MYKOLAS ROMERIS UNIVERSITY
FACULTY OF LAW
PRIVATE LAW INSTITUTE

MARIIA SHCHEKUNOVA
(EUROPEAN AND INTERNATIONAL BUSINESS LAW)

OBLIGATIONS AND RESPONSIBILITIES OF THE INTERNET SERVICE PROVIDERS REGARDING ILLEGAL CONTENT

Master thesis

Supervisor –
Professor, Doctor
Solveiga Palevičienė

Vilnius, 2021

TABLE OF CONTENTS

INTRODUCTION……..... 3

LIST OF ABBREVIATIONS..... 8

1. GENERAL OVERVIEW OF GOVERNMENTAL CONTROL OVER THE INTERNET IN THE EU ……. 9

1.1. Who is Provider……..... 9

1.1.1. The Power of ISP Over Users' Content……..……..……..... 11

1.2. What Constitutes Illegal Content Online……..……..... 14

1.3. EU Legislation: Transition From ISP Liability to Responsibility …….. 20

2. BALANCE BETWEEN FREEDOM OF EXPRESSION AND RIGHT FOR PRIVATE LIFE IN RESTRICTING MEASURES OF ISP ……. 29

2.1. General Approach to the Freedom of Expression and Right for Private Life …. 29

2.2. ECHR Case-law Regarding Blocking and Filtering the Illegal Activities…….. 34

2.3. CJEU Case-law Regarding Copyright Infringement …….. 42

2.4. The Approach of Ukrainian Legislation …….. 49

3. NEW REGULATION IS COMING……..……..... 52

3.1. Regulation TCO……..……..……..... 52

3.2. Digital Services Act……..……..……..... 61

3.2.1. Responsibilities ……..……..…. 68

CONCLUSIONS……..……..... 71

RECOMMENDATIONS……..……..... 73

LIST OF BIBLIOGRAPHY……..... 74

ABSTRACT.....……..……..... 86

SUMMARY.....……..……..... 87

HONESTY DECLARATION 88

INTRODUCTION

The relevance of the master thesis. Due to the hard time of Covid-19 global web networks began to constitute the biggest part of our daily routine as lots of people transferred their routine from offline to the open space of the Internet. From checking the news feed on Instagram or Facebook during the morning cup of coffee till late at night, we use Internet sources for work, studying, communication and just having fun. It is used both by adults and children.

Governments way back have come to the idea that this field should be regulated. First of all, because it's the same profitable market for businesses as offline ones, which gives taxes: online shops, advertisement at web sites, services. And the other reason is security: national, information, economic, personal and proprietary. As any other communication technologies, the Internet keeps an amount of potentially harmful or illegal materials that can be used as a vehicle for criminal activities: calls for terrorist attacks, sale of slaves, the infringement of video games and software, malicious hacking, racial discrimination and plenty of other actions.[1] So, who should be liable for appearing such content in the open space of the Internet?

Internet service providers significantly contribute to innovation, economic growth and job creation all over the world. Most of these providers play an active role in the digital economy by being intermediaries between business and citizens. Unfortnately**,** frequently online platforms are abused by its customers to go through illegal activities**,** for example spreading certain material relating to xenophobic, illegal hate speech, child sexual exploitation or breaches of intellectual property rights. Such cases harm user trust and ruin online systems. However, in certain situations the service providers benefit from that kind of activity - full access to movies, music and books without authorisation of the right holders.[2]

The guidelines and basic principles of effective, appropriate and proportionate way to handle illegal materials are set in Communication from The Commission Tackling Illegal Content Online from the 28th September, 2017[3]. Later the Commission Recommendation of

---

[1] "Communication Illegal and harmful content on the Internet," Commission of the European Communities, Accessed on November 2, 2020, http://aei.pitt.edu/5895/1/5895.pdf.
[2] "Petition No 0777/2018 on the need for measures against bullying, threats or slander of users of digital portals and platforms on 16.9.2019," Europarl, Accessed on November 2, 2020, https://www.europarl.europa.eu/doceo/document/PETI-OJ-2019-11-11-1_EN.html.
[3] "Tackling Illegal Content Online Towards an enhanced responsibility of online platforms," European Commission, Accessed on November 2, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0555&from=EN.

the 1st March, 2018 was presented with a set of operational measures by which online intermediaries are obliged to denote sites with unlawful content on their platforms, also the system of notice and action was established - automated tools must be assisted by supervisors. More importantly, in the case of wrongful removal of the material, the safeguard of counter-notices may be applied with further restitution of the content.[4] However, there is still uncertainty and issues that need to be resolved.

Through the current thesis that is dedicated to the problem of the ISPs' obligations and liability for illegal content, a great part will be made about clarifying terms and conditions of responsibility set in EU law.

Scientific research problem. Absence of a unified legal act in the EU makes it harder to find a precise list of all obligations and liabilities of internet providers regarding illegal content. However, particular definitions, duties and terms are set in different directives by the subject of crimes. Although the E-commerce Directive covers liability for all types of illegal content online, it specifies only conditions when ISPs are not liable for their actions. After legal analysis of EU legislation was conducted, differences in applying the same rules in practice of Member States were found. Directives gave rather broad meaning of its provisions, which led to different interpretations by the Courts of the member states. The ambiguity connected with such terms as "information society services", "passive and active role", "safe harbour" conditions and "notice-and-take down" obligations, a fine line between "harmful" and "illegal" content. Thus, a question arises: **are measures against illegal content established by EU legislation enough to make clear without gaps obligations and liability of Internet service providers, so the fundamental rights and freedoms of EU citizens are protected?** This research is aimed at finding an answer to this question.

Review of the literature. The current thesis is based on both legal acts, case law and works of legal scholars, practitioners. EU legislation: Directive on combating sexual abuse of children, The EU Code of Conduct, Directive on combating terrorism, E-commerse Directive, Directive on Copyright and related rights in the Digital Single Market, Proposal for a Regulation on Preventing the Dissemination of Terrorist Content Online and Proposal for a Regulation on a Single Market For Digital Services. Research on relevant topic was made by

[4] "Commission Recommendation of 1.3.2018 on measures to effectively tackle illegal content online," Frequently asked questions, Europa, Accessed on November 5, 2020, https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_1170.

such scholars as Wolfgang Benedek,[5] Anja Hoffmann & Alessandro Gasparotti [6], Giancarlo Frosio [7], Matthew Sag [8], Tambiama Madiega, Andreas Nanos, Maria Lilla Montagnani [9] and Amos N. Guiora.

Scientific novelty of the master thesis. The problem of existing illegal content online has been arisen by many researchers in their works before. When a new legislative act referring to this issue appears, scholars make their analysis and express opinions into articles. Unfortunately, in most of such works only one specific type of illegal content is discussed. Like in Maria Lilla Montagnani's "Virtues and Perils of Algorithmic Enforcement and Content Regulation in the EU - A Toolkit for a Balanced Algorithmic Copyright Enforcement" the obligations and responsibility of ISP are mentioned only regarding copyright infringement online. While Jack M. Balkin in his research analyses all stakeholders involved in dissemination of illegal content on the Internet[10]. However, this research seeks to disclose the issue from the side of several of the most common types of illegal material on the Internet. It is especially relevant as the thesis presents not only the existing regulation, but also problems and gaps in it with possible solutions based on other countries' experience, academics' opinions and conclusions.

The aim of the master thesis –to clarify the legal uncertainty regarding internet providers' responsibility through "drawing a line", overstepping which intermediaries become liable for infringing rights of online users, based on EU legislation and case study.

The objectives of the master thesis. These tasks must be completed, to achieve the aim set in the master thesis:

---

[5] Wolfgang Benedek and Matthias C. Kettemann, "Freedom Of Expression And The Internet," Council of Europe Publishing, Accessed on November 18, 2020, https://rm.coe.int/prems-167417-gbr-1201-freedom-of-expression-on-internet-web-16x24/1680984ea.

[6] Anja Hoffmann, and Alessandro Gasparotti, "Liability for illegal content online. Weaknesses of the EU legal framework and possible plans of the EU Commission to address them in a "Digital Services Act"," Cepstudy, Accessed on November 15, 2020, https://www.cep.eu/fileadmin/user_upload/cep.eu/Studien/cepStudie_Haftung_fuer_illegale_Online-Inhalte/cepStudy_Liability_for_illegal_content_online.pdf.

[7] Giancarlo Frosio, "Why Keep a Dog and Bark Yourself? From Intermediary Liability to Responsibility," *International journal of law and information technology* 26, 1 (2018): 1-33.

[8] Matthew Sag, "Internet Safe Harbors and the Transformation of Copyright Law," *Notre Dame Law Review* 93, (2017): 66, Accessed on November 15, 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2830184.

[9] Maria Lilla Montagnani, "Virtues and Perils of Algorithmic Enforcement and Content Regulation in the EU - A Toolkit for a Balanced Algorithmic Copyright Enforcement," *Case Western Reserve Journal of Law, Technology and the Internet* 11, (2020): 1-49.

[10] Jack M. Balkin, "OLD-SCHOOL/NEW-SCHOOL SPEECH REGULATION," *Harvard Law Review* 127, 8 (2014): 2296-2342, Accessed on November 15, 2020, https://www-jstor-org.skaitykla.mruni.eu/stable/pdf/23742038.pdf?refreqid=excelsior%3Aff1191b525764a16e11255758f70416c.

1) to analyze duties and responsibility of internet service providers toward the content considered illegal according to current EU legislation;
2) to evaluate governmental EU policy concerning ISPs' voluntary measures against illegal content;
3) to identify legal boundaries established by case law regarding obligations and liability of Internet intermediaries;
4) to discuss suggested ways of improvement to tackle illegal content online more efficiently.

The practical significance of the master thesis. From the practical point of view this research could be useful for academics, lawyers and legal authorities who are involved in the sphere of detecting and extracting the illegal materials from the Internet platforms by means of service providers. Moreover, internet intermediaries that fall within the scope of definition "information society services"[11] and are obliged to comply with the law, can also use this master thesis as a guidance for their duties and obligations. Additionally, as my work points out not only gaps in legislation, but also gives examples of solutions that may help legislators of European Union and its Member States.

Methods used in the master thesis. For the purpose of this scientific research following methods were used:

1. **Data collection** method is one of the most important in this work as its results are the ground for further research. Due to it, the master thesis includes legal acts, case law, both American and European academic articles regarding legal capacity of ISP for illegal content.
2. **Data analysis** method helps to systematically arrange necessary legal information to perform it into coherent structure, point out the view with arguments and draw logical conclusions in the field of IT law.
3. **Comparative analysis** was used to measure the difference between legislation of EU Members and US law relating to the subject of the current research. Moreover, in comparison between legal acts of the EU and case study of its national courts were found to have problematic aspects. Thereby, to show advantages and disadvantages in approaches of each jurisdiction.
4. **Linguistic method** gives a clear understanding of terms used by legal authorities in their strategy against illegal content online with the help of Internet intermediaries. Precise

[11] "DIRECTIVE 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market" EUR-lex, Accessed on November 12, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=FR.

defying the norms of law makes it possible to determine a threshold for ISPs, after which liability comes.

5. **Historical method** was used to show the development of EU regulation about combating illegal content online with an increase in the number of acts concerning this issue.

6. **Logical method** attaches the sum of opinions and arguments in sequence to show the perspective with all uncertainty of current research and find a better solution.

The structure of the master thesis. It consists of several parts:

In the first part of the master thesis is discussed a general description of current legislation in the EU explaining the definitions of illegal content and internet service providers, terms of its duties and boundaries of responsibility.

The second part of the research gives the considered opinion of ECHR and CJEU case study regarding the problem of infringing fundamental rights of users by means of ISPs measures.

In the third part proposals of the EU government in the field of ISP responsibility are presented with comparative analysis based on case law, academic view and current technological developments.

Defence statements.

Having conducted the analysis of the current EU approach regarding obligations and responsibilities of the Internet service providers toward illegal content, it can be concluded that legislation is outdated and the lack of specific provisions generate the interferences with fundamental rights of online users. This difficulty can be managed by adopting new legislative act with transparent and proportionate conditions.

LIST OF ABBREVIATIONS

CJEU – Court of Justice of the European Union

DSA – Digital Services Act

ECD – Electronic Commerce Directive

ECHR – European Court of Human Rights

EFTA – European Free Trade Association

GDPR – General Data Protection Regulation

IP – Intellectual Property

IRU – Internet Referral Unit

ISP – Internet Service Provider

LIBE – The Committee on Civil Liberties, Justice and Home Affairs

TCO – Terrorist Content Online

WHO – World Health Organization

1. GENERAL OVERVIEW OF GOVERNMENTAL CONTROL OVER THE INTERNET IN EU

The European legislation always develops and sometimes even makes trends in the legal sphere for other countries out of the Union. As it puts on the first place individual rights of each person, the EU sets a good example for following, especially, considering the fact that the EU legislation is constructed to fit every MS traditions and legal systems.

The current EU measures for countering illegal content online are ineffective and lack transparency, so the liability regime of providers is going to be changed. There are recent developments in the direction of Digital Single Market and Net Neutrality, which might have an influence on the whole Internet world, for instance, the numbers of Facebook's monthly active users from the EU, which count for 419 millions,[12] might be changed if on;ine platform would not obey new rules.

As the amount of content available on the Internet grows every day, the importance of Internet Service Providers is growing respectively, with regard to unlawful parts of it. They give access to the network, which both adults and children use for studying, working, having fun and some of them unfortunately, for illegal purposes. Thereby, online intermediaries have power over the Internet and the government has the authority over them, thus this issue should be regulated with precise rules and establishing the scope of ISP's responsibilities.

1.1. Who is Provider

According to the Directive 2000 service provider is "any natural or legal person providing an — information society service"[13], by the definition of DIRECTIVE 98/34/EC "Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services." This Directive also provides the Indicative list of services that are excluded from the meaning of the aforementioned Article,[14] thus as the Internet Service Providers are not included in that

[12] "Facebook's monthly active users (MAU) in Europe from 4th quarter 2012 to 4th quarter 2020," Statista, Accessed on April 12, 2021 https://www.statista.com/statistics/745400/facebook-europe-mau-by-quarter/.
[13] "DIRECTIVE 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market" EUR-lex, Accessed on March 12, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=FR.
[14] "DIRECTIVE 98/34/EC of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services," EUR-lex, Accessed on March 12, 2021, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1998L0034:20070101:EN:PDF.

list and meet all conditions by Article 1, they are covered by the definition “service provider”.

By the Encyclopaedia Britannica Internet service provider (ISP) is “company that provides Internet connections and services to individuals and organizations”. Other associated services of ISP might be providing software browsers, email accounts, chat rooms, instant messaging, Internet telephony and others. All ISPs are linked to each other through network access points, public network facilities on the Internet backbone.[15] All ISPs provide services locally, regionally or nationally and register as national companies. The largest ones also provide backbone services for the other ISPs, which create network infrastructure. 1 tier providers (large telecommunications companies) give access to smaller companies with a single connection.[16] Mobile operators are also able to provide access to the Internet for their users such as Vodafone, Orange, T-mobile, MTN.

One of the biggest ISPs are China Telecom (55 million subscribers), Japan's NTT (17 million subscribers), and Deutsche Telekom (less than 10 million subscribers).[17] AOL, known as America Online, is one of the largest Internet service companies in the United States, which globally covers Europe (France, Britain, Germany, the Netherlands, Austria), Asia-Pacific (Japan, Australia, India), and the Americas (Canada, Mexico, Argentina, Puerto Rico).[18]

It is important to distinguish ISPs from other entities such as hosting providers (Bluehost, Hostgator), Social networks (Facebook, Twitter, LinkedIn, Orkut, Google+) and user-generated content platforms (video-sharing sites - Youtube, TikTok, picture-sharing sites - Instagram) etc. As ISP merely gives access to the end user for the content and services mentioned above and not included in the process of publishing and distributing online material by content providers. Nevertheless, sometimes ISPs can perform other services such as web hosting and web page design, which give them more possibilities of controlling the content. In such cases, they are treated according to the functions they perform.

---

[15] “Internet service provider,” Britannica, Accessed on March 10, 2021, https://www.britannica.com/technology/Internet-service-provider.
[16] Karine Perset, “The Economic and social role of internet intermediaries,” OECD, Accessed on April 12, 2021, http://www.oecd.org/digital/ieconomy/44949023.pdf.
[17] Nate Anderson, “Just two Chinese ISPs serve 20% of world broadband users,” Arstechnica, Accessed on April 12, 2021, https://arstechnica.com/tech-policy/2010/07/just-two-chinese-isps-serve-20-of-world-broadband-users/#:~:text=China%20Telecom%20is%20the%20largest,significantly%20in%20more%20developed%20markets.
[18] “AOL,” Britannica, Accessed on March 10, 2021, https://www.britannica.com/topic/AOL.

At the European level ISPs have support, exchange of best-practices and can influence legislation related to the EU intermediary liability through an organization - EuroISPA, which stands for European Internet Services Providers Associations, and connects providers across the EU and EFTA countries. For now the main goal of the EuroISPA is to promote a framework of guiding principles of responsibilities of Internet intermediaries to the present policy-makers.[19]

1.1.1. The Power of ISP Over Users' Content

ISP can track every movement of the user on the web if he/she is not using encryption: so the provider has access to the history of visited sites, passwords, emails, torrents, what device is used, etc. But if the particular web page is encrypted (i.e. site uses HTTPS), it's harder for the provider to know the actions performed by the user there. However, it is not impossible and still ISP can have access to it.[20] For example, as every YouTube video has its unique traffic pattern when appearing on a device, for the ISP it is possible to find out which exact videos the user is watching.[21]

So what can the ISP do with that information? One way is to sell the user's browsing history to the advertisers, the other, especially important to this research, is determination of the user, his/her location and illegal content posted by him/her. This personal data may be delivered to law enforcement authorities for further investigation.[22]

Another ISP's capacity is posing restrictions to access to specific websites. ISP can use Content-control software (simply known as an Internet filter), a program that regulates the Internet content to which a user has access: websites and/or e-mails with restricted material are blocked. The software monitors the user's activity: before opening a web-page or electronic letter, firstly, it checks whether the content comes from software's "blocked" site list, secondly if the material includes "buzzword list" or "blacklist". If none of the above is presented, the user has full access to it. Internet filters can be adjusted at various levels: a government may apply them nationwide (which would mean Internet censorship in the state);

---

[19] "About," Euroispa, Accessed on April 12, 2021, https://www.euroispa.org/about/.
[20] "Just looking? ISPs are watching you browse," Expressvpn, Accessed on April 10, 2021https://www.expressvpn.com/blog/how-much-does-your-isp-know/.
[21] "Your YouTube history exposed: Researcher identifies inherent security flaw in video streaming," Expressvpn, Accessed on April 13, 2021, https://www.expressvpn.com/blog/security-flaw-youtube-video-streaming/.
[22] "Guidelines for the cooperation between law enforcement and internet service providers against cybercrime," Conference Cooperation against Cybercrime, Accessed on April 13, 2021, https://rm.coe.int/16802fa3ba.

clients of an ISP can ask for a purpose to protect students, children, or any user to their own computer.[23]

At the EU level, the first possibility of **blocking access** to the website at the level of access providers was introduced in the Communication "Illegal and harmful content on the Internet". This measure was proposed in cases when illegal content cannot be removed from the server by the host provider. It happens because the server is situated outside the MS and either the authorities refuse to cooperate, or under the law of that country the content is not illegal. The technical possibilities of blocking access to the content in that time wasn't clear, the timing between the illegal content was identified and the access could be blocked, so the degree of liability for ISP could be set. However, this approach was implemented in some third countries in legislation that compels ISPs to block all direct access to the Internet with a requirement for "proxy servers'" (blacklisting of websites), which exclude content estimated as legal by EU law. Due to interference in the freedom of speech of the individuals this restrictive regime is impossible for Europe.[24]

From 2018 such a system has been implemented in Ukraine to block access for 426 different websites, all connected with the Russian influence and propaganda against Ukraine. Imposing this filtering system was based on the Decree of the President of Ukraine No. 126/2018 and then prolonged by Decrees № 82/2019 and № 184/2020.

