GONDOLAT

2022

Doktori Műhelytanulmányok

Szerkesztette • Bartkó Róbert

Doctoral Working Papers

Edited by • Bartkó Róbert

Doktori Műhelytanulmányok 2022

Doctoral Working Papers 2022

DOKTORI MŰHELYTANULMÁNYOK

Doktori Műhelytanulmányok 2022

Szerkesztette • Bartkó Róbert

Doctoral Working Papers 2022

Edited by • Bartkó Róbert

Gondolat Kiadó
Budapest

A kötet az Igazságügyi Minisztérium jogászképzés színvonalának emelését célzó programjai keretében valósult meg.

Szerkesztette

Dr. habil. Bartkó Róbert PhD, habilitált egyetemi docens

Lektorok

Dr. habil. Bartkó Róbert PhD, habilitált egyetemi docens (SZE DF ÁJK Bűnügyi Tudományok Tanszék), Dr. Ferencz Jácint PhD tanszékvezető egyetemi docens (SZE DF ÁJK Munkajogi és Szociális Jogi Tanszék), Dr. Ganczer Mónika PhD egyetemi docens, tudományos és nemzetközi dékánhelyettes (SZE DF ÁJK Nemzetközi és Európai Jogi Tanszék), Dr. Hatwagnerné Dr. Kovács Viktória PhD egyetemi adjunktus (SZE DF ÁJK Kereskedelmi és Agrárjogi Tanszék), Dr. Hulkó Gábor PhD, egyetemi docens (SZE DF ÁJK Közigazgatási és Pénzügyi Jogi Tanszék), Dr. Kecskés Gábor PhD, egyetemi docens (SZE DF ÁJK Nemzetközi és Európai Jogi Tanszék), Dr. Kelemen Roland PhD, egyetemi adjunktus (SZE DF ÁJK Jogtörténeti Tanszék), Dr. Keserű Barna Arnold PhD, tanszékvezető egyetemi docens (SZE DF ÁJK Polgári Jogi és Polgári Eljárásjogi Tanszék), Dr. Knapp László PhD, egyetemi docens, oktatási ügyekért felelős dékánhelyettes (SZE DF ÁJK Nemzetközi és Európai Jogi Tanszék), Dr. habil. Szoboszlai-Kiss Katalin PhD, egyetemi docens (SZE DF ÁJK Jogelméleti Tanszék)

www.gondolatkiado.hu
facebook.com/gondolat

A kiadásért felel Bácskai István
Szöveggondozó Gál Mihály
A kötetet tervezte Lipót Éva

ISSN 2064-1788

Tartalom · Table of Contents

Előszó

A győri Széchenyi István Egyetem Deák Ferenc Állam- és Jogtudományi Doktori Iskolája több mint két évtizede rendezi meg éves konferenciáját. A tudományos találkozó nemcsak az ország doktori iskoláit képviselő doktoranduszok seregszemléje, de kiváló lehetőséget is biztosít a kapcsolatteremtésre, az új tudományos gondolatok megosztására.

A hagyományokat követve, 2021. december 10-én „A jogtudomány sajátosságai 2021 – A hagyomány szerepe a tudomány művelésében: Szladits Károly 150" cím alatt került sor a soron következő tudományos konferencia megtartására.

A pandémia ellenére jelentős számban regisztráltak a kollégák a konferenciára, előadásaikkal szinte valamennyi, az állam- és jogtudományokhoz tartozó tudományterület képviseltette magát. Büszkék vagyunk arra, hogy a konferencia töretlen népszerűséget élvez, melyet erősít, hogy valamennyi regisztrált előadó előtt nyitva áll a lehetőség, hogy gondolatait publikálja is.

Jelen kötet – illeszkedve a Doktori Iskola kiadványainak sorába – ezen elkészült, lektorált tanulmányokat tartalmazza. Bízunk benne, hogy a tanulmánykötet nemcsak az abban publikáló doktoranduszok számára nyújt majd segítséget tudományos fejlődésükben, de haszonnal forgatja majd a szakma és minden érdeklődő is.

A Doktori Iskola egyben köszönetet mond az Igazságügyi Minisztériumnak, hogy támogatta jelen tanulmánykötet megjelenését, mely „az Igazságügyi Minisztérium jogászképzés színvonalának emelését célzó programjai" keretében került kiadásra.

Győr, 2022. június

Dr. habil. Bartkó Róbert PhD. LL.M.
szerkesztő
habilitált egyetemi docens
A Doktori Iskola Titkára

Are internet regulation and freedom of speech at odds? How can the balkanization of the internet affect users' freedoms on the internet?

Yasin, Tokat
University of Szeged, Faculty of Law and Political Sciences

ABSTRACT
In democratic regimes and democratic policymaking, freedom of expression and unrestricted exchange of information are fundamental parts that help maintain the checks and balances of the whole system. The internet is meant to be a free, global platform where constructive ideas would contribute to human development from all around the globe that would increase democratization and individual freedoms. Yet, the dawn of the new millennium began to reveal some harmful effects of this technology in the hands of uninformed or malicious users. In order to adopt a safe and fair use of digital technologies in everyday life, certain changes are needed to ensure the security and reliability of the internet platforms. This way, states tend to respond to new challenges with new regulatory mechanisms. Nevertheless, such issues and rising control mechanisms also trigger concerns regarding the free flow of information and ideas on a globally accessible internet. The challenge is the difficulty of dealing with international legal problems efficiently and accurately over the internet. The apparent dominance of major digital platforms on the internet and the emergence of new concerns such as misinformation, disinformation, fake news, and political extremism, necessitate the establishment of some safety measures through regulations and legislation. Nonetheless, it is not the users' rights that need to be compromised and curbed in order to establish a secure platform. This paper aims to investigate the malevolent use of social media platforms, regulatory aspects of speech on digital platforms, and the positive and negative effects of the potential regulations on the exercise of fundamental human rights such as the freedom of speech and the free exchange of information from various aspects.
Keywords: *The Internet, Internet Laws, Digital IP Regulations, Data Protection, Cyberspace, Cyber Security, Fair Use of Internet, Diplomacy, International Cooperation*

1. Introduction

Internet technologies have brought many benefits and it is hard to envisage a modern society without these technologies. People utilize social media, create videos, write blogs, share digital content, engage with one another, and spread their experiences globally and freely all thanks to internet technologies. From this aspect, the internet serves as a conduit for the most fundamental freedom, the freedom of expression, to be exercised. Nevertheless, like many other things in life, there are also two sides to this technology. The dichotomy stems from the discord between the internet's enormous benefits and its ability to cause substantial damage at the hands of a few bad actors with malicious intentions. Despite all the benefits of internet technologies, there has been a growing concern about the malicious use of internet platforms. This pathology has recently emerged as a growing concern, with various states assessing potential countermeasures to combat this issue. Some restrictions and legislation are necessary to keep the internet safe and beneficial for all users, but they should not infringe on the fundamental rights of the citizens. Currently, there are areas of concern related to misinformation, disinformation, information manipulation, fake news, propaganda, political extremism, religious radicalism, terrorism, sharing of illegal content, cyberbullying, cyber-attacks, hacking, and using social media for malicious intentions. Given the functioning of democratic processes, national security, cybersecurity, financial security, and other socio-cultural aspects, these issues have the potential to cause some disruption in well-established states. This is why some countries are taking more daring steps to regulate the internet, putting more pressure and responsibility on internet service providers, social media platforms, search engines, and other internet hosts. There appear more and more regulations holding internet intermediaries responsible for monitoring, restricting, and removing the content deemed undesirable or illegal which was posted by their users.

The question, on the other hand, is whether the internet should be carefully governed and protected, with access limitations and attributions in place. Furthermore, such protective and restrictive actions pose some threats to democratic values. A democratic and free state must fulfill several conditions in order to function properly. Western Civilization has risen to prominence since the Enlightenment as a result of the advancement of scientific thought, freedom of expression, freedom of thought, liberal values, and legal, political, and religious reforms. Today, democracy is an indispensable characteristic of the Western world, where freedom of expression and knowledge are absolute prerequisites for functioning governance and policy making. If a growing number of countries continue to follow this restrictive paradigm, the internet's immense promise as a tool for innovation and participation in a global society of interconnected networks would be sacrificed. This may appear to be a conundrum, but it is not the first time such

contradictions have arisen. As the two millennia-old Latin proverb "Abusus Non Tollit Usum" goes "abuse does not remove use". This being said, misuse of a beneficial tool or thing cannot be the basis or justification for its removal. In today's interconnected world, this can be applied to the proper use of the internet as a platform for people to exercise their fundamental rights. As a result, this vast, complicated network of interconnected devices necessitates cautious maneuvering to avoid jeopardizing people's rights to use the internet freely and express themselves openly. This study focuses on factors that can lead to constraints on fundamental rights and freedoms, such as freedom of expression. Freedom of speech is a basic human right and the first paragraph of Article 10 (1998) of the Human Rights Act clearly expresses the right to freedom of speech[1]. It asserts that everyone has the right to express themselves freely without fear or threats. This right encompasses the freedom to hold and express opinions and to receive and transmit information and ideas without any interference from governmental authorities or institutions unless the content violates another law or causes national security issues.

Before the internet, the game's rules were clear, with established parties such as the government, the media, and the general public having specific responsibilities and areas of operation. Certain components of the status quo have been shattered by the information age, as new advancements directly challenge old establishments. Yet, the internet began as a simple experiment to carry out simple conversations between university campuses via data packages through a network of cables. Later, the internet's perceivable potential expanded its areas of operation with more and more functions. The United States initiated and triggered the rise of the internet age, and most Western countries developed their infrastructure and technical aspects to make it useful for the general public. Today there are millions and millions of people using computers, smartphones, and internet of things devices to connect to the internet on a daily basis. At first, the early developers and active members of the internet intended to make the platform a globally open place, free from political interference. Previously, it was less profit-oriented and more experimental. Nonetheless, due to its current widespread use, the internet is an appealing business platform for large technology companies to capitalize on. Governments have recognized that certain aspects of internet technologies necessitate regulations for safety, security, and financial reasons, as the internet's use has expanded and its profit potential has increased. The GDPR, for example, aims to protect users' private data from being used and handled without their knowledge or consent within the European Union.

