴⁷. In fact, it can be difficult to fathom how far we have come from this standpoint to the culture of offense and banishing the marginal ideas outside of the public space.

There are several regimes and government systems in place, each with its own set of political, geopolitical, military, economic, and cultural powers. In such a variety, everyone has various views on democracy and freedom, as well as diverse perspectives on their obligations to citizens and the use of force against them. This sort of strategy has the potential to become a template for pushing internet control under the guise of digital security. These efforts promote autocracies by demonstrating that the internet can be efficiently controlled by a central authority. Controlling citizens' interactions, influencing their connection to the outside world, suppressing rival ideas, and wielding an iron grip over media and news are all useful methods for maintaining power and dominance. Therefore, such practices of taking down online content can be indeed abused in the hands of less democratic and autocratic states.

To avoid such negative implications on basic user rights and freedom of expression, it is necessary to create some checks and balances. We can think of it as a free market, where the government intervention is minimal while it is led by a pluralistic interaction of various stakeholders and actors. This way a pluralistic approach where online intermediaries are shielded from government pressure through liability adjustments can elevate the pressure from the shoulders of the digital hosts and give it more time to analyze the content that received complaints. Such limitations can minimize or prevent abuses of power and potential large-scale censorships. It is also important to safeguard individuals against new forms of digital monitoring and exploitation. Fundamental rights should not be subjected to national security or other surveillance reasons. Principles like the Manila, provide policymakers and intermediaries with guidance for drafting, implementing, and revising policy, rules, and practices that regulate intermediary responsibility for third-party material. The ultimate solution lies in educating the public on various aspects to increase their media literacy. Nevertheless, achieving such a level of development, higher level of human development within the society and a better

⁴⁷ HURWICZ, L.: But Who Will Guard the Guardians? *The American Economic Review*, 98(3), 577-58 (2008). Available online at: <http://www.jstor.org/stable/29730087> (date of download: 06/07/2021)

social harmony which is more difficult to achieve. Therefore, the ultimate solution is to invest in public education and awareness in the long term rather than taking refuge in the bluntly restrictive regulations.

Conclusion

The internet has gained a prime position in almost every part of life and this has brought both opportunities and challenges. The opportunities are seized often by the private tech companies while the challenges are left to be dealt with by the relevant parties and policymakers. However, drafting laws in accordance with national frontiers is a highly changing task in borderless cyberspace. Nevertheless, there have been some attempts to regulate challenging aspects of the internet and issues in the digital environment by the European Union. The emergence of new internet regulations in Europe empowers internet intermediaries to monitor the content uploaded by the users and put restrictions if they find the content offensive or illegal. This approach, hence, leads to privatized enforcement of government policies by internet intermediaries and this practice has the potential to blur the line between the public and the private matters and interests. As the big tech companies seek profit, they can influence the rules of the game according to their corporate aims. This is how the laws regulating the legal accountability of intermediaries for the content they host ultimately have an influence on users' rights, including freedom of expression, freedom of association, and privacy. Moreover, governments expect immediate removal of offensive content and if this condition is not met, the internet intermediaries can face huge financial penalties. This poses financial risks which need to be avoided by the companies. This is how any content that received a number of complaints can be removed due to the financial risk potential without going through the long analysis and relevant context. In order to reduce possible side effects of such regulations, several suggestions have been made. To sum up, some immunity for internet intermediaries, greater transparency for corporate practices, and carefully crafted regulations can help to reduce the negative impact of content monitoring and restriction practices, yet there is a need for creating better channels. Better worldwide collaboration between academics, civil society platforms, business sectors, international digital society, and governments is necessary to assist the management of these present and potential future challenges. Such global issues need to be aligned with a global problem-solving capacity to create a secure, free, just, innovative, and a better connected world.

Bibliography

ANDERTON, R. - DI LUPIDIO, B. - JARMULSKA, B.: *Working Paper Series Product market regulation, business churning and productivity: evidence from the European Union countries*. European Central Bank. Paper No. 2332 (November 2019).