For instance, the UK uses 2 different approaches to fight infringement activities. The first one is Voluntary Copyright Alert Program (VCAP), is a scheme between the British Phonographic Industry, the Motion Picture Association and the four biggest ISPs (Virgin Media, BT, TalkTalk and Sky) which targets users, who accessed infringing material, and send to them internet piracy warning emails with educational purpose. Such "*subscriber alerts*" do not imply any punishment or demands for money.[25]Another EU approach regarding the obligation of the ISP is to block websites with illegal content to stop subscribers from accessing infringing material. The request and the process of blocking the

[23] "Content filter," Britannica, Accessed on April 12, 2021, https://www.britannica.com/technology/content-filter.
[24] "Communication Illegal and harmful content on the Internet," Commission of the European Communities, Accessed on April 13, 2021, http://aei.pitt.edu/5895/1/5895.pdf.
[25] Mark Jackson, "Get it Right – Copyright Holders Scrap UK ISP Piracy Letters Scheme," ISPreview, Accessed on April 12, 2021, https://www.ispreview.co.uk/index.php/2019/07/get-it-right-copyright-holders-scrap-uk-isp-piracy-letters-scheme.html.

particular content is conducted by an independent enforcement unit the Police Intellectual Property Crime Unit.[26]

Aforementioned tools of dealing with illegal content are issued from the side of the government and always need special authority to guide. But there is also a way in which ISP protects its customers from ineligible material on the web voluntarily. ISPs can add particular URLs to its **filter system** from Database of Hashes - a cross-platform tool with a list of images, videos, texts and other materials that have been already defined as illegal and noncompliant with relevant legislation. This system was developed under the EU Internet Forum concerning mainly terrorist content, child sexual abuse material and copyright infrigement. In cooperation between service providers, online platforms, responsible agencies and society in general, effectiveness of the Database becomes higher as improvements for identification of illegality of the context continue. After defying the presence of illegal material on the service, comes automatic stay-down procedures, which means either the ISP deletes the content or blocks access to it.[27]

To sum up, ISP gives an entrance to the world wide web for users from all countries. It can control the content that comes into the computer and goes outside to the Internet, has the possibility to keep data of each customer, track the information, etc. All these actions can be used for good purposes in tackling illegal content and making the open space of the Internet a better place. For every country the ISP is the easiest, simplest and shortest way to protect its citizens from all harm the illegal material can cause both to children and adults. Providing specific regulation helps in tackling illegal content down.

---

[26] "International Comparison of Approaches to Online Copyright Infringement: Final Report," Intellectual Property Office, (2015): 78, Accessed on April 14, 2021,https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/549462/International_Comparison_of_Approaches_to_Online_Copyright_Infringement.pdf.

[27] "Tackling Illegal Content Online Towards an enhanced responsibility of online platforms," European Commission, Accessed on April 11, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0555&from=EN.

1.2. What Constitutes Illegal Content Online

Sometimes people confuse the term “illegal content” with another similar, but drastically different in legal terms wording “harmful content”. The difference can be seen in an example: “child gets the access to pornographic content for adults” Vs “adults get access to pornography about children”[28]. The first one describes the situation of getting legal content - pronography, but the person with illegal age - hence, harm for the kid, while the second one exposes sexual solicitation of a child, which constitutes a crime. Some materials indeed can be within the law in one country and correspond to a criminal activity in another. For instance, selling particular types of drugs is legal in the Netherlands but forbidden in most EU countries. However, such cases are rare.

The main concept in the EU is “What is illegal offline remains illegal online”. This statement was used in 1996 in Commission Communication ‘Illegal and harmful content on the Internet’ to signify that Member States should decide in what way to apply existing legislation regarding illegal materials on the Internet. Till nowadays the paper still actual with the best summarize of widespread categories and examples of illegal content, which are “covered by different legal regimes and instruments at the national and international level:

- national security (instructions on bomb-making, illegal drug production, terrorist activities);
- protection of minors (abusive forms of marketing, violence, pornography);
- protection of human dignity (incitement to racial hatred or racial discrimination);
- economic security (fraud, instructions on pirating credit cards);
- information security (malicious hacking);
- protection of privacy (unauthorized communication of personal data, electronic harassment);
- protection of reputation (libel, unlawful comparative advertising);
- intellectual property (unauthorized distribution of copyrighted works, software or music)”[29].

The Commision Recommendation from 2018 ‘On measures to effectively tackle illegal content online’ defined the illegal content as “any information which is not in compliance with Union law or the law of a Member State concerned”. Categories that are alredy covered by EU policy includes IP rights, sales of excise goods and medicine, illegal

[28] See note 24 above, 4.
[29] Ibid., 3.

hate speech alongside with terrorist content, materials with child pornography and unfair commercial practices. Since only certain types of content was mentioned, it seems that the legal framework neither gives an official definition of illegal content, nor harmonises this term among MS. It states in that manner by reason of determination of this term by specific legislation at the EU level and by national laws of MS. Nevertheless, the EU law makes efforts in harmonisation of the most insecured areas like child sexual abuse, online terrorist offences, illegal hate speech and Internet infringement of copyrights and related rights, by imposing minimum reqirements in national legislations with the aim to maintain safety of the single union market. [30]

The research on illegal content that have been encountered by EU users in 2018 showed the most common types of it by EU Members. In 17 countries (including Ireland and UK) economical unlawful activities such as frauds, subscription traps or other illegal commercial practices, were found more frequently, while in Lithuania and Latvia pirated content was mentioned by 19% and 33% of respondents respectively. Hate speech is the second by dissemination of illegal material online, which has been observed by more than half of respondents in Malta, the Czech Republic, Bulgaria and Poland. Child sexual abuse had the same rate as terrorist material and was the most common content in Romania, Bulgaria, Cyprus and Croatia. These stats show the level of dissemination of illegal content in EU MS, which on the average proves that six out of ten people encounter such material on the Internet.[31]

As the right to define what is illegal belongs to national governments, there are no unified official definitions of each category mentioned before. However, similar features and provisions could be found in the MS national legislations, due to the fact that they all signed particular international agreements, which include minimum requirements for some types of illegal materials.

The definition of "**Terrorist content"** is given in the proposal for a Regulation 2018/0331 on preventing the dissemination of terrorist content online. The necessity of establishing this definition on the level of Regulation goes from the danger of dissemination of such content online and need to harmonise it among all EU states, so the measures against this material would be the same.

---

[30] See note 27 above.

[31] "Report. Illegal content online," Flash Eurobarometer 469, (2018), Accessed on April 13, 2021, https://digital-strategy.ec.europa.eu/en/library/flash-eurobarometer-illegal-content.

Article 2 defines 'terrorist content' as any material that includes following acts: "incites the commission of one of the offences, where such material, directly or indirectly, such as by the glorification of terrorist acts, advocates the commission of terrorist offences, thereby causing a danger that one or more such offences may be committed;" or "solicits a person or a group of persons to commit or contribute to the commission of one of the offences"; "provides instruction on the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or on other specific methods or techniques for the purpose of committing or contributing to the commission of one of the terrorist offences"; or "constitutes a threat to commit one of the offences."[32]

However, law scholars, who support the side of the Commissioner, United Nations, human rights NGOs and other regional and international organizations, do not accept and condemn this version of the term, mentioning the overly broad and vague definition may cause problems of "the erosion of freedom of expression resulting from the absence of definitional constraints."[33]

First detailed definition of "**child abuse"** was provided in Report of the Consultation on Child Abuse Prevention, 29-31 March 1999, WHO. There are distinguished and defined 4 types of abuse: physical, emotional, sexual and neglect. [34] Despite the fact of using the wording "child abuse content" in Recital 47 of the Directive 2011/92/EU, Aticle 2 doesn't not include definition of it, only determines "child pornography", "pornographic performance", and "child prostitution", which constitute illegal on the web.[35] Thus, the Directive covers only the sexual side of child abuse.

Although the ECHR has provided minimum requirements for the claim of a child and/or the child's parents to be protected by Article 3 of The European Convention on Human Rights (hereinafter - the Convention), each country has additional provisions. The abuse is indicated in torture, cruel, degrading and inhumane treatment and the state has not established adequate preventative measures for protection of a child. However, each case is

---

[32] "Proposal for a REGULATION on preventing the dissemination of terrorist content online," Eur-lex, Accessed on April 14, 2021, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52018PC0640.

[33] Eliza Bechtold, "Terrorism, the internet, and the threat to freedom of expression: the regulation of digital intermediaries in Europe and the United States," *Journal of Media Law 12,1* (2020): 13-46, Accessed on April 14, 2021, https://www-tandfonline-com.skaitykla.mruni.eu/doi/full/10.1080/17577632.2020.1760474.

[34] "Report of the Consultation on Child Abuse Prevention," World Health Organization, (1999), Accessed on April 14, 2021, https://apps.who.int/iris/handle/10665/65900.

[35] "Directive 2011/92/EU on combating the sexual abuse and sexual exploitation of children and child pornography," Eur-lex, 7, Accessed on April 14, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011L0093&from=EN.

unique and if a child was hurt by the state failure to protect him/her, then the Court would consider all facts.[36]

"**Illegal Hate speech**" is a rather controversial term, which varies from country to country. However, recently in the Framework Decision on combating certain forms and expressions of racism and xenophobia by means of criminal law it was defined as "the public incitement to violence or hatred on the basis of certain characteristics, including race, colour, religion, descent and national or ethnic origin".[37] By the influence of the Code of Conduct regarding hate speech several Member States have provided their own definitions, which additionally to the racist and xenophobic materials also include content constituted intolerance to the disability of a person, his/her sexual orientation and a gender identity.[38]

Such big enterprises as Facebook, Microsoft, Twitter, YouTube, Instagram, Snapchat, TikTok and Dailymotion made an agreement with the Commission, which calls it the "Code of conduct on countering illegal hate speech online". The main purpose of the document is "to prevent and counter the spread of illegal hate speech online", with the special procedure by which, when online platforms get a valid notification (sufficiently precise and adequately substantiated) they will in an appropriate time-frame delete the content.[39]

More precise understanding of content that arises as "hate speech" was given by numerous cases by the ECHR, in particular, Handyside v. the United Kingdom, Erbakan v. Turkey, Vona v. Hungary, Aksu v. Turkey, Féret v. Belgium, Leroy v. France, Jersild v. Denmark.[40] The Court applies Article 17 of the Convention, which states for prohibition of abuse of rights, if "the comments in question amount to hate speech and negate the fundamental values of the Convention" or puts restrictions by Article 10 to protect "the speech in question, although it is hate speech, is not apt to destroy the fundamental values of

---

[36] "Research Report Child sexual abuse and child pornography in the Court's case-law," ECHR, Accessed on April 14, 2021, https://www.echr.coe.int/Documents/Research_report_child_abuse_ENG.pdf.

[37] "Framework Decision on combating certain forms and expressions of racism and xenophobia by means of criminal law," Eur-lex, Accessed on April 11, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l33178.

[38] "Code of Conduct–Illegal online hate speech. Questions and answers," Europa, Accessed on April 14, 2021, https://ec.europa.eu/info/sites/info/files/code_of_conduct_hate_speech_en.pdf.

[39] "The EU Code of conduct on countering illegal hate speech online," Europa, Accessed on April 14, 2021, https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en.

[40] "EU Human Rights Guidelines on Freedom of Expression Online and Offline," Europa, Accessed on April 14, 2021, https://eeas.europa.eu//sites/default/files/eu_human_rights_guidelines_on_freedom_of_expression_online_and_offline_en.pdf.

the Convention". Nevertheless, in every new case the Court examines all related facts and makes the decision according to the case-by-case approach.[41]

In the case of **Stern Taulats and Roura Capellera v. Spain** the ECHR concluded that setting fire to a photograph of the royal couple at a public demonstration, which was held during the King's official visit to Girona, did not constitute neither incitement to violence nor hate speech. Such actions had political nature, but not personal, so the critique of the institution of monarchy in general, considered a "permissible provocation in order to transmit a critical message in the framework of freedom of expression".[42] Similar opinion was in the case **Günduz v Turkey,** where the Court concluded that **"**mere fact of defending sharia, without calling for violence to establish it, cannot be regarded as 'hate speech'", when it was "expressed in the course of a pluralistic debate."[43]

In the area of Internet infringement four methods of "**online copyright infringement"** are distinguished by the means of getting access to it: streaming, downloading, stream ripping and torrenting.

1. Streaming: websites with access to unauthorised content via online streaming directly from an end-user's web browser.
2. Download: websites that enable direct download of the content to the user's web browser.
3. Stream ripping: websites that permit saving of streamed content to files, mainly audio into downloadable MP3 files.
4. Torrenting: a portal, which allows users to search for any content, and then download it through a file that starts the process of downloading the full product from another torrent user. [44]

For the first time the injunction to ISPs to block access to the websites, which merchandise counterfeit luxury goods of Cartier, was granted by the Supreme Court in the

---

[41] "Hate speech," ECHR, Accessed on April 13, 2021, https://www.echr.coe.int/documents/fs_hate_speech_eng.pdf.
[42] Ibid., 17.
[43] "Gündüz V. Turkey, Case 35071/97," ECHR, Accessed on April 13, 2021, https://www.legal-tools.org/doc/74a144/pdf/.
[44] "Online Copyright Infringement in the European Union. Music, Films and TV (2017-2018), Trends and Drivers," Europa, Accessed on April 14, 2021, https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/quantification-of-ipr-infringement/online-copyright-infringement-in-eu/online_copyright_infringement_in_eu_en.pdf.

UK on the grounds of **trade mark infringement** in the case Cartier International AG v British Telecommunications Plc.[45]

The area of **spamming** with illegal content, that sometimes can constitute illegal, is not included in the scope of ISP's responsibilities. The Court clarified this issue is under control of states according to the legal framework they have with national access providers. Such a conclusion was based on the case **Muscio v. Italy(2007),** where the applicant complained about receiving emails with pornographic images from unknown persons that had offended his moral convictions, which constituted interference with a right for private life. The identifying of the addresser was impossible to the fact the sender's email address was concealed. The Court found that getting spam letters with unwanted material does not regard a violation of Article 8 of the Convention as "once connected to the Internet, users of electronic mail systems no longer enjoyed effective protection of their privacy, exposing themselves to what were often unwanted messages, images and information." In such circumstances the Court concluded that there is no need for additional positive obligations under Article 8 for states to make efforts in combating spam, as national authorities and ISPs already have a framework for cooperation but encountered with objective difficulties in tracing the senders of such messages.[46]

So, the definition of illegality of any online content can be given only by each MS separately, as the precise definition of offenses varies from country to country. For instance, certain content may be considered as criminal by the laws of one Member State and not illegal by the law of another one.[47] According to the EU's attempts to harmonize legislation of all MSs regarding illegal content online, it oversees the tendency that only some categories need more attention and protection than the others. That is why recent attention was on materials connected with the terrorist offence, child sexual abuse, hate speeches and copyright violations.

[45] "Cartier International AG and others v British Telecommunications Plc and another, Case [2018] UKSC 28," Bailii, Accessed on April 13, 2021, https://www.bailii.org/uk/cases/UKSC/2018/28.html.
[46] "Information Note on the Court's case-law No. 102. Muscio v. Italy - 31358/03," ECHR.
[47] See note 24 above, 11.

1.3. EU Legislation: Transition from ISP Liability to Responsibility

The activity of the ISPs is a serious issue as they are intermediaries who connect people from all over the world to the worldwide web. Legal rules regarding the process of performing their functions correctly without infringing people's fundamental rights and causing damages to governments should be clear and equitable. ISPs must know how to process all information on the path from the Internet to the user's computer without liability for the illegal content that may appear. That is why in the EU this topic has appeared in the XX century with possible solutions to it.

The scholars emphasize 2 main models of online intermediary liability. The first one is **Generalist**. This model includes the liability into the general rules of civil and criminal legislation. The court decision on the provider's guilt will depend on whether they directly were involved in the illegal activity (contributory liability) or indirectly, as they could control the content (vicarious liability). This generalist model applies in many African and South-American countries.

Another model is "**Safe harbour**". This model constitutes immunity for service providers under specific conditions, which make intermediaries not liable for users' actions. There are 2 types of safe harbour: "vertical", which regulates conditions of one particular area, e.g. infringement, child abuse; "horizontal", which applies in general way to different types of activities. This model is applied in the EU.[48]

The *acquis communautaire* of ISPs' liability regarding illegal content consists of primary legislation (the Treaties, the Charter of Fundamental Rights of the EU), secondary legislation, and case law from the CJEU that form part of the EU legal order. Secondary law includes acts, discussed below, which are the directives and regulation, that have harmonized terrorist content, child abuse, hate speech, copyright and related rights in the Internet area. Other legal instruments presented in this chapter are non-binding legal acts which include only recommendations for MS and clarifications on particular issues.

Many scholars along with policy-makers affirm the latest trend in EU policy of Internet regulation about the slow replacement of intermediary liability by intermediary responsibility.[49] No wonder, if the EU approaches of the Communication from the

---

[48] "Frequently asked questions on internet intermediary liability," APC, Accessed on April 14, 2021, https://www.apc.org/en/pubs/apc%E2%80%99s-frequently-asked-questions-internet-intermed.

[49] Giancarlo Frosio, "Why Keep a Dog and Bark Yourself? From Intermediary Liability to Responsibility," *International journal of law and information technology* 26, 1 (2018): 1-33.

Commission on 'Illegal and harmful content on the internet' (1996) are compared to the Communication on a 'Digital Single Market Strategy for Europe' (2015), drastic differences would be seen. The first attempts of the government to regulate the Internet sphere regarding illegal content in the EU was made by providing the Communication and Green paper on the Protection of minors and human dignity in audiovisual and information services. These documents discussed the problem of illicit materials in the online form, harm it causes and stated measures that might be taken by both Memver States and online platforms. There was set the key role of Internet access providers (ISP) in giving users access to Internet content and identifying the chain of responsible people for illegal content. The document described the general regime for legal responsibility of ISP on that issue, which depending on the form of content might be: "under the criminal law, under civil law (an action for damages for breach of copyright or libel, or a dispute arising under their contracts with users or with network operators) or under administrative law (the system of regulation in place in the country where the access providers and host service providers operate)."[50] The problem of liability of ISPs was mentioned, concerning the cases where users had access to the illegal and harmful content through the providers' technical facilities. According to the fact that access providers do not have direct control over the content available on the Internet, the Commision asked for changes and clarification of law for providers "whose primary business is to provide a service to customers, to steer a path between accusations of censorship and exposure to liability."[51] As both documents have non obligatory forms, a determined legislation on that matter should have been adopted.

General obligations regarding all information in the Internet, that goes through ISPs, were stated in the **DIRECTIVE 2000/31/EC** on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (known as E-Commerce Directive), adopted on 8th of June, 2000. The Directive takes a horizontal approach to the liability of online intermediaries, which sets down conditions for information society service providers under which they can get exemption from liability for the information that involves illegal content.

In the Proposal for the Directive from 1998, the European Commission concluded that "The distinction as regards liability is not based on different categories of operators but on the specific types of activities undertaken by operators. The fact that a provider qualifies for

[50] See note 24 above.
[51] See note 24 above, (13).

an exemption from liability as regards a particular act does not provide him with an exemption for all his other activities."[52]

Safe harbour regime is envisaged in Articles 12-15 and lists obligations, which should be fulfilled by ISSPs according to the type of activities they perform. The Directive does not oblige entities by the name of it (hosting provider, ISP, content provider, video-sharing platform provider, etc), but by the services they provide for their customers. Most ISPs fall within the scope of Articles 12 and 13, if they perform such functions as providing access and merely caching the data. Precise definition of actions that can be performed by ISS is given as "(a) does not initiate the transmission; (b) does not select the receiver of the transmission; and (c) does not select or modify the information contained in the transmission." Thus, the online intermediaries are exempted from liability for the unlawful content that might be provided by them through the communication network of information (the Internet) on the request of a recipient of the service (online user). However, the actions of service providers should be "automatic, intermediate and transient", the storage of such information might be with the only purpose "to carry out the transmission in the communication network, and provide that the information is not stored for any period longer than is reasonably necessary for the transmission".[53]

Categories of ISPs that perform function of caching are also not held liable for their automatic actions, if they are mere intermediary in the transmission of the data to the subscriber and keep 'cach' only for limited period of time with the aim to increase the productivity of transfer of the information, "on conditions that:

(a) the provider does not modify the information;

(b) the provider complies with conditions on access to the information;

(c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;

(d) the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and

(e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been

---

[52] "Amended proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the Internal Market," Eur-lex, Accessed on April 11, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A51999PC0427.

[53] See note 13 above, 12.

disabled, or that a court or an administrative authority has ordered such removal or disablement."[54]

So, as ISP has a passive role in passing on the content and has insufficient knowledge about the information, it meets all aforementioned conditions and the ECD gives exemption from all types of liability, such as contractual liability, administrative liability, delictual, criminal liability, civil liability, etc. However, Member States can demand the ISP to terminate or prevent violation in compliance with a court proceeding or administrative request provided by national legislations. "The fact that intermediaries can be exempted from liability does not affect the possibility of injunctions of different kinds" by **Recital 45**.[55]

Article 15 of ECD clearly constitutes the prohibition for Member States to force ISP on a daily basis "to monitor the information which they transmit or store", and "to actively seek facts or circumstances indicating illegal activity." Although the general monitoring is illicit, such obligations as: informing competent authorities about the facts of known illegal activities, and assisting (on demand) the public authorities by means of providing the identification information about subscribers of ISPs, are legitimate for Member States. It is also reaffirmed in Recital 47 that "this prohibition does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation"[56].

On the other hand, **Giancarlo Frosio** sees this provision as "a well-established trend in recent intermediary liability policy that already emerged at the national level in multiple judicial decisions". He highlights the high recognition of imposition proactive monitoring obligations by national courts in the sphere of copyright infringement, privacy, defamation, and hate/dangerous speech.[57]

In rare cases when ISPs perform not only giving an access to the Internet, but also hosting the information, for the purpose to acquiring safe harbour they need to correspond at least to one of two following conditions from **Article 14**, either:

(a) "does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or

[54] Ibid, 13.
[55] Ibid, 6.
[56] Ibid, 13.
[57] See note 49 above.

