Blokovanie webových stránok ako prostriedok boja proti dezinformáciám na Slovensku: právne limity, európske štandardy a odporúčania pre právnu úpravu

Mesarčík, M.[*]

MESARČÍK, M.: Blokovanie webových stránok ako prostriedok boja proti dezinformáciám na Slovensku: právne limity, európske štandardy a odporúčania pre právnu úpravu. Právny obzor, *108*, 2025, č. 6, s. 560 – 578. **https://doi.org/10.31577/pravnyobzor.2025.6.04**

Blocking websites as a means of combating disinformation in Slovakia: legal limits, European standards and recommendations for legislation. The article examines the legal and technical aspects of website blocking as a tool to combat the spread of disinformation in the Slovak legal environment. It is based on an analysis of the applicable legislation, in particular the Cybersecurity Act, in the context of the requirements arising from the case law of the European Court of Human Rights and the Court of Justice of the European Union, as well as relevant international soft-law instruments. The author compares the Slovak framework with selected foreign models and highlights a good practice example drawn from the Gambling Act. The article critically assesses the current blocking mechanism in the Slovak Republic, pointing to insufficient procedural safeguards, the absence of independent oversight, and a low level of transparency. Based on a qualitative analysis, it proposes de lege ferenda solutions to ensure constitutional and EU compliance, including a clear legal basis, precise definition of blockable content, the introduction of prior notification, effective remedies, time limits on measures, and independent judicial review. The aim of the article is to offer a legislative framework that allows for an effective response to serious disinformation while minimising the risk of disproportionate interference with freedom of expression and the right to information.

Key words: *website blocking, disinformation, cybersecurity, digital regulation*

Úvod

Na jar roka 2022 sa malý spravodajský portál zameraný na lokálne dianie náhle ocitol v situácii, keď jeho webová stránka prestala byť prístupná väčšine používateľov. Dôvodom bolo rozhodnutie príslušného orgánu o blokovaní domény, a to pre údajnú prítomnosť škodlivého obsahu. Podnikateľ prevádzkujúci portál tvrdil, že išlo o nedorozumenie, no počas niekoľkých týždňov nedokázal obnoviť prevádzku. Prišiel o čitateľov, príjmy z reklamy aj reputáciu, pričom jedinou možnosťou obrany bolo podanie žaloby na súde. Tento príbeh je fiktívny, avšak nie výnimočný. Podobné situácie sa odohrali v iných štátoch Európy, kde mechanizmy blokovania webov neboli sprevádzané dostatočnými zárukami ochrany práv dotknutých subjektov a kvalitnou právnou úpravou.

[*] Doc. JUDr. Matúš Mesarčík, PhD., LL.M. Právnická fakulta UK, Ústav práva informačných technológií a práva duševného vlastníctva, Bratislava.

[**] Financované EÚ NextGenerationEU prostredníctvom Plánu obnovy a odolnosti SR v rámci projektu č. 17R05-04-V01-00002 (Kompetenčné centrum pre reguláciu kybernetickej bezpečnosti, ochrany súkromia a kybernetickej kriminality).

Blokovanie prístupu k internetovým stránkam predstavuje veľmi invazívny zásah do práv a slobôd v digitálnom priestore, ktorý môže byť legitímnym nástrojom ochrany verejného záujmu, no zároveň nesie riziko neprimeraného obmedzenia základných ľudských práv a slobôd. V slovenskom právnom prostredí sa tento inštitút stal predmetom diskusie hlavne po prijatí novely zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti (ďalej len „ZoKB“), ktorá umožnila Národnému bezpečnostnému úradu (NBÚ) rozhodovať o blokovaní webov obsahujúcich „škodlivý obsah“. S rozmachom dezinformačných kampaní a hybridných hrozieb, najmä po vypuknutí ozbrojeného konfliktu na Ukrajine, sa diskusia o blokovaní stala politicky aj spoločensky citlivou témou.

Slovenská akademická literatúra venovaná blokovaniu webov je zatiaľ pomerne skromná. Z hľadiska právnej vedy sa téme podrobnejšie venovali napríklad Šamko v kontexte možného rozporu s judikatúrou Európskeho súdu pre ľudské práva (ESĽP),[1] Bachňáková Rózenfeldová v kontexte prehľadu regulácie nezákonného obsahu na internete[2] alebo Svák a Kapišovská v kontexte prehľadu judikatúry ESĽP.[3] Marginálne z pohľadu rôznych mechanizmov využiteľných pri zneužití dominantného postavenia na digitálnom trhu tému blokovania načrtla Kalesná[4] a blokovanie stručne analyzujú aj Kordík a Koprda v kontexte trestnoprávneho postihu dezinformácií v Slovenskej republike.[5] V európskom právnom a akademickom diskurze sa štátom nariaďované blokovanie webov považuje za mimoriadne citlivý zásah do slobody prejavu, ktorý musí byť jasne predpísaný zákonom, predvídateľný a podrobený nezávislej kontrole. Komparatívna štúdia Rady Európy z roku 2016, vypracovaná Švajčiarskym inštitútom pre komparatívne právo, poskytuje prehľad právnych základov a procesov blokovania vo všetkých členských štátoch, pričom rozlišuje súdne a administratívne modely a upozorňuje na riziká plošných opatrení bez primeraného cielenia.[6] Nadväzujúce odporúčania, napríklad CM/Rec(2016),[7] zaviedli indikátory internetovej slobody, ktoré zdôrazňujú požiadavky zákonnosti, proporcionality a transparentnosti.[2] Judikatúra ESĽP, osobitne vo veciach Ahmet Yıldırım v. Turecko, Cengiz a iní v. Turecko a OOO Flavus v. Rusko, opakovane konštatuje, že plošné blokovanie celej služby pre jednotlivý protiprávny obsah je neprimerané a nezlučiteľné s čl. 10 Európskeho dohovoru o ľudských právach, ak neexistuje

[1] ŠAMKO, P. Blokovanie webových stránok a jeho možný rozpor s judikatúrou Európskeho súdu pre ľudské práva. Právne listy. [online]. Dostupné na: https://www.pravnelisty.sk/clanky/a1062-blokovanie-.

[2] BACHŇÁKOVÁ RÓZENFELDOVÁ, L. *Regulácia nezákonného obsahu a súvisiacich deliktov na internete*. Praha : C. H. Beck, 2025.

[3] SVÁK, J., KAPIŠOVSKÁ, A. Vybrané rozsudky Európskeho súdu pre ľudské práva vyhlásené v období apríl – máj 2020 – Vladimir Kharitonov proti Rusku – OOO Flavus a ostatní proti Rusku – Bulgakov proti Rusku – Engels proti Rusku. In *Justičná Revue*. Roč. 72, č. 9, 2020.

[4] KALESNÁ, K. Zneužitie dominantného postavenia na digitálnom trhu. In *Právny obzor.* Roč. 105, č. 6, 2022, s. 497 – 506.

[5] KORDÍK, M., KOPRDA, N. Trestnoprávny postih dezinformácií v podmienkach Slovenskej republiky. In *Právny obzor*. Roč. 107, č. 1, 2024, s. 67 – 78. Dostupné na: https://doi.org/10.31577/pravnyobzor.2024.1.05.

[6] COUNCIL OF EUROPE – SWISS INSTITUTE OF COMPARATIVE LAW: *Comparative study on blocking, filtering and take-down of illegal internet content in the 47 member States of the Council of Europe*. Council of Europe, 2016. [cit. 11. 8. 2025]. Dostupné na: https://edoc.coe.int/.

[7] COMMITTEE OF MINISTERS OF THE COUNCIL OF EUROPE: *Recommendation CM/Rec(2016)5 on Internet freedom* (13 April 2016).

presný právny základ a mechanizmus rýchlej nápravy.[8] Akademické práce potvrdzujú, že v Európe sa využívajú rôzne technické prístupy (DNS, IP, URL blokovanie), pričom pretrváva potreba harmonizácie procesných záruk a minimalizácie zásahov do legálneho obsahu.[9] Odborná diskusia sa dnes posúva od otázky, či je blokovanie prípustné, k otázke, ako ho navrhnúť a uplatňovať tak, aby obstálo v testoch proporcionality a nevyhnutnosti vrátane presného zacielenia, notifikácie dotknutých osôb a dostupnosti účinných opravných prostriedkov.[10]

Hlavným prínosom predkladaného článku je zasadenie požiadaviek na legálne blokovanie webových stránok (ďalej aj „webstránok“) v kontexte dezinformácií do prostredia slovenského právneho poriadku a formulovanie konkrétnych odporúčaní pre slovenského zákonodarcu. Metodologicky sa tento článok opiera o kvalitatívnu analýzu aktuálne platnej slovenskej legislatívy k augustu 2025 vrátane posledných noviel ZoKB súvisiacich s transpozíciou smernice NIS2.[11] Analýza vychádza z interpretácie vnútroštátnych právnych predpisov, judikatúry Súdneho dvora EÚ (ďalej aj „SDEÚ“) a ESĽP. Súčasťou metodiky je aj posúdenie medzinárodných soft law dokumentov a odporúčaní, ktoré formujú štandardy na blokovanie obsahu v online priestore. Cieľom článku je analyzovať možnosti legálneho blokovania webstránok zo strany štátu a formulovať odporúčania pre efektívny, transparentný a ústavne konformný mechanizmus blokovania webov šíriacich dezinformácie v slovenskom právnom poriadku.

Po tomto úvode stručne predstavíme technické aspekty blokovania webstránok a ich význam. Zameriame sa na pojem blokovania, typológiu, technické metódy a limity diskutovaných mechanizmov. V ďalšej časti článku budú predmetom analýzy európske štandardy blokovania, ktoré vyžadujú predovšetkým judikatúra ESĽP a SDEÚ. Následne prostredníctvom normatívnej analýzy zvýrazníme, že v Slovenskej republike už máme legislatívne dobre ukotvený mechanizmus blokovania webových sídel, konkrétne v zákone č. 30/2019 Z. z. o hazardných hrách (ďalej len „zákon o hazardných hrách“). Práve táto právna úprava môže slúžiť ako inšpirácia pre zákonodarcu pri implementácií mechanizmov blokovania zameraných na iný obsah do právneho poriadku Slovenskej republiky. V poslednej časti článku podrobíme kritickej analýze mechanizmus blokovania v ZoKB a poskytneme návrhy a odporúčania na jeho ústavnokonformné a eurokonformné zakotvenie v kontexte boja proti dezinformáciám. Zhrnutie príspevku sa nachádza v závere.