When the matters regarding the free exchange of information, borderless internet, data privacy, digital competition, digital intellectual property, cybersecurity,

[1] Human Rights Act. (1998). Freedom of Expression. Article 10. Paragraph 1.

cyber espionage, data protection, digitalization of business, the rise of artificial intelligence, and ethical use of Information Communication Technologies are taken into consideration, striking a balance in a global level where all countries, all businesses, and individuals participate and benefit from the fruits of the digitalization fairly and peacefully becomes quite difficult. The world is made of different cultures, political ideas, religious thoughts, and various approaches to everyday life matters. As a result, real-world problems outside of the internet can create their resonance also within the digital world. While some governments are taking advantage of the internet by better aligning their national agendas according to the developments in the cyber world, 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 digital marketplace. This inequality and domination often leave some governments unprepared to handle international legal problems on the internet effectively. The dominance of big tech platforms over the internet, as well as the emergence of new cyber challenges, necessitate the development of safety mechanisms through frameworks and regulations, particularly in Europe. Moreover, some regulations and policies that seem fit for the current challenges on the internet, have the potential to create other issues related to the basic rights and freedoms 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 related to the beneficial use of the internet 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. Due to potential illegality, offensiveness, misinformation, and disinformation issues, there are emerging initiatives within the European Union towards adopting some sort of control mechanisms for user-generated content on social media sites. New legal and regulatory measures targeting internet service providers that host and share user-generated content are being implemented, such as Germany's NetzDG, the European Union's Digital Services Act, the United Kingdom's Online Harm Bills, and others. In essence, they are uncharted territories through which governments attempt to navigate based on their concerns, interests, and policy objectives. 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 open internet through firewalls, censorship, and legal attributions. As a result, actions performed in one region of the world might have a variety of repercussions across the entire digital ecosystem, both constructive and detrimental. 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 problems that take place on the internet.

As a result, there are debates about how to best direct the use of technology for the interests of nation-states, while governments have divergent stances on issues such as personal data use, data protection, intellectual property, cybersecurity, state espionage, copyright, free speech, censorship, among many others. When adopted recklessly and without due 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. Furthermore, because the internet is a worldwide platform, it cannot be managed by the laws and regulations of a single country. As a result, even if countries strive to enact domestically tailored legislation, they will be unable to manage the internet globally due to its international and complicated structure that exists in a politically and historically divided world where numerous countries have divergent interests. Such regulation may potentially divide the internet along the same lines as national borders, encouraging more digital nationalism as it happens in the People's Republic of China.

This paper investigates threats to free speech and the open internet while analyzing current issues related to illegal or offensive content such as social media disinformation, politically extremist discourse, hate speech concerns, hosting of such content through international service providers, liability issues related to those intermediaries on the internet, and removal or blocking of such unwanted content. Furthermore, various legal measures drafted by various countries and the EU to combat those issues are compared and the necessity behind such regulations is investigated. One of the research goals is to uncover some of the positive and negative effects of internet regulations on the practice of basic human rights such as free expression and the free exchange of information on digital platforms. This analysis sheds light on the common issues, concerns, and effectiveness of enforcement of such regulations. Concepts like the Manila Intermediary Liability Principles, digital neutrality, and digital due process are included to suggest alternatives for protecting free speech in the digital world. The research is expected to yield beneficial results suggesting how a more formal procedure can be followed to address issues on the internet, and how a balance between fundamental rights and the removal of illegal or unwanted content can be struck without making the public overly reliant on the decisions of internet intermediaries, international cooperations, and large tech companies.

2. Research Goals

1. Investigating the nature of free speech constraints, as well as unwanted or illegal content on the internet.
2. An examination of the potential negative consequences of internet regulations that may result in censorship, restrictions on free expression, state surveillance, and public-private collaboration against internet users.
3. Investigating potential remedies for mitigating the negative effects of internet regulations and improving fundamental rights protection.

3. Methodology

The research employs qualitative analysis. Issues concerning digital content, sharing of content, and content hosting are examined with the help of several expert critiques. Comparative analysis was used to determine the similarities and differences between various regulatory acts drafted in Germany, the EU, and the United Kingdom.

4. Literature Review

Jack M. Balkin presented his paper "Free Speech is a Triangle" at the Columbia Law Review's symposium "A First Amendment for All? Free Expression in an Age of Inequality" in 2018[2]. The paper contends that the notion of free speech that was dominant throughout the twentieth century is no longer adequate to safeguard freedom of expression. He argues that a dualist, dynamic model of speech control exists in contemporary era, with two fundamental types of players: regional states on the one hand, and individuals on the other. According to Balkin, the twenty-first century model is quite diverse with multiple stakeholders. He perceives the basic structure as a triangle, with nation-states on one side, privately held internet platforms on the other side while the users are in the other side. Balkin goes on to argue that the ability to have your voice be heard in the digital realm is influenced by a power struggle between influences such as old-school, new-school, and private regulations targeted directly at speakers, while both state and civil-society organizations press digital service providers to monitor and control speech. Three issues occur as a result of this application, according to his

[2] Balkin, Jack M. (May 28, 2018): "Free Speech is a Triangle". Columbia Law Review. Yale Law School. *Public Law Research Paper,* No. 640, https://ssrn.com/abstract=3186205, 17.07.2021.

analogy. First, nation-states employ new-school speech control to put pressure on digital firms, resulting in problems like collateral censorship and digital prior restraint. Second, social media corporations create complex private governance and bureaucracies that regulate end users arbitrarily and without due process or sufficient clarity. Third, end users are subject to digital monitoring and manipulation. The essay goes on to make several recommendations for how nation-states should govern digital infrastructure in accordance with free speech and press ideals.

Joan Barata is an active researcher in the areas concerning content restrictions on the internet and policies about cyberspace. He has published a number of papers concerning recently drafted regulations in the EU. He published an article titled "Positive Intent Protections: Incorporating a Good Samaritan Principle in the EU Digital Services Act" for the Center for Democracy and Technology in 2020[3]. His paper discusses various facets of hosting illegal, as well as legal but undesirable content that users upload or post on social media and hosting platforms. According to Barata, the "Good Samaritan" concept provides some immunity to internet intermediaries who take reasonable steps in good faith to protect their users from unnecessary content restrictions while at the same time shielding them from unlawful or otherwise lawful but offensive content. Granting immunity for hosting such content can incentivize the creation and implementation of private regulations addressing illegal or inappropriate content. This way, intermediaries have an incentive to operate and develop their operations within a reliable legal environment, which will allow them to filter the material they publish, and to deal with certain types of offensive speech more carefully, thanks to the safeguards provided by law. According to Barata, the Electronic Commerce Directive (ECD) establishes a broad intermediary liability framework applicable to hosting services, as well as a set of regulations for the implementation of potential monitoring responsibilities on intermediaries at the European level. Intermediaries are immune from liability insofar as they play a purely technical, automated, and passive role. However, intermediaries may be held liable if they do not act quickly to remove or disable access to illegal content after becoming aware of its presence on their servers. If they are found guilty, their immunity may be revoked should they fail to notice a specific illegal material when applying voluntary and proactive monitoring methods, causing the actual information to be distorted. This approach, Barata claims, does not fully facilitate the adoption of voluntary and proactive content moderation guidelines by intermediaries because of their active participation in monitoring the material they host. As a result, the more internet

[3] Barata, Joan (29 July 2020): "Positive Intent Protections: Incorporating a Good Samaritan principle in the EU Digital Services Act". the Center for Democracy & Technology, https://cdt.org/wp-content/uploads/2020/07/2020-07-29-Positive-Intent-Protections-Good-Samaritan-principle-EU-Digital-Services-Act-FINAL.pdf, 17.07.2021.

intermediaries screen, the more likely they will encounter potentially illegal data. Upon strict surveillance, the hosting providers become fully cognizant of the illegal content on their servers which leads them to apply more stringent control over the users and the content they upload. Due to the increased workload, this situation will increase the possibility of overlooking particular details, which in turn can increase the risk of liability considerably. 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 proposes clarifying the extent and requirements of notice-and-action mechanisms while exempting intermediaries from the duty of determining the legality of third-party content. He also emphasizes the importance of transparency in content moderation procedures and suggests assessing the effectiveness of reporting illegal content and content that violates service policies.

Dr. Barata has written another article about the Digital Services Act titled "the Digital Services Act and its Impact on the Right to Freedom of Expression: Special Focus on Risk Mitigation Obligations," which puts an emphasis on the Digital Services Act's implications on fundamental rights and freedoms [4]. Barata proposes that, due to its broad scope, the Digital Services Act can be a useful tool for ensuring that fundamental rights are respected and protected by crafting specific legislation tailored to sector-specific cases. Barata cites Article 8, which governs directions from appropriate legal and administrative national authorities to service providers to take action against specific unlawful or undesired content. The scope of these orders would be determined by the relevant authority, whereas national authorities can have extensive and almost unrestricted legal authority to unilaterally impose a particular interpretation of international freedom of expression principles on foreign governments. Barata points to Article 14 which regulates the notification and action processes. He mentions that before making any judgments on access blocking or termination, it is necessary to take the nature of the complaints into consideration. As a result, web hosts have the right and obligation to make an informed decision based on legality, necessity, and proportionality. This results in a complex structure involving government entities at both the national and EU levels. Consequently, the adoption and application of appropriate principles and protections become an essential requirement for the preservation of universal human rights such as freedom of expression and freedom of thought.

[4] Barata, Joan (27 July 2021): "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), https://libertadinformacion.cc/wp-content/uploads/2021/06/DSA-AND-ITS-IMPACT-ON-FREEDOM-OF-EXPRESSION-JOAN-BARATA-PDLI.pdf, 4 August 2021.

In 2019, Joris van Hoboken, Joo Pedro Quintais, Joost Poort, and Nico van Eijk carried out a study for the European Commission.[5] The study "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" outlines the scope of the providing safe harbor in the context of internet regulations governing the hosting and sharing of unlawful content, as well as questions about the legal and practical application of Article 14 of the Electronic Commerce Directive[6] (2000/31/EC). Their study looks at the various revenue streams available to hosting intermediaries, as well as how these revenue streams may influence the incentives for services that address illegal or infringing third-party activities. Finally, the study examines the most pressing legal issues surrounding Article 14 of the Electronic Commerce Directive, with a focus on European Court of Justice case law and other formal discussions.

Prof. Giovanni Sartor and Dr. Andrea Loreggia are researchers from the European University Institute of Florence who specialize in computer law, artificial intelligence, and content law. In 2020, they published a paper titled "The Impact of Algorithms for Online Content Filtering or Moderation – Upload filters" on the European Parliament's Think Tank[7]. Their research is beneficial since manual content monitoring typically necessitates significant resources and money. As a result, using algorithms and machine learning to identify undesired or infringing material is both convenient and cost-effective. The European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs commissioned this research project on automated content filtering systems. Automated filtering is proposed as a component of user-generated content monitoring and management in the study. It outlines the existing filtering methods for dealing with various forms of content, including text, images, and videos. In addition, the study looks at the most challenging obstacles within the current legal framework and makes regulatory proposals for a future EU Digital Services Act.

