ILLEGAL CONTENT CLASSIFICATION IN LIGHT OF THE SLOVAK CASE-LAW[1]

KLASIFIKÁCIA NEZÁKONNÉHO OBSAHU V KONTEXTE SLOVENSKEJ ROZHODOVACEJ PRAXE

Laura Bachňáková Rózenfeldová[2]

https://doi.org/10.33542/SIC2025-S-01

ABSTRACT

Classification of illegal content presents a multifaceted issue requiring complex examination of the applicable regulation adopted on the national, European and international level that defines content categories that are considered unlawful and therefore subject to prosecution by competent state authorities. Following such examination, the practical implementation of the relevant legislation represented in the decision-making practice of state authorities must also be analysed with the objective to identify specific content types sanctioned within the national context. Proposal of such classification forms the subject-matter of this paper, the objective of which is to identify the individual categories of illegal content focusing on the existing case-law of Slovak national authorities.

ABSTRAKT

Klasifikácia nezákonného obsahu predstavuje viacvrstevnú problematiku, ktorá si vyžaduje komplexné preskúmanie platnej regulácie prijatej na národnej, európskej a medzinárodnej úrovni, ktorá vymedzuje druhy obsahu, ktoré sú považované za nezákonné, a teda sankcionovateľné zo strany príslušných štátnych orgánov. Na predmetné preskúmanie nevyhnutne nadväzuje analýza praktickej implementácie príslušnej právnej úpravy vyjadrenej v rozhodovacej praxi štátnych orgánov s cieľom identifikovať, ktoré druhy protiprávneho obsahu sú skutočne postihované na národnej úrovni. Predmetom tohto príspevku je návrh takejto klasifikácie s cieľom identifikovať jednotlivé kategórie nezákonného obsahu na základe analýzy existujúcej rozhodovacej činnosti vnútroštátnych orgánov.

I. INTRODUCTION

Regulation of the digital environment presents a difficult exercise both for the legislator tasked with the formulation of the necessary regulatory framework as well as for the competent authorities ensuring the implementation of the applicable legislation in practice.[3] This is especially true as regards the regulation of illegal activities committed on the Internet, as their ever-expanding variety makes the application of the existing regulation especially difficult.[4] The contributing reason for this is the fact that the majority of the relevant legal acts were

[1] This work was supported by the Slovak Research and Development Agency under contract No. VV-MVP-24-0038 ‚*Analysis of liability for Internet torts with machine learning methods*‘and contract No. APVV-21-0336 ‚*Analysis of judicial decisions using Artificial Intelligence*‘.

[2] JUDr., PhD., Pavol Jozef Šafárik University in Košice, Faculty of Law, Slovak Republic
Univerzita Pavla Jozefa Šafárika v Košiciach, Právnická fakulta, Slovenská republika.

[3] See SAVIN, A. Internet regulation in the European Union. In: EU Internet Law. Cheltenham, UK: Edward Elgar Publishing, 2017. https://doi.org/10.4337/9781784717971.00007.

[4] WALL, D. S. Cybercrime. The Transformation of Crime in the Information Age. Cambridge, U.K.: Polity Press, 2007. ISBN: 9780745627366. https://doi.org/10.1111/j.1468-4446.2007.00187_8.x.

originally formulated with primary focus on unlawful acts committed in the offline world, not considering the specific nature of illegal acts carried out online.[5] In many instances, the existing legislation does not adequately respond to the challenges brought by online offenders, establishing the need for its amendment or broader interpretation by competent national authorities.[6] Moreover, the continuing adoption of legislation responding to partial issues concerning illegal acts online makes it difficult to provide a comprehensive examination of this legal area, including the identification of individual categories of illegal content. Any proposal of illegal content classification must therefore be based on a thorough examination of the applicable national, European and international regulation and its corresponding application in practice by the national authorities.[7] Moreover, the illegal content categories identified in this regard may be sanctioned through the instruments of civil, administrative as well as criminal law. Therefore, the relevant case law adopted by the competent state institutions and national courts must also be examined. The decisions of national authorities that form the basis of conclusions presented in this paper include decisions obtained on the basis of a freedom of information request in accordance with Article 14 of the Act No. 211/2000 Coll. on free access to information (Freedom of Information Act) as amended (e. g. decisions of the Personal Data Protection Office of the Slovak republic), as well as judicial decisions issued by competent courts accessed from the database of decisions created as one of the outputs of the project No. APVV-21/0336, on the solution of which the author participates.[8]

The objective of this paper is, however, not the identification of all categories of illegal content carried out online that may be sanctioned under the applicable regulation, but the proposal of a classification of content categories that cover types of illegal content most prosecuted within the national context. To achieve this, we also examine the crime statistics regularly published by the Ministry of Interior of the Slovak republic, the Ministry of Justice of the Slovak republic and General Prosecutor's Office of the Slovak republic.

The main research question stipulated in this regard is as follows: "*What categories of illegal content can be distinguished within the national context, specifically based on the examination of the applicable regulation followed by the analysis of the corresponding case-law of competent national authorities?*" The formulated research question may be divided into the following research sub-questions:
(RQ1): "*What is the legal definition of the term 'illegal content'?*"
(RQ2): "*What different categories of illegal content can be distinguished and what is the manner of their prosecution within the national context?*"

This paper is organized into three sections. Section I examines the legal definition of the term 'illegal content'. Section II analyses the individual categories of illegal content and their corresponding regulation and representation in the case-law of national authorities. Section III contains discussion and conclusion.