(b) upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information."[58]

However, according to the Recital 42, only in cases when hosting providers play a passive role in their activities, they may be exempted from the liability. In the case **Google France and Louis Vuitton,** the CJEU explained the meaning of the 'neutral role' as a core feature of online providers, when the ISP has no control or knowledge about traffic data, transmission of it "merely technical, automatic and passive". The Court's conclusion was that the intermediaries are not held liable for data stored, if they didn't play an active role and after acknowledging that data was unlawful, the access to the content was disabled.[59]

In conclusion, according to provisions in the E-Commerce Directive regarding obligations of the information society services, which provide "mere conduit", "caching", "hosting", the regime of intermediary liability was established. Online services are under no obligations until they get the knowledge of any illegal activity that takes place on their platforms. Moreover, imposition of such voluntary obligations as "general monitoring the content" is prohibited. So, the directive covers only safe harbor regimes, which includes specific conditions for liability exemptions regarding claims for damages.

After the ECD stipulated general liability regarding all types of illegal or infringing content without specification, the EU legislators went further with taking a sector and problem-specific approach to regulate the tackling of certain kinds of illegal material on the net. The Commission placed obligations and responsibilities on particular information society services into the acts regarding most common types of such content, but not all of them have requirements for ISPs to act in order to tackle illegal content. The acts are based on general liability principles of ECD, but additionally include specific mandatory measures.[60] For example, the **Directive 2010/13/EU** on the provision of audiovisual media services includes obligations for audiovisual media services and video-sharing platform services, hence does not concern ISPs, but makes online video-sharing platforms responsible for third party content.

---

[58] See note 13 above, 13.

[59] Tambiama Madiega, "Reform of the EU liability regime for online intermediaries. Background on the forthcoming digital services act," Europarl, Accessed on April 14, 2021, https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/649404/EPRS_IDA(2020)649404_EN.pdf.

[60] Anja Hoffmann, and Alessandro Gasparotti, "Liability for illegal content online. Weaknesses of the EU legal framework and possible plans of the EU Commission to address them in a "Digital Services Act"," Cepstudy, Accessed on April 15, 2021, https://www.cep.eu/fileadmin/user_upload/cep.eu/Studien/cepStudie_Haftung_fuer_illegale_Online-Inhalte/cepStudy_Liability_for_illegal_content_online.pdf.

Similar liability is placed on ISPs by the **Directive 2001/29/EU** 'On the harmonisation of certain aspects of copyright and related rights in the information society'[61] (InfoSoc-Directive) and the **Directive 2004/48/EC** 'On the Enforcement of intellectual property rights', both of which apply horizontally to all types of IP rights. The remedy for rightholders is provided by Articles 11 and 8 of the Enforcement and InfoSoc Directives. By this provision copyright owners may request for injunction, which would concern intermediaries, if their platforms contain materials infringing intellectual property rights (the term 'intellectual property rights' includes a copyright, related right and industrial property rights) placed by a third party.[62]

The **CJEU** explains this provision as "the third sentence of Article 11 of Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights must be interpreted as requiring the Member States to ensure that the national courts with jurisdiction in relation to the protection of intellectual property rights are able to order the operator of an online marketplace to take measures which contribute, not only to bringing to an end infringements of those rights by users of that marketplace, but also to preventing further infringements of that kind. Those injunctions must be effective, proportionate, and dissuasive and must not create barriers to legitimate trade".[63]

In case **Tommy Hilfiger vs Delta Center** the Court concluded that "as far as concerns electronic commerce, the Court held that an access provider which merely permits Internet access without proposing other services or exercising a review provides a service which is capable of being used by a third party to infringe intellectual property rights and must be classified as an 'intermediary'"[64].

Although the EU sees online intermediaries as the best way to get over infringing activities, which is mentioned in the Recital 59, the only new (compared to ECD) obligation

---

[61] "Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society," Eur-lex, Accessed on April 15, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32001L0029&from=EN.

[62] "Directive 2004/48/EC on the enforcement of intellectual property rights," Eur-lex, Accessed on April 15, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02004L0048-20040430&from=EN.

[63] "L'Oréal SA v eBay International AG, Case C-324/09," Curia, Accessed on April 15, 2021, https://curia.europa.eu/juris/document/document.jsf?text=&docid=107261&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=2371598.

[64] "Tommy Hilfiger Licensing LLC v Delta Center a.s.,Case C-494/15," Curia, Accessed on April 15, 2021, https://curia.europa.eu/juris/document/document.jsf?text=&docid=181465&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=4918082.

is imposing injunctions by court decision, which can prevent illegal activity. Thus, it was a first step towards imposition of responsibility, but not in the way of discretionary measures.

In the **Directive 2011/93/EU** 'On combating the sexual abuse and sexual exploitation of children and child pornography' Article 25 includes measures against websites containing or disseminating child pornography. These provisions describe two approaches: the deletion of web pages with aforementioned content in a very short timeline (which can be done only by hosting or content providers), and blocking the access to the whole website with such materials (which is only possible for ISPs).[65] Both measures should be set by Member States according to the principles of transparent procedures, necessity and proportionality. The adequate safeguards shall be provided with informing users of the reason for the restrictions and the possibility of judicial redress.

Recital 47 sets forth the mechanisms against the Internet pages identified as containing or disseminating child pornography. Member States have the right to choose which methods are appropriate in their policies. These measures may be undertaken either on the grounds of public conduct (legislative, judicial, non-legislative), or voluntary actions. However, the latest has attracted more attention from Member States and became common measures in the national Internet policies in preventing wrong use of online platforms. From the side of MS, the obligation to ensure "adequate level of legal certainty and predictability" for online users and ISPs. To keep the balance with fundamental rights and freedoms of end users, national governments should impose both public and voluntary measures in accordance with the European Convention and the Charter of Fundamental Rights of the European Union.[66]

At the national level Article 25 was implemented in the following way: 14 EU MSs applied blocking as an optional measure. For performing this action a court order is required in Spain, Hungary and Greece. At the request of the authorities or the national regulators, the site can be blocked in Cyprus, France, Italy and Portugal. In Belgium, Chech Republic, Ireland, Finland, Malta, Sweden, and the United Kingdom, ISPs can do so voluntarily. In Hungary, Greece, Italy, Finland and France implemented legislation that governs process of preaparing the blacklists of websites containing or disseminating child pornography by national authorities and forwarding to the ISPs.[67]

---

[65] "Directive 2011/92/EU on combating the sexual abuse and sexual," Eur-lex, Accessed on April 15, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011L0093&from=EN.
[66] Ibid.
[67] "Report assessing the implementation of the measures referred to in Article 25 of Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children

The **European Commision** brought to the question the role of online providers as "in respect of access to information and content for many parts of society, platforms are increasingly taking centre stage. This role, necessarily, brings with it a wider responsibility." The wording shows the intention to change the current regime and put more obligations on Internet platforms: "Online platforms play a key role in innovation and growth in the Digital Single Market."[68] This was said in 2016 and after changes have begun.

Although the **Directive (EU) 2017/541** 'on Combating Terrorism' and Proposed Regulation COM(2018) 640 'on preventing the dissemination of terrorist content' put hosting providers under all duties regarding prompt removal of illegal materials, in Article 21 is defined an action, which can be performed only by Internet service providers. The Directive obliges MS to block the access to the website with a content, which is presumed to contain "public provocation to commit a terrorist offence", in cases when it is not possible to delete the content by hosting provider (happens when the subject is out of MS authority). For application of this measure: "transparent procedures," "possibility of judicial redress" and 'adequate safeguards' should be provided; the action must be "limited to what is necessary and proportionate," and informing users about applied measures is necessary.[69] The Directive mentions the "voluntary action taken by the internet industry to prevent the misuse of its services…such as detecting and flagging terrorist content"[70], which are part of private ordering and voluntary enforcement. Therefore, the Directive does not directly name the ISPs as liable stakeholders, but puts the obligation to block access to materials (that constitute public provocation to commit a terrorist offence), based on both the governmental and private requests.

The **Copyright Directive (EU) 2019/790** refers only to online content-sharing service providers, which exclude ISPs, because their main purpose or one of its main purposes is not storing the content and giving the public access to a large amount of copyright-protected works or other protected subject matter uploaded by its users.[71] **Regulation (EU) 2019/1148**

---

and child pornography," Eur-lex, Accessed on April 13, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016DC0872&from=EN.

[68] "Communication Online Platforms and the Digital Single Market Opportunities and Challenges for Europe," Eur-lex, Accessed on April 13, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0288.

[69] "Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA," Eur-lex, Accessed on April 13, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017L0541&from=EN.

[70] Ibid, 9.

[71] "Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market," Eur-lex, Accessed on April 13, 2021, https://eur-lex.europa.eu/eli/dir/2019/790/oj.

on marketing and use of explosive precursors limits activity of online marketplaces, which are merely websites for online sales. Both these directives impose the obligation on filtering the uploading content, to check whether it includes copyright materials and order the licence for it. In the opinion of **Federico Ferri** "the role played by technical protection measures and the existence of technical difficulties emerging from the obligations established in Arts. 15 and 17 cannot but hamper the interests of many users and a lot of small/medium service providers. The former could face plenty of obstacles in terms of their access to and use of works or other subject matter; the latter—especially small and medium providers—will find it hard (or at times impossible) to bear the weight of the burdens incumbent upon them by virtue of the 'link tax' and the 'upload filter'. Due to such lack of simplification, the position of tech giants will emerge even strengthened."[72] Thus, the switch to online intermediary responsibility in the sphere of protecting copyright works on the Internet was made, but with a few controversial provisions regarding the enforcement of providers' obligations.

Summarizing the aforementioned legal acts, we can conclude that the EU policy has been changing for the last 20 years in the direction of private enforcement and still the main act (E-Commerce Directive) states only the circumstances which exclude liability of online intermediaries. Unfortunately, scholars give more negative reviews about recent changes in their works, as the technical development is not sufficient yet and not all MS has implemented directives. Still the harmonisation of ISP liability/responsibility has been made only in several spheres: terrorist content, child sexual abuse, copyright infrigement, industrial property rights and trademarks. Moreover some issues are not transparent enough, so the problem with infringing fundamental rights and freedoms exists.

[72] Federico Ferri, "The dark side(s) of the EU Directive on copyright and related rights in the Digital Single Market," *China-EU Law J,* (2020), Accessed on April 15, 2021, https://link.springer.com/article/10.1007/s12689-020-00089-5#citeas.

2. BALANCE BETWEEN FREEDOM OF EXPRESSION AND RIGHT FOR PRIVATE LIFE IN RESTRICTING MEASURES OF ISP

For the reason to keep the Internet environment "clean" from unlawful content, states oblige online providers to block access to unwanted content by all means, which creates a danger of unlawful censorship. Internet censorship is commonly used in China and many Arabic countries, but among EU Member States with democratic societies. There is a fine line between the policy of a safe Internet and a free Internet. Especially the duty to filter online content, which is mentioned in legal acts without enough clarity, might interfere with the fundamental rights of EU citizens. Thus, when the governments can not draw the line, only courts have such authority.

2.1. General Approach to the Freedom of Expression and Right for Private Life

Usually it is hard to find a fair balance between giving a full and unlimited right to one person and putting in limits another, while ISP has obligations to both society as a whole and subscribers as individuals.This particular issue arises when ISP deals with illegal content on the Internet. On one side preventing the publication of unlawful material, to comply with EU legislation, on the other giving full access to users provided by Article 10 of the European Convention on Human Rights. The limitations of freedom of expression are interpreted strictly, but not detailed enough, because what is "necessary in a democratic society", which corresponds to "pressing social needs". Moreover, whether the right for private life has higher importance in dealing with illegal activities online. So, the main problem of obligations imposed on ISPs is how to strike a fair balance between different fundamental rights of the several stakeholders, in particular privacy and freedom of expression of users, freedom to conduct business of online intermediaries and the right to property (i.e. Intellectual Property) of right holders.

The legal grounds for Internet EU frameworks that are used by national legislators have been forming for the last twenty years on the basis of national and international (ECHR, CJEU) court decisions, recommendations and communications from EU authorities and legal doctrine. Thus, in 1996 the Commision was already concerned about interference of limiting measures of online intermediaries with the Convention's guarantees: "The full potential of such developments will depend on society as a whole striking the right balance between freedom of speech and public interest considerations, between policies designed to

foster the emergence of new services and the need to ensure that the opportunities they create are not abused by the few at the expense of the many."[73]

Later the Council of Europe with EuroISPA in the Guidelines expressed their concern about full access of ISPs to users' content and traffic data, which in some cases can lead to interference with freedom of expression or the right to private life. The Guidelines "underline their important role and position visà-vis the rights and freedoms of users" and accordingly may oblige providers under exceptional circumstances, defined by law, to support states with "monitoring content or data or impart information about a user to a third party." Moreover, removing, blocking and filtering the content can also have an impact on the rights and freedoms of ISP's subscribers.[74]

Ralf Bendrath and **Milton Mueller** see the future of ISP in monitoring systems with implemented **Deep packet inspection** (DPI). This is a technology which facilitates "comprehensive surveillance and discrimination of data packets moving through the network." It helps ISPs to more successfully "monitor, speed up, slow down, block, filter, or otherwise make decisions about the traffic of their users, based on knowledge of what kind of information they are transmitting". They believe DPI is the way to solve the problem of privacy on the Internet, improve protection of IP online, and increase safety of users from other illegal activities by managing the free flow of information.[75]According to their opinion, introducing the "intelligence technique" for ISPs should be the first step of government policy. ISPs' ability to examine online data will help to decrease the amount of illegal content on the Internet.

The **Human rights guidelines for Internet service providers**, also published in 2008, provided human rights benchmarks for ISPs regarding their services to the extent of fundamental rights, which gave the role of access providers as "gatekeepers of the Internet".[76]

Thereby, in the **Recommendation CM/Rec(2008)6** of the Committee of Ministers 'on measures to promote the respect for freedom of expression and information with regard to Internet filters' was given precise grounds for imposing these measures. First of all, provisions should be applied according to the conditions of Article 10, paragraph 2, of the

[73] See note 24 above, 3-4.
[74] "Human rights guidelines for Internet service providers," EuroIspa, Accessed on April 18, 2021, https://rm.coe.int/16805a39d5.
[75] Ralf Bendrath, Milton Mueller, "The end of the net as we know it? Deep packet inspection and internet governance," *New Media & Society 13*, 7 (2011): 1142–1160.
[76] See note 74 above.

Convention, namely the filters can be used only to specific and clearly identifiable content; the unlawfulness of materials and necessity of action should be determined by a competent national authority; only an independent and impartial judiciary body can review application of certain filters, by requirements from Article 6 of the Convention. Moreover, general blocking of offensive and harmful content should exclude some categories of users who can justify a legitimate interest and prove the need of illegal content under exceptional circumstances, i.e. research purposes.[77]

Finally, the EU **Regulation 2015/2120** established rights of end-users to access and distribute information and content, which can not be limited by agreements with providers of internet access services in Article 3. Accordingly on providers puts the obligation to treat all users and traffic equally, without discrimination, restriction or interference. However, the document envisages the possibility of Internet access providers to apply "reasonable traffic management measures", which means "transparent, non-discriminatory and proportionate, and shall not be based on commercial considerations but on objectively different technical quality of service requirements of specific categories of traffic". Avoiding general monitoring and specifying necessary time, ISPs can be subjects to "block, slow down, alter, restrict, interfere with, degrade or discriminate between specific content, applications or services, or specific categories", but only with purpose to comply with EU and national legislation.[78] It was the first legislative act of direct application, which set guarantees for users in open Internet space regarding the restrictions that can be imposed on them through access providers. The grounds for measures were not detailed, so case law is appropriate.

Wolfgang Benedek and **Matthias C. Kettemann** summed criterias for imposing restrictions for freedom of expression, when the measures *prima facie* interfere and must be justified. Legality provides the need to set the measure in law; legitimacy requires to pursue one or more of the legitimate aims (differs from "national security, territorial integrity or public safety to the prevention of disorder or crime, the protection of health or morals, protection of the reputation or rights of others", etc); necessity is implying only that measures, which are necessary in a democratic society, using principle of proportionality

[77] "Recommendation CM/Rec(2008)6 on measures to promote the respect for freedom of expression and information with regard to Internet filters," Council of Europe, Accessed on April 18, 2021, https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805d3bc4.
[78] "Regulation (EU) 2015/2120 laying down measures concerning open internet access," Eur-lex, Accessed on April 18, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015R2120.

regrading to the legitimate aim pursued.[79] These are general conditions for application of any limiting measure, but the Court would take into consideration the nature of the Internet, in dealing with cases of blocking and filtering online.

As was described above, the ISP can be subject to two types of obligations regarding tackling the illegal material online: filter (monitor) the content and block access for users. However, implementing such measures can interfere with censorship, so legislation on a national level is required. The Comparative study of the Council of Europe shows the ways states implemented blocking, filtering and take-down measures against illegal content on the Internet in their legislation. It states that several jurisdictions still use the **'general' legal framework** established by the EU in the E-commerce Directive. For example, Germany, Austria and the Netherlands have not imposed a targeted legislative framework for regulating these measures. In some countries **self-regulation** by the private sector prevails: codes of conduct, internet intermediary terms of use policies, or voluntary regulation in cooperation of ISPs with the police and other authorities. Few states use **municipal courts** to secure a fair balance between freedom of expression online and safety on the Internet. Nevertheless, many jurisdictions have introduced "**legal framework specifically aimed at regulation of the Internet and other digital media"**, as well as applying blocking and filtering measures by ISPs. Such framework includes provisions on the legal grounds for blocking, warranties, defining the competent administrative or judicial authority and necessary procedures.[80]

Nevertheless, some scholars have the opposite opinion regarding responsibility of ISPs. Raphael Cohen-Almagor argues with american professor Amos N. Guiora about the idea of establishing legal standards and limitations of Internet policy based on values. Latest "prefers adopting standards of civility and social responsibility by all stakeholders" including states, ISPs, online platforms and users. Restriction on social media on the Internet must be imposed due to the harm posed by online hate speech. In simple words he suggests a filtering system for online postings considering "magnitude, frequency, intent of

[79]Wolfgang Benedek and Matthias C. Kettemann, "Freedom Of Expression And The Internet," Council of Europe Publishing, Accessed on April 18, 2021, https://rm.coe.int/prems-167417-gbr-1201-freedom-of-expression-on-internet-web-16x24/1680984ea. 47-48.

[80] "Comparative Study on Blocking, Filtering and Take-down of Illegal Internet Content," Council of Europe, Accessed on April 18, 2021, www.coe.int/freedomofexpression.

the platform, and content of the post and platform".[81] So, Mr.Guiora would transfer the responsibility for illegal materials directly to content providers, neglecting the fact of possible violations of fundamental rights from the side of filters.

Similar opinions have **Christophe Geiger** and **Elena Izyumenko**, who consider the previous strategy with deterrence mechanisms imposed by legislators and judicial system has been replaced with transfer focus to Internet access providers. Current online enforcement strategies keep attention on end users and other "actors involved in the production, distribution and consumption of culture". However, they assume that none of the strategies accomplished assigned goals, thus scholars are "raising the question of their appropriateness and calling for an examination of alternative solutions."[82]

According to the legislation discussed, the MSs put ISPs under obligations to filter the content that goes through users' traffic and block particular material, which is illegal or is deemed to be illegal. Alternative to filtering measures is prohibited general monitoring, which under particular circumstances becomes a fully acceptable procedure in tackling illegal content. On the other hand from 2015 year EU takes the policy of the Net Netrality by adopting Regulation on The Open Internet, which states that internet traffic shall be treated without discrimination, blocking, throttling or prioritisation. Experts' opinions vary from implementation of stricter and detailed legislation to granting freedom of choice to ISPs using high technology in terminating the dissemination of unlawful material, or even relieving access providers from any liability. Limitations on the information of any nature are deemed to impose censorship, which is not permissible in democratic society. But when the information can cause harm to the receivers of it or even to the safety of the whole country, censorship might be an instrument of protection of rights and freedoms of individuals and nations.

---

[81] Raphael Cohen-Almagor, "Balancing Freedom of Expression and Social Responsibility on the Internet," *Philosophia 45,* (2017): 973–985, Accessed on April 19, 2021, https://link.springer.com/article/10.1007/s11406-017-9856-6#Fn13.

[82] Christophe Geiger,Elena Izyumenko, "The Role Of Human Rights In Copyright Enforcement Online: Elaborating A Legal Framework For Website Blocking," *American University International Law Review* 32, 1 (2016): 43-115, Accessed on April 18, 2021, https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1939&context=auilr.

2.2. ECHR Case-law Regarding Blocking and Filtering the Illegal Activities

Law professor **Jack M. Balkin** distinguishes a problem of Collateral censorship, which comes along with filtering and monitoring systems. He explained it with the example of a situation "when the state holds one private party A liable for the speech of another private party B, and A has the power to block, censor, or otherwise control access to B's speech. This will lead A to block B's speech or withdraw infrastructural support from B. In fact, because A's own speech is not involved, A has incentives to err on the side of caution and restrict even fully protected speech in order to avoid any chance of liability"[83]. In other words, ISPs would prefer to block access to all content, both illegal and lawfull (but doubtful), with the reason to avoid any liability, than implement more discriminatory filters that may overlook unlawful material. Thus, a new challenge arises for states to regulate this issue and find the solution how to avoid Collateral censorship within active monitoring obligation. Further the ECHR opinions on this matter are presented.