[5] Van Hoboken, Joris – Quintais, João Pedro – Poort, Joost – Eijk, Nico van (29 January 2019): "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*, ISBN 978-92-79-93002-7, DOI 10.2759/284542 Catalog number KK-06-18-016-EN-N, https://op.europa.eu/en/publication-detail/-/publication/7779caca-2537-11e9-8d04-01aa75ed71a1/language-en, 17.07.2021.

[6] 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, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM:2020:825:FIN, 5 July 2021.

[7] Sartor, Giovanni – Loreggia Andrea (15 September 2020): "The impact of algorithms for online content filtering or moderation – Upload filters". European Parliament. Policy Department for Citizens' Rights and Constitutional Affairs, https://www.europarl.europa.eu/RegData/etudes/STUD/2020/657101/IPOL_STU(2020)657101_EN.pdf, 17.07.2021.

Daphne Keller wrote an article titled "Who Do You Sue?" on Stanford University's Hoover Institute's Aegis Paper Series in 2019 [8]. Keller's research looks into the clashes between rights to free speech and content removal practices on internet platforms such as Facebook, YouTube, and Twitter. The first part of the paper exposes the intricate combination of government and private influences behind various content removals, as well as how this combination hinders the capacity of the individuals to challenge government action. The second portion dives into the legislative conundrum that users and legislators encounter when they attempt to claim their freedom to interact without restrictions on major internet sites. Keller goes on to discuss the challenges caused as a result of the inextricable relationship between state and private powers, which may act against the fundamental freedoms of the users. The government may hold the authority, but the platforms and innovative ideas are owned by the private sector. Her analysis emphasizes that the users could be the weakest link in this chain if there is no strike of balance. As a result, she goes on to emphasize how important it is to understand and communicate with both government and commercial organizations in order to understand and protect internet users' rights.

5. Regulating the Internet and Speech

5.1. Approaches Within the EU

A well-functioning democracy and democratic processes require freedom of expression, free exchange of information, and of course a free press spared from the scourge of political and judicial pressures. When such liberties are not respected and diligently guarded, accountability and the rule of law can be jeopardized. This has the potential to compromise democratic institutions and the fundamental rights of the citizens. The EU went through several wars and various experiments of governance to mature an understanding of human rights, fundamental freedoms, and securities for its citizens. Today it is recognized within the EU that people are getting increasingly more reliant on the internet as an indispensable means for having their everyday activities done such as conversation through audio, text, or video, knowledge transfer, online education, digital healthcare services, entertainment, and commercial transactions. As they have evolved into essential instruments for the free flow of information and ideas, digital communication systems contribute to the enjoyment of a variety of fundamental rights such

[8] Keller, Daphne (29 January 2019): "Who Do You Sue? State And Platform Hybrid Power Over Online Speech". *Aegis Series Paper*, No. 1902, Hoover Institution, Stanford University, https://www.hoover.org/research/who-do-you-sue, 17.07.2021.

as freedom of speech and access to information. The Internet can be a platform for unity and dialogue for the European Union which is based on heterogeneity, and diversity through different languages and cultures. The EU needs a competitive and dynamic digital ecosystem that may foster innovation, improve network availability and performance, reduce costs, and support the free flow of a diverse range of online content and services. Non-transparent traffic management, content and service discrimination, or connectivity restrictions may jeopardize users' right to access and share information online, as well as the creation of new tools and services [9]. As a result of these developments, the users have legitimate expectations that internet services remain accessible, affordable, secure, reliable, and longstanding. In line with Article 10 of the European Convention on Human Rights, all Council of Europe member states have committed to providing the basic right to freedom of expression and information to everyone under their authority. Article 10 of the European Convention on Human Rights also guarantees everyone the right to freedom of speech and access to information when it comes to communications that may take place both offline and online[10]. This includes the fundamental rights to freedom of expression without regard to national borders, to respect for private life and correspondence, rights to freedom of thought and religion, freedom of association, access to education, protection of property, as well as related procedural rights guaranteed by the European Convention on Human Rights. Existing norms for traditional media can be applied to new media as well, implying that the online publishers and users are entitled to those rights and are liable for their actions. These rights are adjusted in harmony with other legitimate interests such as national security, information safety, discrimination, or hate speech. The European Court of Human Rights, which was established by the European Convention on Human Rights, deals with alleged violations of Article 10 when they are submitted to the Court after all the local remedies have been exhausted. When it comes to the assumed illegal content on the internet, the competent national authorities can make a provisional or final decision on the illegality of the subject matter, then appropriate measures can be taken to enforce the removal of the internet content or the blocking access to that particular content. In this case, the safeguards of Article 10, paragraph 2 of the Convention for the Protection of Human Rights and Fundamental Freedoms are to be respected[11]. There are certain issues related

[9] Committee of Ministers (29 September 2010): "Declaration of the Committee of Ministers on network neutrality". the 1094th meeting of the Ministers' Deputies, Council of Europe, https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805ce58f, 30/7/2021.

[10] Committee of Ministers (13 January 2010): "Declaration of the Committee of Ministers on measures to promote the respect of Article 10 of the European Convention on Human Rights". the 1074th meeting of the Ministers' Deputies, Council of Europe, https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cfdad, 30/7/2021.

[11] Id. 54

to the borderless nature of cyberspace that operates within the world that is separated by political frontiers, each with its own jurisdiction. The public internet is expected to be reliable, accessible, and open for everyone so people can fully enjoy their rights to freedom of expression, access to information, and the free exchange of information over online platforms. Furthermore, technical breakdowns and deliberate interruptions can obstruct access to information. The Council of Europe has created a framework for international collaboration in order to avoid and respond to such events in cyberspace. The Council of Europe is working to safeguard and promote freedom of speech and open access to information online, and the following are some of the major challenges they are currently tackling.

It is absolutely necessary to keep human rights norms in regard when developing the regulations to secure and protect the free flow of information while also ensuring legality across borders. It is important to examine how to strike a balance between security concerns and the preservation of people's fundamental rights. This requires working with other stakeholders to develop a framework of understanding and obligations to defend the internet's universality, integrity, and openness as a way of ensuring freedom of speech across borders. Another hurdle is the creation of a network neutrality policy with its principles based on human rights to ensure that internet users have the broadest possible access to the information, applications, and services of their choice. Another challenge is ensuring that internet material is available to all present and future users. Developing suggestions and best practices to assist governments and internet intermediaries functioning as media gateways in fostering freedom of expression and access to a diverse range of pluralistic, high-quality, and diverse sources of information is of vital importance. Increasing technical awareness among individuals of all ages and socioeconomic groups is one of the approaches to make the internet more accessible and beneficial. Furthermore, the internet can also be part of modern governance where relevant information can be shared with the public instantly. This is how the internet can also provide access to official records which may enhance transparency and accountability within a democracy.

Several concepts have already been agreed upon by the members of the committee in terms of ideal conditions in the digital environment. There is a basic idea, known as network neutrality, that should apply regardless of the infrastructure or network used to connect to the internet[12]. The first principle concerns internet content rules. It stipulates that member states should not impose limitations on internet content that are more stringent than those imposed on other forms of content distribution. The second principle deals with self- or co-regulation. So,

[12] Committee of Ministers (8 May 2003): "Declaration on freedom of communication on the Internet". The 840th meeting of the Ministers' Deputies, Council of Europe, https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805dfbd5, 30/7/2021.

EU member states should support self-regulation or co-regulation of online material. The absence of prior governmental control is the third principle. It advises governments not to use blanket blocking or filtering techniques to prevent citizens from accessing information and preventing other forms of communication on the internet, regardless of their geographical location. However, it does not include the installation of filters to safeguard children, particularly in locations where they use internet access to reach learning materials, such as at schools or in libraries. The fourth principle addresses the elimination of hindrances to people's involvement in the information society. It is recommended that EU nations develop and support nondiscriminatory, low-cost access to internet technology and information services for the wider public. Furthermore, the public's active engagement on the internet, such as the creation and maintenance of individual websites, should not be subject to any licensing or other comparable restrictions. The fifth principle addresses the freedom to provide internet-based services. The distribution of internet-based services should not be subject to specific authorization processes based only on the transmission mode used. In other words, member states should take efforts to promote a pluralistic internet service offering that caters to a wide range of user and social group needs. Service providers should be allowed to operate under a regulatory framework that guarantees the equality of access to both national and international communications networks. The sixth principle is about the limited liability of service providers for the digital content they host[13]. The EU states should not impose a general requirement on service providers to monitor the content they maintain in their servers and offer access to other users. Nor should they actively inquire about facts or circumstances suggesting unlawful conduct. They should also guarantee that service providers are not held responsible for material on the internet when their role is confined to just transmitting information or providing access to the internet, as defined by national law. If service providers' functions include handling content from third parties, EU states may hold them jointly liable if they fail to act quickly to remove or disable access to content as soon as possible as defined by national law, regardless of their illegal nature or, in the case of a claim for damages, facts or circumstances revealing the illegality of the activity or information. The freedom of speech of individuals who initially made the material available, as well as the equivalent right of access to the information, must be respected. Such limitations of liability do not rule out the possibility of issuing orders requiring service providers to cease or prevent a breach of the law, to the degree possible. The seventh principle is about anonymity on the internet. Member states should respect the wishes of internet users not to reveal their identities in order to protect them against online monitoring and to promote the free exchange of information and ideas in a safe

[13] Id. 56

way. This does not preclude member states from taking necessary steps to track down those responsible for criminal acts, by national law, the Convention on the Protection of Human Rights and Fundamental Freedoms, and other international agreements in the fields of justice and law enforcement.

Overall, the Committee of Ministers maintains that users, as well as service, application, or content providers, should be able to weigh the impact of network management measures on the enjoyment of fundamental rights and freedoms, particularly the rights to freedom of expression and to share or receive information without regard to borders, as well as the right to privacy[14]. Those interventions should be appropriate, reasonable, and free from discrimination or any unjust approaches. Furthermore, every current case of content restriction or removal should be evaluated on a regular basis and the existing restrictions shall be kept no longer than what is strictly necessary for the purpose of transparency and justice. Any network management actions that have a substantial impact on access to content, applications, or services should be appropriately communicated to users and service providers. In terms of procedural protections, there should be proper mechanisms for challenging network management decisions and, when necessary, seeking resources while respecting rule of law standards.