[8] AHMET YILDIRIM proti Turecku, rozsudok ESĽP z 18. 12. 2012, č. 3111/10, CENGIZ a iní proti Turecku, rozsudok ESĽP z 1. 12. 2015, č. 48226/10 a 14027/11, OOO FLAVUS a iní proti Rusku, rozsudok ESĽP z 23. 6. 2020, č. 12468/15 a ďalšie.

[9] Napríklad BELLI, S. a kol. Website blocking in the European Union: Network interference from the perspective of network research. *Policy & Internet*. 2020. [online]. Dostupné na: https://onlinelibrary.wiley.com/doi/10.1002/poi3.367 [cit. 11. 8. 2025].

[10] K tejto otázke napríklad COUNCIL OF EUROPE: Freedom of Expression in 2023: Report on trends in freedom of expression in Council of Europe member states. 2024. [online]. Dostupné na: https://www.coe.int/en/web/freedom-expression/reports [cit. 11. 8. 2025].

[11] Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa menia nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2). PE/32/2022/REV/2. Ú. v. EÚ L 333, 27. 12. 2022, s. 80 – 152.

1. Stručný úvod do technických aspektov blokovania webových stránok

Blokovanie webových stránok možno definovať ako opatrenie, ktorým oprávnený subjekt (najčastejšie súd alebo správny orgán) uloží poskytovateľovi internetovej siete, prípadne inému sprostredkovateľovi pripojenia, povinnosť technickými prostriedkami znemožniť prístup používateľov k určitému online obsahu. Podstata spočíva v prerušení dátového toku medzi koncovým používateľom a serverom, na ktorom sa nachádza obsah, ktorý má byť zneprístupnený. Blokovanie sa využíva v rôznych právnych kontextoch. V oblasti ochrany autorských práv sa uplatňuje najmä na základe tzv. blocking injunctions, ktoré nariaďujú poskytovateľom internetu zablokovať prístup k stránkam porušujúcim autorské práva.[12] Ďalšími častými oblasťami sú boj proti šíreniu detskej pornografie, propagácia terorizmu či boj proti nelegálnemu hazardu.[13]

Z hľadiska využitých metód možno blokovanie rozdeliť na statické a dynamické:

- Statické blokovanie sa opiera o zoznam konkrétnych identifikátorov (IP adresa, názov domény, URL), ktoré sa aktualizuje manuálne. Ide o relatívne jednoduchý a predvídateľný mechanizmus, no zároveň menej flexibilný pri rýchlo sa meniacom obsahu.
- Dynamické blokovanie umožňuje automatizované rozširovanie blokovaného rozsahu na nové „zrkadlové" weby či subdomény, ktoré vzniknú po zablokovaní pôvodného zdroja. Tento prístup je bežný napríklad pri boji proti nelegálnemu streamingu, no z pohľadu základných práv je rizikovejší, keďže môže zasiahnuť aj legálny obsah.[14]

Ďalším kritériom typológie je rozsah zásahu, a teda, či ide o plošné alebo cielené blokovanie. Plošné blokovanie znamená zneprístupnenie celej domény alebo IP adresy bez ohľadu na to, či je obsah nelegálny. Cielené blokovanie sa zameriava iba na konkrétny nelegálny obsah (napr. konkrétna URL), čím sa minimalizuje riziko tzv. *overblocking-u*.[15]

Blokovanie prístupu k online obsahu môže byť uskutočnené rôznymi technickými metódami, ktoré sa líšia mierou presnosti, náročnosti implementácie, finančnými nákladmi a zároveň aj mierou zásahu do práv používateľov.

---

[12] Pozri napríklad rozsudok Súdneho dvora EÚ z 27. 3. 2014, C-314/12, *UPC Telekabel Wien GmbH* v. *Constantin Film Verleih GmbH* alebo HUSOVEC, M. Injunctions against Innocent Third Parties: The Case of Website Blocking. In *JIPITEC*. Roč. 4, 2013, č. 2, s. 116 alebo MOSTERT, F., LAMBERT, J. Study on IP Enforcement Measures, Especially Anti-Piracy Measures in the Digital Environment. WIPO/ACE/14/7. Geneva : WIPO, 2019.

[13] RADA EURÓPY: Recommendation CM/Rec(2016)5 of the Committee of Ministers to member States on internet freedom. 2016.

ZITTRAIN, J. L., PALFREY Jr., G. J. Access denied: the practice and policy of global internet filtering. 2007, jún. [online]. Dostupné na: https://www.oii.ox.ac.uk/archive/downloads/. SCHMIDT-KESSEN, M. J., HÖRNLE, J., LITTLER, A. Preventing risks from illegal online gambling using effective legal design on landing pages. *SSRN Electronic Journal*. 2019. https://doi.org/10.2139/ssrn.3474296.

[14] EURÓPSKA KOMISIA: Oznámenie Komisie Európskemu parlamentu, Rade a Európskemu hospodárskemu a sociálnemu výboru – Usmernenie k niektorým aspektom smernice Európskeho parlamentu a Rady 2004/48/ES o vymožiteľnosti práv duševného vlastníctva. COM(2017) 708 final.

[15] REIS, F., GODINHO DE MATOS, M., FERREIRA, P. Controlling digital piracy via domain name system blocks: A natural experiment. *Journal of Economic Behavior & Organization*. Roč. 218, 2024, s. 89 – 103. ISSN 0167-2681. https://doi.org/10.1016/j.jebo.2023.12.005.

Jedným z najčastejších prístupov je blokovanie na úrovni systému doménových mien (DNS), ktorý prekladá doménové mená na IP adresy. Pri tejto metóde poskytovateľ upraví odpoveď DNS servera tak, aby neobsahovala správnu IP adresu cieľového servera, čím používateľ nedokáže nadviazať spojenie s cieľovou stránkou. Výhodou sú technická jednoduchosť a nízke náklady, no tento spôsob sa dá ľahko obísť, napríklad zmenou DNS servera na verejný, ako sú Google DNS či Cloudflare DNS.[16]

Ďalšou technikou je blokovanie na úrovni IP adresy, ktoré spočíva v zamedzení prístupu k určitej IP adrese. Nevýhodou tohto riešenia je, že na jednej IP adrese môže byť hosťovaných viacero webových stránok (tzv. shared hosting), čo môže viesť k neúmyselnému zablokovaniu legálneho obsahu. Tento problém bol predmetom kritiky aj v judikatúre ESĽP, napríklad v prípade Cengiz a ostatní proti Turecku, kde plošné blokovanie IP adresy zablokovalo prístup k rozsiahlemu legálnemu obsahu.[17]

Proporcionálnejším riešením z hľadiska zásahu do legálneho obsahu je filtrovanie na úrovni URL, ktoré umožňuje blokovať konkrétne podstránky alebo súbory bez zablokovania celej domény. Táto metóda si vyžaduje inšpekciu HTTP požiadaviek a je technicky náročnejšia, no umožňuje lepšie zacieliť zásah a minimalizovať „vedľajšie" škody.[18]

Ešte sofistikovanejším nástrojom je *deep packet inspection* (DPI), ktorý umožňuje analyzovať dátové pakety a blokovať obsah na základe jeho charakteristík. DPI poskytuje vysokú presnosť blokovania, avšak prináša významné riziká pre ochranu súkromia, keďže umožňuje sledovať online aktivitu používateľov.[19] V praxi sa často využívajú hybridné prístupy, ktoré kombinujú viacero techník, napríklad DNS blokovanie pre rýchle nasadenie a URL filtering pre presnejšie cielenie.[20]

Špecifickým prípadom je geoblokovanie, pri ktorom sa prístup obmedzuje na základe geografickej polohy používateľa určenej podľa jeho IP adresy. Tento postup je bežný v oblasti licenčných obmedzení, avšak môže byť použitý aj na zabránenie prístupu k určitému obsahu z konkrétneho štátu.[21]

Aj napriek technologickej rozmanitosti nástrojov na blokovanie prístupu k online obsahu je ich účinnosť obmedzená predovšetkým možnosťou relatívne jednoduchého obchádzania. Metódy ako blokovanie na úrovni DNS či IP adries môžu byť obídené zmenou DNS servera na verejne dostupný (napr. Google DNS, Cloudflare) alebo použitím siete VPN, proxy serverov a anonymizačných nástrojov ako Tor. Štúdia Internet Society[22] kon-

[16] BROWN, I. Internet Filtering – Be Careful What You Ask for. In KIRCA, S., HANSON, L. (eds.) *Freedom and Prejudice: Approaches to Media and Culture*. Istanbul : Bahcesehir University Press, 2008, s. 74 – 91. [online]. Dostupné na: https://ssrn.com/abstract=1026597 [cit. 12. 8. 2025]. SARVEPALLI, V. DNS Blocking: A Viable Strategy in Malware Defense. Carnegie Mellon University, Software Engineering Institute's Insights (blog), 2017. [online]. Dostupné na: https://www.sei.cmu.edu/blog/dns-blocking-a-viable-strategy-in-malware-defense/ [cit. 12. 8. 2025].

[17] *OFCOM: ‚Site Blocking' to Reduce Online Copyright Infringement,* s. 28 a nasl.

[18] ARTICLE 19: Freedom of Expression Unfiltered, s. 8 – 9.

[19] Internet Society: An Overview of Internet Content Blocking, s. 14.

[20] *OFCOM: ‚Site Blocking' to Reduce Online Copyright Infringement,* s. 39 a nasl.

[21] PETER, K. Y. A Hater's Guide to Geoblocking. In *Boston University Journal of Science & Technology Law.* Roč. 25, č. 2, 2019, s. 503. Dostupné na: https://scholarship.law.tamu.edu/facscholar/1339.

