monografia

NÁSTROJE VEREJNÉHO PRÁVA PRE BOJ S DEZINFORMÁCIAMI V ONLINE PROSTREDÍ

Mesarčík

PRÁVNICKÁ FAKULTA
Univerzita Komenského
v Bratislave

monografia

NÁSTROJE VEREJNÉHO PRÁVA PRE BOJ S DEZINFORMÁCIAMI V ONLINE PROSTREDÍ

Matúš Mesarčík

PRÁVNICKÁ FAKULTA
Univerzita Komenského
v Bratislave

Vzor citácie: *Mesarčík, M. Nástroje verejného práva pre boj s dezinformáciami v online prostredí. 1. vydanie. Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2023.*

2023
Prvé vydanie

Recenzenti

JUDr. Ondrej Hamuľák, PhD.

mjr. doc. PhDr. JUDr. Mgr. Jozef Medelský, PhD.

prof. JUDr. Ing. Bernard Pekár, PhD.

Vydala Právnická fakulta Univerzity Komenského v Bratislave v roku 2023.

ISBN 978-80-7160-706-9

"Strach je cesta k temnej strane. Strach vedie k hnevu. Hnev vedie k nenávisti. Nenávisť vedie k utrpeniu."

Majster Yoda prehovára k mladému Anakinovi Skywalkerovi

(Star Wars Epizóda I: Skrytá hrozba)

OBSAH

PREDHOVOR

V lete 2022 som mal tú česť zúčastniť sa zaujímavých stretnutí v tvorivom prostredí Vysokých Tatier. Na jednom mieste a v rovnakom čase sa stretla skupiny právnikov, sociológov, vedcov, informatikov, štátnych úradníkov a zástupcov súkromnej sféry aby diskutovali o jednej veci, ktorá našu spoločnosť ovplyvňuje – dezinformáciách. Odborníci s rôznym pozadím si na stretnutie priniesli varietné pohľady na to, ako by mal vyzerať boj s dezinformáciami, v ktorom zjavne ako spoločnosť ťaháme za kratší koniec. Prezentované boli regulačné, technické ale aj iné možnosti, ktoré by mohli šírenie dezinformácií zmierniť. Z intenzívnych dvoch dní diskusií som si odniesol námet na ďalší výskum, ktorý sa pretavuje v tejto knihe.

Uvedomil som si, že prístup k dezinformáciám vyžaduje interdisciplinaritu, pretože bez pochopenia fungovania digitálnych služieb, prečo ľudia dezinformáciám veria a ako funguje ekonomika pozornosti, nie je úplne vhodné diskutovať rôzne regulačné nástroje. Zároveň mi bolo zjavné, že dezinformácie môžu mať rôznu intenzitu a kvalitu a tomu by malo byť prispôsobené aj využívanie konkrétnych právnych noriem. Právo na informácie a sloboda prejavu sú síce práva relatívne, ale to neznamená, že štát môže bezbreho blokovať webstránky alebo online platformy môžu bez pravidiel moderovať obsah. Nikoho snáď nechceme posielať do väzenia za to, že šíri a verí v plochosť zemegule. Preto je dôležité zachovať proporcionalitu.

Každý z nás sa už s nejakou dezinformáciou stretol. V ostatnom období sa môže zdať, že je nimi informačný priestor presýtený.

Z vyššie uvedených dôvodov som sa rozhodol k „boju" s dezinformáciami prispieť touto prácou. Netvrdím, že moje názory a úvahy sú jediné správne. Úprimne dúfam, že svojou troškou ku komplikovanej téme prispejem z pohľadu práva.

Za každú spätnú väzbu budem vďačný.

17. novembra 2023 v Bratislave

POĎAKOVANIE

Na tomto mieste si dovolím poďakovať každému inšpiratívnemu človeku vo svojom živote. Osobitne ďakujem rodine, ktorá má so mnou nekonečnú trpezlivosť.

ZOZNAM SKRATIEK

AIA znamená Návrh nariadenia Európskeho parlamentu a Rady, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie (Akt o umelej inteligencii) a menia niektoré legislatívne akty únie.

DSA Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2065 z 19. októbra 2022 o jednotnom trhu s digitálnymi službami a o zmene smernice 2000/31/ES (akt o digitálnych službách).

EÚ znamená Európska únia.

GDPR znamená nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)

SR znamená Slovenská republika.

Trestný zákon znamená zákon č. 300/2005 Z. z. Trestný zákon.

Ústava SR znamená 460/1992 Zb. Ústava Slovenskej republiky.