Despite the existence of such broad concepts, nation-states have differing perspectives on what constitutes freedom of expression and where it ends. As the European Union is made of different states with different cultures, histories, languages, and forms of government, they have the sovereignty to decide how they interpret their national concerns in face of security challenges. For instance, one gesture or a word may be tolerated in one country but can be considered offensive or defamation in another one. Therefore, it can be questionable how a consensus can be reached out of such differences and through some high-level designs. Every geopolitical, political, even public health-related matter might have different ways of being handled or different priorities. Let us consider one recent event brought by the COVID-19 pandemic. As the pandemic rages wild all around the globe, many countries went for massive vaccination campaigns. Social media and the internet were some of the important means to spread awareness during the pandemic. Nevertheless, the reaction of the public was not the same in all countries. Various countries emerged successful in their vaccination campaign with better public support whereas, in some other countries, such campaigns were criticized widely with numerous conspiracy theories and false claims over the internet. The countries that emerged successfully did not owe their success to the restriction of information over the internet but rather to a good media literacy of the citizens and a strong public trust in the state institutions. So, if people have a matured political culture and trust in the government, the voice of the conspiracy

[14] Id. 53

theorists will not be louder than the state officials. Yet, if the public has less trust in the government institutions, such as the ministry of health, they will be suspicious of the official information they receive which might make them more interested in alternative narratives. If those countries handle the spread of such ideas and false news, they will need to take measures and legal steps according to their own circumstances. So what constitutes freedom of thought about vaccines in one country can become a probability of public health threat in another. Therefore, it is a challenge to set a standard in this case as the issue is also related to political, economic, and socio-cultural conditions within a particular country. So, how can such situations be handled through a standard approach in this complexity? The following section will highlight some of the details concerning the perception of fake news and freedom of expression within various European Countries.

5.2. New Speech Regulations

The European Union seems to be an ideal environment for more united and effective approaches toward 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. Due to the vastness of user-generated content, newly drafted regulations empower large social media platforms and internet hosts to monitor content produced by internet users on behalf of state institutions, as states may lack the technical and financial capacity to analyze such content in courts and formal state institutions. New regulations like Germany's NetzDG, the EU's Digital Services Act, or the United Kingdoms' Online Harm Bills utilize new methods to deal with illegal or offensive content on the internet platforms. These new 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. The expansion and spread of private governance are driven by new speech regulations according to Balkin[15]. Such new speech regulations are relevant for private governance because they give the liability and ownership of the possible issues to the host of the content which is private internet companies such as Google, Amazon, Facebook, or Twitter. Individual countries may demand more from digital-infrastructure businesses as they grow more powerful which

[15] BALKIN: *op. cit.* (2018)

helps the states also assert their policies and increase the monitoring and control activities while the internet hosts can collect and analyze content from their end-users. The internet platforms have to respond to the complaints promptly and takedown offensive or illegal content within a short period. If they do not meet these obligations, they have to face huge financial penalties. Consequently, 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 financial consequences 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. As governments attempt to co-opt and compel private internet service providers to work with them, those companies are being charged to carry on administrative functions such as speech control and surveillance on behalf of the states. This is why such practices are deemed as the new speech regulations as they are enforced by the privately-owned companies upon the online users. Moreover, the big tech companies are key to innovation and power which can motivate nation-states to leverage the capabilities of big tech firms to increase their own monitoring and surveillance capacity. As a result, whether it is social media, web hosting platforms, search engines, or video hosting platforms companies, intermediaries on the internet have the capacity to create government bureaucracies and algorithms to achieve nationwide objectives. This development has consequently created a new phenomenon which is privatized bureaucracy[16].

In this broad area, the real question is how to keep the internet global without censorship and still be able to govern the internet in line with the national interests? At the core of this issue lies the following question; how the drafted laws can be enforced in actual cases beyond all the presumptions and theories? If a state needs some regulation, how can it be enforced coherently and thoroughly, especially in areas where there are international disputes. If policies and regulations prove to be unenforceable due to jurisdictional or substantive issues, there can be a threat that the internet actors will treat them as if they were null. Therefore, enforceability is a key aspect of the development of internet laws and regulations. This aspect of the regulation is more difficult to frame so that the legal codes can function well in practice. Unenforceable laws can weaken the very concept of rule and its value within society.

In a privatized bureaucracy, universal jurisdiction is enforced by pressuring or co-opting internet service providers to impose specific content or speech standards across a region or a country. The more effective service providers are in identifying the location of the user and enforcing speech regulations throughout the world, the more nation-states may be tempted to use these technical capabilities

[16] Id. 11

for their own purposes[17]. This would have the potential to ignite the domino effect towards a widely balkanized internet where internet content and access to services can change dramatically from one location to the other. Moreover, when nations use commercial infrastructure to restrict online speech, they may also use the surveillance capacity of the service providers with their data collection, and analytical capabilities to address their own governance and control issues. As a result of these factors, there seems to be a tangle of power, control, and monitoring interactions with a possible cost on individual rights and freedoms. Users, content providers, mainstream media, and civil society organizations have now become the subject of both old-school and new-school speech control by nation-states, as well as private governance by digital infrastructure firms. The question arises whether a compromise on fundamental rights can be justified in digital platforms because of the rising threats and issues on the internet.

5.3. Is the Internet a Universal Human Right?

There are ideas that suggest that the internet should be a basic human right. The years 2020 and 2021 especially saw the rapid expansion of digitalization due to the COVID-19 pandemic. Education, business, work, healthcare, entertainment, and many other daily activities were conducted through the internet because of the pandemic. Indeed, it becomes more and more difficult to operate our lives without computers, smartphones, and an internet connection to make it all possible. Now, the internet is no longer a luxury or an option but an indispensable means to conduct essential activities. Furthermore, access to the internet is closely connected to international human rights as it became the platform where the full exercise of freedom of speech, civic engagement, education, government services, and enjoyment of scientific achievements can take place. From this aspect, it is extremely difficult to isolate most of the essential activities that make daily life up and running from the internet network. UNESCO was one of the first international organizations to call on governments to make efforts to ensure that everyone has access to the internet due to this foreseen functionality of the online platforms. In its 2003 recommendation, UNESCO stated in Article 7 that the member states and international organizations should enhance internet access as a public service by implementing sustainable initiatives to promote the process of enabling people and civil society to have access to it. It further suggests encouragement and support of drafting proper policies and their implementation in developing countries

[17] Id. 11

while taking into account the needs of rural communities[18]. Article 15 goes on by stating that member states should acknowledge and enforce the right of citizens in modern democratic societies to have universal internet access to public and government-held records, including information relating to their activities, while taking confidential information, privacy, and national security concerns, as well as intellectual property protection into account. International bodies should acknowledge and promote each country's right to obtain critical data on its social and economic status. From this perspective, UNESCO perceived the internet as an essential tool for global development and innovation. This is how the internet is suggested as an essential right by them.

The perception of modern life and expected quality of living often include forms of engagement with the larger segments of the community and the even globe via the internet. This position appointed to the internet makes it an indispensable platform for all of these activities to take place. Therefore, it is very critical to examine the relationship between the fundamental rights and the present means to exercise and enjoy those rights as technological advancement affects how individuals engage with one another and conduct civic matters on a daily basis. Some nations such as Greece, Estonia, Finland, Spain, Costa Rica, and France have stated or acknowledged some right of internet access in their legal texts, constitutions, or court judgments. In the end, it is the progress of human civilization and the law is expected to move along as the social needs evolve. The current growth and application of the internet might demand more extensive legal changes to adopt changing social situations. The internet's rising relevance in social, business and educational life necessitates ensuring its accessibility for the greater parts of the global society. From this point of view, there is enough public support that recognizes the growing role of the internet in society.

On the other hand, some approaches oppose the idea of recognizing the internet as part of human rights. Although certain nations, particularly in Europe, have domestic law that establishes a right of access to the internet, there is no international treaty that explicitly establishes such a right. In other words, if the global community has not acknowledged the internet as a human right in a binding document, and there are no talks over the possibility of a new treaty to do so on any platform, it is technically not a human right. Furthermore, the internet is recognized as a means like other means such as television or radio. Because there is no human rights part to the access to television, the telephone, the writ-

[18] UNESCO: "Recommendation Concerning the Promotion and Use of Multilingualism and Universal Access to Cyberspace". 2003, Paris, http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/official_documents/Eng%20-%20Recommendation%20concerning%20the%20Promotion%20and%20Use%20of%20Multilingualism%20and%20Universal%20Access%20to%20Cyberspace.pdf, 3 August 2021.

ten press, or any other equivalent medium, states are not obligated to offer their citizens free internet access. This can be especially a financial burden for underdeveloped countries which can make them take on infrastructure projects too costly for them. Assuredly, for any developed state, a decent internet connection at an affordable price is an expected standard. Nevertheless, this still does not make it obligatory for the governments to take on such tasks. Therefore, according to some people, the internet is accessed through technology, which is a means rather than a fundamental right. Furthermore, access to the internet is not an economic right as defined by Article 11 of the ICESCR[19] and Article 25 of the UDHR[20], because they are reflective of standards of living that cannot be compared across nations at various levels of development. It is not required to have internet access to participate in a political community. A large portion of the world's population does not have access to the internet. This argument can be considered at the national level among the developed nations where such digital engagement is already established within their territory and taking away this access can cause serious disruption in daily life and business which will create dissatisfaction among the citizens of those countries. So, if an underdeveloped country misses such a level of digital experience, culture, and participation, we may not expect it to have such priorities about the quality of internet access, digital products, and online services. Declaring the internet as a fundamental human right without addressing the conditions under which it may be fulfilled can inflate the number of rights while weakening the force of conventional human rights. At this point, the versatility of existing human rights matters can be reminded. It is not essential to create new rights in addition to those that have already been recognized. Rather, it is important to guarantee that the existing rights are exercised and enjoyed while considering the changing technological environment. Let us remind ourselves that there is no equal access to technology in every part of the world. As a result, access arrangements will favor users who have devices that can connect to the internet, increasing disparities among various users. On the other side, a lack of government oversight would necessitate investment in private telecommunications firms, putting them ahead of citizens in terms of economic gain. That being said, the internet might formally become a universal right one day but the current shift occurs locally which means that before it becomes universal, more and more countries need to catch up with the technology level.

[19] United Nations (1976): "International Covenant on Economic, Social and Cultural Rights". Resolution 2200A (XXI) of 16 December 1966 entry into force 3 January 1976.

[20] United Nations (10 December 1948): "Universal Declaration of Human Rights". Draft Committee, Palais de Chaillot, Paris.