The main issue of the case **Cengiz and Others v. Turkey** was a blocking order on YouTube, on the ground that 10 webpages on that website contained materials violating a criminal law prohibition on insulting the memory of Mustafa Kemal Atatürk. As the Court has stated, blocking orders can be imposed on a specific material only when there are grounds to suspect that an offense has been committed and the State has no authority to block access to the entire Internet site on account of just some of its content. Therefore, blocking the entire website would lead to limitation of the access to a large amount of information, which affected the rights of internet users and had a substantial collateral effect.[84]

The Court emphasized the necessity of safeguards against collateral effects in several recent cases. In **OOO Flavus and Others v. Russia** blocking of the URL had influenced an entire website, **Vladimir Kharitonov v. Russia** suffered from a ban of the IP address which was shared by several websites. Thus, the Court stated that the blocking order must strictly aim for the illegal content only and avoid any collateral effects from the blocking measure.[85]

---

[83] Jack M. Balkin, "Old-school/New-school Speech Regulation," *Harvard Law Review* 127, 8 (2014): 2309, Accessed on April 18, 2021, https://www-jstor-org.skaitykla.mruni.eu/stable/pdf/23742038.pdf?refreqid=excelsior%3Aff1191b525764a16e11255758f70416c.

[84] "Cengiz and Others v. Turkey, Case 48226/10 and 14027/11" Hudoc, Accessed on April 18, 2021, http://hudoc.echr.coe.int/eng-press?i=003-5241080-6502267.

[85] "The Strasbourg Court Establishes Standards on Blocking Access to Websites," Strasbourgobservers, Accessed on April 19, 2021, https://strasbourgobservers.com/2020/08/26/the-strasbourg-court-establishes-standards-on-blocking-access-to-websites/.

In the case of **Yildirim v. Turkey** the Court emphasised not only collateral censorship, but also stated a guideline for states to impose blocking measures. State authorities under the court order blocked access to the Google sites, as one of the websites hosted by it contained illegal material. Thus the website of the applicant has also been blocked and couldn't be reached from Turkey. Ahmet Yildirim claimed a violation of his freedom of expression. The Court defined for the first time that "the right to Internet access is protected in theory by the constitutional guarantees applicable to freedom of expression and freedom to receive ideas and information."[86] Any action of blocking access is always in direct conflict with paragraph 1 of Article 10 ECHR as this right is secured "regardless of frontiers". To decide whether the actions have been rational it should pass the "adequacy" test, stated in Article 10 paragraph 2 ECHR: the interference with the freedom of expression can be justified only when it is prescribed by law, pursuing legitimate aims and necessary in a democratic society. The restriction should be proportionally to the legitimate result and does not affect the rights of third person - derives a collateral effect. Furthermore, if there are exceptional circumstances that can justify the blocking of illegal content, restrictions should be applied precisely to the content which is illegal and avoid lawfull ones.[87]

The Court determined the minimum criteria for Convention-compatible legislation on Internet blocking measures:

(1) "a **definition of the categories of persons and institutions** liable to have their publications blocked, such as national or foreign owners of illegal content, websites or platforms, users of these sites or platforms and persons providing hyperlinks to illegal sites or platforms which have endorsed them;

(2) a **definition of the categories of blocking orders**, such as blocking of entire websites, Internet Protocol (IP) addresses, ports, network protocols or types of use, like social networking;

(3) a provision on the **territorial ambit** of the blocking order, which may have region-wide, nationwide, or even worldwide effect;

(4) **a limit on the duration** of the blocking order;

(5) an indication of the '**interests**', in the sense of one or more of those included in Article 10 § 2 of the Convention, that may justify the blocking order;

---

[86] "Ahmet Yildirim v. Turkey, Case 3111/10," Hudoc, Accessed on April 18, 2021, http://hudoc.echr.coe.int/eng-press?i=001-115705.
[87] Ibid.

(6) observance of the **criterion of proportionality**, which provides for a fair balancing of freedom of expression and the competing 'interests' pursued, while ensuring that the essence (or minimum core) of freedom of expression is respected;

(7) compliance with the **principle of necessity**, which enables an assessment to be made as to whether the interference with freedom of expression adequately advances the 'interests' pursued and goes no further than is necessary to meet the said 'social need';

(8) **definition of the authorities** competent to issue a reasoned blocking order;

(9) a **procedure to be followed** for the issuance of that order, which includes the examination by the competent authority of the case file supporting the request for a blocking order and the hearing of evidence from the affected person or institution, unless this is impossible or incompatible with the 'interests' pursued;

(10) **notification** of the blocking order and the grounds for it to the person or institution affected;

(11) a **judicial appeal procedure** against the blocking order."[88]

So, it was the first court ruling defining the right for the Internet as a part of freedom of information and thus is included in the fundamental right for freedom of expression. This decision designated essential terms for the framework regarding limitation of freedom of expression online by blocking measures that should be established by national legislators via specific legal provisions.

Recent 4 cases, that had Russia as an opponent, made the Court to establish a unified guidance of blocking access to illegal content on the Internet to the Member States with comprehensive standards for domestic law, which would comply with the Convention: (**OOO Flavus and Others v. Russia, Bulgakov v. Russia, Engels v. Russia and Vladimir Kharitonov v. Russia**[89]. In all cases the fact of blocking the website was present and, for the first time, the Court compared that action to banning a newspaper or TV station, naming it an extreme measure. The Court held that for such actions the legislation should provide safeguards "from the excessive and arbitrary effects of blocking measures" in order to pass the "quality of law" test under the Convention.

1. **Safeguards against prior restraints**: The Convention does not prohibit such measures either offline or online, but allows them only under exceptional circumstances and requires the most careful scrutiny: "in cases of prior restraints on

[88] Ibid.
[89] "VLADIMIR KHARITONOV v. RUSSIA, Case 10795/14," Hudoc, Accessed on April 20, 2021, http://hudoc.echr.coe.int/fre?i=001-203177.

the operation of media outlets such as the present one, a legal framework is required to ensure both tight control over the scope of bans and an effective Convention-compliant judicial review"[90].

2. **Safeguards against collateral effect:** as was mentioned before.
3. **Procedural safeguards:** (1) notification of the blocking measures should be sent to the website owners in advance to ensure their involvement in the proceeding; (2) authorities are obliged to evaluate the possible effect of such measures before its implementation, or to justify the immediate necessity of them; (3) websites owners should have possibility to remove the illegal content; and (4) independent adjudicatory body is required to question the measures.[91]
4. **Transparency:** the blocking request and the legal grounds of it should be clarified to the website owners before the implementation of the measures. Additionally, Internet users should be able to know the information about the blocked website: legal basis for the blocking, the date and number of the blocking decision, the issuing body and the text of the blocking decision, including the reasoning and the avenues of appeal.[92]
5. **Balancing of all interests at stake:** for necessity and proportionality tests domestic law should require public authorities to evaluate if the desired result can be achieved by means of less invasive measures than blocking access to the whole website.[93]

So, the Strasbourg Court has finally established a comprehensive set of standards on blocking access to illegal content on the Internet in appliance with Article 10. Safeguards against the abuse may have positive influence on MS legislation and national court decisions regarding the balance between the measure to block the website and keep the freedom of expression.The Court specifically holds that national authorities must increase their technical capacity to pursue only the illegal content or impose blocking orders through the hosting service providers instead of access providers.

ISP has a general duty toward its customers to secure **private data** and the obligation of non-disclosure: option for anonymous publishing or using nicknames, minimising and anonymising the collection of personal information, privacy-friendly default settings, etc. But when it comes to situations with illegal content, ISPs should take

---

[90] "OOO FLAVUS AND OTHERS v. RUSSIA, Case 12468/15," Hudoc, Accessed on April 20, 2021, http://hudoc.echr.coe.int/fre?i=001-203178.
[91] "BULGAKOV v. RUSSIA, Case 20159/15," Hudoc, Accessed on April 20, 2021, http://hudoc.echr.coe.int/fre?i=001-203181.
[92] "ENGELS v. RUSSIA, Case 61919/16," Hudoc, Accessed on April 20, 2021, http://hudoc.echr.coe.int/fre?i=001-203180.
[93] See note 83 above.

measures in accordance to avoid liability, so it is a decision whether to violate the right and disclose private information or be responsible for harm that might be caused by such content. The ECHR gave its opinion on this matter in the case **K.U. v. Finland (2009), when** on an Internet dating site an advertisement of a sexual nature (it stated he was looking for an intimate relationship with a boy of his age or older) was posted with personal information of a 12-year-old boy. The boy had no knowledge about this ad, which included his name, year of birth, detailed description of his physical characteristics, a photo and his telephone number (only one digit off from the correct number). The fact of this ad was uncovered when the boy got an email from a man, who offered to meet him and "then to see what you want". For investigation the police asked the ISP to provide the personal information of the author of the ad, but the provider refused to do it. And the case was brought to ECHR.[94]

After considering all facts and current legislation, the Court made a decision that it was a violation of Article 8 in inability to protect the right to private life of a child. It concluded that this crime was serious privacy infringement conserning child sexual abuse. The effective and practical steps need to be taken: identifying and bringing the offender to justice. The Court interpreted provisions in Article 8 of the Convention as imposition on State positive obligations to secure respect for citizens' private lives together with protection from government interference. Thus, national legislation should reconcile the terms of confidentiality for ISPs considering assistance in criminal investigation, so the access provider could give to the police personal data on the author of the ad. "Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others"[95]- was a statement of the Court balancing the public interest and the protection of the rights and freedoms of victims in crimes. Regarding the liability of ISP for damages as a third party, the Court stated that it was not sufficient in the circumstances of the case.

So, with regards to the child pornography and spesifically the sexual child abuse on the Internet, the States should adopt a legal framework for protection of the rights and

[94] "K.U. v. FINLAND, Case 2872/02," Hudoc, Accessed on April 20, 2021, http://hudoc.echr.coe.int/fre?i=001-89964.
[95] Ibid.

interests, including the obligation of ISP to disclose identifying information on perpetrators. This measure does not violate confidentiality of communications as part of the right to respect for private life, provided by Article 8. ISP should give a guarantee that users' privacy and freedom of expression will be respected. It was the first and the only court decision, which allowed ISP to share personal information of a user.

In case **Tamiz v. United Kingdom (2017)** the Court declined in protection of the right for privacy online, due to the nature of revealed information. The applicant complained on Google Inc. for seven anonymous comments of defamatory nature about him on its service "Blogger.com". Despite the fact that comments were removed by the blogger in a few months, Mr Payam Tamiz issued a court proceeding about violation of his right to private and family life by Article 8 of the Convention.[96]

The Court discussed the nature of comments in online blogs. Some are really offensive or even defamatory, but rarely they can cause any considerable damage to someone's reputation. Nevertheless, most of the comments are either very trivial in nature or assumpted by readers as unserious and sketchy. Although expressions can be more than "vulgar abuse" of a kind, due to the context, which is in majority does not include specific allegations and low on language in general.[97]

The Court concluded that interference with the applicant's reputation was "trivial", so there was no violation of provider's right to freedom of expression according to these points: "the nature of the comments and the context in which they were made, the action taken by Google Inc. following notification, the potential liability of the actual authors of the comments, and the consequences of the domestic proceedings for both the applicant's reputation and for Google Inc.'s role as the provider of a platform for the free exchange of information and ideas.[98]

In the area of the Internet, the Court has maintained the importance of the "real and substantial tort test" for the aim to achieve fair balance between Articles 8 and 10: the state's margin of appreciation should have been wide regarding the importance of such ISSP as Google Inc, which "facilitates access to information and debates on a wide range of political, social and cultural topics."[99]

---

[96] "Payam Tamiz against the United Kingdom, Case 3877/14," Hudoc, Accessed on April 20, 2021, http://hudoc.echr.coe.int/eng?i=001-178106.
[97] "Guide on Article 8 of the European Convention on Human Rights," Council of Europe, Accessed on April 22, 2021, https://www.echr.coe.int/documents/guide_art_8_eng.pdf.
[98] See note 96 above, 22.
[99] Ibid, 23.

So, the Court pointed to two important aspects. First is the scope of the right to respect for private life safeguarded by Article 8 regarding the comments in online platforms, which can be an abuse for a person and count as illegal. This scope is under the control and appreciation of the state. Second is the significance of the "real and substantial tort test" in balancing respect for private life in reference to the freedom of expression in ISSPs. For this matter the Court upheld "strong reasons" for justifying decisions regarding fair balance of national courts.

Perrin v. the United Kingdom (2005) was another example of significance for child protection in the online sphere. In this case the conviction for publishing obscene material on the Internet was contested. The applicant was sentenced for 30 months in prison for publishing a free preview of photos with scenes of coprophilia, coprophagia and homosexual fellation on a website with subscribtion.[100]

Two important provisions were in the Court ruling regarding the topic of the research. First, although the applicant argued that his imprisonment would have "no significant impact on the protection of morals because similar material was available on other sites" as in case of Observer and Guardian v. the United Kingdom, the Court clarified that "There is a clear difference between what is necessary to preserve the confidentiality of secret information, which is compromised after the very first publication of the information, and what is necessary to protect morals, where harm can be caused at any time at which a person is confronted with the material."[101] Thus, the statement says that every following publication with the same illegal material causes the same harm as the first one did. Legal actions need to be performed in each single case.

Another essential issue concerns the effectiveness of measures against illegal content online. Parental control software packages, illegality of the accessing of the sites and blocking access by Internet Service Providers are "measures [that] have not been shown to be more effective", rather than application of a criminal prosecution by the State, which is more proportionate to protect against the harm.[102]

Thereby, the ECHR made clear about the harm of obscene materials that can be found on the net by children. Moreover, the measure that can be applied by ISPs in tacking illegal content down will never be the same effective as criminal liability of the author - guilty side.

---

[100] "PERRIN v. THE UNITED KINGDOM, Case 5446/03," Stradalex, Accessed on April 20, 2021, https://www.stradalex.com/en/sl_src_publ_jur_int/document/echr_5446-03.
[101] "Internet: Case-law of the European Court of Human Rights," Refworld, Accessed on April 20, 2021, https://www.refworld.org/pdfid/4ee1d5bf1a.pdf.
[102] See note 98 above.

Although general monitoring obligation is prohibited by ECD, states can establish obligations in national legislation for ISP to filter online content for specific purposes. The ECHR established guidelines for applying this measure in case **Szabó And Vissy V. Hungary.**

The Hungurian government wanted to impose a **monitoring** system (alongside with other measures) as a surveillance measure regarding tackling terrorist content. The Court declined the government to establish monitoring activity on the national level as it would intervene with the right given by Article 8, because the state hasn't provided securing adequate safeguards in its legislation. Specifically, lack of procedure to notify an individual, who has been monitored, and therefore "absence of any formal remedies in case of abuse". Notification system is crucial, because unless a person does not know that he/she was under this action, he/she is not able to contest the justification of such a measure. The Court concluded that "the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies and hence to the existence of effective safeguards against the abuse of monitoring powers".[103]

Thus, a monitoring system can be applied to the Internet area, but with restrictions and safeguards provided by law. This action should be with aim and has a strategy to look for only specific content, users should be in possession of information if they have been monitored already, and effective remedies should be implemented in cases of violation.

So, according to the case law of ECHR, application of blocking actions is more common and acceptable by the Court measure to exclude illegal content from users' view, but to comply with the Convention particular requirements should be met. In order to not interfere with freedom of expression the measure should be proportional and necessary, justifying the interest of the state/community, limited in time and ordered by appointed authorities with the possibility to appeal. For the reason of avoiding collateral censorship, a court order must be precise in determination of the amount of content, which is subject to block. Main problem of States lies in lack of safeguards established in national legislation for appropriateness of limiting measures in democratic society. Less common measures, such as monitoring/filtering and communicating personal data of users to state authorities, require stricter framework from states with the focus on "real and substantial tort test".

[103] "Szabó and Vissy v. Hungary, Case 37138/14," Statewatch, Accessed on April 20, 2021, https://www.statewatch.org/media/documents/news/2016/jan/echr-case-SZAB-%20AND-VISSY-v-%20HUNGARY.pdf.

2.3. CJEU Case-law Regarding Copyright Infringement

The situation is different with copyright infringements spreading online. By the Report almost half of the respondents from Spain, Portugal, Greece and Bulgaria met pirated content on online platforms.[104] Harm caused by infringement covers only individuals, who own IP rights for goods, but at the same time affects big production enterprises of entertaining materials (i.e. movies, music, books), which obstructs in dissemination the same material on the Internet by legal means. Christophe Geiger expressed the idea that the role of copyright is in "finding a balance between all the competing interests that surround the act of cultural creation". He explains the positions of both sides: creators, as owners of rights, who receive monetary benefit from the limited access to their works; and the society and public in general, with the aim to obtain free information from the open Internet. So, the author concluded that "access is the reason for which we are interested in cultural production."[105] Thus, admission to the copyright material, through the website, by means of an access provider creates a gate to infringement, which can be and should be closed (or at least controlled) by the ISP.

The most precise and fair estimation of measures and injunctions toward online intermediaries in dealing with illegal usage of copyright content. João Pedro Quintais approves that "the CJEU's judgments play a vital role in shaping the law applicable to online use". The Court applies the principles of effectiveness and autonomous interpretation, according to the objectives of EU copyright protection, thus giving uniform interpretation of the InfoSoc Directive and the European Convention.[106]

First significant case concerned copyright infringement online and imposing injunction on ISP was **Scarlet Extended SA v SABAM(2001).** The Court clarified requirements for injunctions that can be used by rightholders against the ISPs, provided by Article 8 of the InfoSoc-Directive. The issue of the case was about the request of SABAM (Belgian management company) for Scarlet Extended (the UK ISP) to install and implement a filtering system of all communications carried by its services for unlimited period and at own expenses with a purpose to identify infringing files of works from SABAM's catalogue. The Court ruled that this injunction was not legitimate, based on EU legislation and the

---

[104] See note 31 above.
[105] See note 82 above, 114.
[106] João Pedro Quintais, "Global Online Piracy Study: Legal Background Report," Ivir, Accessed on April 22, 2021, http://docplayer.net/87609818-Global-online-piracy-study-legal-background-report.html.

European Convention.[107] The requirement to filter all communications was seen by the Court as "general monitoring", which is prohibited by Article 15(1) of the E-Commerce Directive. The cost of implementation of such system shouldn't be excessively costly, but fair and proportionate with the timing of the injunction as stated in Article 3 of Directive 2004/48[108]. The protection of fundamental rights of different parties was at stake, so the Court made the conclusion on how not to put it into conflict: the need of balance between the protection of property (copyright) on the one side and other fundamental rights on the other, namely privacy, as "IP addresses (...) are protected as personal data"; the freedom to conduct a business; freedom of expression (as freedom of information its part).[109]

Emily Parris, Senior Associate (PSL), IP and Technology, Technology and Outsourcing at Fieldfisher, thinks that: "The ruling sets out clearly the factors that national courts must take into account when deciding whether to grant an injunction against an ISP. Tackling online infringement through the courts is clearly more challenging when the infringing activity is widely distributed and mixed-in with legitimate use."[110] Thus, despite the CJEU making clarification of requirements for intermediaries' injunctions, it is still hard to obtain through the court or other authority as cases with infringement only increase.

So, the main point of this case is to achieve balance between the protection of intellectual property rights and freedom of expression and privacy in filtering as a preventive measure for access providers. The injunctions must be proportionate and not unduly costly. A national court must find the following conditions for injunctions: keep proportionality principle, do not impose a general filtering obligation to actively seek for infringing content, stay in balance with fundamental rights.

Although in the case in the UK it was ordered that right holders should bear the costs of implementing the website blocking order, the innocent ISP was obliged to bear the litigation costs.[111]Similar regulation has the Irish Graduated Response System, which splits the cost of monitoring measures between the access provider (80 %) and the claimant/rights holder (20 %). While national courts in France and many other MS put the cost of the

[107] "Scarlet Extended SA v SCRL (SABAM), Case C-70/10," Eur-lex, Accessed on April 22, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62010CJ0070.
[108] "L'Oréal SA and Others v eBay International AG and Others, Case C-324/09," Curia, Accessed on April 20, 2021,https://curia.europa.eu/juris/liste.jsf?num=C-324/09.
[109] See note 107 above, I - 12027.
[110] Emily Parris and Nick Rose, "European Court of Justice rules on ISP injunction," Fieldfisher, Accessed on April 22, 2021, https://www.fieldfisher.com/en/insights/european-court-of-justice-rules-on-isp-injunction.
[111] See note 45 above.

implementation of filtering measures on ISPs, the CJEU gave the opposite opinion in the case Scarlet Extended SA v SABAM. [112]

The CJEU does not always authorize implementation of monitoring measures on ISPs with the purpose to prevent further infringement if the filtering mechanism is not precise enough to exclude the communications not connected to copyright. Such a conclusion was made in case **SABAM v. Netlog NV**[113] (2012).