Zákon o mediálnych službách znamená zákon č. 264/2022 Z. z. o mediálnych službách a o zmene a doplnení niektorých zákonov (zákon o mediálnych službách).

Zákon o priestupkoch znamená zákon č. 372/1990 Zb. o priestupkoch.

Zákon o SIS znamená zákon č. 46/1993 Z. z. o Slovenskej informačnej službe.

Zákon o vojenskom spravodajstve znamená zákon č. 500/2022 Z. z. o Vojenskom spravodajstve.

ZoKB alebo Zákon o kybernetickej bezpečnosti znamená zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.

ÚVOD

14. decembra v roku 2012 to vyzeralo na bežný vyučovací deň na základnej škole Sandy Hook so sídlom v Newtown, štáte Connecticut v Spojených štátoch amerických. Všetko ale zmenil 20-ročný Adam Lanza, ktorý vošiel ráno do priestorov základnej školy s útočnou puškou a usmrtil 27 ľudí, vrátane dvadsiatich detí vo veku šesť až sedem rokov. Ide o jednu z najväčších tragédií v americkej histórií, ktorá sa týka útokov na školské zariadenia a študentov.[1] O tejto tragédií sa následne začalo šíriť množstvo dezinformácií a konšpirácií. Jedným z najhlasnejších jednotlivcov spochybňujúcich útok bol aj Alex Jones, známy americký konšpirátor. V kontexte útoku šíril dezinformácie, že útok sa vôbec nestal, bol zinscenovaný a nikto počas neho nezomrel.[2] Rodiny obetí podali na Alexa Jonesa viacero žalôb. Na základe jednej z nich musí Alex Jones zaplatiť obetiam odškodné vo výške 965 miliónov dolárov za spôsobenú ujmu.[3]

V roku 2015 úspešná sociálna sieť Facebook integrovala do svojho rozhrania novú funkciu pre užívateľov. Dovtedy mohli užívatelia príspevky iných iba zdieľať alebo označiť tlačidlom „Páči sa mi to" (*like*). Od tohto roku sociálna sieť pridala ďalšiu škálu emócií, ktorými užívatelia môžu príspevok označiť ako „Ha Ha" „Smútok" alebo „Hnev." Odporúčacie systémy Facebooku počas nasledujúcich troch rokov podporovali príspevky, na ktoré používatelia reagovali "nahnevane", a to na základe internej analýzy, ktorá ukázala, že takéto príspevky viedli k päťkrát väčšej angažovanosti a mali väčší počet interakcií ako príspevky s bežnými lajkami. Po rokoch výskumníci Facebooku poukázali na to, že príspevky s "nahnevanými" reakciami boli s vyššou pravdepodobnosťou toxické, polarizujúce, falošné alebo nekvalitné vrátane dezinformácií.[4] V roku 2018 urobil Facebook ďalšiu zmenu, na základe ktorej platforma preferovala zdieľanie príspevkov pred inými reakciami. Facebook v roku 2019 koncipoval štúdiu, v rámci ktorej bol vytvorený falošný účet so sídlom v Indii. Následne bol urobený výskum s cieľom zistiť, aký typ obsahu bol prezentovaný a s akým obsahom užívatelia interagovali.

[1] ESPOSITO, R. et al. *20 Children Died in Newtown, Conn., School Massacre*. ABC News. Associated Press. Dostupné na: https://abcnews.go.com/US/twenty-children-died-newtown-connecticut-school-shooting/story?id=17973836.
[2] Napríklad RYSER, R. *Alex Jones back on the hook for damages after bankruptcy judge sends Sandy Hook cases to Texas court*. The News-Times. Dostupné na: https://www.newstimes.com/news/article/Alex-Jones-back-on-the-hook-for-damages-after-17187680.php.
[3] QUEEN, J. *Alex Jones must pay Sandy Hook families nearly $1 billion for hoax claims, jury says*. Reuters. Dostupné na: https://www.reuters.com/legal/jury-begins-third-day-deliberations-alex-jones-sandy-hook-defamation-trial-2022-10-12/.
[4] MERRILL, J. – OREMUS, W. *Facebook prioritized 'angry' emoji reaction posts in news feeds*. The Washington Post. Dostupné na: https://www.washingtonpost.com/technology/2021/10/26/facebook-angry-emoji-algorithm/.