[22] Internet Society: An Overview of Internet Content Blocking, s. 21.

štatuje, že pri plošnom DNS blokovaní je možné prístup k blokovanému obsahu obnoviť v priebehu niekoľkých minút až hodín, pričom technicky zdatnejší používatelia disponujú návodmi a nástrojmi, ktoré tento proces uľahčujú. Podobne Ofcom v kontexte blokovania porušovania autorských práv uvádza, že významná časť používateľov sa naučila blokovanie obísť, pričom efektivita takýchto opatrení časom klesá.[23]

Ekonomické náklady implementácie blokovania sa líšia v závislosti od zvolenej metódy. DNS blokovanie patrí medzi lacnejšie riešenia, avšak pri sofistikovanejších prístupoch, ako sú filtrovanie na úrovni URL alebo *deep packet inspection*, dochádza k výraznému navýšeniu investičných aj prevádzkových nákladov, a to nielen na technickú infraštruktúru, ale aj na personálne zabezpečenie a údržbu. Okrem toho tieto technológie prinášajú aj vedľajšie dosahy na ochranu súkromia, keďže umožňujú monitorovanie online aktivity používateľov.

Osobitnú pozornosť si vyžaduje problém tzv. *overblockingu*, teda neúmyselného zablokovania zákonného obsahu. Podľa správy Article 19 plošné blokovanie IP adries často vedie k zneprístupneniu rozsiahleho množstva legálneho materiálu, keďže na jednej IP adrese môže hosťovať viacero nezávislých webových stránok. Tento jav má negatívny dosah nielen na slobodu prejavu, ale aj na hospodársku činnosť prevádzkovateľov zasiahnutých webov. Riziko *overblockingu* sa dá čiastočne minimalizovať cieleným blokovaním konkrétnych URL, avšak aj táto metóda nie je bezchybná a vyžaduje si technicky náročnejšie implementačné postupy.[24]

2. Požiadavky na blokovanie v zmysle judikatúry SDEÚ a ESĽP

V súčasnosti neexistuje jednotný a záväzný právny rámec blokovania webových stránok v podobe unifikovaného právneho aktu, či už na úrovni Rady Európy alebo EÚ. Z tohto dôvodu určitý návod pre zákonodarcov pri zakotvení mechanizmov pre blokovanie webstránok predstavuje judikatúra SDEÚ a ESĽP, ktorá vo viacerých diskutovaných prípadoch naznačila, aké požiadavky musia byť legislatívou splnené pre legálne ústavno – a eurokonformné zakotvenie blokovania do právneho poriadku.

Blokovanie prístupu k internetovým stránkam je zásahom, ktorý má viacrozmerný dosah na základné práva garantované medzinárodnými aj vnútroštátnymi predpismi. Primárne ide o slobodu prejavu a právo na informácie podľa článku 10 Európskeho dohovoru o ľudských právach (ďalej len „EDĽP“) a článku 11 Charty základných práv Európskej únie (ďalej len „Charta EÚ“). Oba tieto dokumenty chránia nielen právo vyjadrovať sa, ale aj právo prijímať a rozširovať informácie, pričom ochrana sa vzťahuje aj na informácie, ktoré môžu byť pre časť spoločnosti sporné alebo nepríjemné.[25] Okrem toho sa blokovaním môže zasiahnuť do práva na pokojné užívanie majetku (čl. 1 Protokolu č. 1 k EDĽP), ak je blokovaná stránka zdrojom príjmov alebo súvisí s obchodnou činnosťou, do slobody podnikania (čl. 16 Charty EÚ) a do práva na spravodlivý proces (čl. 6 EDĽP, čl. 47 Charty EÚ), ak mechanizmus blokovania neposkytuje primerané možnosti obrany.

[23] *OFCOM: Site Blocking' to Reduce Online Copyright Infringement, s.* 46 – 50.
[24] ARTICLE 19: Freedom of Expression Unfiltered, s. 19.
[25] HANDYSIDE proti Spojenému kráľovstvu, rozsudok ESĽP z 7. 12. 1976, č. 5493/72.

Jedným zo základných kritérií prípustnosti zásahu je, aby bol „ustanovený zákonom“. ESĽP tento pojem vykladá nielen formálne (existencia právnej normy), ale aj materiálne – norma musí byť dostatočne jasná, prístupná a predvídateľná.[26] V prípade Ahmet Yıldırım proti Turecku[27] súd kritizoval, že turecká právna úprava umožňovala plošné blokovanie celej platformy Google Sites bez toho, aby jasne stanovila procesné garancie a kritériá pre taký zásah. Podobne v prípade OOO Flavus proti Rusku[28] bolo rozhodnutie o blokovaní založené na nejasných administratívnych postupoch bez explicitného zákonného rámca, čo viedlo k porušeniu čl. 10 EDĽP.

Podľa čl. 10 ods. 2 EDĽP je obmedzenie slobody prejavu prípustné len vtedy, ak sleduje legitímny cieľ, ako je národná bezpečnosť, verejná bezpečnosť, prevencia kriminality, ochrana zdravia alebo morálky, či ochrana práv iných. Podobné vymedzenie obsahuje aj čl. 52 ods. 1 Charty EÚ. Problém nastáva, ak vnútroštátna úprava operuje s vágne definovanými cieľmi, ako sú „hybridné hrozby“ či „závažné dezinformácie“. Bez presnej definície hrozí riziko svojvoľného výkladu a zneužitia. Štát musí byť schopný preukázať, že konkrétny zásah bol nevyhnutný na dosiahnutie legitímneho cieľa a že tento cieľ je reálny, a nie len hypotetický. S týmito požiadavkami sa štát musí vyrovnať v legislatívnom procese, v ktorom musí predmetný invazívny zásah vyargumentovať a podložiť.[29] Minimalizácia zásahu je kľúčovým princípom vyplývajúcim z oboch súdnych systémov. Znamená, že štát má povinnosť zvoliť takú metódu, ktorá v najväčšej miere rešpektuje práva a zároveň dosahuje cieľ. Cielené blokovanie konkrétnej URL alebo súboru je spravidla preferované pred plošným blokovaním celej domény alebo IP adresy. Riziko tzv. overblocking-u musí byť zohľadnené už v legislatívnom procese.[30]

ESĽP požaduje, aby zásah spĺňal test naliehavej spoločenskej potreby (pressing social need). V praxi to znamená, že orgány musia zvážiť, či neexistuje iné, menej invazívne opatrenie, ktoré by cieľ dosiahlo. V prípade Cengiz a iní proti Turecku[31] súd zdôraznil, že plošné blokovanie YouTube nebolo nevyhnutné, pretože bolo možné odstrániť len konkrétny sporný obsah. Zároveň je potrebné dbať na dodržanie testu proporcionality v kontexte posúdenia vhodnosti opatrenia na dosiahnutie cieľa, neexistencie menej invazívnej alternatívy a primeranosti v užšom zmysle, konkrétne vyváženia prínosu a zásahu do práv. V prípade *UPC Telekabel Wien*[32] SDEÚ blokovanie uznal za vhodné, no zdôraznil, že musí byť technicky realizovateľné a nesmie neprimerane obmedziť prístup k legálnemu obsahu. V prípade *LSG-Gesellschaft*[33] SDEÚ dodal, že opatrenie musí rešpek-

[26] *Sunday Times* v. Spojené kráľovstvo (č. 1), rozsudok Európskeho súdu pre ľudské práva z 26. 4. 1979, č. 6538/74.

[27] AHMET YILDIRIM proti Turecku.

[28] OOO FLAVUS a iní proti Rusku.

[29] HUSOVEC, M. *(Ir)Responsible Legislature? Speech Risks under the EU's Rules on Delegated Digital Enforcement*. Dostupné na SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3784149.

[30] Tamže.

[31] AHMET YILDIRIM proti Turecku.

[32] ROZSUDOK SDEÚ z 27. 3. 2014, C-314/12, UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH.

[33] ROZSUDOK SDEÚ z 19. 2. 2009, C-557/07, LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v. Tele2 Telecommunication GmbH.

tovať podstatu dotknutých práv. Technické aspekty a výber metódy blokovania sú súčasťou testu proporcionality. To znamená, že ak je cieľom minimalizovať zásah do legálneho obsahu, plošné blokovanie IP adries je menej vhodné než cielené blokovanie konkrétnych URL.

ESĽP a SDEÚ čoraz výraznejšie vo svojej judikatúre dbajú na zakotvenie tzv. záruk proti zneužitiu (*safeguards against misuse*). Nie je to inak ani pri mechanizme blokovania. Judikatúra ESĽP zdôrazňuje, že len následná súdna kontrola často nestačí, pretože škoda spôsobená blokovaním môže byť nezvratná. Preto by rozhodnutia mali byť podrobené nezávislému posúdeniu pred vykonaním, ideálne súdom alebo iným nezávislým orgánom.

Kľúčovým prvkom je transparentnosť, ktorá má dve roviny: (1) zverejňovanie rozhodnutí a (2) informovanie používateľov. Rozhodnutia o blokovaní by mali byť dostupné verejnosti, s výnimkou citlivých prípadov, v ktorých je možné anonymizovať údaje. Používateľ by mal byť pri pokuse o prístup k blokovanej stránke informovaný, že ide o rozhodnutie orgánu verejnej moci, s uvedením dôvodu a odkazu na verejný register rozhodnutí.[34]

Podľa čl. 13 EDĽP a čl. 47 Charty EÚ musí mať každý dotknutý subjekt reálnu možnosť brániť sa proti rozhodnutiu o blokovaní. Opravný prostriedok musí byť dostupný, efektívny a rýchly. V prípade OOO Flavus[35] ESĽP kritizoval, že ruská úprava neumožňovala promptné súdne preskúmanie rozhodnutia, čo viedlo k neprimeranému zásahu. Zároveň, musí existovať „rovnosť zbraní" (*equality of arms*). Prakticky to znamená, že blokovaný subjekt by mal mať k dispozícii nástroje, ktorým môže blokovanie efektívne zvrátiť resp. dať preskúmať nezávislému orgánu.[36] Judikatúra ESĽP vyžaduje aj tzv. notifikáciu vopred (*advanced notofication*), ktorá má zabezpečiť možnosť dotknutého subjektu brániť svoje základné práva a slobody a dať mu možnosť nezákonný obsah odstrániť.[37] Spoločne možno tieto záruky považovať za tzv. procesné záruky a prvky spravodlivého procesu.