BALKIN, J. M.: Free Speech is a Triangle. *Columbia Law Review*. Yale Law School. Public Law Research Paper No. 640, (May 28, 2018).

BARATA, J.: Positive Intent Protections: Incorporating a Good Samaritan principle in the EU Digital Services Act. *The Center for Democracy & Technology* (29 July 2020).

BARATA, J.: *Regulating content moderation in Europe beyond the AVMSD*. London School of Economics (25 February 2020).

BARATA, J.: *The Digital Services Act and its Impact on the Right to Freedom of Expression: Special Focus on Risk Mitigation Obligations*. the Plataforma en Defensa de la Libertad de Información (PDLI). (27 July 2021).

BÖTTCHER, L.: *Network Enforcement Act (Netzdurchsetzungsgesetz, NetzDG)*. German Law Achieve, In section 'Media, Post, Information and Data' (26 January 2018).

BURNETT, D.: Why government censorship [in no way at all] carries greater risks than benefits. *The Guardian*. (May 22, 2015).

BURNS, H.: *Online Harms: Freedom of Expression Remains Under Threat*. Open Rights Group (ORG), London, the UK (15 December 2020).

ERIXON, F.: 'Too Big to Care' or 'Too Big to Share': *The Digital Services Act and the Consequences of Reforming Intermediary Liability Rules*. European Centre for International Political Economy (ECIPE) (April 2020).

ESPINOZA, J. - HINDLEY, S.: Brussels' plans to tackle digital 'gatekeepers' spark fevered debate. *Financial Times* (December 16, 2020).

GEUSS, M.: Wikipedia editor allegedly forced by French intelligence to delete "classified" entry. *Ars Technica* (7 April 2013).

GOOGLE: Removals under the Network Enforcement Law. *Google Transparency Reports*. (2020).

HERN, A.: Online harms bill: firms may face multibillion-pound fines for illegal content. *The Guardian*. (5 Dec 2020).

Human Rights Watch: *Germany: Flawed Social Media Law*. New York, NY, the USA (14 February 2018).

HURWICZ, L.: But Who Will Guard the Guardians? *The American Economic Review*, 98(3), 577-58 (2008).

JUVENALIS, D. - J.: *Satires. Satire VI*, lines 347–348 (2nd Century AD)

KAYALI, L.: Brussels' plan to rein in Big Tech takes shape. *Politico* (2020).

- KELLER, D.: *Who Do You Sue? State And Platform Hybrid Power Over Online Speech. Aegis Series Paper No. 1902*. Hoover Institution, Stanford University (29 January 2019).
- KETTEMANN, C. M. - TIEDEKE, A. S.: Back Up: Can Users Sue Platforms To Reinstate Deleted Content? *Internet Policy Review*, 9(2). (2020). DOI: 10.14763/2020.2.1484
- KNIGHT, B.: Germany implements new internet hate speech crackdown. *Deutsche Welle* (1 January 2018).
- LOMAS, N.: UK publishes draft Online Safety Bill. *Tech Crunch* (12 May 2021).
- SAMPSON, T.: Greek politician who sued Wikipedia editor clearly never heard of the Streisand Effect. *Daily Dot* (19 February, 2014).
- SMITH, G.: The Online Harms edifice takes shape. *Cyberlegal Blog* (17 December 220).
- STOLTON, S.: Digital agenda: Autumn/Winter Policy Briefing. *Euroactiv*. (18 August, 2020).
- STOLTON, S.: Vestager calls for EU-US ‘common vision’ on platform competition policy. *Euroactiv* (30 July, 2020).
- VAN HOBOKEN, J. - QUINTAIS, J. P. - POORT, J. - VAN EIJK, N.: *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: final report*. Publications Office of the European Union (29.01.2019) DOI 10.2759/284542
- WISEMAN, T.: What is the Streisand Effect?. *Morris Law Center* (27 August 2020).