Výsledky štúdie ukázali, že v priebehu troch týždňov sa na stene falošného účtu nachádzala pornografia a bol plný polarizujúceho obsahu, nenávistných prejavov a dezinformácií.[5]

Večer 12. októbra došlo v Bratislave k teroristickému útoku, keď páchateľ zavraždil dvoch ľudí do veku 30 rokov. Útok bol motivovaný nenávisťou voči skupine osôb pre ich skutočnú alebo domnelú sexuálnu orientáciu.[6] Prakticky hneď po útoku sa na sociálnych sieťach začali šíriť dezinformácie, ktoré ponúkali alternatívne vysvetlenie udalostí a motívov páchateľa alebo obviňovali z tohto činu vtedajších predstaviteľov vlády, prezidentku alebo špeciálneho prokurátora.[7]

Dezinformácie ovplyvnili aj predvolebnú kampaň pred voľbami do Národnej rady Slovenskej republiky 2023. Centrum boja proti hybridným hrozbám Ministerstva vnútra Slovenskej republiky vo svojej správe[8] uvádza minimálne dva prípady dezinformačnej kampane pred voľbami, ktoré mali významný dopad na dôveryhodnosť volieb. Prvým prípadom je deepfake (umelo vytvorené) video jedného z lídrov politickej strany, kde so známou žurnalistkou diskutuje ohľadom manipulovania volieb. Predmetné video sa virálne šírilo prostredníctvom sociálnych sietí. Druhým prípadom je šírenie správy spravodajskej služby tretej krajiny, ktorá tvrdí, že iná tretia krajina ovplyvňuje volebný proces v Slovenskej republike.[9]

Všetky vyššie uvedené prípady potvrdzujú, že šírenie dezinformácií môže mať negatívne dôsledky na jednotlivcov ako aj na spoločnosť. Jednotlivcom môžu spôsobiť ujmu na zdraví, na živote alebo iných chránených hodnotách. Pre spoločnosť predstavuje šírenie dezinformácií hrozbu z hľadiska zachovania demokracie a právneho štátu. Dezinformácie neobchádzajú ani

---

[5] SARITHA, R. *In Just 21 Days, Facebook Led New India User to Porn, Fake News*. Bloomberg. Dostupné na: https://www.bloomberg.com/news/articles/2021-10-23/how-facebook-s-algorithm-led-a-new-india-user-to-fake-news-violence?sref=X1c60Hpu.

[6] TASR. *Tragickú streľbu v Bratislave prekvalifikovali na teroristický útok*. teraz.sk (Bratislava: TASR). Dostupné na: https://www.teraz.sk/slovensko/tragicku-strelbu-v-bratislave-prekvali/667778-clanok.html.

[7] RADA PRE MEDIÁLNE SLUŽBY. *Teroristický útok na Zámockej ulici v Bratislave: bezprostredné a preventívne aktivity Rady pre mediálne služby na zamedzenie šírenia nelegálneho a škodlivého obsahu. Správa o reakciách digitálnych platforiem na útok a o ich podiele na radikalizácii páchateľa*. Dostupné na webovom sídle Rady pre mediálne služby, s. 33.

[8] CENTRUM BOJA PROTI HYBRIDNÝM HROZBÁM. INŠTITÚT SPRÁVNYCH A BEZPEČNOSTNÝCH ANALÝZ MINISTERSTVA VNÚTRA SLOVENSKEJ REPUBLIKY. *Voľby 2023 a dezinformácie: Analýza šírenia klamlivého a zavádzajúceho obsahu súvisiaceho s voľbami do Národnej rady Slovenskej republiky 2023*. Dostupné na: https://www.hybridnehrozby.sk/wp-content/uploads/2023/10/Zaverecna-analyza-k-doveryhodnosti-volieb.pdf.

[9] Tamže.

priestor Európskej únie a Slovenska. Podľa prieskumu z roku 2022 až 52 % respondentov verí v konšpiračné teórie[10] typu ovládanie sveta elitami alebo neexistencia demokracie.

Jednou zo základných úloh práva je primerane reagovať na spoločenské fenomény a nové spoločenské vzťahy.[11] Dezinformácie sa bez pochybností stali dôležitým faktorom v 21. storočí, literatúra dokonca túto éru označuje ako post-faktuálnu.[12] Tento negatívny fenomén neobchádza ani Slovenskú republiku. Z týchto dôvodov sa v tejto práci venujeme dezinformáciám a nástrojom, ktoré môžu napomôcť pri ich minimalizovaní v online priestore.