Ak teda zhrnieme požiadavky na blokovanie webov v zmysle judikatúry ESĽP a SDEÚ, úprava mechanizmu blokovania musí (i) byť na základe zákona, (ii) sledovať legitímny cieľ, (iii) reagovať na naliehavú spoločenskú potrebu, (iv) reflektovať požiadavky proporcionality, ktoré sa primárne prejavujú prostredníctvom vhodného technického riešenia blokovania, a (v) obsahovať záruky proti zneužitiu v podobe notifikácie vopred, rovnosti zbraní, transparentnosti a nezávislého dohľadu.

[34] KHARITONOV proti Rusku, rozsudok ESĽP č. 10795/14, BULGAKOV proti Rusku, rozsudok ESĽP č. 20159/15, OOO FLAVUS a iní proti Rusku, rozsudok ESĽP z 23. 6. 2020, č. 12468/15.

[35] OOO FLAVUS a iní proti Rusku.

[36] ENGELS proti. Rusku, rozsudok ESĽP č. 61919/16, KHARITONOV proti Rusku, rozsudok ESĽP č. 10795/14, BULGAKOV proti Rusku, rozsudok ESĽP č. 20159/15, OOO FLAVUS a iní proti Rusku, rozsudok ESĽP z 23. 6. 2020, č. 12468/15.

[37] KHARITONOV proti Rusku, rozsudok ESĽP č.10795/14, BULGAKOV proti Rusku, rozsudok ESĽP č. 20159/15, OOO FLAVUS a iní proti Rusku, rozsudok ESĽP z 23. 6. 2020, č. 12468/15, ENGELS proti Rusku, rozsudok ESĽP č. 61919/16.

2.1 Zákon o hazardných hrách ako príklad dobrej praxe

Zákon o hazardných hrách predstavuje v slovenskom právnom poriadku najucelenejší príklad legislatívneho mechanizmu, ktorý explicitne umožňuje blokovanie prístupu k určitým internetovým stránkam. Tento model bol primárne zavedený s cieľom regulovať poskytovanie hazardných hier na území Slovenskej republiky a zabrániť neoprávnenému prevádzkovaniu hazardu zo zahraničia, avšak jeho procesné a technické riešenia môžu byť inšpiratívne aj pre iné oblasti regulácie online obsahu.

Právny základ blokovania hazardných webov je upravený v § 85 zákona o hazardných hrách v podobe úpravy dozoru nad poskytovaním zakázaných ponúk. V kontexte tejto právnej úpravy sa pod poskytovaním zakázanej ponuky rozumie *„propagovanie hazardnej hry alebo prevádzkovanie hazardnej hry dostupnej na území Slovenskej republiky bez licencie v latinskej abecede a v latinkovom systéme písma prostredníctvom elektronickej komunikačnej siete alebo elektronickej komunikačnej služby; hazardnou hrou dostupnou na území Slovenskej republiky je hazardná hra, na ktorej sa možno zúčastniť na území alebo z územia Slovenskej republiky najmä zaplatením vkladu, uskutočnením stávky alebo vyplatením výhry.“*[38] Podľa týchto ustanovení môže Úrad pre reguláciu hazardných hier (ďalej len „Úrad“) na základe príkazu súdu uložiť poskytovateľovi prístupu k internetu povinnosť zamedziť prístup k webovému sídlu.[39]

Zákon o hazardných hrách precízne upravuje žiadosť[40] Úradu o vydanie príkazu z hľadiska podmienok a náležitosti príkazu súdu na blokovanie.[41] Právna úprava v tomto smere presne definuje dôvody blokovania (poskytovanie zakázanej ponuky) a transparentne stanovuje podmienky jeho vykonania. Zároveň nemožno opomenúť, že § 85 zákona o hazardných hrách obsahuje aj konkrétne záruky proti zneužitiu. Notifikácia vopred je upravená v § 85 ods. 5 a dáva dozorovanému subjektu možnosť na výzvu Úradu ukončiť poskytovanie zakázanej ponuky v lehote desiatich dní odo dňa odoslania výzvy. Predmetná výzva zároveň musí obsahovať upozornenie na dôsledky v prípade neukončenia poskytovania zakázanej ponuky. Dozorovaný subjekt má možnosť preukázať, že neposkytuje zakázanú ponuku alebo že ukončil poskytovanie zakázanej ponuky.[42] Nezávislé vyhodnotenie je zabezpečené prostredníctvom zahrnutia súdnej moci do procesu blokovania. Právna úprava zároveň vyžaduje silné záruky transparentnosti v podobe zverejnenia príkazov súdov[43] a vedenia zoznamu zakázaných webových sídel a ponúk.[44] Ku dňu odoslania článku bolo takýmto spôsobom Úradom zablokovaných 304 webových sídel.[45]

[38] Zákon o hazardných hrách, § 2, ods. aa).
[39] Zákon o hazardných hrách, § 85 ods. 8.
[40] Zákon o hazardných hrách § 85 ods. 10.
[41] Zákon o hazardných hrách, § 85 ods. 11.
[42] Zákon o hazardných hrách, § 85 ods. 6.
[43] Zákon o hazardných hrách, § 85 ods. 14. Dostupné na: https://www.urhh.sk/web/guest/225.
[44] Zákon o hazardných hrách, § 85 ods. 1.
[45] Pozri Úrad pre reguláciu hazardných hier. *Zakázané ponuky. Zoznam blokovaných webov*. Dostupné na: https://www.urhh.sk/web/guest/zakazane-ponuky.

3. Zákon o kybernetickej bezpečnosti a blokovanie

3.1 Právna úprava blokovania v ZoKB

Po vypuknutí plnoformátovej vojny na Ukrajine sa v dôsledku zamedzenia šírenia dezinformácií rozhodol slovenský zákonodarca upraviť inštitút blokovania webových stránok v ZoKB, konkrétne v § 27b (blokovanie z vlastnej iniciatívy) a § 27c (blokovanie na podnet). V zmysle danej právnej úpravy mohol NBÚ vydať rozhodnutie o blokovaní webstránky, na ktorej sa nachádza škodlivý obsah. Škodlivý obsah je legálne definovaný ako *„programový prostriedok alebo údaj, ktorý zapríčiňuje alebo môže zapríčiniť kybernetický bezpečnostný incident. Škodlivou aktivitou sa rozumie akákoľvek činnosť, ktorá zapríčiňuje alebo môže zapríčiniť kybernetický bezpečnostný incident, podvodnú činnosť, odcudzenie osobných údajov alebo citlivých údajov,* ***závažné dezinformácie*** *a iné formy hybridných hrozieb.“*[46] Pri procesnom postupe viaceré ustanovenia odkazujú na tzv. pravidlá blokovania, ktoré k dnešnému dňu neboli publikované v právnej forme. Právna úprava obsahuje pomerne presnú identifikáciu náležitostí rozhodnutia o blokovaní[47] a požiadavku účelnosti, primeranosti a účinnosti.[48]

NBÚ môže z vlastnej iniciatívy rozhodnúť o blokovaní iba s platnosťou do 30. júna 2022. Na blokovania vykonané na podnet iného orgánu sa daný limit nevzťahuje.[49] Zaujímavosťou je, že v prípade blokovania na žiadosť iného subjektu: *„náklady spojené s výkonom blokovania na základe žiadosti žiadateľa a zodpovednosť za škodu spôsobenú blokovaním znáša žiadateľ“.* Ide o pomerne jedinečný prenos zodpovednosti pri výkone štátnej moci v slovenskom právnom poriadku na nahlasovateľa.

Zároveň je potrebné konštatovať, že aj po veľkej novele ZoKB v dôsledku nevyhnutnosti transpozície smernice NIS 2 ostala táto právna úprava nedotknutá a je stále súčasťou slovenského právneho poriadku.

3.2 Kritika právnej úpravy blokovania v ZoKB

Samotný mechanizmus blokovania webstránok bol podrobený odbornej kritike.[50] Ako už bolo uvedené, aj judikatúra ESĽP a SDEÚ formuluje jasné požiadavky na mechanizmus blokovania webstránok. Základnou požiadavkou je, aby bol mechanizmus blokovania komplexne upravený v zákone. Nestačí, že časť mechanizmu bude súčasťou podzákonného právneho aktu alebo bude stáť úplne mimo právneho rámca v podobe usmernenia. Takýto prístup zákonodarcu je preto ústavne neudržateľný. Navyše, v zmysle uvedenej judikatúry musí blokovanie disponovať penzom záruk proti zneužitiu.

[46] ZoKB, § 27b ods. 3.

[47] ZoKB, § 27b ods. 2.

[48] ZoKB, § 27b ods. 4 a § 27c ods. 5.

[49] Pozri ZoKB, § 27c ods. 9, ktorý v zmysle primeranosti použitia ustanovení § 28b odkazuje iba na odseky 5 až 7.

[50] Napríklad HUSOVEC, M. Súčasné blokovanie dezinformačných stránok je ústavne problematické. Čo s tým? *Denník N*. [online]. Dostupné na: https://dennikn.sk/2818631/sucasne-blokovanie-dezinformacnych-stranok-je-ustavne-problematicke-co-s-tym/?ref=list [cit. 12. 8. 2025].

Ak požiadavky diskutované v predchádzajúcich častiach článku zhrnieme, kvalita právnej úpravy blokovania webstránok v ZoKB je nasledujúca:

Požiadavka	Právna úprava v ZoKB
Zákonný základ	Čiastočne existuje, avšak detaily blokovania sú ponechané na iný právny akt.
Legitímny cieľ	Existuje, avšak je nedostatočne odôvodnený.
Naliehavá spoločenská potreba	Existuje.
Proporcionalita	Čiastočne §27b (4) a § 27c (5) vyžadujúce účinné, účelné a primerané vykonanie blokovania.
Notifikácia vopred	Nie je upravená.
Rovnosť zbraní	Nie je upravená.
Transparentnosť	Nie je upravená.
Nezávislý dohľad	Nie je upravený.