SABAM, the same company from the previous case, brought an action against Netlog, a social network, to install a filtering system for forbidding copyright works of its clients. The CJEU provided an answer to a preliminary question regarding the legitimacy of this action under the EU legislation. The Court's conclusion stated that the filtering mechanism, determined as a general obligation to monitor, would violate both principles covered by Directive 2000/31, Directive 2001/29, and Directive 2004/48, and fundamental rights defined in Articles 8 and 10 of The European Convention on Human Rights.[114]

Matthew Sag is confident about the undeniable advantages of Automatic Copyright Enforcement Systems for protection of IP rights. He states that such mechanisms can lower the harm of copyright infringement and give online platforms assurance of safety of certain types of user content. Anyway, he makes an emphasis on placing "an undue burden on fair use and other forms of noninfringing speech" by automatic systems, as its programming is based on the policy of intermediaries and rights holders. Mattew sees prevailing "private ordering and control" over the public regulation in the future, thus online user participation in Internet policy will be more influential in adaptation of copyright robots.[115] So, the professor is sure that governing this sphere should be transferred from the state to the area of intermediaries and IP right holders. Implementing automatic filtering systems would definitely have a positive influence, but on the condition that such software should be built as precisely as possible, so no harm and blocking of fully legally content could be done.

---

[112] "IPR Enforcement Case-law Collection: The Liability and Obligations of Intermediary Service Providers in the European Union," Euipo, Accessed on April 20, 2021, https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_IPR_Enforcement_Case_Law_Collection/2019_IPR_Enforcement_Case_Law_Collection_en.pdf.

[113] "CVBA (SABAM) v Netlog NV, Case C-360/10," Curia, Accessed on April 20, 2021, https://curia.europa.eu/juris/document/document.jsf?text=&docid=119512&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=4146183.

[114] Emily Parris, "Injunction against social networking site is too wide, rules European Court," Fieldfisher, Accessed on April 22, 2021, https://www.fieldfisher.com/en/insights/injunction-against-social-networking-site-is-too-wide-rules-european-court.

[115] Matthew Sag, "Internet Safe Harbors and the Transformation of Copyright Law," *Notre Dame Law Review* 93, (2017): 66, Accessed on April 22, 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2830184.

On the other hand, **Martin Husovec** has the opinion that there is an alternative Internet policy of enforcing IP rights online. Although ISPs should be "excluded as potential tortfeasors", government policy must base on "alternative systems that make them [ISP] accountable". He states that Internet access providers can either rely on **voluntary measures** (implemented by themselves), or institute a **general claim for assistance** (right holders pay for expenses).[116]

Voluntary measures provide free cooperation between ISPs and online platforms without interference from the government, but only facilitating and observing it. If "situations of negotiation deadlock" occur, "the state could intervene in the form of specific legislation prescribing a certain type of measures". The deadlock might occur with providing personal data of infringing users by ISP, in this case legal remedies are necessary (subpoenas, claims for information, etc). Another way to regulate IP enforcement is to give to the IP owner a right to claim for "**assistance in enforcement** of their rights from an intermediary providing a proximate service on the condition that the observable direct costs are fully funded by him [right holder]"[117].

Thus, enforcement cooperations will be only those, which are demanded by claimants. After some period of time judicial practice of corresponding decisions will be reviewed by courts and follow up in general public policies with all available measures that can be implemented in such cooperation, considering right for privacy and freedom of expression. States must ensure a dialogue in parallel with litigation, by which voluntary agreements can be signed, so the courts would not put stricter measures on ISP.

So, the main point of Professor Husovec lies in agreement between Internet intermediaries on one side and the IP industry on another. The ways of obtaining the arrangement are contrary, either through public authorities (courts) or directly without assistance. Anyway the contact established by the voluntary agreement between ISP and right holder should be observed by states and controlled if necessary.

Different important issue was discussed in case **UPC Telekabel v Constantin Film** (2014) regarding liability of ISP for third party infringing activities committed through its services. The main question in this case was whether an Austrian anti-piracy group (VAP) can get a court order for injunction against UPC Telekabel (ISP) to block access to a website

---

[116] Martin Husovec, "Accountable, Not Liable: Injunctions Against Intermediaries," *TILEC Discussion Paper* 012, (2016), Accessed on April 22, 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2773768.
[117] Ibid.

with infringing content (movies). In its ruling the Court made clear the conditions for applying injunctions for intermediaries. First of all, the position of ISPs was determined as an intermediary within the meaning of Article 8(3) of Directive 2001/29, which means they can be subject to injunctions. Regarding the issue of placing an order to block access to an infringing website, the Court decided that the EU law does not preclude such injunction, so national courts must not interfere with fundamental rights, but compromise between the rights protected and the legal order of the European Union in line with the EU directives. Thus, an injunction is compatible with fundamental rights on two conditions:

1) "They do not unnecessarily deprive internet users of the possibility of lawfully accessing the information available;
2) They have the effect of preventing unauthorised access to protected subject-matter or, at least, of making it difficult to achieve and of seriously discouraging internet users who are using the services of the addressee of that injunction from accessing the subject-matter that has been made available to them in breach of the intellectual property right."[118]

If both conditions are met, an injunction would not infringe neither right to conduct business (the addressee still has a right to determine the measures to achieve the goal), nor the rights to intellectual property (as the right is not absolutely it should be balanced with the public interest). Moreover, the ISP is allowed to avoid the liability for copyright infringement, as necessary precautions have been taken.[119]

The CJEU stated that EU law does not prohibit a court order injunction that does not specify the measures that must be taken by an intermediary to block access to a website with infringing materials. The opposite conclusions were made by the **Advocate General Cruz Villalón** who suggested ISP blocking orders are legitimate if the injunctions determine specific blocking measures and appropriately consider the fundamental property rights and the importance of facilitating Internet access in a democratic society.[120] Despite the difference toward understanding the EU law, both views have agreed on obtaining a balance on fundamental rights as the main condition.[121]

---

[118] "UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH, Case C-314/12," Curia, Accessed on April 20, 2021, https://curia.europa.eu/juris/document/document.jsf?text=&docid=149924&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=4146537.

[119] See note 112 above, 15.

[120] "Opinion of Mr Advocate General Cruz Villalón, Case C-314/12," Eur-lex, Accessed on April 20, 2021, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62012CC0314.

[121] See note 118.

So, the concept of imposing a blocking order is composed from the fair balance between fundamental rights (right for property) and right to conduct business for providers, which means that the court should not specify what actions exactly must the ISP take, but state the goal of such measures. By complying the order, the access provider is no longer under the liability as it has taken all reasonable measures against infringement. Such provisions must be sufficiently effective to ensure genuine protection of the fundamental owners' rights with the purpose of preventing, hampering or discouraging unauthorised access to infringing content.

In case **Productores de Música de España (Promusicae)** v **Telefónica de España SAU** a company on behalf of intellectual property right holders asked ISP (Telefónica) to disclose "the identities and physical addresses of certain persons", who were involved in illegal activity using file exchange program and gave the access to shared files from personal computers to phonograms (Promusicae's members held the exploitation rights on it).[122] IP address, date and time of connection were known by the provider. So, the CJEU concluded that provisions in InfoSocDirective neither impose "an obligation to communicate personal data in order to ensure effective protection of copyright in the context of civil proceedings", nor prohibit MS from binding ISPs to disclose personal information of their users in the context of copyright infringement criminal proceedings.[123] Proper implementation and interpretation of EU directives into national legislation ensures a fair balance between the fundamental rights protected by the EU legal order.

The grounds for disclosement of information in this case was rather similar to the case of **K.U. v. Finland,** as in both situations the criminal proceedings were placed. As the court noted before, it was more important to find the guilty party (who spreaded the infringing material) and prosecute them, than just make ISP liable for third-party content. However, taking into account that K.U. was harmed by sexual abuse and Promusicae is just property right issue, the Court could not impose an obligation to share the identities and IP adresses due to the absence of vilation of fundamental rights in facts of the case.

Compared to the analysis of the national case law, the MS order three types of injunctions, that can be applied to ISPs against copyright infringement, can be distinguished. Most often courts use a **general website blocking order** (cases from DK, ES, FR, NL, AT,

---

[122] "Productores de Música de España (Promusicae) v Telefónica de España SAU, Case C-275/06," Curia, Accessed on April 22, 2021, https://curia.europa.eu/juris/document/document.jsf?text=&docid=70107&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=6970545.

[123] Ibid.

SE and UK). Another variation of this measure is a **live blocking order,** which prevents users from access to live streaming servers (in the case it concerned particular football seasons).[124] Toward the search engines courts applied obligations to **de-list infringing links** from search results and to **block searches,** which brought to websites with protected works. **Imposition of "dynamic" injunctions (**blocking of both primary domain name, IP address of websites and any subsequent domains that might be used in future[125]**)** were granted only once by Italian court. The court in France concluded that search engines were able to **detect the domain name of the web source** that gives access to infringing content.[126]

Conclusion

The EU case law has determined the most significant questions regarding injunctions that can be granted and imposed on ISP, if exclusive rights were infringed by a third party through its services, provided by Article 8 of the InfoSoc-Directive, which are general website blocking order, dynamic injunctions, disclosing of personal data of ISP's subscriber, and filtering/monitoring mechanism. The conditions and requirements for imposing these measures were clarified by the CJEU. Such measures should be precise in determination by the national legislation, keep in balance with other fundamental rights such as freedom of expression, right to conduct business and for private life, and not transfer to general monitoring. It has become common practise of national and EU courts to place orders on ISPs with measures to stop and/or prevent infringing activities. The problem arises when the cost of implementation of monitoring measures are too high for ISP and the right holder is not capable of bearing it.

Although the courts order filtering measures under very strict control with legal requirements, many scholars see implementation of copyright robots by the private sector as the only sufficient solution as a reaction to dissemination of copyright works without author's permission. New technologies should be installed by ISPs as the Digital era demands. The only question remains open, whether the filtering software will be fair regarding other lawful content and do not interfere with freedom of expression.

---

[124] "The Football Association Premier League Limited v. British Telecommunications Plc, Case HC-2017-000458," Vlex, Accessed on April 22, 2021, https://vlex.co.uk/vid/the-football-association-premier-793317289.

[125] Nigel Cory, "Adaptive Antipiracy Tools: An Update on Dynamic and Live Blocking Injunctions," ITIF, Accessed on April 21, 2021, https://itif.org/publications/2020/10/22/adaptive-antipiracy-tools-update-dynamic-and-live-blocking-injunctions.

[126] See note 110 above, 21.

2.4. The Approach of Ukrainian Legislation

Ukraine is not a part of the EU yet, but it makes best effort to comply with EU acquis communautaire and legislation. Although Ukraine has not implemented laws concerning spreading illegal content online and obligations of ISPs in ceasing it, there is only one provision regarding child pornography and few legal documents referring to blocking measures of Ukrainian ISPs against several russian websites. According to Article 39 of Law of Ukraine "About telecommunications": "telecommunications operators are obliged to restrict the access of their subscribers to the resources through which the distribution of child pornography is carried out, on the basis of a court decision".[127] So, ISPs have duty to deal only with child pornography through the court procedure and should not worry about other types of content. However in practice, there are multiple cases concerning blocking access to online platforms, which maintain video and comments with obscene words, unjustifiably insult and threaten physical violence regarding the plaintiff (case №2-1346/12); false information (cases №757/36221/16-ц and №457/349/18); sale of drugs in online shop (№757/59245/19-к); sale of goods with communist symbols (№757/33556/18-к), etc.[128]

As from 2014 Russian Federation began hostilities in the East of Ukraine, the government was concerned about the hybrid war, which is coming from the east, so they made changes to the state's information policy. On May 15, 2017 President Decree put an official ban on access to russian online platforms (namely VK, Yandex, mail.ru, Odnoklassniki, RBC, etc).[129] By 2018 the ban was extended to 426 different websites, all connected with the Russian influence and propaganda against Ukraine. Imposing this filtering system was based on the Decree of the President of Ukraine No. 126/2018 and then prolonged by Decrees № 82/2019 and № 184/2020.[130] The legality of the aim of this measure legislators justified in national security. However, many scholars and international

---

[127] "Закон України Про Телекомунікації," Zakon, Accessed on April 17, 2021, https://zakon.rada.gov.ua/laws/show/1280-15#Text.
[128] Сергей Студенников, "Блокування сайтів: судова практика розділилася," Sud, Accessed on April 17, 2021, https://sud.ua/ru/news/publication/156424-blokuvannya-saytiv-sudova-praktika-rozdililasya.
[129] "Указ Президента України №133/2017," President, Accessed on April 17, 2021, https://www.president.gov.ua/documents/1332017-21850.
[130] "УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №126/2018," President, https://www.president.gov.ua/documents/1262018-24150;
"УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №184/2020," President, https://www.president.gov.ua/documents/1842020-33629;
"УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №82/2019," President, Accessed on April 17, 2021, https://www.president.gov.ua/documents/822019-26290.

organisations claimed such actions interfere with freedom of speech by Article 10 of the Convention (which Ukraine also signed).[131]

Olga Kyryliuk analysed the above mentioned legal act with regards to a three-part test created by the ECHR for legitimate restrictions of freedom of expression. She underlined that the government has not achieved the goal by blocking the websites "the sanctions do not seem to have eliminated the threat of Russian propaganda or significantly contributed to building a more secure national information space. It is increasingly clear that the threat of disinformation is not unique to the Russian-controlled platforms that were targeted with sanctions." As all restrictions were implemented by enforcement bodies, she suggested "that the only legal grounds for removal of content or access is a court decision that follows a thorough and fair investigation of each case, provided that such a measure is necessary and proportionate to the pursued aim as required by international law."[132] Thus, Olga Kyryliuk concluded about inconsistency of government's actions with the approach of ECHR and imposing censorship on the Internet sphere of ukrainians, which leads to violation of Article 10 of Convention.

On the contrary, the group of scholars from Ukrainian Helsinki Human Rights Union considers blocking measures "appropriate and (in the short term) effective given the context", but also insists on the necessity of a court decision as a ground for such actions. They justify it with the reasons of excess of the Russian information with anti-Ukrainian and anti-democratic ideas, military aggression from the side of the Russian Federation.[133] So, there are also opinions, which support such severe measures of dealing with illegal content due to the wartime.

Another important content that keeps out of sight of the government is the existence of the website "myrotvorets.center". This webpage contains personal information about people who are considered as "enemies of Ukraine". It reveals their name, surname, address of living, date of birth, id and accusation of committing crimes against the national security of Ukraine.[134] Thus, it is not only a violation of right for private life, but also right to a fair trial, as this online resource is used by courts in criminal and civil cases as

---

[131] Блага А.Б., Мартиненко, "Свобода Слова в Умовах Інформаційної Війни та Збройного Конфлікту," Українська Гельсінська спілка з прав людини, (2017), Accessed on April 17, 2021, https://helsinki.org.ua/wp-content/uploads/2018/01/Web_Svoboda_Slova_A5_Ukr3.pdf.
[132] Olga Kyryliuk, "Should Ukraine Drop Sanctions against Russian Tech Companies?," Freedomhouse, Accessed on April 17, 2021, https://freedomhouse.org/report/policy-brief/2019/should-ukraine-drop-sanctions-against-russian-tech-companies.
[133] See note 131 above.
[134] "Про Центр," Myrotvorets, Accessed on April 17, 2021, https://myrotvorets.center/about/.

evidence.Ukrainian Association "Successful Guards" recognized Hate speech in actions made on this website, “it is common practice when Ukrainian citizens are found guilty without trial only because of the fact that they were included in the list of the website Mirotvorets. All of this, in the government's opinion, does not affect the protection of personal data expressed in the relevant Law. Thus, the state maintains this illegal practice by its silence”.[135]

Accordingly, neither the government nor the enforcement bodies do not use the capacity of Ukrainian ISPs to block all the content on “myrotvorets.center” for further investigation and deleting all unlawful information from the website.

In summary, according to the Ukrainian legislation and case law there is an explicit need in regulation on illegal content online and the role of ISPs in relation to this issue. Although in 2019 there was an attempt to implement rules regarding blocking access in Draft Law No. 6688 on the extrajudicial blocking of Internet resources, it was withdrawn. It is hard to say that blocking measures imposed by President Decree and court decisions are lawful with the meaning of the Convention and ECHR practice. Currently the government should resolve such problems as: insufficiency of laws on the Internet, applying the principle of proportionality in choosing the measures to justify the aim, putting safeguards and guarantees for those affected by unlawful blocking.

[135] “The right to freedom of speech and opinion in Ukraine: threats and opportunities,” Osce, Accessed on April 17, 2021, https://www.osce.org/files/f/documents/d/f/393431_0.pdf.

3. NEW REGULATION IS COMING

Due to the fact that current legislation regarding dissemination of illegal content has been adopted more than a decade ago, society demands changes. Great number of national and ECHR cases with unsolved questions regarding obligations of online intermediaries to act shows the necessity of actions from the governments. Even EU citizens feel the insufficiency of current measures in their daily life. On the public Consultation that was held in 2018 by European Commission most respondents agreed to the importance of protecting free speech online, as half of them had issues of unreasonable removal of their content with no further restoration.[136] So, the end of 2020 year became important in the field of appearing new ideas and approaches in cleaning the Internet from unlawfulness without infringing fundamental rights of users. The Proposal for a Regulation on terrorist content online, with rather controversial provisions, has been agreed to by the political consensus of Council and Parliament. It represents rather strict rules on Internet censorship that are necessary in fighting terrorist activity online. Another legal act that has appeared recently is Proposal for a Regulation on a Single Market For Digital Services, which renews the E-commerce Directive by applying a new approach.

3.1. Regulation TCO

On 12 September 2018, the European Commission presented a Proposal for a **Regulation** **'**On Preventing The Dissemination Of Terrorist Content Online'[137]. Such rapid change from voluntary regulation to **compulsory** is justified by the nature of incitement to the terroristic acts and serious harm that is at stake. On 10 December 2020, the Parliament and the Council presidency reached a political agreement on the Proposal and on 11 January 2021, the LIBE Committee approved the agreed text. So the next step is to formally adopt the new Terroristic act by the European Parliament and the Council. Vice-President for Promoting our European Way of Life, Margaritis Schinas, said: "Today's agreement will

[136] "Summary report of the public consultation on measures to further improve the effectiveness of the fight against illegal content online," Europa, Accessed on April 23, 2021, https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-measures-further-improve-effectiveness-fight-against-illegal.
[137] "Proposal for a REGULATION on preventing the dissemination of terrorist content online," Eur-lex, Accessed on April 23, 2021, https://eur-lex.europa.eu/resource.html?uri=cellar:dc0b5b0f-b65f-11e8-99ee-01aa75ed71a1.0001.02/DOC_1&format=PDF.

make the internet safer. When left online, terrorist content causes serious harm – it can motivate new attacks, radicalise people and is a means to disseminate dangerous technical expertise. The Regulation will provide a clear legal framework that sets out the responsibilities for Member States and service providers. Today's agreement is an important milestone in helping to prevent future attacks. Our Security Union is becoming a reality."[138]

The main objective provided by Proposal is to establish a unified and clear definition of terrorist content among all MS and fast removal of such material, which Regulation names as "an effective mechanism to address terrorist content online".[139] There is no secret, in recent years terrorist activity has increased and many EU countries are concerned about security. That's why the demand for taking proactive measures and harmonisation in the field of monitoring corresponding material has appeared now. By the words of Europol "the line between online and offline communities becomes increasingly blurred, terrorist propaganda preying on human suffering abroad reaches audiences in Europe to unprecedented extents, inciting someone to act and driving others to embrace extremist views on the opposite end".[140] Especially terrorist groups with religious goals tend to use the Internet alongside with social media platforms with the aim of obtaining instruments of crime, while the online messengers (such as WhatsApp, Viber and Skype) are used for sharing secret information regarding the future acts, to gain more "followers" in crimes they advocate on Facebook and Instagram, which helps to recruit new members.[141]

Below is presented the main new provisions of the Proposal, which distincts from the existing ones in **Directive (EU) 2017/541 on Combating Terrorism.** The analysis is based on case practice and legal doctrine**:**

1. **The one-hour rule**:

Emma Llansó debated about the speed of removals. According to her article, such rapid deletion can abuse the right to a fair hearing, protected under Article 6 ECHR, as upcoming pressure from the state on the provider for fast removal would decrease the quality of proper review. Moreover she suggests to pay more attention to the safeguards for human

---

[138] "Security Union: Commission welcomes political agreement on removing terrorist content online," Eur-lex, Accessed on April 20, 2021, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2372.
[139] See note 137, 1-2.
[140] "The European Union Terrorism Situation and Trend Report 2019," EUROPOL, Accessed on April 20, 2021, https://www.europol.europa.eu/activities-services/main-reports/terrorismsituation-and-trend-report-2019-te-sat.
[141] "Internet Organised Crime Threat Assessment (IOCTA)," EUROPOL, Accessed on April 19, 2021, https://www.europol.europa.eu/iocta-report.

rights in questions of filtering technologies and removal of content.[142] So, this rule might interfere with **effective judicial remedies**, as the platform would not have enough time to question the removal orders and make the right conclusion. On the other hand, the terrorist content can lead to damage in the first hours after publication.[143] Respectively the earlier the less.