Pri analýze súčasného stavu poznania sme vzhľadom na interdisciplinárny charakter práce a dôraz ako na právny poriadok Slovenskej republiky, tak Európskej únie vykonali rešerš odbornej literatúry prostredníctvom troch primárnych zdrojov. Primárne zdroje tvorila databáza SCOPUS, ISI (Web of Science) a SUMMON. Databázy SCOPUS a ISI sme zvolili z dôvodu medzinárodného rešpektovania kvality výstupov v rámci časopisov, ktoré sú indexované v predmetných databázach. Vyhľadávanie prostredníctvom systému SUMMON poskytlo náhľad ďalších zdrojov, ku ktorým má prístup Univerzita Komenského v Bratislave. Do vyhľadávania v týchto databázach boli zadávané nasledujúce príkazy na vyhľadávanie (v anglickom a slovenskom jazyku):

- Disinformation AND regulation AND EU (Dezinformácie A regulácia a EÚ), a
- Disinformation AND law AND EU (Dezinformácie A právo a EÚ).

Na základe takto zadaných príkazov bolo vygenerovaný nasledujúci počet dokumentov:

SCOPUS	ISI	SUMMON
25 dokumentov	46 dokumentov	89 dokumentov

Tabuľka: Vyhľadávanie relevantnej literatúry.
Zdroj: Webové sídla databáz.

Následne bol na základe jazyka, dostupnosti a po odstránení duplicít zohľadnený nasledujúci počet dokumentov:

[10] HAJDU, D. a kol. *GLOBSEC Trends 2022: Väčšina ľudí na Slovensku stále verí konšpiráciám a cíti sa ohrozene*. Dostupné na: https://www.globsec.org/what-we-do/press-releases/globsec-trends-2022-vacsina-ludi-na-slovensku-stale-veri-konspiraciam.
[11] KOLEKTÍV AUTOROV. *Aktuálne otázky teórie práva*. 1. vydanie. Bratislava: Wolters Kluwer, 2018, s. 178 a nasl.
[12] Napríklad WIGHT, C. Post-Truth, Postmodernism and Alternative Facts. In *New Perspectives*, vol. 26, no. 3, 2018, s. 17–30. JSTOR, https://www.jstor.org/stable/26675072 alebo SZAKÁCS, J. -BOGNÁR, É. *The impact of disinformation campaigns about migrants and minority groups in the EU*. IN-DEPTH ANALYSIS Requested by the INGE committee.

SCOPUS	ISI	SUMMON
20 dokumentov	32 dokumentov	46 dokumentov

Tabuľka: Vyhľadávanie relevantnej literatúry.
Zdroj: Webové sídla databáz.

Primárne zahraničná odborná literatúra sa téme dezinformácií a regulácie venuje z viacerých pohľadov. Spomenúť možno všeobecnejšie príspevky z pohľadu činnosti veľkých technologických firiem a reakcií EÚ na šírenie dezinformácií.[13] Prirodzene, rezonuje pohľad na regulačné mechanizmy a ich ovplyvňovanie slobody prejavu a práva na informácie,[14] či trestnoprávnej regulácie a postihu za šírenie dezinformácií.[15] Osobitnú pozornosť si v odbornej literatúre vyžiadala regulácia sociálnych médií a ich vplyv na dezinformácie.[16] Nakoľko dezinformácie predstavujú fenomén, ktorému sa systematicky venuje aj legislatíva a politika na úrovní Európskej únie, identifikovali sme odborné štúdie vypracované pre orgány EÚ venujúce

[13] Napríklad BOUZA GARCÍA, L. – ALVAR, O. Regulating Disinformation and Big Tech in the EU: A Research Agenda on the Institutional Strategies, Public Spheres and Analytical Challenges. In *Journal of Common Market Studies*, 2023; SHATTOCK, E. Self-Regulation 2:0? A Critical Reflection of the European Fight Against Disinformation. In *Harvard Kennedy School Misinformation Review*., vol. 2/no. 3, (2021); CASERO-RIPOLLÉS, A. - JORGE T. - BOUZA-GARCÍA, L. The European Approach to Online Disinformation: Geopolitical and Regulatory Dissonance. In *Humanities & Social Sciences Communications*, vol. 10/no. 1, (2023), s. 657-10; SHATTOCK, E. Fake News in Strasbourg: Electoral Disinformation and Freedom of Expression in the European Court of Human Rights (ECtHR). *European Journal of Law and Technology*, vol. 13/no. 1, (2022), KOUROUTAKIS, A. EU Action Plan Against Disinformation: Public Authorities, Platforms and the People. In *The International Lawyer*, vol. 53/no. 2, (2020), s. 277-290; LONARDO, L. EU Law Against Hybrid Threats: A First Assessment. In *European Papers* (Online. Periodico), vol. 6/no. 2, (2021), s. 1075-1096; REGLITZ, M. Fake News and Democracy. In *Journal of Ethics & Social Philosophy*, vol. 22/no. 2, (2022), s. 162; BENDIEK, A. – STÜRZER, I. *Advancing European Internal and External Digital Sovereignty: The Brussels Effect and the EU-US Trade and Technology Council.* IDEAS Working Paper Series from RePEc, (2022).