---

5 See also YAR, M. (2018) A Failure to Regulate? The Demands and Dilemmas of Tackling Illegal Content and Behaviour on Social Media. International Journal of Cybersecurity Intelligence & Cybercrime: 1(1), 5-20. https://www.doi.org/10.52306/01010318RVZE9940.

6 See also FICO, M. Základy trestnej zodpovednosti v procese unifikácie trestného práva medzivojnovej Československej republiky. Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, 2020. ISBN 9788081528408.

7 See also ROMŽA, S. Privatizácia trestného práva. Praha: Nakladatelství Leges, 2021. ISBN 9788075025289.

8 This database includes more than 4 million decisions published by the Ministry of Justice of the Slovak republic. The decisions analysed for the purposes of this paper were selected through the methods for decision selection created and implemented by the research team and use different machine learning methods allowing, e. g. the selection based on the presence of a reference to a specific provision of the legal regulation in the relevant decision.

II. DEFINITION OF ILLEGAL CONTENT

The first legal definition of the term 'illegal content' was provided within the context of the European Union regulation by the Commission in its Communication titled 'Tackling Illegal Content Online. Towards an enhanced responsibility of online platforms', according to which illegal content may be defined in the following manner: „*what is illegal offline is also illegal online.*"[9] This general definition was later specified in Article 4 (b) of the Commission Recommendation (EU) 2018/334 on measures to effectively tackle illegal content online, according to which illegal content "*means any information which is not in compliance with Union law or the law of a Member State concerned*".[10] This interpretation considered the existence of possible differences in the definition of illegal content as specified in the national law of individual Member States. Concurrently it confirmed the fact that if information violates the European Union regulation, it will be considered illegal, regardless of the differences in the provisions of Member States' national legal systems.

On this basis, the recently enacted Regulation (EU) 2022/2065 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)[11] provided a new definition of illegal content in its Article 3 (h), under which this term covers "*any information that, in itself or in relation to an activity, including the sale of products or the provision of services, is not in compliance with Union law or the law of any Member State which is in compliance with Union law, irrespective of the precise subject matter or nature of that law.*" In determining whether content is illegal, it is not decisive whether the illegality of the information or activity results from the European Union law or from the legal order of a Member State. The form in which the illegal information is contained is also not relevant, nor is the precise nature or subject matter of the legal provision from which the illegality of the information results. The Digital Services Act "*does not distinguish between different types of infringement with respect to any of the obligations. This means that criminal offences, intellectual property rights violations and infringements of personal rights all face uniform compliance rules.*"[12] Concurrently the regulation does not specify individual categories of illegal content covered by it. Recital 12 of the Digital Services Act only lists illustrative examples of content types that are considered illegal, which include illegal hate speech or terrorist content, unlawful discriminatory content, the sharing of images depicting child sexual abuse, the unlawful non-consensual sharing of private images, online stalking, the sale of non-compliant or counterfeit products, the sale of products or the provision of services in infringement of consumer protection law, the non-authorised use of copyright protected material, the illegal offer of accommodation services or the illegal sale of live animals.

Within the national context, we can find the definition of the term illegal content in the Act No. 264/2022 Coll. on media services as amended. Article 151 (2) of this Act defines illegal content as content that:

a) "*fulfills the characteristics of child pornography or extremist material,*
b) *incites to conduct that fulfills the characteristics of any of the crimes of terrorism,*
c) *approves conduct that fulfills the characteristics of any of the crimes of terrorism, or*

[9] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Tackling illegal content online. Towards an enhanced responsibility of online platforms. *COM (2017) 555 final. P. 2.*

[10] Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online. *OJ L 63, 6.3.2018, p. 50–61.*

[11] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act). *OJ L 277, 27.10.2022, p. 1-102.*

[12] BUITEN, M., C. The Digital Services Act from Intermediary Liability to Platform Regulation. In: JIPITEC 12 (5) 2021. S. 366. https://dx.doi.org/10.2139/ssrn.3876328.

d) fulfills the characteristics of the crime of denial and approval of the Holocaust, crimes of political regimes and crimes against humanity, the crime of defamation of a nation, race and belief or the crime of incitement to national, racial and ethnic hatred."

Nevertheless, this definition does not cover all content types that may be considered unlawful under the provisions of the national law. Different categories of illegal content can be identified in this regard, following the provisions of applicable legislation and the relevant case-law of competent authorities. These categories are examined in the following chapter of this paper.

III. CLASSIFICATION OF ILLEGAL CONTENT

This chapter provides a classification of illegal content categories based on the examination of the applicable regulation, reflecting the existing case-law of national authorities. Individual categories of illegal content can be differentiated on the basis of their seriousness and the related extent of the harm that may arise as a result of the dissemination of a certain category of illegal content on the Internet. While, for example, harm caused by the infringement of intellectual property rights, such as the unlawful making available of audiovisual or musical works on the Internet, is primarily of the nature of quantifiable material damage localized in relation to the relevant right holders, harm that may arise as a result of a failure to prevent the dissemination of terrorist propaganda may result in harm to life and health of persons affected by the commission of a terrorist attack, including significant property damage.

A. Terrorist content

Terrorist content presents a category of illegal content, the dissemination of which may result in serious consequences including harm to the functioning of democracy and the rule of law. Significant effort was executed within the European Union to address the misuse of the Internet for terrorist purposes, including the creation of a common collaborative framework by the Commission - the EU Internet Forum (EUIF) aiming to reduce the accessibility to terrorist content online and increase the volume of effective alternative narratives online[13], formation of the EU Internet Referral Unit (EU IRU) within the EUROPOL that detects and investigates malicious content on the Internet, including social media, and the adoption of corresponding legislative, as well as other measures within the European Union context.