2. New **definition** of illegal terrorist content;

Lots of debates come around a new definition of terrorist content established by Proposal (which refers to the Directive (EU) 2017/541). **Eliza Bechtold** argues that the definition has been negatively influenced by the European trend of "adopting increasingly broad and vague definitions of glorification-related offences". She explains her idea in the example of including "advocacy", "apology" and "encouragement" of terrorism into the category of "glorification offences", which leads to narrowing down the free speech and broadening of censorship.[144] Additionally the **Romanian Senate** expressed against this definition as the previous one from the Directive on Combating Terrorism (541/2017) has not yet been unified among all Member States, which makes difficult to develop related sanctions, and added that it might also cause limitations to the freedom of expression.[145]

As was mentioned before, the main issue in defying whether a certain act is a terrorist crime or not is **its aim**. Only on the basis of objective circumstances can be defined the true intentions of a person committed the act. Each one of the following aims indicates the terrorist offence: seriously intimidating a population; unduly compelling a government or an international organisation to perform or abstain from performing any act; seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation.[146] To figure out whether certain material posted with one of the above mentioned aims, the information alongside with the content of the website as unified should be considered together. While most automatic

---

[142] Emma Llansó, Laura Blanco, "EC Recommendation on Tackling Illegal Content Online Doubles Down on Push for Privatized Law Enforcement," Center for Democracy & Technology, Accessed on April 12, 2021, https://cdt.org/insights/ec-recommendation-on-tackling-illegal-content-online-doubles-down-on-push-for-privatized-law-enforcement/.

[143] See note 138 above.

[144] See note 33 above, 21.

[145] Katrien Luyten, "Addressing the dissemination of terrorist content online," EuroParl, Accessed on April 12, 2021, https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/649326/EPRS_BRI(2020)649326_EN.pdf.

[146] See note 69 above, 13.

filtering tools use only the wording/phrasing system of estimation. So, can automatic monitoring systems consider the aim of published content?

Eugénie Coche in her research acknowledges the point that "technological means are not (yet) able to contextualise posts, whereas 'context of content' is a factor that needs to be taken into account" and even when the Proposal "seems to provide better safeguards as it suggests that human oversight and verification should be provided where there is no 'human in the loop' (when automated means are used)".[147]

3. **The duty of care obligation**

The Proposal, besides the obligation to delete/block access, in Article 6 suggests for hosting providers to take proactive measures regarding terrorist content, namely establishing "deploying automated detection tools", which filter all the content and hide unnecessary one. Accordingly, the decision to remove/block content can be made by both administrative or judicial competent authority (based on removal order) and provider itself. Although on an annual basis providers should make a report to authorities, regarding automatic tools they are using, one year is too long a time for estimating such measures on effectiveness and proportionality with the risk to interfere with freedom of speech. As was mentioned in section 2, in the cases **Ahmet Yildirim V. Turkey, Bulgakov V. Russia, Hasan And Chaush V. Bulgaria the ECHR** referred to the Article 10 of the Convention regarding "the safeguards are respected, measures may be taken to enforce the removal of clearly identifiable Internet content or, alternatively, the blockage of access to it, if the competent national authorities have taken a provisional or final decision on its illegality."[148] Thereby, host providers could be granted with a wide discretion in deciding the fate of content, measuring its illegality and applying restrictive measures to it, while the Court perceives in such actions incompatibility with Convention and the rule of law. It stated that "Consequently, the law must indicate with sufficient clarity the scope of any such discretion conferred on the competent authorities and the manner of its exercise."[149]So, this provision may indicate the switch of the EU Internet policy regarding illegal content to voluntary measures established by ISP. However, the states still have to govern these measures annually. The problem occurs with the correspondence of

---

[147] Eugénie Coche, "Privatised enforcement and the right to freedom of expression in a world confronted with terrorism propaganda online," *Internet Policy Review* 7, 4 (2018), Accessed on April 12, 2021, https://policyreview.info/articles/analysis/privatised-enforcement-and-right-freedom-expression-world-confronted-terrorism.

[148] "Ahmet Yildirim v. Turkey, Case 3111/10," Hudoc, Accessed on April 18, 2021, http://hudoc.echr.coe.int/eng-press?i=001-115705.

[149] "Hasan and Chaush v. Bulgaria, Case 30985/96," Hudoc, Accessed on April 10, 2021, http://hudoc.echr.coe.int/eng?i=001-58921.

voluntary measures to the provisions of Convention, as either the Court should change its view toward competence of Internet intermediaries or states should establish strict safeguards for balancing fundamental rights in this relationship.

The Proposal covers the measures of effectiveness and proportionality of automated tools by adding the human oversight and verification mechanisms,[150] which might lead to the problem of either processing a large amount of content by employees (people will not keep pace on all content) or hiring a separate department with a particular task to deal with illegal materials (high cost). However, the core goal is to achieve balance in these issues.

4. **Strengthened cooperation**;

The cooperation between state authorities and host providers proceed through the special 24/7 representatives for executing removal orders and referrals. Hiring new employees for three working shifts per day all week long might cost much for hosting providers, considering not all of them have high profit. As CJEU has indicated in cases **Scarlet Extended SA v SABAM and UPC Telekabel v Constantin Film,** putting additional cost for online platforms should be in balance between the freedom to conduct a business and other fundamental rights. The Proposal's core aim is to reduce accessibility to terrorist content online, achieving it leads to the protection of national security from terrorist attacks. Concluding that national safety is more valuable, additional expenses of performing these obligations might be in balance with host providers' rights, if they are proportionate to the turnover of the company, or if the cost is too high, the state could suggest financial support.

5. **Effective complaint mechanisms:**

Required effective procedural safeguards against abuse were established by ECHR in recent cases against Russia (OOO Flavus, Bulgakov, Kharitonov and Engels). The Court explained that first of all the websites' owners should have the opportunity to delete the unlawful content, further a right for an effective Convention-compliant judicial review. Consequently, a state should arrange "a court or other independent adjudicatory body providing a forum in which the interested parties could have been heard".[151] In case the forum decides the content was not unlawful, the service provider should restore the material as soon as possible.

6. **Financial penalties**:

Financial penalties imposed by Member States may vary up to 4% of the hosting service provider's global turnover of the last business year for systematic non-compliance

[150] See note 137 above, 26.
[151] See note 89 above, 14.

with removal orders.[152] Non-compliance sanctions should be proportionate to the nature and size of the provider, in accordance to estimate the burden and penalties for small, medium and micro enterprises estimated according to the Commission Recommendation 2003/361/EC. The Presidency's suggestion on the Proposal states that the "decision to impose or not financial penalties for breaches of the obligations should be also based on such circumstances as: whether a legal or natural person is responsible and should be liable for violation".[153]

The conformity of this Proposal with the E-Commerce Directive shows disparity in several provisions. First of all it puts under question the safe harbour regime established by Article 14, which excludes the liability of hosting providers, if they acted as merely intermediaries. On the contrary the Proposal puts sanctions if the content wasn't deleted within one hour. Moreover the general obligation to monitor hosting content, which is provided by automatic filtering tools, is prohibited under Article 15 of the E-Commerce Directive. As this provision is contrary with the aim of Article 15 - to protect the rights of the online intermediaries and the rights of the Internet users. So, it seems as the EU legislators try to put the responsibility to tackle illegal content on the private sector of the Internet companies by delegating most obligations to hosting service providers.

On the one side "the dangers to freedom of expression that result from aggressive efforts to regulate online content by way of intermediaries"[154], on the other threat of terrorist attack (when the national security and lives of thousands of people are at stake). Following the principle of proportionality limitation of some aspects of freedom of speech may reduce the hazardous problem of dissemination of content threatening lives and health of the population. This choice should be made by the government in deciding what is more important for the country and dealing with consequences.

Naomi Klompmaker in her research raised the problem of consequences for deleting the illegal content instead of tracking the source of it. On the example of social media (Facebook, Youtube), she shows that deleting extremist and terrorist material from there by platforms causes the "unintended effects related to the removal of all radical or extremist ideas from social media platforms". This means after the content has been deleted a few times and "legal content" policy has been published, the authors of such content would probably transfer their activity to another more encrypted social media or messenger. After that there is

[152] See note 137 above, 32.
[153] "Presidency Proposal TCO," Europal, Accessed on April 15, 2021, https://cdn.netzpolitik.org/wp-upload/2020/10/DE-Vorschlag-zu-Terror-Inhalte-Verordnung.pdf.
[154] See note 33 above, 27.

no possibility to track these individuals for further criminal investigation, as "the removal of extremist and terrorist content on social media platforms interferes with online deradicalisation strategies, because it takes away the opportunity to dismantle extremist messages, provide for counter narratives or start discussions with radicalising individuals".[155] This opinion leads to the conclusion of establishing the cooperation between host providers and access providers in assistance to the enforcement bodies. As was mentioned in the case **K.U. v. Finland** providing personal information on ISP's customer helps to identify the person.

In the point of view of German Presidency the justification of the restriction of fundamental rights should come from the states, but not vice versa. Thus the decision to obtain the removal orders must be from state authorities (not the intermediaries themself). They must show that such measures are necessary and proportionate, since the material is unlawful and might cause harm. Moreover the grounds for removal of the content should be only the removal order issued by the court. Hence, it is not in the power of service providers to seek "reasonable grounds to believe that the removal order manifestly and seriously breaches the fundamental rights and freedoms set out in the EU-Charter of Fundamental Rights".[156]

While the national authorities suggest making the obligations for hosting service providers more transparent by changing the proactive measures to specific, which respectively should be determined by the Regulation: usage of automated filtering should be rare, only when it is applicable, on the grounds of adopted by service provider terms of use and the policy, which clearly clarify users' rights and obligations.[157]The scholar sees this compulsory framework as a necessary move of protection against the unique threat posed by terrorist-related expressions on the Internet, as the severeness of this threat would justify states' departing from the measures provided by the ECD.[158]

For more successful results in finding the terrorist content online ISPs should establish effective communication with respective authorities and enforcement bodies: most important with the EU IRU and the national IRUs. Exchanging information regarding

---

[155] Naomi Klompmaker, "Censor Them at Any Cost: A Social and Legal Assessment of Enhanced Action against Terrorist Content Online," *Amsterdam Law Forum* 11, 3 (2019): 3.
[156] "EU: German Presidency Proposal for Terrorist Content Online Regulation fails to protect freedom of speech," Article19, Accessed on April 13, 2021, https://www.article19.org/resources/eu-german-presidency-proposal-terrorist-content-online-fails-freedom-of-speech/#:~:text=Overbroad%20definition%20of%20terrorist%20content,for%20recruitment%20and%20radicalisation%20purposes%E2%80%9D.
[157] See note 153 above.
[158] See note 33 above, 27.

suspicious links, new updates in Database of Hashes, illegal movement of IP addresses, private information on blocked content, etc. Effectives is also provided by means of the most prompt response and deleting illegal content, as any information with incitement to terrorist acts is the most harmful in the first hours after its appearance. Online platforms and law enforcement should find an effective way of communication with appropriate digital interfaces to facilitate their interaction. Such cooperation may include the technical community for achieving more effective technical solutions in this challenge.

Conclusion

Thereby, the new Proposal for Regulation on Terrorist Content Online should make an efficient contribution to preventing terrorist attacks and spreading anti-peaceful ideas. Definition of terrorist content should not make the existing censorship among EU countries more wider than it is necessary for all democratic societies. The Regulation would establish new obligations for service providers, which were not compulsory before, but can be the right solution nowadays. Definitely, the procedures of deleting content, reacting on removal orders and referrals should be established clearly in provisions of the Regulation, namely the time of removal might include some exceptions under unexpected circumstances, which would not interfere with effective judicial remedies. The similar provisions should concern the process of filtering by means of automatic tools, where procedural safeguards are the core issue in keeping the balance with the freedom of speech. All these measures with proper integration in the EU legal system would help to stop the dissemination of terrorist content with the help of online intermediaries.

As from the negative side, the problems may arise with freedom of service providers to conduct business, by maintaining the cost of fast removal of content, application of automatic filtering systems and appointment of special representation employees for these purposes; high financial sanctions in case of systematic failure to comply with obligations, that are not clarified enough. Another side of harm comes to users and content providers, who would be limited not only by illegal materials, but also the legal ones, as the collateral effect may influence the whole scope of information online even distantly connected with the “terrorism”. Filtering robots might increase the amount of content that has been catched by the actions with the collateral effect.

In conclusion, the provisions of the Proposal demonstrate the major transition of the EU Internet approach regarding illegal content from the state regulated to voluntary measures created by service providers. In the literature such a system is defined as privatized

censorship. Some scholars address against privatized censorship that shows in some provisions of the Proposal (active measures of providers, automatic filtering tools, etc).[159]

Anyway, some others recommend combining different approaches in order to find the right solution for accomplishing necessary goals. As **Professor Roraback** suggests "differentiated liability combined with targeted oversight and user-centered design as a model for realistic and balanced regulation of intermediaries". She underlines that governments can't hide behind online intermediaries to achieve certain goals regarding dissemination of illegal content on the Internet, as the human rights approach disallows broad delegations of powers in issues concerning fundamental rights. The delegation might have positive influence if it complies with human rights principles and provides safeguards for accountability.[160] So, the balance should be achieved in sharing the responsibility between internet service providers, hosting and content providers, online platforms and Internet users. The main subject in this relationship should stay the state, represented by competent authorities.

For now the next step for the Proposal will be formal adaptation by the European Parliament and the Council, in line with their respective roles and procedures. As the Commission remains fully committed to support the process, including the application of the Regulation, the Regulation might come next year.[161]

3.2. Digital Services Act

[159] See note 33 above.
[160] Molly K. Land, "Against Privatized Censorship: Proposals for Responsible Delegation," *Virginia Journal of International Law 60,* 2 (2020): 363-432.
[161] See note 138 above.

Due to the fact that new challenges have appeared since the E-Commerce Directive twenty years ago, connected with emerging the number of online platforms and increasing the ways of sharing unlawful and harmful content, a Proposal for a Regulation on a Single Market For Digital Services (new Digital Services Act [DSA]) has appeared on the 15th of December in 2020 as a part of the EU Digital Single Market Strategy. The main goal of this act is to face problems that were not resolved by the E-Commerce Directive and to meet current challenges of the Digital Age. Hence, the Proposal amends some provisions of the ECD and uses another approach by establishing new objectives and rules. Moreover, transfer to a binding legislative act shows the need of EU Member States in harmonization on many issues revealed in the DSA. The need for uniform harmonisation of the Internet policy among EU members was based on the problem of obstacles for the single market by the difference in the provisions at national level of the states, which helped only big platforms in EU competition. Moreover, divergent national regulations were exposed as **ineffective** in protection of rights of online intermediaries and their users.[162] Thus, the legislators concluded that this problem should be set in the form of EU Regulation.

The dissemination of illegal content, which harms not only individuals but also national safety, has been expanded in recent years.[163] Due to the EU and ECHR case law the concern was increased about more interference with fundamental rights and freedoms of citizens by imposing blocking/deleting obligations on service providers by national governments. Also the question of effective enforcement has not been answered yet, so the Proposal endeavors on improvement of the governmental supervision of online intermediaries and effective cooperation between national and union authorities.[164] Maintaining a safe online environment and empowering users and protecting their fundamental rights online are two other important objectives of the Digital Service Act.[165]

This time the Commission used a different approach in the base of making changes to the legislation. For making a conclusion which of the following options is the most appropriate for achieving the goal the Extensive consultation with stakeholders was held, where they left behind **limited measures against illegal activities** and **fully harmonised**

---

[162] "Liability of online intermediaries," EU study on the Legal analysis of a Single Market for the Information Society, Accessed on April 15, 2021, https://op.europa.eu/en/publication-detail/-/publication/a856513e-ddd9-45e2-b3f1-6c9a0ea6c722.
[163] See note 31 above.
[164] "Proposal for a REGULATION on a Single Market For Digital Services (Digital Services Act)," Eur-lex, Accessed on April 15, 2021, https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608117147218&uri=COM%3A2020%3A825%3AFIN.
[165] "Executive Summary of the Impact Assessment Report," Europa, Accessed on April 15, 2021, https://ec.europa.eu/competition/sectors/ICT/DMA_summary_of_impact_assessment.pdf.

measures, but chose **Asymmetric measures** with higher obligations for a large online platforms.[166] The last option states for defining the liability of online intermediaries with effective supervision of EU authorities.

According to the Proposal the right to **define** what exactly constitutes "illegal content" still stays by national legislators. However, the DSA lists the most important categories of unlawful material, namely terrorist content, material with child sexual abuse, non-consensual sharing of private images, illegal hate speech, counterfeit products, and copyright infringing data. **Margrethe Vestager**, as the Executive Vice President of the European Commission for A Europe Fit for the Digital Age, explained this provision: "The act in itself is not about content, also because there will be differences between [EU] member states. For instance, hate speech is not outlawed in every member state in the same manner. So here platforms will have to deal with the national provisions when it comes to content."[167] However, the problem of collateral effect can appear, due to the fact that by the one MS's request to take down particular content (illegal according to its national legislation) online platforms will delete or block access to it alongside with hiding it from users of other MS, where such content is not deemed to be illegal. The only option is to block this material by the means of the Internet access provider, who's actions influence only specific territory (country/region).

Provisions about services that provide 'Mere conduit' and 'Caching' were duplicated from the E-Commerce Directive (which corresponds to Articles 12-13), without making additional definitions. In general all **obligations** of service providers are divided in four groups: removing or disabling access to the illegal content, providing the information, publishing terms and conditions of restrictions, reporting on applied measures.

As to application of the monitoring obligations by providers in the field of copyright infringement **Severine Dusollier** suggests to "limit the application of preventive measures imposed by the directive [Copyright Directive (EU) 2019/790] by default of a proper licence, to prima facie **copyright infringements,** i.e. to uploads of materials identical or equivalent to the work for which rightholders have provided information. In other cases … The uploaded content should not be presumed to be infringing and more legal evidence should be provided by copyright owners to allow for its removal from the platform."[168]

---

[166] Ibid.
[167] David Meyer, "The Conversation MARGRETHE VESTAGER," Fortune 183, 2 (2021): 12.
[168] Severine Dusollier, "Editorial," *JIPITEC* 10, (2020): 275-276.

The Proposal **defines** the nature of the **Orders** to act against illegal content (Article 8) as "an order to act against a specific item of illegal content, issued by the relevant national judicial or administrative authorities, on the basis of the applicable Union or national law, in conformity with Union law."[169] The main point of it is that the request should point only to the particular material that is considered as illegal, and ordered either by the court or some other administrative competent body. The controversial issue is the legal power that has any "administrative authorities", as according to the principle of the rule of law, only an independent judiciary body can decide what is illegal in the national or international system of law. Thus, giving a right to other entities either administrative authorities, or law enforcement officers, or even online intermediaries, to evaluate the information by the legal provisions, balance with the respect human rights can be upset. However, if the state sees non-judicial review as the only way in tackling the illegal content, then safeguards are essential.

The Commission proposes to use **IA algorithm** in automatic filtering tools in searching the illegal content, as the Study for the JURI committee proved the effectiveness of it and named it as "reasonable measures".[170] Although installation of such a mechanism can be costly for micro and small enterprises, they might be excluded from the obligation to monitor and **extensively report**. The principle of proportionality will be achieved by placing the size of direct cost on intermediaries according to their size and reach of users.[171]

Maria Lilla Montagnani encourages the idea of **algorithmic society** that exists nowadays and is going to grow in the future to maintain the balance of enforcing online and fundamental rights of users. She is sure that "the current development of autonomous systems and self-learning algorithms indicates that technology will continue to provide an **increasingly sophisticated tool of compliance**. In such a setting it becomes crucial to govern adequately the development that we are witnessing."[172] So, even if now such technology is not perfect in application, the government and intermediaries should not stop in using it, as in this way it would develop sufficiently.

---

[169] See note 164 above, 47-48.
[170] Giovanni Sartor, "The impact of algorithms for online content filtering or moderation: 'Upload filters'," Europarl, Accessed on April 15, 2021, https://www.europarl.europa.eu/RegData/etudes/STUD/2020/657101/IPOL_STU(2020)657101_EN.pdf.
[171] See note 162 above, 6-7.
[172] Maria Lilla Montagnani, "Virtues and Perils of Algorithmic Enforcement and Content Regulation in the EU - A Toolkit for a Balanced Algorithmic Copyright Enforcement," *Case Western Reserve Journal of Law, Technology and the Internet* 11, (2020): 1-49.

Hosting providers, as a separate category who keeps the information from numbers of online platforms, should enable **notice and action mechanisms** (Article 14), performed partially by automatic tools and human presence, which allows "any individual or entity to notify them of the presence on their service of specific items of information that the individual or entity considers to be illegal content"[173] and afterwards take actions according to its terms of use.