[14] Pozri napríklad SHATTOCK, E. Fake News in Strasbourg: Electoral Disinformation and Freedom of Expression in the European Court of Human Rights (ECtHR). In *European Journal of Law and Technology*, vol. 13/no. 1, (2022); IGLESIAS KELLER, C. Don't Shoot the Message: Regulating Disinformation Beyond Conten. In *Direito Público* (Porto Alegre), vol. 18/no. 99, (2021).

[15] Napríklad ESPALIÚ-BERDUD, C. Legal and Criminal Prosecution of Disinformation in Spain in the Context of the European Union. In *El Profesional De La Informacion*, vol. 31/no. 3, (2022).

[16] Napríklad LEISER, M. *Reimagining Digital Governance: The EU's Digital Service Act and the Fight Against Disinformation* 2023. Dostupné na: https://ssrn.com/abstract=4427493; BUITEN, M. *Combating Disinformation and Ensuring Diversity on Online Platforms: Goals and Limits of EU Platform*. 2022. Dostupné na: https://ssrn.com/abstract=4009079.

sa tejto téme z pohľadu dezinformačných kampaní,[17] médií,[18] reklamy,[19] hybridných hrozieb,[20] slobody prejavu,[21] digitálnych služieb,[22] ľudských práv,[23] špecifických legislatív[24] alebo v konkrétnom kontexte ako je napríklad pandémia COVID-19.[25]

Dodatočne sme vykonali vyhľadávanie v slovenských právnych časopisoch prostredníctvom portálu legalis.sk, ktorý obsahuje archív najvýznamnejších slovenských právnych odborných časopisov (Justičná revue, Právny obzor, Súkromné právo a Zo súdnej praxe). Po zadaní slova „dezinformácie" do vyhľadávania systém identifikoval iba štyri články, ktoré sa téme venujú veľmi okrajovo alebo teoreticky s ohľadom na širšie spoločenské problémy.[26] V prostredí Slovenskej republiky však boli publikované viaceré zaujímavé práce, ktoré s témou dezinformácii imanentne súvisia. Šíreniu dezinformácií z právneho pohľadu sa osobitne venoval zborník príspevkov Dezinformácie a právo (úlohy a postavenie bezpečnostných zložiek).[27] V rámci popularizačno-odbornej literatúry boli publikované diela

[17] BAYER, J. et al. *Disinformation and propaganda: impact on the functioning of the rule of law and democratic processes in the EU and its Member States - 2021 update*. Dostupné na: https://www.europarl.europa.eu/thinktank/en/document/EXPO_STU(2021)653633.

[18] EUROPEAN PARLIAMENT, DIRECTORATE-GENERAL FOR PARLIAMENTARY RESEARCH SERVICES, DUMBRAVA, C. *Key social media risks to democracy – Risks from surveillance, personalisation, disinformation, moderation and microtargeting*. European Parliament, 2021. Dostupné na: https://data.europa.eu/doi/10.2861/135170.

[19] EUROPEAN PARLIAMENT, DIRECTORATE-GENERAL FOR INTERNAL POLICIES OF THE UNION, GALLI, F., SARTOR, G., LAGIOIA, F. *Regulating targeted and behavioural advertising in digital services : how to ensure users' informed consent*. European Parliament, 2021. Dostupné na: https://data.europa.eu/doi/10.2861/264833.

[20] EUROPEAN COMMISSION, JOINT RESEARCH CENTRE, GIANNOPOULOS, G., SMITH, H., THEOCHARIDOU, M. *The landscape of hybrid threats : a conceptual model : public version*. Publications Office of the European Union, 2021. Dostupné na: https://data.europa.eu/doi/10.2760/44985.

[21] EUROPEAN PARLIAMENT, DIRECTORATE-GENERAL FOR INTERNAL POLICIES OF THE UNION, BATURA, O., HOLZNAGEL, B., LUBIANIE, K. *The fight against disinformation and the right to freedom of expression*. European Parliament, 2021. Dostupné na: https://data.europa.eu/doi/10.2861/305.

[22] EUROPEAN PARLIAMENT, DIRECTORATE-GENERAL FOR INTERNAL POLICIES OF THE UNION, BOTERO ARCILA, B., GRIFFIN, R. *Social media platforms and challenges for democracy, rule of law and fundamental rights : executive summary*. European Parliament, 2023. Dostupné na: https://data.europa.eu/doi/10.2861/304062.