Právna úprava síce predstavuje zákonný základ, avšak nie je ústavne udržateľné, aby boli podmienky blokovania ponechané na podzákonnú právnu úpravu v inom právnom akte, nehovoriac o tom, že kompetentné orgány tento právny akt ani nevydajú a nezverejnia.

Ak chceme posúdiť splnenie požiadaviek legitímneho cieľa a naliehavej spoločenskej potreby, je potrebné nazrieť do dôvodovej správy k originálnej verzii zákona.[51] V kontexte blokovania dôvodová správa iba stroho konštatuje, že cieľom je zamedzenie šírenia škodlivého obsahu v dôsledku nepriaznivého vývoja situácie medzi Ukrajinou a Ruskom.[52] *„V tejto súvislosti je potrebné vytvoriť legislatívny rámec na vykonanie potrebných opatrení a okamžitej reakcie Slovenskej republiky na vzniknutú situáciu.“*[53] Dôvody na využitie blokovania zhŕňa dôvodová správa do viacerých oblastí: ochrana používateľov legitímnych, avšak napadnutých služieb, ako aj tých, ktorí sa nevedomky stanú terčom podvodných stránok; zmiernenie alebo úplné zabránenie škodlivým následkom tým, že sa včas preruší prístup k nebezpečným zdrojom; a zastavenie ďalšieho šírenia škodlivého obsahu vrátane malvéru, phishingových stránok či riadiacich serverov botnetov.[54]

V kontexte naliehavosti spoločenskej požiadavky dôvodová správa konštatuje: *„Návrh zákona dochádza k úprave právomocí Národného bezpečnostného úradu a zavádza sa legislatívne vymedzenie inštitútu „blokovania“, ktorý slúži na efektívne zamedzenie šírenia škodlivého obsahu na internete v* ***súlade s vznesenou spoločenskou požiadavkou*** *v záujme zabezpečenia dôveryhodnosti služieb a aktivít poskytovaných prostredníctvom*

[51] Vládny návrh zákona o niektorých opatreniach v súvislosti so situáciou na Ukrajine. Číslo ZZ: 55/2022. *Dôvodová správa*.

[52] Tamže.

[53] Tamže.

[54] Tamže.

internetu a ochrany práv osôb zúčastňujúcich sa na týchto aktivitách, ako aj ochrany konečného užívateľa týchto služieb alebo škodlivého obsahu na internete, vzhľadom na to, že škodlivých aktivít na internete z roka na rok pribúda šírením škodlivého obsahu ako aj šírením dezinformácii a zavádzajúcich kampaní."[55] Dôvodová správa však neuvádza žiadne prieskumy verejnej mienky alebo prípadové štúdie, ktoré by nasvedčovali naliehavosti zakotvenia inštitútu blokovania.

Metóda blokovania má byť určená v rozhodnutí o blokovaní, ktoré vydáva NBÚ.[56] Mechanizmus blokovania je nastavený nedostatočným spôsobom, ktorý takmer vôbec nereflektuje požiadavky plynúce z judikatúry ESĽP a SDEÚ. Azda najvýraznejšou je absencia akýchkoľvek záruk obrany proti rozhodnutiu. Nezávislý dohľad nad rozhodnutiami NBÚ zabezpečený nie je, pričom iba tento štátny orgán rozhoduje o blokovaní. Zároveň považujeme za nevyhnutné uviesť, že v kontexte využitej metódy blokovania sa javí, že NBÚ nevolil vždy vhodné riešenie. Rozhodnutie NBÚ o zablokovaní celej domény hlavnespravy.sk je z hľadiska judikatúry ESĽP fakticky identické s plošným blokovaním služby Google Sites v prípade *Ahmet Yıldırım* proti Turecku a služby YouTube v prípade *Cengiz*. V oboch prípadoch súd konštatoval, že plošné opatrenia zasiahli nielen sporný obsah, ale aj stovky ďalších legálnych materiálov, čím došlo k tzv. kolaterálnej cenzúre (*collateral censorship*). Podobne ako turecké orgány, ani NBÚ nenariadil odstránenie konkrétnych článkov (URL adries), ktoré považoval za škodlivé, ale prikázal poskytovateľom internetu a správcovi domény zablokovať prístup k celej službe. Takýmto postupom môže byť obmedzený aj prístup k legálnemu obsahu.

Ďalšie rozhodnutia ESĽP ukazujú, že postup NBÚ nemožno považovať za súladný ani pri širšom porovnaní. V prípade *Kharitonov* súd konštatoval porušenie práva na slobodu prejavu, keď ruské orgány zablokovali IP adresu poskytovateľa hostingu, čím znemožnili prístup k tisíckam nesúvisiacich webových sídiel. Rovnaký problém tzv. *overblockingu* nastal aj pri zablokovaní celej domény v slovenskom prostredí. Podobne vo veci *Engels* ESĽP kritizoval plošné blokovanie celej webstránky za jediný článok, pričom zdôraznil potrebu selektívnych opatrení. SDEÚ vo veci *UPC Telekabel Wien* síce pripustil možnosť blokovania, avšak pod podmienkou, že nesmie neprimerane obmedziť prístup k legálnemu obsahu. NBÚ legálny obsah zablokoval spoločne s nelegálnym obsahom. Ďalšia paralela sa ponúka s prípadom *OOO Flavus*, kde ESĽP kritizoval absenciu možnosti rýchleho a efektívneho súdneho preskúmania rozhodnutia o blokovaní. Aj v slovenskom kontexte NBÚ rozhodol bez predchádzajúceho nezávislého dohľadu a bez toho, aby mal dotknutý subjekt k dispozícii účinný opravný prostriedok. Považujeme za nevyhnutné uviesť, že v hraničných situáciách si možno pod efektívnym prostriedkom predstaviť aj zablokovanie celej domény resp. IP adresy, napríklad v prípade identifikácie hybridnej hrozby alebo šírenia extrémistkách či teroristických materiálov vo veľkom rozsahu. Takémuto postupu však musí predchádzať poctivá aplikácia princípov nevyhnutnosti a proporcionality.

[55] Tamže. K tomu body 2 článku III osobitnej časti dôvodovej správy.

[56] ZoKB, § 27b ods. 2 e).

Vyššie uvedené nedostatky mala odstrániť navrhovaná vládna novela ZoKB, ktorou sa štát snažil zaviesť systémové opatrenie pre blokovanie škodlivého obsahu.[57] Navrhovaná právna úprava už neobsahovala termín „závažné dezinformácie", ale tento fenomén by sme mohli zaradiť pod hybridné hrozby s určitou intenzitou. Pozitívom je, že na blokovanie bol v zmysle predkladanej novely potrebný súhlas Najvyššieho správneho súdu SR a NBÚ mal všetky rozhodnutia zverejňovať na svojom webovom sídle. Nedostatkom však stále ostávali záruky v podobe prostriedkov obrany zo strany blokovaného subjektu, ktoré nejestvovali. Navyše, návrh predmetnej novely sa už nedostal do parlamentu.

3.3 Alternatívy a návrhy pre reguláciu blokovania webov v dôsledku šírenia dezinformácií

Ak vezmeme do úvahy podmienky artikulované pre mechanizmus blokovania, ktoré sme diskutovali vyššie, môžeme uviesť nasledujúce alternatívy a odporúčania pre zákonodarcu pri zakotvovaní predmetného mechanizmu v kontexte šírenia dezinformácií.

V prvom rade je vhodné uviesť, že blokovanie webov na základe šírenia dezinformácií považujeme za mimoriadne invazívny zásah do práv a slobôd nielen blokovaného subjektu, ale aj akéhokoľvek jednotlivca z hľadiska prístupu k informáciám. Z tohto dôvodu by právna úprava mala precízne reflektovať princípy nevyhnutnosti a proporcionality a taktiež požiadavky diskutované v predchádzajúcich častiach. Vzhľadom na to by mal mať mechanizmus blokovania jednoznačný právny základ v podobe zákona, ktorý spĺňa formálne a materiálne kritéria z pohľadu judikatúry ESĽP. Alternatíva v podobe úpravy tohto mechanizmu alebo jeho časti v podzákonnom právnom predpise neprichádza do úvahy.

V druhom rade by právna úprava mala sledovať legitímny cieľ. Rozumieme potrebám ochrany verejnosti pred šírením dezinformácií. Je však potrebné poznamenať, že judikatúra ESĽP v kontexte slobody prejavu chráni aj nepravdivé prejavy.[58] Preto na blokovanie dezinformácií musí existovať závažný dôvod a tento mechanizmus by nemal byť používaný pre blokovanie webov obsahujúcich akékoľvek nepravdivé alebo zavádzajúce informácie. Aj z tohto dôvodu obsahovala pôvodná právna úprava termín „závažné dezinformácie" a návrh novely „forma hybridnej hrozby". Problematické v tomto kontexte je, že obe vyjadrenia sú veľmi vágne.

Slovenská a ani európska právna úprava neobsahujú legálnu definíciu pojmu dezinformácia. Odkázať možno iba na všeobecne akceptovateľnú definíciu[59] od vysokej expertnej skupiny na úrovni Európskej komisie, ktorú následne preberá aj európske *soft*

[57] *Návrh zákona, ktorým sa mení a dopĺňa zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov – nové znenie*. Dostupné na: https://rokovania.gov.sk/RVL/Material/27764/1.

[58] Napríklad HANDYSIDE proti Spojenému kráľovstvu, rozsudok ESĽP z 7. 12. 1976, č. 5493/72.

[59] EURÓPSKA KOMISIA: *Final report of the High Level Expert Group on Fake News and Online Disinformation*. [cit. 12. 8. 2025]. Dostupné na: https://digital-strategy.ec.europa.eu/en/library/final-report-high-level-expert-group-fake-news-and-online-disinformation.

law.[60] Riešením pre tieto úvahy teda môže byť buď zakotvenie legálnej definície obsahu, ktorý sa má blokovať, a to s vysokým levelom precíznosti, alebo zavedenie kritérií na hodnotenie závažnosti škodlivého obsahu.