The legislative basis for the regulation of terrorist content is contained in the Directive (EU) 2017/541 on combating terrorism.[14] Specifically, Article 5 requires the Member States to punish as a criminal offence when committed intentionally the public provocation to commit a terrorist offence, specifically the distribution, or otherwise making available by any means, whether online or offline, of a message to the public, with the intent to incite the commission of one of the terrorist offences listed in points (a) to (i) of Article 3(1), where such conduct, 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. Specific examples of this offence include the glorification and justification of terrorism or the dissemination of messages or images online and offline, including those related to the victims of terrorism as a way to gather support for terrorist causes or to seriously intimidate the population.[15] Later adopted Commission Recommendation (EU) 2018/334 of 1 March 2018 on

[13] See European Union Internet Forum. Available: https://home-affairs.ec.europa.eu/networks/european-union-internet-forum_en.

[14] 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. *OJ L 88, 31.3.2017, p. 6–21.*

[15] Ibid. Recital 10.

measures to effectively tackle illegal content online focused on the role of hosting services providers in the dissemination of terrorist content and formulated the definition of this category of illegal content in its Article 4 (h). These initiatives later led to the adoption of the Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online[16] that extended the definition of terrorist content.[17]

Within the national context, the Act No. 300/2005 Coll. on Criminal Code (Criminal Code) provides in its Article 140b a list of offences classified as criminal offences of terrorism that also cover the individual types of material defined as terrorist content in the Regulation (EU) 2021/784. The criminal sanctioning of terrorism offences in the Slovak Republic is rare. To illustrate, the offence of certain forms of participation in terrorism (Article 419b of the Criminal Code) which sanctions public incitement to commit terrorism offences, as well as public approval of such offences, has been detected by the competent law enforcement authorities in only a number of cases annually, e. g. 5 cases in 2023.[18] Similarly, the statistics published by the General Prosecutor's Office of the Slovak Republic and the statistical yearbooks of the Ministry of Justice of the Slovak Republic record no more than one case of conviction of a person for committing this offence in the calendar years 2022 and 2023. Nonetheless, the example of a material that falls under the definition of terrorist content in the national context can be provided. In 2022, a terrorist attack against the members of the LGBTIQ+ community was committed on the territory of the Slovak republic. A few hours before the attack, the perpetrator posted a document on his Twitter account titled "A call to arms" (manifesto), in which he explained his racist, anti-Semitic and extremist motives that led him to commit this act. Given that the attacker repeatedly glorified the terrorist offences, advocated them and incited others to commit such offences, the document in question was classified as terrorist content. Following the attack, to ensure a more effective monitoring of the availability of this content, the file containing the manifesto in the form of a hash (a unique digital file identifier) has been included in a global database of terrorist content operated by the Global Internet Forum for Counter Terrorism (GIFTC).

B. Extremist content, including xenophobic and racially motivated speech that publicly incites hatred and violence (hate speech)

The national legal order does not contain the legal definition of the term ‘extremism’. This concept is only defined in legally non-binding documents.[19] The availability of extremist

[16] Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online. *OJ L 172, 17.5.2021, p. 79–109.*

[17] According to its Article 2 (7), the terrorist content covers one or more of the following types of material, namely material that a) incites the commission of one of the offences referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541, 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; b) solicits a person or a group of persons to commit or contribute to the commission of one of the offences referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541; c) solicits a person or a group of persons to participate in the activities of a terrorist group, within the meaning of point (b) of Article 4 of Directive (EU) 2017/541; d) 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 referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541; e) constitutes a threat to commit one of the offences referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541.

[18] Criminality Statistics. Ministry of Interior of the Slovak republic. Available: https://www.minv.sk/?statistika-kriminality-v-slovenskej-republike-xml.

[19] See Counter Extremism Concept for 2015-2019, and later revised Counter Extremism Concept until 2024. Available: https://www.minv.sk/swift_data/source/policia/naka_opr/nptj/koncepcia%20extremizmus%202015-2019.pdf and https://www.minv.sk/?zakladne-dokumenty-3&subor=395760.

content on the Internet[20] has been a long-standing issue in the Slovak Republic.[21] The dissemination of extremist content can be sanctioned within the national context either as the administrative delict of extremism pursuant to Article 47a(1) of Act No 372/1990 Coll. on delicts, or as one of the extremist criminal offences defined in Article 140a of the Criminal Code, most commonly as the distribution of extremist material (Article 422b) that sanctions a perpetrator that copies transports, procures, makes accessible, puts into circulation, imports, exports, offers, sells, ships or distributes extremist material. The legal definition of extremist material can be found in Article 130 (7) of the Criminal Code, according to which it covers "*written, graphic, video, audio or audio-video works:*

a) *of texts and declarations, flags, badges, passwords, or symbols, groups and movements that lead or led in the past to the suppression of fundamental human rights and freedoms,*
b) *of programmes or ideologies of groups and movements that lead or led in the past to the suppression of fundamental human rights and freedoms,*
c) *advocating, promoting or inciting hatred, violence or unreasonable differential treatment of groups of persons or an individual because of their belonging to one race, nation, nationality, skin colour, ethnicity, origin, or their religion, if it is an excuse for the above reasons, or*
d) *justifying, approving, denying or seriously derogating genocide, crimes against peace, crimes against humanity or military crimes, if the offender or an accessory to such an act was convicted by a final judgment of an international court established under international public law, the authority of which is recognised by the Slovak Republic, or by a final judgment of a court of the Slovak Republic.*"