[23] EUROPEAN PARLIAMENT, DIRECTORATE-GENERAL FOR EXTERNAL POLICIES OF THE UNION, COLOMINA, C., SÁNCHEZ MARGALEF, H., YOUNGS, R. *The impact of disinformation on democratic processes and human rights in the world*. European Parliament, 2021. Dostupné na: https://data.europa.eu/doi/10.2861/59161.

[24] EUROPEAN COMMISSION, DIRECTORATE-GENERAL FOR COMMUNICATIONS NETWORKS, CONTENT AND TECHNOLOGY. *Digital Services Act : application of the risk management framework to Russian disinformation campaigns*. Publications Office of the European Union, 2023. Dostupné na: https://data.europa.eu/doi/10.2759/764631.

[25] EUROPEAN PARLIAMENT, DIRECTORATE-GENERAL FOR PARLIAMENTARY RESEARCH SERVICES, BEKE, M., BERENSCHOT, L., DUTTA, S. *The European public health response to the COVID-19 pandemic : lessons for future cross-border health threats*. European Parliament, 2023. Dostupné na: https://data.europa.eu/doi/10.2861/459491

[26] REDAKCIA ČASOPISU ZO SÚDNEJ PRAXE. Ochrana osobných údajov a ochrana súkromia v novej legislatívnej kvalite. In *Zo súdnej praxe* 3/2018; BRAŽINOVÁ, A. a kol. Očkovanie v kontexte ochrany zdravia nielen v boji s pandémiou COVID-19 - Právne, etické a medicínske aspekty. In *Justičná revue*, 6-7/2022; ABELOVSKÝ, T. Virtualizácia ako metóda riešenia spoločenských problémov. In *Právny obzor*, 98, 2015, č.2, s. 164 – 177; CIBIK, S. Vývoj konceptu brániacej sa demokracie v slovenskom právnom poriadku. In *Právny obzor*, 106, 2023, č. 3, s. 189 – 201.

[27] MEDELSKÝ, J., LACA, N. *Dezinformácie a právo (úlohy a postavenie bezpečnostných zložiek)*. Zborník príspevkov. Bratislava. Akadémia Policajného zboru v Bratislave. 2022.

týkajúce sa kritického myslenia[28] a dôvodom dôvery v nepravdivé informácie.[29] Sekundárnymi zdrojmi boli prirodzene ďalšie referencie v identifikovanej literatúre. Možno uzavrieť, že téma dezinformácií nebola v Slovenskej republike z pohľadu regulačných nástrojov na zamedzenie ich šírenia komplexnejšie preskúmaná.

Predkladaná práca má už vo svojom názve definované tri limity výskumu. Prvým limitom výskumu je dôraz na nástroje verejného práva. Napriek tomu, že evidujeme stieranie rozdielov medzi verejným a súkromným právom,[30] fenomén dezinformácií podrobíme analýze prostredníctvom nástrojov, ktoré ponúka verejné právo. Ide o pragmatickú voľbu z dôvodu predpokladu, že verejné právo bude obsahovať systematickejšie nástroje pre ochranu spoločnosti pred dezinformáciami ako súkromné právo v podobe možnosti uplatňovania konkrétnych nárokov.[31] Druhým limitom je dôraz na nástroje verejného práva využiteľné v online priestore. Za online priestor považujeme prepojené digitálne prostredie, typicky popularizované prostredníctvom internetu.[32] Nebudeme sa v práci venovať tradičným médiám ako tlač a ich regulácií. Predmetná voľba bola urobená z toho dôvodu, že dezinformácie sa primárne šíria prostredníctvom internetu na sociálnych médiách a ich zásah prostredníctvom tradičných médií je slabší. Tretím limitom je dôraz na všeobecnejšiu reguláciu a jej nástroje ako na sektorovú alebo špecifickú reguláciu. Z toho dôvodu sa nebudeme obšírnejšie venovať regulácií politickej reklamy, činnosti a výrokom verejne činných osôb alebo regulácií slobodných médií (tradičnej žurnalistiky). Táto voľba bola urobená z toho dôvodu, že tieto otázky si zasluhujú osobitý prístup a predstavujú samostatný problém z pohľadu právneho výskumu. Napriek vyššie uvedeným limitom, na niektoré osobitosti budeme stručne poukazovať.

Pri skúmaní fenoménu dezinformácií z pohľadu nástrojov verejného práva sme si stanovili nasledujúcu výskumnú otázku:

Verejné právo poskytuje dostatok efektívnych nástrojov pre minimalizovanie šírenia a vplyvu dezinformácií v online priestore.