Prvý prístup, teda explicitná zákonná definícia, má výhodu v tom, že poskytuje vyššiu právnu istotu, predvídateľnosť a znižuje riziko svojvoľného alebo neprimeraného zásahu do slobody prejavu. Jasne vymedzený obsah, ktorý možno považovať za dezinformáciu hodnú blokovania, by zároveň uľahčil prácu orgánom, ktoré rozhodujú o blokovaní, a umožnil lepšiu obranu subjektov, ktorých obsah má byť predmetom zásahu. Slabinou tohto prístupu je však jeho rigidnosť. Právna definícia nemusí pružne reagovať na dynamiku informačného prostredia a nové formy manipulatívneho obsahu, čím sa môže znižovať jej účinnosť v praxi. Druhý prístup, založený na vymedzení kritérií pre posúdenie závažnosti obsahu, ponúka flexibilitu a možnosť adaptácie na meniace sa hrozby. Môže zahŕňať posudzovanie faktorov, ako je miera potenciálnej ujmy, úmysel autora, rozsah a rýchlosť šírenia, či cielenie na zraniteľné skupiny. Tento prístup však nesie riziko väčšej miery diskrečnej právomoci orgánov a tým aj vyššej subjektivity pri rozhodovaní, čo môže ohroziť proporcionalitu zásahu a viesť k obmedzovaniu legitímneho, aj keď nepravdivého prejavu. Vhodným riešením by preto mohlo byť hybridné nastavenie v podobe základného rámcového vymedzenia pojmu dezinformácia v zákone, doplnený podrobnejšími kritériami pre jeho vyhodnocovanie.

Po tretie, naliehavú spoločenskú potrebu je nevyhnutné podložiť konkrétnymi dátami. V súvislosti s dezinformáciami možno uvažovať nad referenciami na zverejniteľné časti správ tajných služieb ohľadom informačných operácií alebo prieskumami s verifikovateľnou a transparentnou metodikou. Tieto informácie by mali byť súčasťou legislatívneho posúdenia vplyvu a referencované v dôvodovej správe.

Proporcionalitu blokovania je možné dosiahnuť viacerými spôsobmi. Sympatickou možnosťou sa javí návrh slovenského zákonodarcu pri novele ZoKB, ktorý navrhoval zakotvenie požiadavky blokovania *„v rozsahu nevyhnutnom na dosiahnutie cieľa a spôsobom primeraným vo vzťahu k následkom na majetku, právach a právom chránených záujmoch iných osôb.“*[61] Zároveň je vhodné blokovanie limitovať na presne určený čas s následným opätovným preskúmaním zo strany nezávislého orgánu. Technické metódy blokovania by mali byť predvídateľné a minimálne uvedené v dôvodovej správe.

Kameňom úrazu v slovenskej právnej úprave sú práve záruky proti zneužitiu. K blokovaniu by sa nemalo pristupovať arbitrárne a takým spôsobom, že blokovaný subjekt nedostane lehotu na vyjadrenie a možnosť sám potenciálne nebezpečný obsah odstrániť. Naopak, blokovaný subjekt by mal dostať lehotu na vyjadrenie ako aj možnosť obsah sám odstrániť, a ak by ho v lehote neodstránil, až následne by sa malo pristúpiť k bloko-

[60] SPOLOČNÉ OZNÁMENIE EURÓPSKEMU PARLAMENTU, EURÓPSKEJ RADE, RADE, EURÓPSKEMU HOSPODÁRSKEMU A SOCIÁLNEMU VÝBORU A VÝBORU REGIÓNOV: *Akčný plán proti dezinformáciám*. JOIN/2018/36 final.

[61] *Návrh zákona, ktorým sa mení a dopĺňa zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov – nové znenie*. Dostupné na: https://rokovania.gov.sk/RVL/Material/27764/1, navrhovaný § 27b ods. 4.

vaniu. Prirodzene, ak by išlo o veľmi škodlivý obsah, vieme si z tohto pravidla predstaviť výnimky napríklad pri detskej pornografií alebo extrémistickom či nenávistnom obsahu.

Vyjadrujeme názor, že proti rozhodnutiu o blokovaní by malo byť možné podať opravný prostriedok a nielen mať možnosť preskúmať napadnuté rozhodnutie na súde.

V ďalšom rade je potrebné zabezpečiť transparentnosť celého procesu. Rozhodnutia o blokovaní by mali byť verejne dostupné do takej miery, ako je to možné. Rozumieme limitom, ak boli webové stránky blokované na základe spravodajských informácií, avšak mala by byť dodržaná čo najväčšia miera možnej transparentnosti. V prípade zablokovanej webstránky by mal mať užívateľ hneď informáciu o tom, že stránka bola zablokovaná zo špecifických dôvodov, s odkazom na rozhodnutie o jej zablokovaní. Zároveň, proces vyhodnocovania dezinformácií by mal byť taktiež do určitej miery transparentný. Verejne dostupná by mala byť metodika alebo analytický prístup orgánu, ktorý blokovanie vykonáva. Bez dostatočnej transparentnosti niet možnosti adekvátnej obrany od dotknutých subjektov, nakoľko sa nevedia brániť.

Celý mechanizmus musí mať nezávislý dohľad. Nemôže ísť o blokovanie po rozhodnutí orgánu štátnej moci takým spôsobom, ako je to v súčasnej legislatíve nastavené. Medzi vydaním rozhodnutia o blokovaní a návrhom na blokovanie by malo byť posúdenie nezávislým orgánom. V tejto súvislosti sa núkajú dve alternatívy, a to buď dozor vykonávaný nezávislým súdom, alebo iným orgánom. Slovenské právo pozná ako nezávislý dozorný orgán aj výbor Národnej rady SR.[62] Ako vhodný kandidát sa javí Najvyšší správny súd Slovenskej republiky, ktorý by v určenej lehote posudzoval splnenie kritérií na blokovanie na návrh orgánu štátnej moci. Ten by rozhodnutie o blokovaní vydával až po schválení súdom. Vklad zákonodarnej moci prostredníctvom výboru nepovažujeme za vhodný nezávislý dohľad z dvoch dôvodov. V prvom rade je možné polemizovať o skutočnej nezávislosti jednotlivých výborov, ktoré nezriedka obsadzujú poslanci vládnej koalície. V druhom rade, nezávislý dohľad musí mať aj efektívne prostriedky pre schválenie alebo neschválenie návrhu na blokovanie.

Skúsenosti iných európskych krajín ukazujú, že blokovanie webových stránok šíriacich dezinformácie nie je výlučne slovenským fenoménom. Viaceré štáty po vypuknutí vojny na Ukrajine v roku 2022 zaviedli podobné opatrenia, avšak ich prístupy sa líšia rozsahom právnych základov, zapojením nezávislých orgánov a mierou transparentnosti. Krátko po začiatku invázie Ruska na Ukrajinu v roku 2022 došlo k blokovaniu niekoľkých webov v Českej republike vrátane Aeronet.cz a Protiproud.cz. Opatrenie však nevychádzalo zo zákona, ale zo súkromnoprávneho kroku poskytovateľov internetu koordinovaných „Národným centrom kybernetických operácií“ patriaceho pod Vojenské spravodajstvo. Tento postup možno kritizovať pre absenciu právneho rámca a nezávislej kontroly. Za zmienku stojí aj reakcia pobaltských štátov – Estónska, Litvy a Lotyšska. Všetky tri štáty kombinujú uplatňovanie sankcií EÚ s národnými mechanizmami, no líšia sa mierou procesných záruk. Estónsko umožňuje prostredníctvom správneho orgánu

[62] Pozri § 119 ods. 22 zákona č. 452/2021 Z. z. o elektronických komunikáciách, kde v prípade prenosu údajov vykonáva dozor Ústavnoprávny výbor NR SR.

nariadiť obmedzenie až po úroveň znefunkčnenia domény pri podnecovaní k nenávisti/vojne alebo vážnej hrozbe pre národnú bezpečnosť, pričom zákon vyžaduje test nevyhnutnosti a menej invazívnych alternatív.[63] Lotyšsko po marcových novelách príslušnej legislatívy dalo správnemu orgánu explicitnú právomoc administratívne nariadiť blokovanie domén alebo IP webových sídel, ktorých obsah ohrozuje národnú bezpečnosť alebo verejný poriadok, s povinnosťou vykonania blokovania zo strany poskytovateľov prístupu a správcu lotyšskej národnej domény.[64] Litva masívne uplatňuje sankčné blokovania a mimo výkonu predmetných sankcií používa „príkazy na plnenie" prostredníctvom orgánov presadzovania práva smerované poskytovateľom internetového pripojenia s predchádzajúcim súdnym súhlasom v prípade šírenia dezinformácií alebo iného zákonom definovaného nelegálneho obsahu, ako teroristický obsah či podnecovanie k vojne.[65]

Blokovanie webových stránok však predstavuje krajné riešenie, ktoré by malo byť využívané len v prípadoch, keď iné, menej invazívne nástroje zlyhali alebo nie sú efektívne. Medzi menej invazívne alternatívy patrí najmä označovanie obsahu (*content labelling*), rozvoj mediálnej a digitálnej gramotnosti a zvyšovanie algoritmickej transparentnosti.

Označovanie obsahu spočíva v jasnom vizuálnom označení sporných alebo neoverených informácií s odkazom na overené zdroje či fact-checkingové portály. Predmetná metóda zachováva prístup k informáciám, no zároveň poskytuje používateľovi kontext potrebný na kritické posúdenie obsahu. Výhodou je minimalizácia zásahu do slobody prejavu, nevýhodou však môže byť obmedzený dosah, ak používatelia takéto označenia ignorujú alebo vnímajú ako prejav zaujatosti.[66]

Mediálna a digitálna gramotnosť zvyšuje schopnosť obyvateľstva kriticky hodnotiť zdroje a rozpoznávať manipulatívne techniky. Ide o dlhodobú stratégiu, ktorá nemá okamžitý efekt, avšak v čase znižuje zraniteľnosť spoločnosti voči dezinformáciám. Nevýhodou je potreba systematických investícií do vzdelávacích programov a ich prepojenia s formálnym aj neformálnym vzdelávaním.[67]

Algoritmická transparentnosť sa zameriava na to, aby platformy zverejňovali informácie o fungovaní odporúčacích systémov a moderovaní obsahu, čím sa znižuje riziko,

[63] Information Society Services Act. Anglický preklad. [cit. 12. 8. 2025]. Dostupné na: https://www.riigiteataja.ee/en/eli/525082022006/consolide.