Article 130 (8) of the Criminal Code further specifies that extremist material does not include material that is demonstrably produced, distributed, put into circulation, made publicly accessible or kept in possession for the purpose of educational, collection or research activities. The examination of the national case-law concerning the dissemination of extremist content online reveals that in the majority of cases, the competent authorities sanctioned the dissemination of such content on social media (prevalently on Facebook) of the perpetrator, specifically its publication on the public profile of the offender. Similarly, posting comments in the discussion on other users' posts or in the various groups created on the social network were also found to constitute extremist content dissemination. In one instance, a user was sanctioned (not exclusively) for flagging another user's post containing extremist material via the "Like" function. Other examples of extremist content dissemination included the possession of extremist material in a form that allows it to be made available online (photographs, audio or visual-sound recordings) on external media, in particular on the mobile phones of the perpetrators,[22] offering extremist materials for sale and distribution, in particular by publishing advertisements on various websites (in particular bazos.sk, bazar.sk or Facebook Marketplace), operation of a website, on which the accused published photographs, pictures, articles, reviews and links to events of right-wing musical formations, as well as other extremist material, or even sending out a mass email containing extremist material by which the accused incited various persons to hatred against persons belonging to a specific nationality.

[20] See also OECD Current approaches to terrorist and violent extremist content among the global top 50 online content-sharing services. OECD Digital Economy Papers, No. 296, OECD Publishing, Paris, 2020. https://doi.org/10.1787/68058b95-en.

[21] See LETKOVÁ, L. Trestné činy extrémizmu z pohľadu štatistiky a rozhodovacej praxe od roku 2017. Bratislava: C. H. Beck, 2023. ISBN: 978-80-8232-026-1.

[22] Such images also included photographs of the offenders themselves, if they showcased their extremist tattoos.

The category of content that publicly incites hatred and violence (the so-called hate speech) forms an integral part of the category of extremist content. The concept of hate speech appears in international, European, as well as national legal norms, but lacks a uniform definition.[23] Noteworthy is the definition provided in the first Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems that defines in its Article 2 (1) racist and xenophobic material as „*any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.*" Within the national context, criminal offences of extremism include a criminal offence committed out of a special motive under Article 140 (e) of the Criminal Code, which covers offences committed out of hatred against a group of persons or an individual because of their actual or deemed belonging to a race, nation, nationality, ethnicity, because of their actual or deemed origin, skin colour, gender, sexual orientation, political opinions or religion. The related term 'hate crime' is a concept covering a group of different offences defined by the national legislation, which may take different forms, for example, the offence of bodily harm, violence against a group of population, dangerous threats (e.g. such as in the case where the perpetrator through his mobile devices threatened his former partner with death, serious bodily harm and other serious harm in such a way that it could have raised reasonable concern, while he committed the said act out of a specific motive - hatred towards a group of persons because of their race and religion).[24]

C. Child pornography

The illegality of child pornography is confirmed in numerous international, European as well as national legal norms. The Budapest Convention on Cybercrime (2001) for example regulates in its Article 9 offences related to child pornography that covers "*pornographic material that visually depicts: a) a minor engaged in sexually explicit conduct; b) a person appearing to be a minor engaged in sexually explicit conduct; c) realistic images representing a minor engaged in sexually explicit conduct*." Parties to this Convention are required to establish as criminal offences under their national law when committed intentionally and without right, the following acts: a) producing child pornography for the purpose of its distribution through a computer system; b) offering or making available child pornography through a computer system; c) distributing or transmitting child pornography through a computer system; d) procuring child pornography through a computer system for oneself or for another person; and e) possessing child pornography in a computer system or on a computer-data storage medium.

Similar regulation is also contained in the Council of Europe Convention on the protection of children against sexual exploitation and sexual abuse that, moreover, criminalises the act of knowingly obtaining access, through information and communication technologies, to child pornography which covers offenders who visit child pornography websites without downloading and storing the material on their own devices. Liability of offenders in this context arises if they intentionally visit a website where child pornography is available with knowledge of the presence of such content on it. The offender's intent in this respect may be inferred from

[23] See PEJCHAL, V. Hate speech and human rights in Eastern Europe. Legislating for divergent values. London: Routledge, 2021. ISBN: 9781032236322. https://doi.org/10.4324/9781003005742.

[24] Rozsudok Špecializovaného trestného súdu z 30. januára 2019, sp. zn. 2T/41/2018. In this case, the offender was sanctioned with a six-month prison sentence, the execution of which was conditionally suspended. Concurrently the court prohibited the perpetrator from contacting the injured party in any form, including via electronic communication services or other similar means, during the probationary period, and ordered him not to approach the injured party at a distance of less than five meters and not to stay near her home or in a place where she stays or visits.

the fact that their visits to such sites are repeated or that the offender has gained access to the site on the basis of the payment of some consideration.[25]

The European Union regulation of child pornography is currently contained in the Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography that establishes minimum rules concerning the definition of criminal offences and sanctions in the area of sexual abuse and sexual exploitation of children, child pornography and solicitation of children for sexual purposes. Offences concerning child pornography (Article 5) similarly cover acquisition or possession of child pornography, knowingly obtaining access, by means of information and communication technology, to child pornography, distribution, dissemination or transmission of child pornography, offering, supplying or making available child pornography as well as its production. With the objective to make the fight against child sexual abuse, sexual exploitation and child pornography more effective, the Commission adopted a new strategy in this area (2020)[26] which reflects the increase in the demand for child sexual abuse material leading to the creation of a global market, and a dramatic increase in reports of online child sexual abuse, indicating that the EU has become the largest producer of child sexual abuse material in the world. On this basis, the Regulation (EU) 2021/1232 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse[27] was later adopted and a new proposal (not yet adopted) for a Regulation laying down rules to prevent and combat child sexual abuse was presented.[28]