6. Current Issues and Limits of Free Speech

6.1. Fake News

The "fake news" phenomenon is one of the terms that gained huge popularity at the beginning of this decade. Despite its popularity, the term itself does not have a precise definition and is used to define a wide range of incorrect information that circulates within the public. In more detail, the concept of fake news is about a wide range of misleading or erroneous information, including unintended and unconscious activities, as well as a combination of truth and personal viewpoints from high-profile figures. Alternative to term fake news, junk news, pseudo-news, alternative facts, and hoax news are all names used to describe the same underlying problem. In a nutshell, fake news is information that is incorrect or misleading in truth yet presented as news[21]. It is frequently utilized to harm the reputation of a person or an entity. Fake news can also be used for monetary gain or profit through false advertising or marketing. In this age of digital transformation, the internet is the primary source of information, which also makes news consumers more likely than ever to come across and share fake news on their social media channels and messaging platforms. Social media users across the world constantly engage with the newsfeed, read, watch, or listen to the news every day for updates on any subject matter. A level of trust and accuracy is expected and the users can sometimes assume that whatever they discover over the internet is accurate and reliable. According to Amy Watson from Statista, navigating the news media environment is becoming more difficult than ever before for many people, leading to some consumers throughout the world intentionally ignoring the news[22]. Michael Hameleers, Anna Brosious, and Claes H. de Verses conducted a study about news users who are concerned about misinformation in their information environment across ten different European countries. According to their findings, respondents are more inclined to connect disinformation with politicians, businesses, and foreign actors. In a large-scale poll of individuals in 10 European nations, 6,643 people reported their opinions on which sources they hold responsible for the spread of incorrect information and which issues are most impacted by disinformation[23]. Their findings show that disinformation is

[21] Higdon Nolan (August 15, 2020): "The anatomy of fake news: A critical news literacy education". University of California Press, https://www.jstor.org/stable/j.ctv1503gc8, 30 July, 2020.

[22] Watson, Amy (28 May 2021): "Statistics and facts about fake news worldwide". *Statista*, https://www.statista.com/topics/6341/fake-news-worldwide/, 11/08/2021.

[23] Hameleers, M., Brosius, A. – de Vreese, C. H. (2021): Where's the fake news at? European news consumers' perceptions of misinformation across information sources and topics. *Harvard Kennedy School Misinformation Review*, 2(3), https://doi.org/10.37016/mr-2020-70

linked to perceptions of fallacies regarding a wide range of sources and subjects, not only highly contested matters like climate change or immigration. Politicians, businesses, and foreign entities are also seen to be the most probable sources of misleading information. Participants were more likely to link disinformation with critical issues in their regards. Of course, modest levels of skepticism about important problems may be beneficial for a healthy democracy, a high level of suspicion regarding all information can create problems by preventing empirical facts and expert knowledge from being accepted. Therefore, there needs to be media literacy and critical thinking within the public. The researchers propose that treatments aimed at rebuilding trust in information sources should include a decent level of transparency regarding verification and assessing contradictory evidence.

Open Society Institute in Sofia has published "Media Literacy Index 2018" which uses media freedom, education, and interpersonal trust measures to assess the resistance capacity of 35 European nations to the post-truth phenomena. Index results suggest that with more exceptional education, open media, and strong interpersonal trust, Scandinavian countries have a higher resistance potential against fake news[24]. The highest weight is given to media freedom and education indicators, with reading literacy being seen as the most important aspect of education. The remaining percentage is ascribed to trust and e-participation metrics. The index transforms the data into standardized scores ranging from zero to one hundred and ranks the nations from one to thirty-five. With its tightly controlled media, educational deficiencies, and poor levels of confidence in society, the Balkan nations are particularly exposed to the negative impacts of false news and post-truth. Let us go through the top five and the bottom five of the list in more detail. Finland is on the top of the list with a score of 76, which is followed respectively by Denmark with 71, the Netherlands with 70, and Sweden with 69. Estonia from the Baltic area is within the top five with a score of 69. The bottom five are as follows: Montenegro is in the fifth position on the bottom of the list with a score of 28. Bosnia Herzegovina is on the bottom four with a score of 25 then Albania comes in the bottom three with 22. Turkey holds the second-lowest position with a score of 16 and Macedonia is the country with the lowest media literacy index with a score of 10[25].

Another development can add fuel to the fire, namely algorithms and machine learning. Even though algorithms are designed to augment user experience on a digital platform through a better-personalized content suggestion, and retaining the user attention on the contents, there are some rising issues from the aspect

[24] Lessenki, Marin (March 2018): "Common Sense Wanted Resilience To 'Post-Truth' And Its Predictors In The New Media Literacy Index 2018". Open Society Institute, Sofia, https://osis.bg/wp-content/uploads/2018/04/MediaLiteracyIndex2018_publishENG.pdf, 30/7/2021.

[25] Id. 62

of dissemination of fake news. There are various content producers over the internet and each of them can have various claims with varying reliability. Users can normally diversify their news sources to listen to various opinions considering an event or an issue. However, with the use of algorithms, the platforms can keep suggesting content from the same issue with the same narration and political ideology, which can eventually come from inaccurate or unreliable sources. This way, the employment of machine learning into content suggestion may as well be a problematic practice if they keep promoting the inaccurate information to the users with the same interest who are hooked up to the content in their previous searches. This way fake news can loop within a wider and wider group of users, leading to the rise of conspiracy theories, online frauds, political extremism, hate speech, and other issues as well. This is why some EU states have begun to demonstrate their reservation regarding the use of algorithms by various platforms to tackle the dissemination of misinformation and conspiracy through fake news.

6.2. The doctrine of prior restraint

In traditional terms, prior restraint is a kind of censorship that enables government authorities to evaluate the content of printed items before allowing them to be published. This kind of censorship can include various forms, for example, restricting the display of works of art or the release of a film. The media or artwork may require special permission from the government entities before they can be released. In practice, there are instances where the state is either unable or reluctant to give a license or they revoke an existing license. This sort of barrier to the free press and media can indicate a type of censorship that gives control of the flow of information into the hands of the government. With prior restraint, the state can ban any material that has the potential to threaten its authority. The rule against prior restraint of speech has been a basic First Amendment tenet since the 1930s in the United States of America. The First Amendment guarantees the freedom of speech with unwavering solitude. Prior restraint was seen as a threat to democratic society by the founding fathers in the United States[26]. Consequently, there are strong limitations on the validity of prohibiting speech, especially the ones that occur before the expression or publication of speech. Restriction of speech should normally only be enforced by ex-post criminal or civil punishments, according to the doctrine . Even though it is acceptable to penalize harmful speech such as libels after they have been disseminated, the legitimacy

[26] Baracskay Daniel (2009): *Prior Restraint. The First Amendment Encyclopedia.* https://www.mtsu.edu:8443/first-amendment/article/1009/prior-restraint, 31 August 2021.

of preventing such speech before they are expressed is severely limited[27]. Nevertheless, in former days, the media and newspaper publishers were certain entities with their owners, employees, offices, and registries. The advent of the network society has generated new questions about how the First Amendment should be read in an era where anybody with a computer and an internet connection can create or share media or content with the entire world of internet users. Thanks to widespread internet use, social media can be used as a news or media platform, and creating and sharing journalistic content is no longer exclusively reserved for professional journalists bound by professional and ethical norms. The new media is no longer narrated from the perspective of a few news outlets. Today, everyone's opinion has the potential to reach a greater international public. Ideally, this makes the information society more democratic by nature. Moreover, the range of internet access is global while the time it takes to post a piece of writing or media content is extremely short in comparison with the old media. Content on social media sites or in digital magazines has the capacity to become viral globally and reach a large audience via sharing. The downside of this ease of sharing and global extent is the increase of disinformation, fake news, conspiracy theories, and other information manipulation activities. This is where the challenges occur concerning separating truth from falsehood over the internet while also drawing a line between restricting or removing the harmful digital content and state censorship on the practice of freedom of speech through prior restraint.

In the US, the First Amendment's safeguards are still relevant today and they obviously extend to new media as the major part of the public no longer requires traditional means such as letters or printed papers to be informed and to interact with one another. This way, it is only reasonable to think that the First Amendment's safeguards against prior restrictions are geared more toward digital media today. Nevertheless, there are plenty of issue areas due to the global and complex nature of the internet. For this reason, there are opinions about revising the First Amendment to accommodate new features and challenges brought by the Information Communication Technologies. Conor M. Reardon suggests in his article "Cell Phones, Police Recording, And The Intersection Of The First And Fourth Amendments" in Duke Law Review that citizens utilize cell phones equipped with video cameras to film violent arrests and upload their videos on the internet for public scrutiny in highly publicized cases as such actions are protected by the First Amendment. Reardon expresses that if such materials are considered as evidence of the crime, this First Amendment right can be crippled with the Fourth Amend-

[27] Ariel L. Bendor (1999): Prior Restraint, Incommensurability, and the Constitutionalism of Means, 68 *Fordham L. Rev.* 289, https://ir.lawnet.fordham.edu/flr/vol68/iss2/2, 31 August 2021.

ment which allows the seizure of the crime evidence by the authorities [28]. Hence, there are new challenges to the old code of laws as well. If the authority to seize the digital materials is used, the state can use it to deter the people's will to expose corruption and wrongdoings of the public officials. Such practices can be part of the chilling effect. The chilling effect refers to the idea of reducing free speech, freedom of expression, and association rights as a result of government legislation or actions that appear to target speech[29]. A chilling effect occurs when the prospect of legal repercussions discourages or intimidates the lawful exercise of natural and legal rights[30]. These legal acts might include the ratification of legislation, a court judgment, the threat of a lawsuit, or any other legal action that makes individuals fearful of legal penalties when they practice their fundamental rights. One thing to keep in mind is that chilling effects usually arise when legislation is either too wide or too ambiguous, causing people to stay away from the law's reach with the fear of retribution, arrest, or punitive state intervention[31]. The reason individuals are frightened by vague regulations is that they are unsure when their expressive behavior or speech exceeds the line and breaches the laws. So, such uncertainty leads to the abandonment of expression of their opinion about the event or the case. Furthermore, it is not only the vague laws that can cause chilling effects but also the overbroad laws. They impose a prior restraint on an expression which is also part of the same issue.