[64] Viac informácií na The Saeima delegates NEPLP to restrict access to websites that threaten national security. Anglický preklad. [cit. 12. 8. 2025]. Dostupné na: https://www.saeima.lv/aktualitates/saeimas-zinas/30744-saeima-delege-neplp-ierobezot-piekluvi-timekla-vietnem-kas-apdraud-valsts-drosibu.

[65] Republic of Lithuania Law on the Provision of Information to the Public. Anglický preklad. [cit. 12. 8. 2025]. Dostupné na: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/b90a7c321c7b11ecad9fbbf5f006237b?jfwid=10nvo6shnk.

[66] Pozri napríklad NASSETTA, J., GROSS, K. State media warning labels can counteract the effects of foreign misinformation. In Harvard Kennedy School (HKS) Misinformation Review, 2020. Dostupné na: https://doi.org/10.37016/mr-2020-45

alebo MARTEL, C., RAND, D. G. Misinformation warning labels are widely effective: A review of warning effects and their moderating features. In Current Opinion in Psychology, roč. 54, 2023, 101710. Dostupné na: https://doi.org/10.1016/j.copsyc.2023.101710.

[67] Nygren T, Efimova E (2025) Investigating the long-term impact of misinformation interventions in upper secondary education. PLoS One 20(7): e0326928. https://doi.org/10.1371/journal.pone.0326928.

že manipulatívny obsah bude masovo šírený v dôsledku netransparentných algoritmických rozhodnutí.[68] Tento prístup je podporovaný legislatívou, ako je nariadenie o digitálnych službách (DSA), ktoré zavádza povinnosti veľkých online platforiem v oblasti transparentnosti a prístupu k údajom pre výskumníkov.[69]

Z praktického hľadiska sa ako najefektívnejšie javí kombinované uplatňovanie týchto nástrojov. Blokovanie môže slúžiť ako výnimočný prostriedok pri obsahu, ktorý predstavuje okamžitú a závažnú hrozbu (napr. extrémistický či násilný obsah), zatiaľ čo menej invazívne opatrenia by mali tvoriť základnú líniu obrany proti dezinformáciám. Tento viacvrstvový prístup znižuje riziko neprimeraného zásahu do základných práv a zároveň zvyšuje odolnosť informačného prostredia voči manipulatívnemu obsahu.

Záver

Blokovanie webových stránok predstavuje mimoriadne invazívny zásah do základných práv, najmä slobody prejavu a práva na prístup k informáciám, a preto musí jeho právna úprava spĺňať prísne materiálne aj procesné požiadavky vyplývajúce z judikatúry ESĽP a Súdneho dvora EÚ. Súčasný mechanizmus zakotvený v ZoKB tieto požiadavky v plnom rozsahu nenapĺňa, keďže absentujú kľúčové záruky, akými sú predchádzajúca notifikácia, efektívny opravný prostriedok, nezávislý dohľad či vysoká miera transparentnosti. Nedostatočná je aj presnosť právnej úpravy, ktorá využíva vágne pojmy ako „závažné dezinformácie“ alebo „hybridné hrozby“, bez jasného zákonného vymedzenia alebo objektívnych kritérií na posúdenie závažnosti obsahu.

Pozitívnym príkladom v slovenskom právnom prostredí je právna úprava blokovania podľa zákona o hazardných hrách, ktorá ponúka precízne procesné rámce a môže slúžiť ako vzor pre úpravu blokovania webov z dôvodu šírenia dezinformácií. Pri navrhovaní novej legislatívy je potrebné zabezpečiť jednoznačný zákonný základ, vymedziť blokovateľný obsah s dostatočnou presnosťou, podložiť existenciu naliehavej spoločenskej potreby empirickými dátami a zaviesť proporcionalitu prostredníctvom časového obmedzenia blokovania a výberu menej invazívnych technických riešení.

Kľúčovým prvkom ústavne a európsky konformného mechanizmu je existencia nezávislého predbežného posúdenia návrhu na blokovanie, ideálne súdom, a povinnosť orgánov verejnej moci viesť transparentný register rozhodnutí a poskytovať informácie používateľom o dôvodoch blokovania. Takto nastavený rámec môže zabezpečiť efektívnu ochranu pred závažnými dezinformáciami a zároveň garantovať ochranu demokratických princípov a základných práv jednotlivcov.

[68] METZLER, H., GARCIA, D. Social Drivers and Algorithmic Mechanisms on Digital Media. In Perspectives on Psychological Science. Roč. 19, č. 5, 2024, s. 735 – 748. Dostupné na: https://doi.org/10.1177/17456916231185057.

[69] K tomu napríklad NANNINI, L., BONEL, E., BASSI, D. et al. Beyond phase-in: assessing impacts on disinformation of the EU Digital Services Act. In AI & Ethics. Roč. 5, 2025, s. 1241 – 1269. Dostupné na: https://doi.org/10.1007/s43681-024-00467-w.

Literatúra

AHMET YILDIRIM proti Turecku, rozsudok ESĽP z 18. 12. 2012, č. 3111/10

ARTICLE 19: *Freedom of Expression Unfiltered: How Blocking and Filtering Affect Free Speech*. Policy Brief, december 2016. [cit. 12. 8. 2025]. Dostupné na: https://www.article19.org/data/files/medialibrary/38586/Blocking_and_filtering_final.pdf

BACHŇÁKOVÁ RÓZENFELDOVÁ, L. *Regulácia nezákonného obsahu a súvisiacich deliktov na internete*. Praha : C. H. Beck, 2025. ISBN 978-80-8232-063-6

BROWN, I. Internet Filtering – Be Careful What You Ask for. In *FREEDOM AND PREJUDICE: APPROACHES TO MEDIA AND CULTURE*, S. Kirca, L. Hanson (eds.) Istanbul : Bahcesehir University Press, 2008, s. 74–91. Available at SSRN: https://ssrn.com/abstract=1026597

CENGIZ a iní proti Turecku, rozsudok ESĽP z 1. 12. 2015, č. 48226/10 a 14027/11

CHARTA ZÁKLADNÝCH PRÁV EURÓPSKEJ ÚNIE (2012/C 326/02). Ú. v. EÚ C 326, 26. 10. 2012

COMMITTEE OF MINISTERS OF THE COUNCIL OF EUROPE: *Recommendation CM/Rec(2016)5 on Internet freedom* (13 April 2016)

COUNCIL OF EUROPE – SWISS INSTITUTE OF COMPARATIVE LAW: *Comparative study on blocking, filtering and take-down of illegal internet content in the 47 member States of the Council of Europe*. Council of Europe, 2016. [cit. 11. 8. 2025]. Dostupné na: https://edoc.coe.int/

DOHOVOR O OCHRANE ĽUDSKÝCH PRÁV A ZÁKLADNÝCH SLOBÔD (*Európsky dohovor o ľudských právach*), Rím, 4. 11. 1950, v znení protokolov

EURÓPSKA KOMISIA: *Final report of the High Level Expert Group on Fake News and Online Disinformation*. [cit. 12. 8. 2025]. Dostupné na: https://digital-strategy.ec.europa.eu/en/library/final-report-high-level-expert-group-fake-news-and-online-disinformation

HANDYSIDE proti Spojenému kráľovstvu, rozsudok ESĽP z 7. 12. 1976, č. 5493/72

HUSOVEC, M. Injunctions against Innocent Third Parties: The Case of Website Blocking. In *Jipitec*. Roč. 4, č. 2, 2013, s. 116

HUSOVEC, M. *(Ir)Responsible Legislature? Speech Risks under the EU's Rules on Delegated Digital Enforcement*. Dostupné na SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3784149

INTERNET SOCIETY. *An Overview of Internet Content Blocking*. Policy Brief, 24. 3. 2017. [cit. 12. 8. 2025]. Dostupné na: https://www.internetsociety.org/resources/doc/2017/internet-content-blocking/

KALESNÁ, K. Zneužitie dominantného postavenia na digitálnom trhu. In *Právny obzor*. Roč. 105, č. 6, 2022, s. 497 – 506

KORDÍK, M., KOPRDA, N. Trestnoprávny postih dezinformácií v podmienkach Slovenskej republiky. In *Právny obzor.* Roč. 107, č. 1, 2024, s. 67 – 78. Dostupné na: https://doi.org/10.31577/pravnyobzor.2024.1.05

MARTEL, C., RAND, D. G. Misinformation warning labels are widely effective: A review of warning effects and their moderating features. In *Current Opinion in Psychology*. Roč. 54, 2023, 101710. https://doi.org/10.1016/j.copsyc.2023.101710

METZLER, H., GARCIA, D. Social Drivers and Algorithmic Mechanisms on Digital Media. In *Perspectives on Psychological Science.* Roč. 19, č. 5, 2024, s. 735 – 748. Dostupné na: https://doi.org/10.1177/17456916231185057

NASSETTA, J., GROSS, K. State media warning labels can counteract the effects of foreign misinformation. In *Harvard Kennedy School (HKS) Misinformation Review*, 2020. Dostupné na: https://doi.org/10.37016/mr-2020-45

NANNINI, L., BONEL, E., BASSI, D. et al. Beyond phase-in: assessing impacts on disinformation of the EU Digital Services Act. In *AI & Ethics.* Roč. 5, 2025, s. 1241 – 1269. Dostupné na: https://doi.org/10.1007/s43681-024-00467-w

NYGREN, T. – EFIMOVA, E. Investigating the long-term impact of misinformation interventions in upper secondary education. In *PLoS One*. Roč. 20, č. 7, 2025, e0326928. Dostupné na: https://doi.org/10.1371/journal.pone.0326928