While most legal scholars see positive influence in adaptation of **ex-ante regulation** in the new act, Jorg Hoffmann and Begona Gonzalez Otero consider such applications with some notations. First of all these rules will be imposed in an open digital market, so the question of competition would arise regarding regulating this data and access to it. That is why they suggest national governments to "refrain from directly innovation-enabling **ex ante regulation** going beyond merely safeguarding the well-functioning of open competitive markets."[174] On the contrary, **Maria Lilla Montagnani** sees this shift from **ex-post** algorithmic, which was made by the automatic notice with further takedown, to **ex-ante provisions,** with the help of which the unnecessary content would be avoided and not corrected.[175] So, the upcoming autonomous filtering systems are for the help of online service providers.

This approach puts the need for the implementation of "**safeguards** of the rights and interests of consumers and businesses and the protection of fundamental rights online" as a core issue.[176] The general conception of Digital Service Act in the own words of one of its creators is to "put a lot of responsibility on the platforms. When we say you have to take illegal content down fast … you need to have this system where people can protest against things being taken down, while at the same time saying, "Do not use general upload filters." If you have an upload filter, then the risk of censorship becomes very big, and we don't want to take that risk. That's quite a strong principle in a digital world, even though it's more resource intensive [to review and remove material after it's been uploaded]."[177] **Margrethe Vestager** explains the idea by improving the system of **safeguards** for users' rights in the sphere of using automated tools for monitoring the uploaded content. She supports the concept of putting more efforts on preventing the broadening of censorship on the Internet,

[173] See note 164 above, 51-52.
[174] Jorg Hoffmann; Begona Gonzalez Otero, "Demystifying the Role of Data Interoperability in the Access and Sharing Debate," *Journal of Intellectual Property, Information Technology and Electronic Commerce Law 11*, 3 (2020): 252-273.
[175] See note 172 above.
[176] See note 165 above.
[177] See note 169 above, 13-14.

even by increasing the financial and human resources. However, it is not for sure that applying such striving would be proportionate to the set goal.

Some types of online services are obliged to establish effective **internal complaint-handling system** (Article 17), "which enables the complaints to be lodged electronically and free of charge, against the following decisions taken by the online platform on the ground that the information provided by the recipients is illegal content or incompatible with its terms and conditions". For more complicated situations, when the platform could not handle, out-of-court dispute settlement (Article 18) should be applied. These procedural safeguards were explained by the ECHR in the case Bulgakov v. Russia, for protection of the users against the abuse.

Måns Sjöstrand, the head of intellectual property and brand protection at Swedish watch brand Daniel Wellington, also highlights the need that "the EU cannot miss this opportunity to make sure that there is more **transparency** and **accountability** online to help legitimate actors flourish." He sees protection of citizens as the core goal of the EU: "It's also an essential milestone to protect European consumers in all spheres of life and create a safe and trusted digital ecosystem."[178]

The necessity of such obligations for intermediaries as regular **inspections** by competent authorities and reports with a review of applied measures was discussed by **Maria Lilla Montagnani** in her research. These additional obligations in copyright enforcement, that were not used before by EU legislation, in her opinion would be safeguards for the users "the starting point is the principle for a more balanced algorithmic copyright enforcement regime which translates into the need for open record policies and a right to explanation. This is coupled with the obligation of a rights-based impact assessment and a right to **audit**...From an operational point of view, an open-record policy and a right to explainability should correspond to an obligation to perform an **impact assessment**, which in turn would enable auditing by affected parties."[179] On the example of GDPR she shows the successful use of Data Protection Impact Assessment with positive results.

Thus one point in balancing the freedoms of users and constraints of illegal content online will be achieved by **auditing** by the governmental authorities the voluntary measures applied by service providers. Moreover, another point goes for the estimation of these

---

[178] "Together Against Counterfeiting Alliance calls for ambitious proactive measures against online counterfeiting in upcoming Digital Services Act (DSA)," TacAlliance, Accessed on April 15, 2021, https://tacalliance.eu/news/together-against-counterfeiting-alliance-calls-for-ambitious-proactive-measures-against-online-counterfeiting-in-upcoming-digital-services-act-dsa/.

[179] See note 172 above.

measures that would be given by intermediaries to states or the union, hence the government can rethink the application of specific types of measures if they cause more harm and are not efficient enough.

The obligation for all intermediaries to send different types of **reports** to the public authorities to keep transparency in application of the measures regarding: using automatic tools for content moderation (Article 13), amount of cases with out-of-court dispute settlement and its impact (Article 23), the number of orders, results of the risk assessment (Article 33), voluntary activity, etc. The statements of online services should include the reasoning for their decisions, its results and effectiveness. For the reason of being these measures transparent, both regarding the state authorities and for users, the providers should implement their own terms of use. This document would contain conditions for imposing restrictions on users' rights and freedoms in the form of removing content or denying access to it. Mentioning the fact of the usage of automatic tools, alongside with providing reasons for measures and their accuracy, is sufficient there.

The critics of these provisions come to the side of financial opportunities of online providers, "nonetheless, it is inevitable that many hosting providers and platforms will simply not be able to hire teams of lawyers to peer through Article 15 notices. In practice, it will be easier for them to remove content to avoid any liability risk."[180] Reasoning the fact of removing content is easier and less unsafe for intermediaries, than giving arguments why the content was not illegal, thus collateral effect might take place.

The separate Section 4 in Chapter 3 is dedicated to **very large online platforms,** which should count at least 45 millions users in the EU. Articles 25-33 impose additional obligations on these intermediaries with the aim to manage systemic risks that can appear to the such huge amount of subscribers. These provisions regulate the process of identification, analysis and assess of "significant systemic risks stemming from the functioning and use made of their services"[181], complementing it with the mitigation measures for decreasing risks. To keep all activities transparent and efficient the Independent audit should be provided annually at the own expenses on these platforms (Article 28). Compliance officers are appointed with the responsibilities to monitor the activity of the company, perform platform's obligations according to the Proposal and cooperate with competent EU authorities (Article

[180] "At a glance: Does the EU Digital Services Act protect freedom of expression?," Article19, Accessed on April 15, 2021, https://www.article19.org/resources/does-the-digital-services-act-protect-freedom-of-expression/.
[181] See note 164 above, 59-60.

32). All above mentioned measures from Section 4 should be established by platforms by their own expenses, which means a great cost, which is not favourable for them in any way.

Some scholars agree with the EU approach to "ensure that gatekeepers' platforms **behave fairly** and can be challenged by new entrants and existing competitors, so that consumers have the widest choice, fostering innovation and competition" by the means of "the inclusion of **asymmetrical interoperability obligations** for **dominant platforms (gatekeepers)** could help to correct market foreclosures and **information asymmetries**."[182]

The **asymmetric approach**, which is leading in the Digital Markets Act, was also used in the 10th Amendment of the German Antitrust Code regarding only the companies with the dominant role and significance in the digital market - Internet gatekeepers.[183]

The most focus in the Proposal made on the **large and very big online platforms**, as the spreading of unlawful content is more inherent to the online services with a huge amount of users as audience. For instance, sharing terroristic content or hate speech on the platform among a few hundred viewers, more than half of which would not be interested, will not bring the result for such effort. Consequently, authors of illegal material are more interested in covering online services with more users in it to convey their unlawful thoughts. Thus, large online platforms are victims of illegal material posted by third parties in most cases, so more attention is given to such companies.

On of the articles where the protection of fundamental rights takes important place is Article 26, which dedicated to the risk assessment made by very large online platforms regarding the dissemination of illegal material by means of their services and "any negative effects for the exercise of the fundamental rights to respect for private and family life, freedom of expression and information, the prohibition of discrimination and the rights of the child"[184] By this provision platforms make the estimation of possible difficulties, while Article 27 offers theoretical measures which would help in decreasing the risks. However, in practice finding measures which would correspond to reasonable, proportionate and effective actions means vast discretion on both sides: companies and authorities. The measures suggested in the article are the same as usual obligations of providers, with the only difference that they might help in mitigating those risks. Thus, by the logic of the Proposal all necessary measures mentioned before will either diminish the chances or they are just ineffective in general, so online providers should invent other more efficient practices.

---

[182] See note 174 above.
[183] Ibid.
[184] See note 181 above.

3.2.1. Responsibilities

Some reporters claim that the question of **liability** of Internet service providers stays open due to the wording of **Article 6** with not transparent enough voluntary own-initiative investigations and legal compliance. Such services "shall not be deemed ineligible for the exemptions from liability" for the investigations, initiated and conducted by them, and some other not determined actions, that were performed with the aim of "detecting, identifying and removing, or disabling of access to, illegal content". More questions come from the "necessary measures to comply with the requirements of Union law",[185] which are probably fundamental rights of the EU citizens. Thus, the main principle of transparency of all obligations and measures imposed on Internet providers was not upheld by the Commission. That is why "Article 19" calls this provision "ambiguous since it only promises that internet intermediaries will not lose immunity from liability 'solely' ... That raises the question of the circumstances in which adopting voluntary measures combined with some other, undefined, measures might lead internet intermediaries to lose immunity from liability."[186]

Same point gives **Måns Sjöstrand** saying that "the current **voluntary measures** lack transparency.. platforms claim they are doing a lot, but it's impossible to verify that."[187] So, the online intermediaries should not be **penalized** for giving an inaccurate determination of unlawfulness of the content, otherwise they would practice overblocking of the legal content or exclude the doubtful from removing.

On the other hand the news calls this Article as a "**Good Samaritan type of provision**", which has been adopted in the EU Internet law for the first time, and promotes the effort of content moderation among online platforms. "ARTICLE 19 had been advocating for this as we believe that content moderation by social media companies has benefits and is indeed desirable in many instances. We believe that companies should be encouraged to innovate in their content moderation practices, such as the use of labels and the provision of contextual information in relation to disinformation, demonetisation, disabling of certain features in certain instances etc."[188] Thereby, despite the questions that remained open, some positive influence this provision would have in the future.

---

[185] See note 164 above, 47.
[186] See note 180 above.
[187] Steven Overly, "Big brands bring counterfeit fight to Big Tech," Politico, Accessed on April 15, 2021, https://www.politico.com/news/2020/06/08/counterfeit-brands-big-tech-308364.
[188] See note 180 above.

The **financial** sanctions, stated in **Articles 42 and 59**, foreseen "for failure to comply with the regulations" go up to 6% of turnover of the company, and the fines of up to 1% of annual revenue if platforms "supply incorrect, incomplete or misleading information" to regulators, or "refuse to submit to an on-site inspection". The liability of the providers is based on the guilt, either on direct intentions or negligence, in not performing their obligations. [189]

Hence, for example, Facebook for failure to report in the right way or not providing the supervision on its platform would pay around 86 million of dollars, according to the stats of 2020.[190] Although such great fines could be imposed only on the very large online platforms, the precise amount of repayment can be estimated by the criterias of nature, gravity, duration and recurrence of the infringement.[191]

Conclusion

The need for the Regulations goes already for several years, as the harmonisation on the EU level is necessary to bring down the economical and political barriers that exist in the EU Internet market, which undermines the competition in the favour of big enterprises.

The new Digital Service Act is a step forward to a brighter future with a more safe Internet by the means of automatic tools governed by states. New approach that was used as a basis for the Digital Service Act might bring positive results in regulating online content with the help of the private sector - Internet intermediaries and platforms.

Although the cornerstones of the E-Commerce Directive were kept without changes (prohibition on general monitoring, conditional immunity from liability), it was made by the decision of the Consultation from the European Commission. Except for previous measures to block access and remove the content, new voluntary measures were involved. Through the whole act principles of transparency and accountability are maintained. The ex-ante regulation came in place of ex-post, which was insufficient enough.

Even the fact of duplication of liability clause from E-Commerce Directive does not preclude from the conclusion that the Digital Service Act, by imposing private enforcement with voluntary measures of Internet providers, proves the shift from intermediary liability to intermediary responsibility. According to Giancarlo Frosio, "policy approaches might be returning to implement moral theories of intermediary liability, rather than utilitarian or

[189] See note 164 above, 71, 80.
[190] H.Tankovska, "Facebook: annual revenue 2009-2020," Statista, Accessed on April 15, 2021, https://www.statista.com/statistics/268604/annual-revenue-of-facebook/.
[191] See note 164 above, 80.

welfare theories. In this case, justification for policy intervention would be based on responsibility for the actions of users as opposed to efficiency or balance innovation vs harm"[192]. Thus, the financial sanctions for failure to fulfill the obligations are rather high for online platforms, but the state might consider every situation individually.

The approach of implementing the asymmetric measures with more obligations for large online platforms and less to small ones was chosen as a priority by all stakeholders. According to the stats used in preparation for the Proposal and all scholars' research discussed above a broad consensus was made in favour of EU actions described in the Digital Service Act.

Definitely positive results might be achieved in the field of warranting users and protecting their fundamental rights online and establishing an effective control of Internet services. Numbers of safeguards were included to protect users' fundamental rights and freedoms in the Internet and maintain a safe online environment: internal complaint-handling system, out-of-court dispute settlement, reporting with impact assessment, inspections and auditing. Although using voluntary measures by service providers would be under governmental control, it will help in developing old and new technologies.

The idea of using IA algorithm in filtering automatic tools met the approval in the Proposal. Further development of this technology is primary, even though it lacks in perfection now, the government and intermediaries should not stop in using it, as in this way it would develop sufficiently.

However, some problems still exist, namely with defying the range of providers' responsibilities, types of voluntary measures that can be performed, collateral effect by the notice and action mechanisms. As this is only the beginning of the Digital Service Act, there is a chance of making amendments to doubtful provisions.

CONCLUSIONS

[192] See note 49 above.

Due to the fact that ISPs are gatekeepers to the world wide web, they possess power over the users' content, accordingly have access to their data, can track the information, etc. Therefore, all these opportunities should be used for good purposes in tackling illegal content and making the open space of the Internet safer. For this purpose specific regulation is necessary, which the EU has adopted twenty years ago as E-Commerce Directive 2000/31/EC. It was a first attempt and was based mostly on safe harbour regimes for online intermediaries rather than specific obligations in this sphere. Several legal acts regarding certain type of illegal material, which need more attention and protection, have been adopted (Copyright Directive, Terrorist offence Directive and Directive on combating child sexual abuse). However, the level of harmonisation of ISP responsibility among MS is not sufficient enough yet and needs more efforts. For instance, the definition of illegal content varies among countries, which sometimes causes problems for online intermediaries.

For the last two decades the EU legislation has changed in the direction of private enforcement with imposition of duty of care on online providers, but these provisions met critics from the side of legal practitioners and scholars. Lack of transparency and safeguards leads to the problem of violating fundamental rights and freedoms of online users: freedom of expression, right for private life and to conduct business, etc. Imposed censorship caused numbers of ECHR and CJEU cases on the ground of discrepancy with articles of European Convention on Human Rights. Most ISPs' measures are blocking access to the website with all its content and filtering Internet data for specific material. The courts concluded that for imposing these measures the focus should be made on "real and substantial tort test", by which they should be proportional and necessary, justifying the interest of the state/community, limited in time and ordered by appointed authorities with the possibility to appeal. In tackling copyright infringements case law allows general website blocking order, dynamic injunctions, disclosing of personal data of ISP's subscriber, and filtering/monitoring mechanism, under the conditions of safeguards and keep balance with fundamental rights.

The EU Internet policy is still developing, hence two main proposals on regulations were made recently: Terrorist Content Online and Digital Service Act. The first one, contains strict obligations for online service providers regarding deleting and blocking the access to terrorist content, filtering systems and financial liability for non compliance with it. Although practitioners are against some main provisions of the proposal, apparently the Regulation will come into force this year, as the severity of measures is justified by the threat of terroristic harm. Another proposal has general nature regarding the responsibility of all types of online providers with core principles of transparency and accountability. The proposal is a

consensus from stakeholders in applying the approach of asymmetric measures with more obligations for large online platforms and ex-ante regulation. Thereby, a step to the future of technologies was made.

RECOMMENDATIONS

On the basis of this research the EU legislator can be recommended to take the following steps:

1. To transfer to the ex-ante regulation of ISP responsibility with prevalence of the private sector in tackling the illegal content;
2. To apply safeguards to blocking measures such as the transparent procedure defined by the law, removal orders can be issued only by judicial authority, no collateral effect to legal content, possibility to appeal on removal order with following recovery of the content, keep the balance of all interests at stake;
3. To use IA algorithm in automatic filtering tools in searching the illegal content for further development of high technologies;
4. To clarify the boundaries of voluntary measures provided in Article 6 of a Proposal for a Regulation on a Single Market For Digital Services by naming specific actions.

LIST OF BIBLIOGRAPHY

1. "About." Euroispa. Accessed on April 12, 2021. https://www.euroispa.org/about/.

2. “Ahmet Yildirim v. Turkey. Case 3111/10.” Hudoc. Accessed on April 18, 2021. http://hudoc.echr.coe.int/eng-press?i=001-115705.
3. “Amended proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the Internal Market.” Eur-lex. Accessed on April 11, 2021. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A51999PC0427.
4. Hoffmann, Anja and Alessandro Gasparotti. “Liability for illegal content online. Weaknesses of the EU legal framework and possible plans of the EU Commission to address them in a “Digital Services Act”.” Cepstudy. Accessed on November 15, 2020. https://www.cep.eu/fileadmin/user_upload/cep.eu/Studien/cepStudie_Haftung_fuer_illegale_Online-Inhalte/cepStudy_Liability_for_illegal_content_online.pdf.
5. “AOL.” Britannica. Accessed on March 10, 2021. https://www.britannica.com/topic/AOL.
6. “At a glance: Does the EU Digital Services Act protect freedom of expression?.” Article19. Accessed on April 15, 2021. https://www.article19.org/resources/does-the-digital-services-act-protect-freedom-of-expression/.
7. “BULGAKOV v. RUSSIA. Case 20159/15.” Hudoc. Accessed on April 20, 2021. http://hudoc.echr.coe.int/fre?i=001-203181.
8. “Cartier International AG and others v British Telecommunications Plc and another. Case [2018] UKSC 28.” Supremecourt. Accessed on April 20, 2021. https://www.supremecourt.uk/cases/docs/uksc-2016-0159-judgment.pdf.
9. “Cengiz and Others v. Turkey. Case 48226/10 and 14027/11” Hudoc. Accessed on April 18, 2021. http://hudoc.echr.coe.int/eng-press?i=003-5241080-6502267.
10. Geiger, Christophe and Elena Izyumenko. “The Role Of Human Rights In Copyright Enforcement Online: Elaborating A Legal Framework For Website Blocking.” American University International Law Review 32. 1 (2016): 43-115. Accessed on April 18, 2021. https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1939&context=auilr.
11. “Code of Conduct–Illegal online hate speech. Questions and answers.” Europa. Accessed on April 14, 2021. https://ec.europa.eu/info/sites/info/files/code_of_conduct_hate_speech_en.pdf.

12. “Commission Recommendation of 1.3.2018 on measures to effectively tackle illegal content online.” Didigat-strategy. Accessed on November 5, 2020. https://digital-strategy.ec.europa.eu/en/library/commission-recommendation-measures-effectively-tackle-illegal-content-online.
13. “Communication Illegal and harmful content on the Internet.” Commission of the European Communities. Accessed on November 2, 2020. http://aei.pitt.edu/5895/1/5895.pdf.
14. “Communication Online Platforms and the Digital Single Market Opportunities and Challenges for Europe.” Eur-lex. Accessed on April 13, 2021. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0288.
15. “Comparative Study on Blocking. Filtering and Take-down of Illegal Internet Content.” Council of Europe. Accessed on April 18, 2021. www.coe.int/freedomofexpression.
16. “Content filter.” Britannica. Accessed on April 12, 2021. https://www.britannica.com/technology/content-filter.
17. “CVBA (SABAM) v Netlog NV. Case C-360/10.” Curia. Accessed on April 20, 2021. https://curia.europa.eu/juris/document/document.jsf?text=&docid=119512&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=4146183.
18. Meyer, David. “The Conversation Margrethe Vestager.” Fortune 183. 2 (2021): 12.
19. “DIRECTIVE 98/34/EC of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services.” EUR-lex. Accessed on March 12, 2021. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1998L0034:20070101:EN:PDF.
20. “DIRECTIVE 2000/31/EC of 8 June 2000 on certain legal aspects of information society services. in particular electronic commerce. in the Internal Market” EUR-lex. Accessed on November 12, 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=FR.
21. “Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society.” Eur-lex. Accessed on April 15, 2021. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32001L0029&from=EN.