Vyššie uvedenú výskumnú otázku budeme skúmať s podporou niekoľkých hypotéz, ktoré nám pomôžu odpovedať na výskumnú otázku.

[28] MARKOŠ, J. *Sila rozumu v bláznivej dobe. Manuál kritického myslenia*. Bratislava: N Press, 2019.
[29] JURKOVIČ, M. – ČAVOJOVÁ, V. – BREZINA, I. *Prečo ľudia veria nezmyslom*. Bratislava: Pramedia, 2109.
[30] FÁBRY, B. – KASINEC. R. – TURČAN, M. *Teória práva*. 2. vydanie. Bratislava: Wolters Kluwer, 2019, s. 100 a nasl.
[31] Nebudeme sa v tejto práci zaoberať napríklad nárokmi vyplývajúcich z právnej úpravy ochrany osobnosti podľa § 11 a nasl. zákona č. 40/1964 Zb. Občiansky zákonník.
[32] Porovnaj DELFANTI, A. - ARVIDSSON, A. *Introduction to Digital Media*. Wiley, 2019, s. 150.

Prvá hypotéza sa zaoberá legálnou definíciou dezinformácie, ako základným predpokladom pre uplatnenie nástrojov verejného práva voči takémuto obsahu. Hypotéza je formulovaná nasledovným spôsobom:

Právny poriadok Slovenskej republiky alebo Európskej únie definuje pojem dezinformácia.

Druhá hypotéza sa týka samotných nástrojov verejného práva, ktoré môžu byť použité na minimalizáciu šírenia dezinformácií. S poukazom na limity explicitne komunikované vyššie, sme hypotézu formulovali nasledovným spôsobom:

Právny poriadok Slovenskej republiky alebo Európskej únie poskytuje nástroje na minimalizáciu šírenia dezinformácií v online priestore z pohľadu všeobecnej regulácie verejného práva.

Tretia hypotéza sa zameriava na skúmanie proporcionality a efektívnosti vybraných nástrojov ktoré môžu byť použité na minimalizáciu šírenia dezinformácií v online prostredí prostredníctvom noriem verejného práva. Skúmanie predmetnej hypotézy zahŕňa aj identifikovanie medzier a nedostatkov v legislatívne a návrhom na ich úpravu *de lege ferenda.* Hypotéza je formulovaná nasledovným spôsobom:

Právny poriadok Slovenskej republiky alebo Európskej únie poskytuje proporcionálne a efektívne nástroje na minimalizáciu šírenia dezinformácií v online priestore z pohľadu všeobecnej regulácie verejného práva.

Hypotézy budú postupne overované prostredníctvom jednotlivých kapitol predkladanej práce. Prvá kapitola sa venuje konceptu dezinformácií z pohľadu jeho zadefinovania, znakov, posudzovania ich vplyvu a faktorov, ktoré dôveru a šírenie dezinformácií ovplyvňujú. V rámci tejto kapitoly budú využité metódy analýzy, syntézy a komparácie. Základným zdrojom pre získanie poznatkov z tejto oblasti je štúdium dostupnej literatúry, právnej úpravy, politických deklarácií a dokumentov. V časti faktory ovplyvňujúce dôveru a šírenie dezinformácií sa zameriavame na psychologické, sociologické, ekonomické a technické faktory. Nie je ambíciou autora poskytnúť komplexný hĺbkový prehľad týchto faktorov vzhľadom na to, že ide o doménu iných vied. Pri definovaní kľúčových faktorov sme vychádzali z prehľadových štúdií a zhode v akademickej literatúre.

Druhá kapitola je venovaná politickým dokumentom na úrovní Európskej únie a Slovenskej republiky, ktoré zachytávajú trend šírenia dezinformácií a načrtávajú stratégie a konkrétne kroky pri boji štátu s týmto fenoménom. V rámci tejto kapitoly budú využité

metódy analýzy a syntézy. Cieľom tejto kapitoly je poskytnúť politický kontext pre prijímanie legislatívy, ktoré môže minimalizovať dôveru a šírenie dezinformácií.

Tretia kapitola je ťažisková a zameriava sa na kritickú analýzu nástrojov boja proti dezinformáciami v online priestore, ktoré poskytuje verejné právo. Zameriava sa na legislatívu Slovenskej republiky a Európskej únie. Predmetom skúmania bude regulácia sociálnych sietí, umelej inteligencie, ochrany osobných údajov, priestupkového práva, mediálneho práva, trestného práva a činnosti spravodajských služieb. V rámci tejto kapitoly budú využité metódy analýzy, syntézy, komparácie a dedukcie. Základným zdrojom pre získanie poznatkov z tejto oblasti je štúdium dostupnej literatúry, právnej úpravy, politických deklarácií a dokumentov. Zároveň upozorníme na nedostatky právnej úpravy v prípade ich identifikovania.