In the national context, the relevant regulation is contained in the Criminal Code that criminalises production of child pornography (Article 368), its distribution (Article 369), possession of child pornography and participation in a child pornographic performance (Article 370) and sexual abuse (Article 201b). The criminal offence of child pornography distribution sanctions whoever copies, transports, procures, makes accessible or otherwise distributes child pornography. Based on the available statistical data for the last five calendar years, this offence was identified by the competent law enforcement authorities in an average of 253 cases per year, which seems to be a relatively low number of investigated cases, considering the amount of child pornography material available on the Internet.[29] The clearance rate for identified offences averages 30 % per year. The number of people sentenced for this crime is similarly low (52 in 2023, 61 in 2022, 44 in 2021, 47 in 2020).[30] Based on the examination of the available case law, the distribution of such content covered the making of available of child pornography through different communication applications to other unidentified users (often through apps such as Messenger, Pokec, WhatsApp, Telegram, Skype, Snapchat, Instagram etc.), the publication of child pornography on the public profile of the offender's social media, the sending of such material through email or making it available through peer-to-peer (P2P) programmes. The punishment to which the offenders were sentenced included primarily prison sentence (the execution of which was in most cases suspended for a probationary period),

---

25 Council of Europe. Explanatory Report to the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. P. 140. Available: https://rm.coe.int/16800d3832.

26 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. EU strategy for a more effective fight against child sexual abuse. *COM/2020/607 final.*

27 *OJ L 274, 30.7.2021, p. 41–51.*

28 Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse. *COM/2022/209 final.*

29 See WORTLEY, R. – SMALLBONE, S. Investigating Child Pornography. In: Internet Child Pornography. Causes, investigation and prevention. Praeger, 2012. P. 50-70. https://doi.org/10.5040/9798400671708.ch-004.

30 Statistical data of the Ministry of Justice of the Slovak republic. Available: https://web.ac-mssr.sk/statisticke-rocenky/

forfeiture of property, specifically electronic devices used for the commission of a crime, and even the imposition of a pecuniary fine.

D. Content in violation of the fundamental right to privacy and the right to personal data protection

The right to privacy was defined for the first time as the right to be left alone.[31] Today, the framework of this fundamental right is interpreted more broadly, encompassing various aspects of an individual's private life, the definition of which is constantly evolving.[32] As the Supreme Court of the Slovak Republic has stated in this regard, "*the wide range of manifestations and components of the private life of a natural person corresponds to the possibility of a variety of manifestations of interference with privacy and their consequences on protected personality rights*."[33] This is particularly valid as regards the application of this right online. Considering the diversity of the possible infringement forms, it is not possible to provide an exhaustive list of examples of illegal content whose unauthorised disclosure on the Internet infringes the right to privacy of the individuals concerned. The examples provided in this chapter cover the most common infringements based on their occurrence in the national case law. These include content whereby someone, without the consent of the person concerned, takes and/or makes available images or video and audio recordings relating to that person, for example by posting them on their social media or other platforms allowing the sharing of user-generated content. A number of cases of unauthorised disclosure of such content relate to the disclosure of intimate photographs or videos taken without the consent of the concerned subjects (using hidden cameras, gaining unauthorised access to the devices or user accounts, recording incidents of sexual abuse); even if consent was initially provided for the creation of intimate media, the subsequent dissemination of such content often after the end of the relationship ('revenge porn')[34] without consent is unlawful. Further examples of illegal content include cases of unauthorized dissemination of information regarding private individuals concerning their private life that may include false or misleading statements capable of interfering with the protection of the personality of the person concerned guaranteed, *inter alia,* by Article 11 of the Act No. 40/1964 Coll. Civil Code, in particular their civil honour, dignity and privacy, as well as the unauthorized dissemination of electronic communication of the user.

Closely connected with the right to privacy is the fundamental right to personal data protection guaranteed by Article 8 of the Charter of Fundamental Rights of the EU.[35] According to the Constitutional Court of the Slovak republic, this right ensures the protection of the data subject from "*obtaining, storing, using or further processing data relating to the private sphere of their life. Such protection is a necessary prerequisite for the individual's ability to decide which information relating to their privacy they will publish, which in a broader context protects their ability to make decisions freely and on their own responsibility regarding their private life.*"[36] This protection is ensured in the national context through the instruments of administrative, as well as criminal law. The corresponding case-law of the Personal Data

[31] WARREN, S. D. - BRANDEIS, L. D. The right to privacy. *Harvard Law Review*, 1890 4(5), P. 193-220. https://doi.org/10.2307/1321160.

[32] See PFISTERER V. M. The Right to Privacy - A Fundamental Right in Search of Its Identity: Uncovering the CJEU's Flawed Concept of the Right to Privacy. German Law Journal. 2019;20(5):722-733. https://doi.org/10.1017/glj.2019.57.

[33] Uznesenie Najvyššieho súdu Slovenskej republiky sp. zn. 3 Cdo 137/2008 z 18. februára 2010.

[34] See DVOŘÁKOVÁ, M. Revenge porn a deepfakes: ochrana soukromí v éře moderních technologií. In: Revue pro právo a technologie, Vol. 11, No. 22 (2020). ISSN: 1805-2797. P. 51-89. https://doi.org/10.5817/RPT2020-2-2.

[35] TZANOU, M. Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right. In: International Data Privacy Law, Vol. 3, No. 2. ISSN: 2044-4001. P. 88–99, https://doi.org/10.1093/idpl/ipt004.

[36] Nález Ústavného súdu Slovenskej republiky, sp. zn. II. ÚS 53/2010 z 9. decembra 2010.