On the other hand, national security concerns also remain as a justification for intervening with users' access to the internet and online activities. This kind of intervention can also be seen as a form of prior restraint. Even when this might have valid and justifiable reasons in some scenarios, it also has the tendency to be used to suppress dissent opinions and highlight propaganda, and cover-up governmental misdeeds. National security continues to be the primary motivation for authorities to curtail the freedom of speech of journalists, bloggers, and media entities, regardless of whether they are using conventional or digital media. Because of the imprecise boundaries of national security-related measures and their tendency to bypass constitutional checks and balances, courts might limit the extent of applicability of national security legislation to prevent prior restraint attempts. Furthermore, a sacrifice of fundamental freedoms for the sake of secu-

[28] Reardon M. Conor (2013): Cell Phones, Police Recording, and the Intersection of the First and Fourth Amendments. *Duke University School of Law,* Vol. 63:735, https://scholarship.law.duke.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=3407&context=dlj, 31 August 2021.

[29] Askin, Frank (2009): "Chilling Effect". *The First Amendment Encyclopedia,* https://www.mtsu.edu/first-amendment/article/897/chilling-effect, 2 August 2021.

[30] Hudson, David L. Jr. (15 February 2021): "Chilling Effect Overview". *Fire,* https://www.thefire.org/chilling-effect/, 2 August 2021.

[31] Id. 68

rity concerns might seem legitimate if the concerns are pressing. However, if such applications are prolonged and the citizens get used to such stricter practices, it can end up with further restrictions with more and more pressure on the freedom of expression and the free exchange of information on the internet. For this reason, activist groups, attorneys, and members of the press should stay alert to such events and ensure that all national security-related legislation is compliant with international law. The safeguarding of such fundamental rights requires diligent work and the active participation of civil society and experts in the field.

6.3. New Speech Regulations and Needs for Better Solutions

Beyond their intended targets and desired outcomes, the rise of internet regulations such as NetzDG, Digital Services Act, and Online Harm Bills has the potential to bring some side effects along with them. Particularly in Europe, if member states begin pressing on internet service providers to shape the internet according to their national interests, the internet will be further fragmented. Since there are no borders in cyberspace, a widespread practice can further impact users on a global scale. There are ideas about how new regulations and restrictions resemble traditional restrictions and old-school censorship. In his paper "Free Speech is a Triangle", Jack M. Balkin points out three particular problems created by such regulation. The first problem according to Balkin is that governments aim to exert pressure on digital firms via "new-school speech regulations", resulting in issues such as collateral censorship and digital prior restraint[32]. Such methods are modernized versions of old constraints with broader applicability. These new-school speech limitations pose significant obstacles to free expression. There is usually some form of collateral censoring at work. They also raise concerns such as the digital version of the old prior restraint, which is carried out by private actors and AI-powered algorithms. The new speech regulation is the privatization of access restriction and content removal techniques imposed by governments through laws on internet intermediaries. In this approach, the contemporary digital environment remodeled the prior restraints issues of the 1700s and the 1800s. Nevertheless, there are some differences between the traditional prior restraint and the digital prior restraint. Now in the digital world, the contents are generated by millions of users and can be posted from anywhere from the globe. Moreover, the undesired content can show up on the platform even for a brief time. Another distinction is that the constraint comes from private-sector firms rather than government bureaucrats, who seek to prevent nation-state liability concerns. Another argument raised by Balkin is that internet hosts and social media firms have all the technical capacity and influence to tailor elaborate systems of private government and private bureaucracy to rule end-users unilaterally and without due process or any disclosure. This can fragment formal and standard legal ways

[32] BALKIN: *op. cit.* (2018)

to deal with public issues by empowering the big tech and social media companies to determine the fate of the user content and posts. This would resemble cyber feudalism, in which any corporation may monitor and impose terms on content creators based on widely established legal definitions inside their cyber realm. The final issue raised by Balkin is that end-users are vulnerable to surveillance and manipulation via digital methods[33]. This can especially entice governments with autocratic tendencies to discover better ways to deal with political opponents through censorship under the pretense of social media regulation and internet safety.

In order to avoid such negative implications on basic user rights and freedom of expression, it is necessary to create some checks and balances. Balkin proposes several solutions to the problems of censorship and needless prohibitions. According to him, 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[34]. Here, the fundamental goal is to eliminate or minimize potential large-scale censorships and new techniques of digital prior restriction as much as possible. The second objective is to safeguard individuals against new forms of digital monitoring and exploitation. Large international corporations that rely on the collection, monitoring, analysis, management, and dissemination of personal data have formulated new techniques that can be detrimental to online users. The Internet has a huge potential to get connected, share ideas and bring innovation to existing world problems. In essence, online freedom of speech also encompasses scientific and creative expressions. If restrictions become a norm and are abused in the hands of private companies and the governments, this innovative and intricate network of interactions at the global level will receive the impact with difficult-to-resolve entanglements. Furthermore, an environment where any group can get offended and raise complaints on user-generated content can cause the content to be taken down without impartial judgments. This may lead to collisions with other rights like freedom of religion and political expression in global cyberspace which is used by users with varying political and cultural orientations. Historical enmities, cultural matters, and political ideas are often subjective and relative topics. Global cyberspace with such diversity can be expected to tolerate varying shades of ideas, beliefs, and expressions. This worldwide diversity can be fascinating, but it can also be a major issue owing to the aforementioned sensitivity to delicate topics. This might be minimalized by encouraging tolerance, inclusion, and respect among the users on online platforms through campaigns, training, and education rather than employing strict monitoring and censorship

[33] Id. 70
[34] Id. 70

approaches which can push such ideas under the ground with further radicalization. Nevertheless, education and raising such awareness at an international level is a challenge that requires time and effort.

There is another area where conflicts occur between the right to freedom of expression, the right to accessing information, and national security concerns. National security matters are often given high priority and if such priorities lead to suspension of the right to freedom of expression, the democratic foundation within a state can be shaken from its core. In any case, there should be checks and balances and a proportionality principle when adopting such regulations and practices. Issues of suppressing freedom of speech due to national security grounds can only be resolved by a careful balance of priorities and fundamental rights. Essentially, fundamental rights are not something that can be compromised due to national security matters on a regular basis.

The last point to mention is the cases where the authorities revoke an internet service provider's license for failing to meet the proportionality requirement, or when a monopolistic service provider invokes the right to property to exclude users from its services. Beyond the right to freedom of expression, there are also other rights, such as the right to property. Today, technology firms and internet services create a huge market with massive financial activities. Revoking internet service providers' licenses or monopolistic behavior has the consequence of disrupting the market. This is why the right to property and other commercial rights can be negatively impacted due to imposed content removals and access restrictions. Enhancing such rights can play a role in terms of enhancing online freedom of expression[35].

7. Safeguarding the Fundamental Rights, the Manila Principles

The Manila Principles is a remarkable framework regarding the liability of internet intermediaries and the protection of freedom of speech for internet users. As its name suggests, it was created in Manila, the Philippines where civil society organizations from around the globe have joined together to present a framework of fundamental protections and best practices with the goal of safeguarding freedom of speech and providing an appropriate environment for innovation while balancing the demands of governments and other stakeholders. The Manila Principles

[35] Benedek, Wolfgang – Kettemann, C. Matthias. (December 2013). "Freedom of expression and the Internet". *Council of Europe Publishing*, ISBN 978-92-871-7702-5, https://rm.coe.int/prems-167417-gbr-1201-freedom-of-expression-on-internet-web-16x24/1680984eae, 3 August 2021.

were developed in accordance with international human rights treaties and other legal frameworks. Those principles provide policymakers and intermediaries with guidance for drafting, implementing, and revising policy, rules, and practices that regulate intermediary responsibility for third-party material. Its aim is to strengthen the advancement of integrated and synchronized liability regimes that promote innovation while respecting users' rights, in accordance with the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the UN Guiding Principles on Business and Human Rights[36]. The framework lays forth explicit, reasonable standards for content takedown requests and explains how to limit the impact that a content removal or restriction might cause. The guidelines also call for the enactment of legislation that exempts intermediaries from accountability for third-party material, promoting the development of platforms that allow for online discussion and debate on contentious subjects.

Internet service providers play a vital role in the digital world as they facilitate the exchange of information over the internet. Essentially, there are numerous exchanges of data packages, where data is transferred from one target to the other through various protocols when someone tries to connect to the internet and establish access to a particular internet address. The user data or any other information is stored and broadcasted by various hosts over the internet. Intermediaries such as internet access providers, social networks, and search engines are primarily responsible for building and maintaining this type of communication. Those intermediaries have various responsibilities and operational areas. As a result, they have created a number of policies to guide their operations, as well as provide security and confidence to users regarding their data and rights. As mentioned in the previous sections, regulatory measures enforced by the governments upon the internet service providers change how internet service providers draft their own user rights and agreements. Consequently, regulations governing the legal accountability of intermediaries for the content of these communications have an influence on users' rights, such as freedom of speech, freedom of association, and the right to privacy. A growing number of such regulations have raised various concerns as open-ended arguments and broad definitions can become doorways to government suppression on internet access, and balkanization of the open internet with superficial pieces of evidence. Inadequately informed intermediary liability policies, strict and rigorous administrative measures, failure

[36] Jeschke, Rebecca (15 March 2015). "International Coalition Launches 'Manila Principles' to Protect Freedom of Expression Worldwide New 'Best Practice' Roadmap to Protect Rights and Promote Innovation". Press Release, Electronic Frontier Foundation, https://www.eff.org/press/releases/international-coalition-launches-manila-principles-protect-freedom-expression, 25 July 2021.

to meet the principles of necessity and proportionality, and a lack of consistency across the policies increase the likelihood of censorship and other human rights abuses by governments and private parties, through the limitation of the freedoms of expression for the individuals while creating an uncertain environment for innovation and global integration.

There are six main principles of the Manila Principle that was published in March 2015 and they are separated under the main titles[37]. The first principle is about why intermediaries should be shielded from liability for third-party content. The second principle suggests that content must not be required to be restricted without an order by a judicial authority. The third one is about requests for restrictions of content and why they must be clear, unambiguous, and follow due process. The fourth principle mentions that laws and content restriction orders and practices must comply with the tests of necessity and proportionality. The fifth one is about laws and content restriction policies and practices and how they must respect due process and finally. The final principle is discussing transparency and accountability and why it should be built into laws and content restriction policies and practices. The next section will investigate each individual principle with further details about their aim and extent.

7.1. Intermediaries Should be Shielded from Liability for Third-party Content

The first principle implies that any regulations aimed at controlling intermediary liability must be established by clear legal codes that are specific, unambiguous, and easily available. Furthermore, it is proposed that intermediaries should be exempt from responsibility for third-party material uploaded to their servers if they are not engaged with any content modification. Another suggestion of the first principle is that intermediaries should not be made accountable for failing to block or restrict content on their own. In other words, intermediaries should never be held strictly responsible for hosting illegal third-party content, nor should they be forced to constantly monitor content as part of an Intermediary liability system[38]. Normally, such decisions may be taken by the courts after a thorough investigation. The first principle seeks to avoid the privatization of governance by making internet intermediaries accountable for continually monitoring and

[37] Manila Principles on Intermediary Liability (March 2015): "Best Practices Guidelines for Limiting Intermediary Liability for Content to Promote Freedom of Expression and Innovation". A Global Civil Society Initiative, Electronic Frontier Foundation, https://manilaprinciples.org/index.html, 25 July 2021.