22. “Directive 2004/48/EC on the enforcement of intellectual property rights.” Eur-lex. Accessed on April 15, 2021. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02004L0048-20040430&from=EN.
23. “DIRECTIVE 2011/92/EU on combating the sexual abuse and sexual exploitation of children and child pornography.” Eur-lex. 7. Accessed on April 14, 2021. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011L0093&from=EN.
24. “Directive (EU) 2017/541 on combating terrorism.” Eur-lex. Accessed on April 13, 2021.https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017L0541.
25. “Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market.” Eur-lex. Accessed on April 13, 2021. https://eur-lex.europa.eu/eli/dir/2019/790/oj.
26. Bechtold, Eliza. “Terrorism. the internet. and the threat to freedom of expression: the regulation of digital intermediaries in Europe and the United States.” Journal of Media Law 12.1 (2020): 13-46. Accessed on April 14, 2021. https://www-tandfonline-com.skaitykla.mruni.eu/doi/full/10.1080/17577632.2020.1760474.
27. Parris, Emily and Nick Rose. “European Court of Justice rules on ISP injunction.” Fieldfisher. Accessed on April 22, 2021. https://www.fieldfisher.com/en/insights/european-court-of-justice-rules-on-isp-injunction.
28. Parris, Emily. “Injunction against social networking site is too wide. rules European Court.” Fieldfisher. Accessed on April 22, 2021. https://www.fieldfisher.com/en/insights/injunction-against-social-networking-site-is-too-wide-rules-european-court.
29. Llansó, Emma and Laura Blanco. “EC Recommendation on Tackling Illegal Content Online Doubles Down on Push for Privatized Law Enforcement.” Center for Democracy & Technology. Accessed on April 12, 2021. https://cdt.org/insights/ec-recommendation-on-tackling-illegal-content-online-doubles-down-on-push-for-privatized-law-enforcement/.
30. “ENGELS v. RUSSIA. Case 61919/16.” Hudoc. Accessed on April 20, 2021. http://hudoc.echr.coe.int/fre?i=001-203180.

31. Coche, Eugénie. “Privatised enforcement and the right to freedom of expression in a world confronted with terrorism propaganda online.” Internet Policy Review 7. 4 (2018). Accessed on April 12, 2021. https://policyreview.info/articles/analysis/privatised-enforcement-and-right-freedom-expression-world-confronted-terrorism.
32. “EU: German Presidency Proposal for Terrorist Content Online Regulation fails to protect freedom of speech.” Article19. Accessed on April 13, 2021. https://www.article19.org/resources/eu-german-presidency-proposal-terrorist-content-online-fails-freedom-of-speech/#:~:text=Overbroad%20definition%20of%20terrorist%20content.for%20recruitment%20and%20radicalisation%20purposes%E2%80%9D.
33. “EU Human Rights Guidelines on Freedom of Expression Online and Offline.” Europa. Accessed on April 14, 2021. https://eeas.europa.eu//sites/default/files/eu_human_rights_guidelines_on_freedom_of_expression_online_and_offline_en.pdf.
34. “Executive Summary of the Impact Assessment Report.” Europa. Accessed on April 15, 2021. https://ec.europa.eu/competition/sectors/ICT/DMA_summary_of_impact_assessment.pdf.
35. “Facebook's monthly active users (MAU) in Europe from 4th quarter 2012 to 4th quarter 2020.” Statista. Accessed on April 12, 2021 https://www.statista.com/statistics/745400/facebook-europe-mau-by-quarter/.
36. Ferri, Federico. “The dark side(s) of the EU Directive on copyright and related rights in the Digital Single Market.” China-EU Law J. (2020). Accessed on April 15, 2021. https://link.springer.com/article/10.1007/s12689-020-00089-5#citeas.
37. “Framework Decision on combating certain forms and expressions of racism and xenophobia by means of criminal law.” Eur-lex. Accessed on April 11, 2021. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l33178.
38. “Frequently asked questions on internet intermediary liability.” APC. Accessed on April 14, 2021. https://www.apc.org/en/pubs/apc%E2%80%99s-frequently-asked-questions-internet-interme.
39. Frosio, Giancarlo. “Why Keep a Dog and Bark Yourself? From Intermediary Liability to Responsibility.” International journal of law and information technology 26. 1 (2018): 1-33.

40. Sartor, Giovanni. “The impact of algorithms for online content filtering or moderation: ‘Upload filters’.” Europarl. Accessed on April 15, 2021. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/657101/IPOL_STU(2020)657101_EN.pdf.
41. “Guidelines for the cooperation between law enforcement and internet service providers against cybercrime.” Conference Cooperation against Cybercrime. Accessed on April 13, 2021. https://rm.coe.int/16802fa3ba.
42. “Guide on Article 8 of the European Convention on Human Rights.” Council of Europe. Accessed on April 22, 2021. https://www.echr.coe.int/documents/guide_art_8_eng.pdf.
43. “Gündüz V. Turkey. Case 35071/97.” ECHR. Accessed on April 13, 2021. https://www.legal-tools.org/doc/74a144/pdf/.
44. “Hasan and Chaush v. Bulgaria. Case 30985/96.” Hudoc. Accessed on April 10, 2021. http://hudoc.echr.coe.int/eng?i=001-58921.
45. “Hate speech.” ECHR. Accessed on April 13, 2021. https://www.echr.coe.int/documents/fs_hate_speech_eng.pdf.
46. Tankovska, H. “Facebook: annual revenue 2009-2020.” Statista. Accessed on April 15, 2021. https://www.statista.com/statistics/268604/annual-revenue-of-facebook/.
47. “Human rights guidelines for Internet service providers.” EuroIspa. Accessed on April 18, 2021. https://rm.coe.int/16805a39d5.
48. “Information Note on the Court’s case-law No. 102. Muscio v. Italy - 31358/03.” ECHR.
49. “International Comparison of Approaches to Online Copyright Infringement: Final Report.” Intellectual Property Office. (2015): 78. Accessed on April 14, 2021. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/549462/International_Comparison_of_Approaches_to_Online_Copyright_Infringement.pdf.
50. “Internet: Case-law of the European Court of Human Rights.” Refworld. Accessed on April 20, 2021. https://www.refworld.org/pdfid/4ee1d5bf1a.pdf.
51. “Internet Organised Crime Threat Assessment (IOCTA).” EUROPOL. Accessed on April 19, 2021. https://www.europol.europa.eu/iocta-report.
52. “Internet service provider.” Britannica. Accessed on March 10, 2021. https://www.britannica.com/technology/Internet-service-provider.

53. “IPR Enforcement Case-law Collection: The Liability and Obligations of Intermediary Service Providers in the European Union.” Euipo. Accessed on April 20, 2021. https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_IPR_Enforcement_Case_Law_Collection/2019_IPR_Enforcement_Case_Law_Collection_en.pdf.
54. Balkin, Jack M. “Old-school/New-school Speech Regulation.” Harvard Law Review 127. 8 (2014): 2296-2342. Accessed on November 15, 2020. https://www-jstor-org.skaitykla.mruni.eu/stable/pdf/23742038.pdf?refreqid=excelsior%3Aff1191b525764a16e11255758f70416c.
55. Quintais, João Pedro. “Global Online Piracy Study: Legal Background Report.” Ivir. Accessed on April 22, 2021. http://docplayer.net/87609818-Global-online-piracy-study-legal-background-report.html.
56. Hoffmann, Jorg and Begona Gonzalez Otero. "Demystifying the Role of Data Interoperability in the Access and Sharing Debate." Journal of Intellectual Property. Information Technology and Electronic Commerce Law 11. 3 (2020): 252-273.
57. “Just looking? ISPs are watching you browse.” Expressvpn. Accessed on April 10, 2021. https://www.expressvpn.com/blog/how-much-does-your-isp-know/.
58. Perset, Karine. “The Economic and social role of internet intermediaries.” OECD. Accessed on April 12, 2021. http://www.oecd.org/digital/ieconomy/44949023.pdf.
59. Luyten, Katrien. “Addressing the dissemination of terrorist content online.” EuroParl. Accessed on April 12, 2021. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/649326/EPRS_BRI(2020)649326_EN.pdf.
60. “K.U. v. FINLAND. Case 2872/02.” Hudoc. Accessed on April 20, 2021. http://hudoc.echr.coe.int/fre?i=001-89964.
61. “Liability of online intermediaries.” EU study on the Legal analysis of a Single Market for the Information Society. Accessed on April 15, 2021. https://op.europa.eu/en/publication-detail/-/publication/a856513e-ddd9-45e2-b3f1-6c9a0ea6c722.
62. “L’Oréal SA v eBay International AG. Case C-324/09.” Curia. Accessed on April 15, 2021.

https://curia.europa.eu/juris/document/document.jsf?text=&docid=107261&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=2371598.

63. Montagnani, Maria Lilla. "Virtues and Perils of Algorithmic Enforcement and Content Regulation in the EU - A Toolkit for a Balanced Algorithmic Copyright Enforcement." Case Western Reserve Journal of Law. Technology and the Internet 11. (2020): 1-49.
64. Jackson, Mark. "Get it Right – Copyright Holders Scrap UK ISP Piracy Letters Scheme." ISPreview. Accessed on April 12, 2021. https://www.ispreview.co.uk/index.php/2019/07/get-it-right-copyright-holders-scrap-uk-isp-piracy-letters-scheme.html.
65. Husovec, Martin. "Accountable. Not Liable: Injunctions Against Intermediaries." TILEC Discussion Paper 012. (2016). Accessed on April 22, 2021. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2773768.
66. Sag, Matthew. "Internet Safe Harbors and the Transformation of Copyright Law." Notre Dame Law Review 93. (2017): 66. Accessed on November 15, 2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2830184.
67. K. Land, Molly. "Against Privatized Censorship: Proposals for Responsible Delegation." Virginia Journal of International Law 60. 2 (2020): 363-432.
68. Klompmaker, Naomi. "Censor Them at Any Cost: A Social and Legal Assessment of Enhanced Action against Terrorist Content Online." Amsterdam Law Forum 11. 3 (2019): 3.
69. Anderson, Nate. "Just two Chinese ISPs serve 20% of world broadband users." Arstechnica. Accessed on April 12, 2021. https://arstechnica.com/tech-policy/2010/07/just-two-chinese-isps-serve-20-of-world-broadband-users/#:~:text=China%20Telecom%20is%20the%20largest.significantly%20in%20more%20developed%20markets.
70. Cory, Nigel. "Adaptive Antipiracy Tools: An Update on Dynamic and Live Blocking Injunctions." ITIF. Accessed on April 21, 2021. https://itif.org/publications/2020/10/22/adaptive-antipiracy-tools-update-dynamic-and-live-blocking-injunctions.
71. Kyryliuk, Olga. "Should Ukraine Drop Sanctions against Russian Tech Companies?." Freedomhouse. Accessed on April 17, 2021. https://freedomhouse.org/report/policy-brief/2019/should-ukraine-drop-sanctions-against-russian-tech-companies.

72. “Online Copyright Infringement in the European Union. Music. Films and TV (2017-2018). Trends and Drivers.” Europa. Accessed on April 14, 2021. https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/quantification-of-ipr-infringement/online-copyright-infringement-in-eu/online_copyright_infringement_in_eu_en.pdf.
73. “OOO FLAVUS AND OTHERS v. RUSSIA. Case 12468/15.” Hudoc. Accessed on April 20, 2021. http://hudoc.echr.coe.int/fre?i=001-203178.
74. “Opinion of Mr Advocate General Cruz Villalón. Case C-314/12.” Eur-lex. Accessed on April 20, 2021. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62012CC0314.
75. “Payam Tamiz against the United Kingdom. Case 3877/14.” Hudoc. Accessed on April 20, 2021. http://hudoc.echr.coe.int/eng?i=001-178106.
76. “PERRIN v. THE UNITED KINGDOM. Case 5446/03.” Stradalex. Accessed on April 20, 2021. https://www.stradalex.com/en/sl_src_publ_jur_int/document/echr_5446-03.
77. “Petition No 0777/2018 on the need for measures against bullying. threats or slander of users of digital portals and platforms on 16.9.2019.” Europarl. Accessed on November 2, 2020. https://www.europarl.europa.eu/doceo/document/PETI-OJ-2019-11-11-1_EN.html.
78. “Presidency Proposal TCO.” Europal. Accessed on April 15, 2021. https://cdn.netzpolitik.org/wp-upload/2020/10/DE-Vorschlag-zu-Terror-Inhalte-Verordnung.pdf.
79. “Productores de Música de España (Promusicae) v Telefónica de España SAU. Case C-275/06.” Curia. Accessed on April 22, 2021. https://curia.europa.eu/juris/document/document.jsf?text=&docid=70107&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=6970545.
80. “Proposal for a REGULATION on a Single Market For Digital Services (Digital Services Act).” Eur-lex. Accessed on April 15, 2021. https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608117147218&uri=COM%3A2020%3A825%3AFIN.
81. “Proposal for a REGULATION on preventing the dissemination of terrorist content online.” Eur-lex. Accessed on April 23, 2021. https://eur-lex.europa.eu/resource.html?uri=cellar:dc0b5b0f-b65f-11e8-99ee-01aa75ed71a1.0001.02/DOC_1&format=PDF.

82. Bendrath, Ralf and Milton Mueller. “The end of the net as we know it? Deep packet inspection and internet governance.” New Media & Society 13. 7 (2011): 1142–1160.
83. Cohen-Almagor, Raphael. “Balancing Freedom of Expression and Social Responsibility on the Internet.” Philosophia 45. (2017): 973–985. Accessed on April 19, 2021. https://link.springer.com/article/10.1007/s11406-017-9856-6#Fn13.
84. “Recommendation CM/Rec(2008)6 on measures to promote the respect for freedom of expression and information with regard to Internet filters.” Council of Europe. Accessed on April 18, 2021. https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805d3bc4.
85. “Regulation (EU) 2015/2120 laying down measures concerning open internet access.” Eur-lex. Accessed on April 18, 2021. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015R2120.
86. “REPORT assessing the implementation of the measures referred to in Article 25 of Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography.” Eur-lex. Accessed on April 13, 2021. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016DC0872&from=EN.
87. “Report. Illegal content online.” Flash Eurobarometer 469. (2018). Accessed on April 13, 2021. https://digital-strategy.ec.europa.eu/en/library/flash-eurobarometer-illegal-content.
88. “Report of the Consultation on Child Abuse Prevention.” World Health Organization. (1999). Accessed on April 14, 2021. https://apps.who.int/iris/handle/10665/65900.
89. “Research Report Child sexual abuse and child pornography in the Court’s case-law.” ECHR. Accessed on April 14, 2021. https://www.echr.coe.int/Documents/Research_report_child_abuse_ENG.pdf.
90. “Scarlet Extended SA v SCRL (SABAM). Case C-70/10.” Eur-lex. Accessed on April 22, 2021. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62010CJ0070.
91. “Security Union: Commission welcomes political agreement on removing terrorist content online.” Eur-lex. Accessed on April 20, 2021. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2372.
92. Dusollier, Severine. “Editorial.” JIPITEC 10. (2020): 275-276.

93. Overly, Steven. “Big brands bring counterfeit fight to Big Tech.” Politico. Accessed on April 15, 2021. https://www.politico.com/news/2020/06/08/counterfeit-brands-big-tech-308364.
94. “Summary report of the public consultation on measures to further improve the effectiveness of the fight against illegal content online.” Europa. Accessed on April 23, 2021. https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-measures-further-improve-effectiveness-fight-against-illegal.
95. “Szabó and Vissy v. Hungary. Case 37138/14.” Statewatch. Accessed on April 20, 2021. https://www.statewatch.org/media/documents/news/2016/jan/echr-case-SZAB-%20AND-VISSY-v-%20HUNGARY.pdf.
96. “Tackling Illegal Content Online Towards an enhanced responsibility of online platforms.” European Commission. Accessed on April 11, 2021. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC055&from=EN.
97. Madiega, Tambiama. “Reform of the EU liability regime for online intermediaries. Background on the forthcoming digital services act.” Europarl. Accessed on April 14, 2021. https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/649404/EPRS_IDA(2020)649404_EN.pdf.
98. “The EU Code of conduct on countering illegal hate speech online.” Europa. Accessed on April 14, 2021. https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en.
99. “The European Union Terrorism Situation and Trend Report 2019.” EUROPOL. Accessed on April 20, 2021. https://www.europol.europa.eu/activities-services/main-reports/terrorismsituation-and-trend-report-2019-te-sat.
100. “The Football Association Premier League Limited v. British Telecommunications Plc. Case HC-2017-000458.” Vlex. Accessed on April 22, 2021. https://vlex.co.uk/vid/the-football-association-premier-793317289.

101. “The right to freedom of speech and opinion in Ukraine: threats and opportunities.” Osce. Accessed on April 17, 2021. https://www.osce.org/files/f/documents/d/f/393431_0.pdf.

102. “The Strasbourg Court Establishes Standards on Blocking Access to Websites.” Strasbourgobservers. Accessed on April 19, 2021. https://strasbourgobservers.com/2020/08/26/the-strasbourg-court-establishes-standards-on-blocking-access-to-websites/.

103. “Together Against Counterfeiting Alliance calls for ambitious proactive measures against online counterfeiting in upcoming Digital Services Act (DSA).” TacAlliance. Accessed on April 15, 2021. https://tacalliance.eu/news/together-against-counterfeiting-alliance-calls-for-ambitious-proactive-measures-against-online-counterfeiting-in-upcoming-digital-services-act-dsa/.

104. “Tommy Hilfiger Licensing LLC v Delta Center a.s..Case C-494/15.” Curia. Accessed on April 15, 2021. https://curia.europa.eu/juris/document/document.jsf?text=&docid=181465&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=4918082.

105. “UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH. Wega Filmproduktionsgesellschaft mbH. Case C-314/12.” Curia. Accessed on April 20, 2021. https://curia.europa.eu/juris/document/document.jsf?text=&docid=149924&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=4146537.

106. “VLADIMIR KHARITONOV v. RUSSIA. Case 10795/14.” Hudoc. Accessed on April 20, 2021. http://hudoc.echr.coe.int/fre?i=001-203177.

107. Benedek, Wolfgang and Matthias C. Kettemann. “Freedom Of Expression And The Internet.” Council of Europe Publishing. Accessed on November 18, 2020. https://rm.coe.int/prems-167417-gbr-1201-freedom-of-expression-on-internet-web-16x24/1680984ea.

108. “Your YouTube history exposed: Researcher identifies inherent security flaw in video streaming.” Expressvpn. Accessed on April 13, 2021. https://www.expressvpn.com/blog/security-flaw-youtube-video-streaming/.

109. А.Б., Блага, and Мартиненко. “Свобода Слова в Умовах Інформаційної Війни та Збройного Конфлікту.” Українська Гельсінська спілка з прав людини. (2017). Accessed on April 17, 2021.

https://helsinki.org.ua/wp-content/uploads/2018/01/Web_Svoboda_Slova_A5_Ukr3.pdf.

110. “Закон України Про Телекомунікації.” Zakon. Accessed on April 17, 2021. https://zakon.rada.gov.ua/laws/show/1280-15#Text.

111. “Про Центр.” Myrotvorets. Accessed on April 17, 2021. https://myrotvorets.center/about/.

112. Студенников, Сергей. “Блокування сайтів: судова практика розділилася.” Sud. Accessed on April 17, 2021. https://sud.ua/ru/news/publication/156424-blokuvannya-saytiv-sudova-praktika-rozdililasya.

113. “Указ Президента України №126/2018.” President. Accessed on April 17, 2021. https://www.president.gov.ua/documents/1262018-24150;

114. “Указ Президента України №133/2017.” President. Accessed on April 17, 2021. https://www.president.gov.ua/documents/1332017-21850.

115. “Указ Президента України №184/2020.” President. Accessed on April 17, 2021.https://www.president.gov.ua/documents/1842020-33629;

116. “Указ Президента України №82/2019.” President. Accessed on April, 17 2021. https://www.president.gov.ua/documents/822019-26290.

ABSTRACT

This research represents the analysis of the transition of Internet service providers' responsibilities in the sphere of online illegal material in the EU, by studying the balancing of fundamental rights of users in obligations to block and filter the content, by examining possible voluntary measures applied by ISPs and evaluating the upcoming regulations in this field of EU law.

Furthermore, the drawbacks of current EU legislation regarding Internet censorship established by online providers were found and recommendations in eliminating this issue were stated.

Keywords: the European Union, responsibilities of ISP, freedom of expression online, automatic filtering tools, Digital Service Act.

SUMMARY

OBLIGATIONS AND RESPONSIBILITIES OF THE INTERNET SERVICE PROVIDERS REGARDING ILLEGAL CONTENT

In the last decades the importance of the Internet has increased along with the amount of content both legal and not. The EU community has begun the fight with dissemination of illegal content online more than twenty years ago and still makes efforts in this direction.

The core goal of this research is to determine the boundaries of ISPs responsibilities in tackling illegal material on their platforms by means of specific obligations, which would not interfere with fundamental rights and freedoms of subscribers.

For this purpose, the first step is the review of the current EU legislation on the issues of determining the categories of illegal content, clarifying the status of ISP, exploring safe harbour regime for online providers and analysing the necessary actions, which should be taken by them in dealing with unlawful content.

Furthermore, the existing approaches among the EU MS and scholars to the voluntary measures of online providers are discussed and the evaluation of each of them is given, including the comparison of ex post and ex ante types of regulation regarding implementation of automatic tools and safeguards.

The research explains necessary legal boundaries of ISP obligations, which are based on the ECHR and CJEU case study concerning Internet censorship by means of online intermediaries.

Comparative analysis of two proposals for regulations (Digital Service Act and Terrorist content online) is provided with the aim to find efficient measures for future development of the opposition to the unlawful content and to discuss the appropriateness of these provisions.

In the result, the conclusion about required changes to the current EU legislation is made, which covers upcoming legal acts, with the recommendations to modify several provisions in favour for high technologies and the transparency of wording.