Protection Office of the Slovak republic[37] also covers infringement cases, where the unlawful processing of personal data can be classified as illegal content. The include, primarily the unauthorized recording of data subjects through camera information systems. The processing of personal data in this manner often infringes different personal data processing principles, including the principle of lawfulness (failure to demonstrate the legal basis for processing), transparency principle (failure to provide necessary information to data subjects), principle of data minimisation (data processed are not limited to what is necessary in relation to the purposes for which they are processed) and storage limitation (storing of data for longer period than necessary for the purposes sought by processing). Further examples include the unauthorized disclosure of personal data on the Internet, e. g. on the controller's website, social media, in the obligatorily published contracts that are incorrectly anonymized etc., and the unauthorized sending of personal data to third parties via online communication tools, e. g. sending of emails to an unauthorized third parties due to the entering of an incorrect email address (often associated with insufficient security of the attached documents containing personal data, such as contractual agreements) or even making of available documents containing personal data through email on the basis of a freedom of information request.

E. Content infringing intellectual property rights

Another standard example of illegal content is content that infringes intellectual property rights, specifically copyright and trademark protection. Both categories of content may be protected through instruments of civil, administrative, as well as criminal law. As regards copyright infringement, it covers primarily the following cases of infringement sanctioned as a criminal offence according to the Article 283 of the Criminal Code:

a) making available of copyrighted works via peer-to-peer (P2P) networks. In these cases, the user of a P2P network unlawfully creates copies of copyrighted works and makes them available via a computer program (µTorrent, BitTorrent, etc.) to an unlimited number of other P2P network users, who can download these works without any restrictions and free of charge.
b) unlawful storage of copyrighted content on file hosting servers and the subsequent publication of links to the digital content thus published on various discussion forums, usually with the aim of obtaining financial compensation for each download of the content made available in this manner.
c) the unauthorized publication of copyrighted content online in another manner, e. g. on different websites or Internet forums.[38]

Trademark infringements that may be classified as illegal content, on the other hand, usually cover cases, in which the offender creates, purchases or in another way procures imitations or counterfeits of different goods or services that are offered for sale online, often through advertisements published on different e-commerce platforms.[39]

F. Content in violation of unfair competition regulation

The development of e-commerce led to the introduction of new business practices, through which competitors try to maximize their profits. In order to reach the largest number of potential

[37] See BACHŇÁKOVÁ RÓZENFELDOVÁ, L. – SOKOL, P. – HUČKOVÁ, R. – MESARČÍK, M. Personal data protection enforcement under GDPR – the Slovak experience. In: International Data Privacy Law, Vol. 14, Issue 3, 2024. https://doi.org/10.1093/idpl/ipae008.

[38] See BACHŇÁKOVÁ RÓZENFELDOVÁ, L. Prosecution of copyright infringements as a criminal offence in Slovakia. In: Journal of Intellectual Property Law & Practice. Roč. 17, č. 12 (2022). ISSN 1747-1532. P. 1023-1031. https://doi.org/10.1093/jiplp/jpac103.

[39] As regards the role of intermediaries in trademark infringement, see Riordan, J. The Liability of Internet Intermediaries. Oxford: Oxford University Press, 2016, 1st ed. https://doi.org/10.1093/oso/9780198719779.001.0001.

customers, entrepreneurs use different methods of content creation aimed at users, reflecting their behaviour and activities carried out online (often to a highly personalized extent). The content with which these competitors try to attract the attention of individual users (especially through advertising) may, under certain circumstances, be classified as illegal due to the violation of competition rules, including unfair competition according to the relevant provisions of the Act No. 513/1991 Coll. Commercial Code. A standard example of unfair competition illegal content is content fulfilling the nature of misleading advertising (Article 45 of the Commercial Code). Advertising is misleading, if it misleads or may mislead the persons to whom it is addressed or to whom it reaches, and concurrently it can influence the economic behaviour of the affected persons or may harm another competitor or consumer. The competent courts must consider "*the perception of an average consumer of the products or services being advertised who is reasonably well informed and reasonably observant and circumspect*."[40] Another example of illegal content include misleading description of goods and services offered online (Article 46 of the Commercial Code). In the context of e-commerce, this will primarily concern the sale of counterfeit products on various electronic marketplaces (Amazon, Ebay, Alibaba, Aliexpress), including marketplaces created on social networks (Facebook Marketplace, etc.). Further examples may include the provision of goods and services under the name of another competitor (creating the risk of confusion – Article 47 of the Commercial Code) or the unauthorised use of the trade secrets (Article 51 of the Commercial Code), e. g. the operation of an online store, the content of which was similar to or identical to the applicant's online store, both functionally and visually, whereby the store operator (former employee of the applicant) allegedly used a summary of information including the portfolio of the goods sold, the selection of suppliers and the setting of business conditions to establish their own business.[41]

G. Other types of illegal content

In the national context, other specific examples of illegal content can be identified, such as a) the promoting or operating of gambling websites without the necessary license granted by the Gambling Regulatory Authority, b) the dissemination of political content during election moratorium (48 hours before voting) by a political party, political movement, coalition of political parties and political movements and/or individual candidates, c) the sale of goods or services that are prohibited or subject to special restrictions (medicaments, narcotic or psychotropic substances, alcohol, tobacco and tobacco products, guns, etc.), d) fraudulent content that aims to mislead other users or exploit their mistake for the purpose of self-enrichment, e.g. by obtaining login details, payment details or other sensitive data of users, which the attacker can then use to his advantage, e) violent content depicting violent crimes shared through social networks or other types of intermediary services, f) content whose dissemination meets the factual basis of the crime of spreading alarm messages under the Article 361 of the Criminal Code, specifically in the case of spreading alarm messages via the Internet, e. g. by sending threatening emails about the presence of explosives in schools, universities, courts, hospitals or other publicly accessible places, or g) other hidden or undisclosed advertising practices including the promotion of goods or services by influencers without providing a notice identifying the commercial nature of the promotion, infringing the prohibition of unfair commercial practices regulation.[42]

---

[40] Judgement of the Court of Justice of the European Union from 19. September 2006 in the case C-356/04 Lidl Belgium. ECLI:EU:C:2006:585. P. 77-79.