[38] Id. 75

removing allegedly unlawful or objectionable information on behalf of courts and government agencies. In essence, the first principle contributes to the second principle that content uploaded by a user may be considered illegal if the courts, rather than private corporations, rule that it is. Otherwise, the private internet companies should not be granted the power and role of deciding on legality or illegality of any content and taking executive action based on their conviction.

7.2. Content Must Not be Required to be Restricted Without an Order by a Judicial Authority

The second principle states that intermediaries cannot be forced to limit content unless an order has been issued by an objective and unbiased judiciary authority that has concluded that the material in question is illegal. They are expected to provide adequate evidence to support the legal grounds for the order, as well as specify the timeframe for which the content should be blocked. Any responsibility imposed on an intermediary ought to be proportional to the intermediary's unlawful action in failing to comply with the content restriction order promptly. As a result, intermediaries cannot be held responsible for non-compliance with any order that violates this principle[39]. This approach would relieve the pressure from the intermediaries to continually monitor user content and hasten to delete or remove it owing to the risk of financial repercussions that might be disastrous. Furthermore, even if courts maintain the authority to rule on the legality or illegality of content, the decision must be made within clear boundaries. This is what the following third principle recommends.

7.3. Requests for Restrictions of Content Must be Clear, be Unambiguous, and Follow Due Process

The third principle states that complaints coming from the government or private sector about a particular content alone cannot hold intermediaries liable for determining the legality of any third-party content. Furthermore, a content restriction request for illegal content must include foremost a legal basis, an internet identification, a detailed description of the content, as well as any constraints, exceptions, or defenses accessible to the intermediaries. Unless prohibited by law, contact information for the issuing party or their agent, proof necessary to demonstrate legal standing to make the request, and a declaration of good faith that the information supplied are true should also be included. Content restriction

[39] Id. 75

requests relating to a third-party content uploaded to the intermediary's server must include the reasons why the content violates the intermediary's content restriction policies, the internet identification, and a description of the alleged content restriction policy infringement. Unless forbidden by law, they should also include the issuing party's or agent's contact information, as well as a declaration of good faith that the information supplied is true.

Intermediaries may be obligated to react to requests for content restriction relating to illegal content by informing the user about the decision on their content, providing details about the content to the courts, or passing the requests to related content providers. If for any reason, they are unable to perform this part, intermediaries must inform the complaining party about the reasons why they are unable to do so. It should not be necessary for intermediaries to demonstrate that they can identify users. When sending the request, the intermediary must give a clear and accessible explanation of the user content provider's rights, including a description of any applicable counter-notice or appeal processes, and where the intermediary is required to limit the material. On the other hand, if a content removal application is made with abusive or ill intentions, there should be legal consequences to prevent the censorship and misuse of this function[40].

7.4. Laws and Content Restriction Orders and Practices Must Comply With the Tests of Necessity and Proportionality

The fourth principle suggests rules, regulations, and practices regarding content regulation should be appropriate and reasonable which can be expected from a democratic state. Furthermore, all content restrictions should be confined only to the specific content in question, using the least restrictive technical means possible. Furthermore, if the material is removed because of illegality in a certain geographic area where the intermediary renders services globally in geographically diverse locations, the geographic extent of the content restriction must not go beyond that particular jurisdiction area. Furthermore, if the content is prohibited for a limited time due to its illegality, the restriction must not be prolonged and the restriction order must be reviewed on a regular basis to ensure that it remains legitimate[41].

[40] Id. 75
[41] Id. 75

7.5. Laws and Content Restriction Policies and Practices Must Respect Due Process

According to the fifth principle, before any restriction is mandated, the intermediary and the user must be given the opportunity to be heard, unless extraordinary circumstances exist, in which case a post facto review of the order and its implementation must be provided as quickly as possible. Any rule governing intermediaries must include a right of appeal for both users and intermediaries regarding content blocking actions. Content providers should have access to procedures that allow them to appeal decisions that limit the content that is in a clash with the policies. In the event that a user wins an appeal against a content restriction case, intermediaries must restore back the material. Without a legal order, an intermediary ought not to expose any personally identifying information about a user nor can an intermediary liability regime force an intermediary to disclose any personally identifiable user information. Intermediaries should respect human rights when establishing and executing their content restriction policies. States also have a responsibility to guarantee that the content restriction practices of intermediaries respect human rights[42].

7.6. Transparency and Accountability Must be Built into Laws and Content Restriction Policies and Practices.

Lastly, according to the sixth principle, governments must disclose all laws, policies, decisions, and other kinds of regulation related to intermediary responsibility online in a timely and accessible manner. They shall not employ extrajudicial methods to limit material, such as collateral pressures to compel changes in service conditions, advocate or enforce any allegedly voluntary practices, or obtain agreements restricting content sharing and dissemination. Intermediaries should post their content restriction rules online in plain language and in easily accessible forms, and maintain them up to date by notifying users of any upcoming change. Similarly, governments must issue transparency reports that detail their requests for information from intermediaries. Government requests, court rulings, private complainant demands, and enforcement of content restriction policies are all examples of where intermediaries should publish transparency reports that provide precise details about all content restrictions taken by them, explaining where the order came from. When the material is blocked, the intermediary must present a clear notice that explains why the item is restricted. Governments, intermediaries, and civil society should also collaborate to establish and maintain

[42] Id. 75

impartial, accessible, and fair inspection measures to guarantee that content restriction rules and practices are held accountable. Regular, systematic reviews of rules and guidelines should be required by intermediary liability frameworks and laws to assure that they are up to date, functional, and not overly onerous. Regular evaluations should include procedures for gathering information about their implementation, impact, as well as an independent assessment of their costs, shown benefits, and any impact on human rights[43].

8. Discussions

The internet is a conduit for exercising the most fundamental freedom, freedom of expression, via instant and global access. There is growing concern about the malicious use of internet platforms despite all of the benefits of digital technologies. A new set of issues raises the possibility of a conflict of interest among private corporations, government entities, and users. There is a possibility of further restrictions on the open and global exchange of information and ideas on the internet. These issues compel the government to act to regulate certain aspects of the internet. In a way, the law is attempting to catch up with technology, though there are many gaps in the effective enforcement of legislation and rules in cyberspace, with possible ramifications for user rights. The European Union appears to be taking more stringent measures to track and restrict unwanted content that users upload to social media platforms. Furthermore, some regulations and policies that appear to be appropriate in response to internet challenges have the potential to inflame tensions with the fundamental rights of internet users and content producers in the long run. Furthermore, it becomes a challenge when borderless cyberspace is attempted to be ruled by local laws. This dilemma may reflect a clash between the modern and the traditional, as well as the individual versus the collective, in which the internet's globalizing power is confronted by established institutions such as states and authorities. Even though the internet has created a cyberspace domain with enormous economic and social prospects, states as traditional sovereign powers have no intention of leaving cyberspace alone with their rather lesser developed instruments. Thus, creating a global balance in which all countries, enterprises, and communities participate in and profit from the benefits of digitalization in a fair and peaceful way becomes increasingly difficult in a world shaped by many cultures, political ideologies, religious beliefs, and approaches to everyday life issues. Ergo, a one-size-fits-all type of solution cannot be expected here. In the digital environment, where everything moves quickly, the outcome of

[43] Id. 75

the real-world application of the new internet legislation is hard to predict. This factor raises a number of concerns and criticisms from experts and parties.

New regulations, such as NetzDG, the Digital Services Act, or the Online Harm Bills, apply novel techniques to deal with prohibited or inappropriate content posted on internet platforms. These new regulations hold social media platforms and internet service providers accountable for reporting and responding to complaints about illegal or undesirable content. This approach generates a new process of private governance that may appear to be a solution. It can lead to issues, especially with content that touches on delicate matters, political extremists or hate speech. Furthermore, not every marginal idea can be marked as fully-fledged extremism or fundamentalism. The opinions do not have to be categorized and placed on an ideological spectrum by placing them according to the mainstream version of rhetoric. Another pertinent issue is that private corporations are granted the exclusive authority to remove or blacklist content. Certain legal regulations require corporations to censor content on behalf of the government which can set a precedent for authoritarian regimes to survey their citizens' online activities and put strict controls on freedom of expression on the internet. If this becomes common practice among less democratic states, the internet once envisioned as an open platform for the free exchange of information can become a tool of oppressive force and a state-of-art means of monitoring and suppressing political opposition.

There are also differences within the European Union because it is comprised of various states with various jurisdictions. Despite binding common laws concerning the single market, freedom of movement, and certain foreign policy objectives, European countries are nation-states with legal differences. As a result, different states may hold opposing views on issues such as the use of personal data, data protection, free speech, and censorship, among many others. Because the internet is global, there is no reason to believe that the consequences of such restrictive practices will be limited to the EU. When these restriction practices grow more prevalent among different states, the Balkanization of the internet can be imminent with yet unknown outcomes. Since the internet has become the primary venue where important day-to-day activities happen, recklessly adopted laws without proper diligence, these restrictive methods can compromise fundamental human rights. Less democratic states may find incentives to increase authoritarian practices, censorship, and political pressure on their citizens if more democratic countries impose more restrictive regulations. This is how a restricted internet within one powerful country has the potential to set off a vicious cycle of digital nationalism and censorship by serving as a model for other countries to follow increasingly draconian measures to remove unwanted content from the internet. Normally, this is not how the internet was conceived or designed.

Another issue is involving the difficulty of prescribing how things ought to be for such a phenomenon as big and complex as the internet. Why should people

allow the government to intervene in their communication with security expectations? In the end, they will have to outsource this task to third parties due to their limited resources and technical capacity. This can raise further philosophical and moral concerns about security versus freedom. Should people compromise on some of their freedom in exchange for feeling digitally secure? If security is the most important concern, the ultimate safety will be turning off the internet completely, so there can be no more troubles. However, just as a strong ship is not constructed to wear down in the harbor, fear of change cannot be used to prevent people from expressing themselves and interacting with one another.