OFCOM: *„Site Blocking' to Reduce Online Copyright Infringement: A Review of Sections 17 and 18 of the Digital Economy Ac*t. 27. 5. 2011. [cit. 12. 8. 2025]. Dostupné na: https://assets.publishing.service.gov.uk/media/5a79583740f0b642860d748f/Ofcom_Site-Blocking-_report_with_redactions_vs2.pdf

OOO FLAVUS a iní proti Rusku, rozsudok ESĽP z 23. 6. 2020, č. 12468/15 a ďalšie
PETER, K. Y. A Hater's Guide to Geoblocking. In *Boston University Journal of Science & Technology Law*. Roč. 25, č. 2, 2019, s. 503. Dostupné na: https://scholarship.law.tamu.edu/facscholar/1339
ROZSUDOK SDEÚ z 19. 2. 2009, C-557/07, LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v. Tele2 Telecommunication GmbH.
ROZSUDOK SDEÚ z 27. 3. 2014, C-314/12, UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH.
SARVEPALLI, V. DNS Blocking: A Viable Strategy in Malware Defense. Carnegie Mellon University, *Software Engineering Institute's Insights* (blog), 2017. [cit. 12. 8. 2025]. Dostupné na: https://www.sei.cmu.edu/blog/dns-blocking-a-viable-strategy-in-malware-defense/
SPOLOČNÉ OZNÁMENIE EURÓPSKEMU PARLAMENTU, EURÓPSKEJ RADE, RADE, EURÓPSKEMU HOSPODÁRSKEMU A SOCIÁLNEMU VÝBORU A VÝBORU REGIÓNOV: *Akčný plán proti dezinformáciám*. JOIN/2018/36 final
SVÁK, J., KAPIŠOVSKÁ, A. Vybrané rozsudky Európskeho súdu pre ľudské práva vyhlásené v období apríl – máj 2020 – Vladimir Kharitonov proti Rusku – OOO Flavus a ostatní proti Rusku – Bulgakov proti Rusku – Engels proti Rusku. In *Justičná revue.* Roč. 72, č. 9, 2020
ZÁKON č. 30/2019 Z. z. o hazardných hrách a o zmene a doplnení niektorých zákonov
ZÁKON č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
ZÁKON č. 452/2021 Z. z. o elektronických komunikáciách a o zmene a doplnení niektorých zákonov

Hrubá nedbanlivosť v trestnom práve ako základ budúcej rekodifikácie Trestného zákona?

Kiko, M., Richter, D.[*]

KIKO, M., RICHTER, D.: Hrubá nedbanlivosť v trestnom práve ako základ budúcej rekodifikácie Trestného zákona?[**] Právny obzor, *108*, 2025, č. 6, s. 579 – 602. **https://doi.org/10.31577/pravnyobzor.2025.6.05**

Gross negligence in criminal law as the basis for the future recodification of the Criminal Code? This paper addresses the issue of gross negligence in criminal law from the perspective of legal doctrine, case law, and proposed legislative reforms. Its primary aim is to assess whether gross negligence constitutes a distinct form of culpability or merely a more intense expression of conscious or unconscious negligence. The analysis includes doctrinal interpretations from Czech and Slovak legal scholarship, judicial decisions, and the influence of EU law. The article proposes criteria for distinguishing gross negligence from other forms of culpability and evaluates their relevance in light of the ultima ratio principle. The authors conclude that gross negligence does not constitute a new type of culpability, but rather a heightened level of existing negligence. Legislative recognition of this concept may improve legal certainty and predictability in the prosecution of negligent offenses.

Key words*: gross negligence, culpability, negligence in criminal law, ultima ratio principle, recodification, decriminalization*

Úvod alebo pohľad na hrubú nedbanlivosť očami právnej doktríny, súdov, národného zákonodarcu a Európskej únie

Pojem hrubá nedbanlivosť bol známy trestnoprávnej doktríne ešte pred prijatím nového trestného kódexu v ČR – zákona č. 40/2009 Sb. Trestní zákonník v znení neskorších predpisov (ďalej aj ako „ČTZ“) a pred úvahami o prijatí noviel zákona č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov (ďalej aj ako „Trestný zákon“ alebo „TZ“), na ktoré v ďalšom texte poukážeme.

Zároveň s hrubou nedbanlivosťou pracovali a pracujú aj iné právne odvetvia ako trestného právo, napríklad české civilné právo operuje s pojmom hrubá nedbanlivosť pri náhrade nemajetkovej ujmy v § 2971 zákona č. 89/2012 Sb. Občanský zákoník v znení neskorších predpisov: „*Odůvodňují-li to zvláštní okolnosti, za nichž škůdce způsobil újmu protiprávním činem, zejména porušil-li z hrubé nedbalosti důležitou právní povinnost, anebo způsobil-li újmu úmyslně z touhy ničit, ublížit nebo z jiné pohnutky zvlášť zavrženíhodné, nahradí škůdce též nemajetkovou újmu každému, kdo způsobenou újmu důvodně pociťuje jako osobní neštěstí, které nelze jinak odčinit.*“ Alebo pri odvolaní daru

[*] JUDr. Maximilián Kiko, LL.M., interný doktorand Katedry trestného práva, kriminológie a kriminalistiky, Právnická fakulta UK Bratislava.

Bc. Daniel Richter, interný doktorand Katedry trestného práva, kriminológie a kriminalistiky, Právnická fakulta UK Bratislava.

[**] Tento príspevok bol podporený grantom s názvom Excelentný grant Univerzity Komenského č. UK/3114/2024.

podľa § 2071 zákona č. 89/2012 Sb. Občanský zákoník: „*Právo odvolat dar nemá dárce, který si stav nouze přivodil úmyslně nebo z hrubé nedbalosti.*“ Je notorietou, že civilné právo – či už slovenské alebo české – si pri problematike civilnej zodpovednosti „*prepožičiava*“ poznatky zavinenia z trestného práva, čo zvyšuje dôležitosť správneho zadefinovania a výkladového uchopenia hrubej nedbanlivosti na úrovni trestného práva. Nanešťastie, aj tu narážame na nejednotnosť názorov predstaviteľov právnej doktríny.

V tejto súvislosti existujú v zásade dve názorovo rozdielne skupiny vo vzťahu k chápaniu hrubej nedbanlivosti. Prvá skupina zostáva názor, že hrubá nedbanlivosť nie je považovaná za novú formu zavinenia, ale predstavuje vyšší stupeň intenzity vedomej alebo nevedomej nedbanlivosti. Podľa Stanislava Mihálika „*hrubá nedbanlivosť pritom nie je považovaná za ďalšiu formu zavinenia (s ohľadom na ustálené diferencovanie úmyslu a nedbanlivosti), ale predstavuje vyšší stupeň intenzity samotnej nedbanlivosti, či už vedomej alebo nevedomej. Hodnotiacim kritériom je potom prístup páchateľa k požiadavkám dodržania náležitej miery opatrnosti, pričom o hrubej nedbanlivosti možno hovoriť v spojitosti s identifikovaním zrejmej bezohľadnosti páchateľa k záujmom chráneným trestným právom (čo sa osobitne odráža v súvislosti s nevedomou nedbanlivosťou). Aj v danom prípade je zachovanie príslušnej miery opatrnosti odvodzované zo spojenia objektívneho a subjektívneho hľadiska, pričom s ohľadom na definovanie hrubej nedbanlivosti bude prevažovať práve hľadisko subjektívne.“*[1] Podľa predstaviteľa českej trestnoprávnej doktríny Pavela Šámala: *„Hrubou nedbalostí se tedy rozumí vyšší stupeň intenzity nedbalosti, ať již vědomé či nevědomé, a to na základě přístupu (postoje) pachatele k požadavku náležité opatrnosti, kterou zákon charakterizuje jako „zřejmou bezohlednost“. Tato definice je potřebná, neboť některé trestné činy jsou stíhatelné jen v případě tzv. hrubé nedbalosti (např. § 221 odst. 1, 232 odst. 1, § 277 odst. 1, § 294 odst. 1, § 300 nebo § 303 odst. 1; dále srov. § 224 odst. 1 nebo 2, § 281 odst. 1, § 282 odst. 1, 2, § 294a, § 298a odst. 1 nebo § 301, kde je použita formulace „byť i z hrubé nedbalosti“, což znamená buď úmyslně, nebo alespoň z hrubé nedbalosti, ať už vědomé či nevědomé).“*[2] Aj podľa predstaviteľa českej civilnej právnej doktríny Bezouška hrubá nedbanlivosť „*není dalším typem nedbalosti, ale jde o vyšší míru nedbalosti (ve smyslu její intenzity), a to ať už ve formě nedbalosti vědomé, nebo nevědomé. Míří se tím na lehkomyslnost až bezohlednost škůdce, s jakou přistupuje k plnění své právní povinnosti; např. se i přes několikeré upozornění neseznámil s předpisy nutnými pro výkon jeho činnosti, takže při jejich porušení se sice jedná o nevědomou nedbalost, ale v intenzitě hrubé nedbalosti*.“[3]

Druhá skupina zostáva názor, že hrubá nedbanlivosť je novou formou zavinenia, resp. novým druhom len vedomej nedbanlivosti a neprichádza do úvahy pri nevedomej nedbanlivosti. Podľa Andreja Beleša: „*Hrubá nedbanlivosť je osobitným druhom ne-*

[1] ČENTÉŠ, J., KURILOVSKÁ, L., STRÉMY, T., TURAY, L. a kol. *Zásady trestného práva v teórii a praxi*. Praha : Wolters Kluwer ČR, 2022, s. 139.

[2] ŠÁMAL, P. Nedbalost. § 16. In ŠÁMAL, P. a kol. *Trestní zákoník. Komentář.* 3. vyd. Praha : C. H. Beck, 2023. [online CH BECK CZ].

[3] BEZOUŠKA, P. Náhrada nemajetkové újmy. § 2971. In Hulmák, M. a kol. *Občanský zákoník VI. Závazkové právo. Zvláštní část (§ 2055 – 3014). Komentář.* Praha : C. H. Beck, 2014. [online CH BECK CZ].