[41] Uznesenie Okresného súdu Košice II z 8. 4. 2019, sp. zn. 35Cb/18/2019.

[42] See Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC,

IV. CONCLUSION

The classification of illegal content presented in this paper and the examples provided in this regard cover the individual categories of illegal content that can be distinguished within the national context, specifically based on the examination of the applicable regulation followed by the analysis of the corresponding case-law of competent national authorities. The illegal content categories identified in this regard include terrorist content, extremist content, including xenophobic and racially motivated speech that publicly incites hatred and violence (hate speech), child pornography, content in violation of the fundamental right to privacy and personal data protection, content infringing intellectual property rights, content in violation of unfair competition regulation and other categories of content that are sanctioned through the instruments of civil, administrative as well as criminal law. As mentioned above, this paper does not aim to identify all categories of illegal content that may be sanctioned under the applicable regulation, as such enumeration would not be feasible within the scope of this article. Nonetheless, we focus on the examination of the standard illegal content categories, reflecting also the practical implementation of the relevant legislation represented in the decision-making practice of state authorities, providing specific examples in this regard.

The national case-law examined confirms that the existing mechanisms for sanctioning cases of illegal content online are currently almost exclusively focused on individual infringers. Nonetheless, a possible change in this approach can be expected, considering the possibility of establishing the liability of intermediary service providers based on the provisions of the newly adopted Digital Services Act, which stipulates new obligations in this regard. However, a necessary prerequisite for this would be the more intensive involvement of national authorities, which is presumed in the Digital Services Act. This may include, e. g. the Slovak Council for Media Services which has the right to issue an order to act against illegal content directly to providers of intermediary services,[43] reflecting Article 9 of the Digital Services Act, if within the scope of proceedings on the prevention of illegal content it is proven that the content in question constitutes illegal content (within the definition of this term provided in the Act No. 264/2022 Coll. On media services) and concurrently its dissemination endangers the public interest or constitutes a significant interference with the individual rights or legitimate interests of a person within the scope of the national legal order, to achieve the removal of and prevent the dissemination of illegal content in question. So far, one such decision has been issued in the national context,[44] namely the decision No. RNO/1/2024 of 24 April 2024 in relation to Twitter International Unlimited Company, which imposed the obligation to remove a user's post distributed on the content sharing platform X and the obligation to prevent its distribution. The reason for imposing the aforementioned obligations was the fact that the disputed post was assessed as illegal content fulfilling the characteristics of extremist material pursuant to Article 151(2)(a) of the Act No. 264/2022 Coll. on media services and the characteristics of the criminal offence of incitement to national, racial and ethnic hatred pursuant to the Article 424 of the Criminal Code, including the corresponding European Union and international regulation. It remains to be seen, to what extent the Digital Services Act and its corresponding provisions in the national law will be employed in practice by the competent national authorities, reflecting the current state of prosecution of illegal content.

98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'). *OJ L 149, 11.6.2005, p. 22–39.*

[43] Article 153 of the Act No. 264/2022 Coll. on media services as amended.

[44] Decision of the Council for Media Services No. RNO/1/2024 from 24th April 2024 against Twitter International Unlimited Company. Available: https://rpms.sk/sites/default/files/2024-10/RNO_1_2024.pdf.

KEYWORDS
illegal content classification, terrorist content, extremist content, hate speech, child pornography, privacy, personal data, intellectual property rights, unfair competition

KĽÚČOVÉ SLOVÁ
klasifikácia nezákonného obsahu, teroristický obsah, extrémistický obsah, hate speech, detská pornografia, súkromie, osobné údaje, duševné vlastníctvo, nekalá súťaž

BIBLIOGRAPHY

1. Act No. 264/2022 Coll. on media services as amended
2. Act No. 40/1964 Coll. Civil Code as amended
3. Act No. 513/1991 Coll. Commercial Code as amended
4. Act No. 300/2005 Coll. Criminal Code as amended
5. BACHŇÁKOVÁ RÓZENFELDOVÁ, L. Prosecution of copyright infringements as a criminal offence in Slovakia. In: Journal of Intellectual Property Law & Practice. Roč. 17, č. 12 (2022). ISSN 1747-1532. P. 1023-1031. https://doi.org/10.1093/jiplp/jpac103
6. BACHŇÁKOVÁ RÓZENFELDOVÁ, L. – SOKOL, P. – HUČKOVÁ, R. – MESARČÍK, M. Personal data protection enforcement under GDPR – the Slovak experience. In: International Data Privacy Law, Vol. 14, Issue 3, 2024. https://doi.org/10.1093/idpl/ipae008
7. BUITEN, M., C. The Digital Services Act from Intermediary Liability to Platform Regulation. In: JIPITEC 12 (5) 2021. https://dx.doi.org/10.2139/ssrn.3876328
8. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Tackling illegal content online. Towards an enhanced responsibility of online platforms. *COM (2017) 555 final.*
9. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. EU strategy for a more effective fight against child sexual abuse. *COM/2020/607 final.*
10. Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online. *OJ L 63, 6.3.2018, p. 50–61.*
11. Council of Europe. Explanatory Report to the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse.
12. Counter Extremism Concept for 2015-2019, and later revised Counter Extremism Concept until 2024.
13. Criminality Statistics. Ministry of Interior of the Slovak republic. Available: https://www.minv.sk/?statistika-kriminality-v-slovenskej-republike-xml
14. Council of Europe Convention on the protection of children against sexual exploitation and sexual abuse
15. Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'). *OJ L 149, 11.6.2005, p. 22–39.*
16. Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography. *OJ L 335, 17.12.2011, p. 1–14.*