Another question is whether the users are guilty until proven innocent on digital platforms? A default mode of constant monitoring can be used to detect and remove unwanted or illegal content within 24 hours. However, offensiveness is a highly subjective and relative issue with varying sensitivities. Certain circumstances create quandaries, and private internet companies are expected to act on behalf of governments to address such content issues. How well can a privately held company protect user rights and content, and where are the checks and balances? Who will check the big tech? The problem has been revoked by Juvenal in his Satires in the second century BC in ancient Rome when he wrote: "Quis custodiet ipsos custodesipsos"[44] which can be translated as "Who will guard the guardians themselves". If we consider social media and the digital environment to be realms, who and how will we delegate authority to guard it? When deemed offensive, however, censorship of unwanted content or extreme political opinions will not prevent such ideas from spreading. With an overly broad definition of offensive, unwanted, or illegal internet speech, countries may eventually increase censorship, leading to the dominance of popular opinion and the radicalization of dissident voices. This takes us to the polar opposite of the movement that gave birth to Western democracy and tolerance.

It is necessary to create some checks and balances to avoid such negative implications on rights and freedom of the users. Indeed, if government intervention is minimal and platforms are led by a pluralistic interaction of diverse stakeholders and actors, they will be protected from government pressure through liability adjustments, giving them more time to review content that receives complaints. Such restrictions can help to curb or prevent power abuses and large-scale censorship. Individuals must also be protected from new forms of digital surveillance and exploitation[45]. Furthermore, fundamental rights should not be compromised for reasons of national security. Policymakers and intermediaries can better create, execute, and revise policy, norms, and procedures that regulate intermedi-

[44] Juvenalis Decimus Junius (2nd Century AD). "Satires". Satire VI, lines 347–348. Satire VI, lines 347–348, https://www.thelatinlibrary.com/juvenal/6.shtml, 06.07.2021.

[45] Id. 70

ary responsibility for third-party material thanks to resolutions like the Manila principles.The most effective strategy is to educate the public about media literacy. With their great education, open media, and strong interpersonal trust, the Scandinavian countries lead the media literacy. They have developed a defense mechanism against the spread of fake news and hate speech online. While they are less prone to online threats, their governments do not have to perpetually watch or control their internet access. Nonetheless, obtaining this high level of development is a long term process. As a result, reliance on strictly restrictive restrictions can be alluring.

9. Conclusion

The internet has accelerated both opportunities and challenges, as it has attained a prime position in virtually every aspect of life. The private tech corporations seized the opportunities and left the challenges to be dealt with by the relevant parties. In borderless cyberspace, drafting laws in accordance with national frontiers is a challenging task. There have been attempts by the European Union to regulate some features of the internet. The development of new internet regulations in Europe permits internet intermediaries to monitor the content uploaded by the users and impose restrictions if they conclude that the content is offensive or illegal. This procedure, hence, leads to privatized enforcement of government policies by internet intermediaries which has the potential to blur the line between the public and the private matters and interests. Big tech companies can affect how the rules are made according to their corporate aims. This way the laws regulating the legal accountability of intermediaries influence the rights of the users such as freedom of expression, freedom of association, and data privacy. Moreover, authorities call for the prompt removal of offensive content and if this condition is not satisfied, the internet intermediaries can deal with tremendous monetary penalties. This poses financial risks that need to be warded off by those parties. This is how content that drew several complaints can be cleared away as the financial risk potential is more important than going through a long analysis of the content and its context. To curtail possible side effects of these regulations, several propositions have been made. In general lines, they recommend some immunity for internet intermediaries, greater transparency for corporate practices, and carefully crafted regulations to assure that laws remain relevant and respected. Manila Principles recommend shielding intermediaries from accountability for third-party content, a judicial order before any content restriction, a clear due process, compliance with a test of necessity and proportionality, as well as transparency and accountability. There is a need to establish better channels to facilitate diminishing the negative impact of content monitoring and restriction

processes. Improved worldwide collaboration between academics, civil society platforms, business sectors, international digital society, and governments is necessary to reinforce the handling of such present and potential future challenges. To create a secure, free, just, innovative, and better-connected world, global issues call for a well-integrated global problem-solving capacity.

References

1. Bendor, Ariel L. (1999): Prior Restraint, Incommensurability, and the Constitutionalism of Means, 68 *Fordham L. Rev.* 289, https://ir.lawnet.fordham.edu/flr/vol68/iss2/2, 31 August 2021.
2. Askin, Frank (2009): "Chilling Effect". The First Amendment Encyclopedia, https://www.mtsu.edu/first-amendment/article/897/chilling-effect, 2 August 2021.
3. Balkin, Jack M. (May 28, 2018): "Free Speech is a Triangle". Columbia Law Review. Yale Law School. *Public Law Research Paper,* No. 640, https://ssrn.com/abstract=3186205, 17.07.2021.
4. Baracskay, Daniel (2009): *Prior Restraint. The First Amendment Encyclopedia.* https://www.mtsu.edu:8443/first-amendment/article/1009/prior-restraint, 31 August 2021.
5. Barata, Joan (27 July 2021): "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), https://libertadinformacion.cc/wp-content/uploads/2021/06/DSA-AND-ITS-IMPACT-ON-FREEDOM-OF-EXPRESSION-JOAN-BARATA-PDLI.pdf, 4 August 2021.
6. Barata, Joan (29 July 2020): "Positive Intent Protections: Incorporating a Good Samaritan principle in the EU Digital Services Act". the Center for Democracy & Technology, https://cdt.org/wp-content/uploads/2020/07/2020-07-29-Positive-Intent-Protections-Good-Samaritan-principle-EU-Digital-Services-Act-FINAL.pdf, 17.07.2021.
7. Benedek, Wolfgang – Kettemann, C. Matthias. (December 2013). "Freedom of expression and the Internet". *Council of Europe Publishing,* ISBN 978-92-871-7702-5, https://rm.coe.int/prems-167417-gbr-1201-freedom-of-expression-on-internet-web-16x24/1680984eae, 3 August 2021.
8. Committee of Ministers (13 January 2010): "Declaration of the Committee of Ministers on measures to promote the respect of Article 10 of the European Convention on Human Rights". the 1074th meeting of the Ministers' Deputies. Council of Europe, https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cfdad, 30/7/2021.
9. Committee of Ministers (29 September 2010): "Declaration of the Committee of Ministers on network neutrality". the 1094th meeting of the Ministers' Deputies, Council of Europe, https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805ce58f, 30/7/2021.
10. Committee of Ministers (8 May 2003): "Declaration on freedom of communication on the Internet". the 840th meeting of the Ministers' Deputies, Council of Europe,

https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805dfbd5, 30/7/2021.

11. 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, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=-COM:2020:825:FIN, 5 July 2021.
12. Hameleers, M., Brosius, A. – de Vreese, C. H. (2021): Where's the fake news at? European news consumers' perceptions of misinformation across information sources and topics. *Harvard Kennedy School Misinformation Review,* 2(3), https://doi.org/10.37016/mr-2020-70
13. Higdon Nolan (August 15, 2020): "The anatomy of fake news: A critical news literacy education". University of California Press, https://www.jstor.org/stable/j.ctv1503gc8, 30 July, 2020.
14. Hudson, David L. Jr. (15 February 2021): "Chilling Effect Overview". *Fire,* https://www.thefire.org/chilling-effect/, 2 August 2021.
15. Human Rights Act (1998): Freedom of Expression. Article 10. Paragraph 1
16. Jeschke, Rebecca (15 March 2015). "International Coalition Launches 'Manila Principles' to Protect Freedom of Expression Worldwide New 'Best Practice' Roadmap to Protect Rights and Promote Innovation". Press Release, Electronic Frontier Foundation, https://www.eff.org/press/releases/international-coalition-launches-manila-principles-protect-freedom-expression, 25 July 2021.
17. Juvenalis Decimus Junius (2nd Century AD): "Satires". Satire VI, lines 347–348. Satire VI, lines 347–348, https://www.thelatinlibrary.com/juvenal/6.shtml, 06.07.2021.
18. Keller, Daphne (29 January 2019): "Who Do You Sue? State And Platform Hybrid Power Over Online Speech". *Aegis Series Paper,* No. 1902, Hoover Institution, Stanford University, https://www.hoover.org/research/who-do-you-sue, 17.07.2021.
19. Lessenki, Marin (March 2018): "Common Sense Wanted Resilience To 'Post-Truth' And Its Predictors In The New Media Literacy Index 2018". Open Society Institute, Sofia, https://osis.bg/wp-content/uploads/2018/04/MediaLiteracyIndex2018_publishENG.pdf, 30/7/2021
20. Manila Principles on Intermediary Liability (March 2015): "Best Practices Guidelines for Limiting Intermediary Liability for Content to Promote Freedom of Expression and Innovation". A Global Civil Society Initiative. Electronic Frontier Foundation, https://manilaprinciples.org/index.html, 25 July 2021.
21. Reardon M. Conor (2013): Cell Phones, Police Recording, and the Intersection of the First and Fourth Amendments. *Duke University School of Law,* Vol. 63:735, https://scholarship.law.duke.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=3407&context=dlj, 31 August 2021.
22. Sartor, Giovanni – Loreggia Andrea (15 September 2020): "The impact of algorithms for online content filtering or moderation – Upload filters". European Parliament. Policy Department for Citizens' Rights and Constitutional Affairs, https://www.europarl.europa.eu/RegData/etudes/STUD/2020/657101/IPOL_STU(2020)657101_EN.pdf, 17.07.2021.
23. UNESCO (2003): "Recommendation Concerning the Promotion and Use of Multilingualism and Universal Access to Cyberspace". Paris, http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/official_documents/Eng%20-%20Recom-

mendation%20concerning%20the%20Promotion%20and%20Use%20of%20Multilingualism%20and%20Universal%20Access%20to%20Cyberspace.pdf, 3 August 2021)

24. United Nations (10 December 1948): "Universal Declaration of Human Rights". Draft Committee, Palais de Chaillot, Paris, United Nations. (1976). "International Covenant on Economic, Social and Cultural Rights". Resolution 2200A (XXI) of 16 December 1966 entry into force 3 January 1976.
25. Van Hoboken Joris – Quintais João Pedro – Poort Joost – Eijk Nico van (29 January 2019): "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, ISBN 978-92-79-93002-7, DOI 10.2759/284542 Catalog number KK-06-18-016-EN-N, https://op.europa.eu/en/publication-detail/-/publication/7779caca-2537-11e9-8d04-01aa75ed71a1/language-en, 17.07.2021.
26. Watson, Amy (28 May 2021): "Statistics and facts about fake news worldwide". *Statista*, https://www.statista.com/topics/6341/fake-news-worldwide/, 11/08/2021.