17. 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. *OJ L 88, 31.3.2017, p. 6–21.*
18. DVOŘÁKOVÁ, M. Revenge porn a deepfakes: ochrana soukromí v éře moderních technologií. In: Revue pro právo a technologie, Vol. 11, No. 22 (2020). ISSN: 1805-2797. P. 51-89. https://doi.org/10.5817/RPT2020-2-2
19. FICO, M. Základy trestnej zodpovednosti v procese unifikácie trestného práva medzivojnovej Československej republiky. Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, 2020. ISBN 9788081528408.
20. Judgement of the Court of Justice of the European Union from 19. September 2006 in the case C-356/04 Lidl Belgium. ECLI:EU:C:2006:585. P. 77-79.
21. LETKOVÁ, L. Trestné činy extrémizmu z pohľadu štatistiky a rozhodovacej praxe od roku 2017. Bratislava: C. H. Beck, 2023. ISBN: 978-80-8232-026-1.
22. Nález Ústavného súdu Slovenskej republiky, sp. zn. II. ÚS 53/2010 z 9. decembra 2010.
23. OECD Current approaches to terrorist and violent extremist content among the global top 50 online content-sharing services. OECD Digital Economy Papers, No. 296, OECD Publishing, Paris, 2020. https://doi.org/10.1787/68058b95-en.
24. PEJCHAL, V. Hate speech and human rights in Eastern Europe. Legislating for divergent values. London: Routledge, 2021. ISBN: 9781032236322. https://doi.org/10.4324/9781003005742
25. PFISTERER, V.M. The Right to Privacy - A Fundamental Right in Search of Its Identity: Uncovering the CJEU's Flawed Concept of the Right to Privacy. German Law Journal. 2019;20(5):722-733. https://doi.org/10.1017/glj.2019.57
26. Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse. *COM/2022/209 final.*
27. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act). *OJ L 277, 27.10.2022, p. 1-102.*
28. Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online. *OJ L 172, 17.5.2021, p. 79–109.*
29. Regulation (EU) 2021/1232 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse. *OJ L 274, 30.7.2021, p. 41–51.*
30. RIORDAN, J. The Liability of Internet Intermediaries. Oxford: Oxford University Press, 2016, 1. ed. ISBN: 9780198719779. https://doi.org/10.1093/oso/9780198719779.001.0001
31. ROMŽA, S. Privatizácia trestného práva. Praha: Nakladatelství Leges, 2021. ISBN 9788075025289.
32. Rozsudok Špecializovaného trestného súdu z 30. januára 2019, sp. zn. 2T/41/2018
33. SAVIN, A. Internet regulation in the European Union. In: EU Internet Law. Cheltenham, UK: Edward Elgar Publishing, 2017. https://doi.org/10.4337/9781784717971.00007
34. Statistics published by the General Prosecutor's Office of the Slovak Republic. https://www.genpro.gov.sk/statistiky/statisticky-prehlad-trestnej-a-netrestnej-cinnosti-za-rok-2023/

35. Statistical data of the Ministry of Justice of the Slovak republic. https://web.ac-mssr.sk/statisticke-rocenky/
36. The first Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems
37. The Budapest Convention on Cybercrime.
38. The Charter of Fundamental Rights of the EU.
39. TZANOU, M. Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right. In: International Data Privacy Law, Vol. 3, No. 2. ISSN: 2044-4001. P. 88–99, https://doi.org/10.1093/idpl/ipt004
40. Uznesenie Najvyššieho súdu Slovenskej republiky z 18. februára 2010, sp. zn. 3 Cdo 137/2008.
41. Uznesenie Okresného súdu Košice II z 8. 4. 2019, sp. zn. 35Cb/18/2019.
42. WALL, D. S. Cybercrime. The Transformation of Crime in the Information Age. Cambridge, U.K.: Polity Press, 2007. ISBN: 9780745627366. https://doi.org/10.1111/j.1468-4446.2007.00187_8.x
43. WARREN, S. D. - BRANDEIS, L. D. The right to privacy. *Harvard Law Review*, 1890 4(5). https://doi.org/10.2307/1321160
44. WORTLEY, R. – SMALLBONE, S. Investigating Child Pornography. In: Internet Child Pornography. Causes, investigation and prevention. Praeger, 2012. P. 50-70. https://doi.org/10.5040/9798400671708.ch-004
45. YAR, M. (2018) A Failure to Regulate? The Demands and Dilemmas of Tackling Illegal Content and Behaviour on Social Media, International Journal of Cybersecurity Intelligence & Cybercrime: 1(1), 5-20. https://www.doi.org/10.52306/01010318 RVZ E9940

CONTACT DETAILS OF THE AUTHOR
JUDr. Laura Bachňáková Rózenfeldová, PhD.
ORCID: 0000-0002-7111-9565
Researcher
Pavol Jozef Šafárik University in Košice, Faculty of Law,
Department of Commercial Law and Business Law
Kováčska 26, 040 75 Košice, Slovak Republic
Phone number: +421 55 234 4176
E-mail: laura.rozenfeldova@upjs.sk