Štvrtá kapitola predstavuje diskusiu a odporúčania pri nastavovaní legislatívy, ktorá môže minimalizovať vplyv dezinformácií na spoločnosť. Na základe poznatkov získaných v predchádzajúcich kapitolách budeme definovať tri základné princípy, ktoré by mala takáto legislatíva rešpektovať. Taktiež dáme jednotlivé nástroje verejného práva do kontextu s princípom proporcionality v zmysle metodiky pre posudzovanie vplyvu dezinformácií. Prezentovať budeme aj návrhy *de lege ferenda*.

Predkladanú prácu uzatvára záver, ktorý zodpovie na výskumnú otázku a reflektuje vytýčené hypotézy. Práca obsahuje aj rozšírený záver v anglickom jazyku z dôvodu šírenia poznatkov aj v inom ako slovenskom jazyku.

1. KAPITOLA

DEZINFORMÁCIE A KONTEXT ICH ŠÍRENIA

Predkladaná práca sa zameriava na fenomén dezinformácií. Z tohto dôvodu považujeme za nevyhnutné tento pojem charakterizovať, či už z pohľadu spoločenských alebo humanitných vied, počítačových vied a právnej úpravy. Zameriame sa na strategické dokumenty na úrovni EÚ a SR, neopomenieme ani návrhy zákonov, ktoré mali ambíciu predmetný pojem legálne zadefinovať.

Kľúčovou časťou akejkoľvek regulácie je pôsobnosť právneho predpisu, ktorá sa často odvíja od definovania základných pojmov. Ak skúmame reguláciu dezinformácií, je nevyhnutné poukázať na to, že predmetný pojem nemá v slovenskom právnom poriadku svoju legálnu definíciu. Totožné konštatovanie platí aj v kontexte práva EÚ.

1.1. Doktrinálny prístup k definícii dezinformácie

Pred tým, ako analyzujeme pojem dezinformácia považujeme za vhodné uviesť, čo rozumieme pod termínom „informácia." Z hľadiska teórie informačnej bezpečnosti sa informáciou zachytávajú stavy subjektov, okolia či iných subjektov prípadne javov. Informácie môžu reflektovať rôzne metódy zapísania a jednou z týchto foriem zápisu je zápis prostredníctvom údajov. Tá istá informácia sa dá zapísať prostredníctvom rôznych údajov (napríklad informácia „sto" sa dá zaznamenať prostredníctvom slovného vyjadrenia alebo numerickou hodnotou v podobe rímskeho alebo arabského čísla). Rozdiel medzi týmito dvoma pojmami teda spočíva v tom, že *„údaje sú formou záznamu informácie a informácia je obsahom údajov.*[33] K takémuto ponímaniu sa hlási aj zahraničná právna doktrína.[34] Podobne aj filozofická doktrína označuje za informácie reprezentáciu určitého obsahu.[35] K potrebe charakterizovať a analyzovať potrebu pojmu dezinformácie sa prihlásil aj Floridi, nakoľko informácie môžu byť aj chybné.[36] Svetová zdravotnícka organizácia dokonca označila stav počas pandémie ako infodémiu, v zmysle ktorej tento fenomén predstavuje príliš veľa informácií vrátane nepravdivých alebo zavádzajúcich informácií v digitálnej a fyzickej podobe počas vypuknutia nebezpečne nákazlivej choroby COVID-19. Spôsobuje to zmätok a rizikové správanie, ktoré

[33] OLEJÁR, D. Krátky úvod do informačnej a kybernetickej bezpečnosti. In ANDRAŠKO, J. – GÁBRIŠ, T. – HOCHMANN, J. – OLEJÁR, D. *Zákon o kybernetickej bezpečnosti. Komentár*. Bratislava: Wolters Kluwer SR, 2018, s. 14-15.

[34] Pozri napr. BYGRAVE, L. Information Concepts in Law: Generic Dreams and Definitional Daylight. In *Oxford Journal of Legal Studies,* Vol. 35, No. 1 (2015), s. 95.

[35] Napríklad SCARANTINO, A. - PICCININI, G. Information without truth. In *Metaphilosophy*, 2021, 41(3), s. 313–330.

[36] FLORIDI, L. Brave.net.world: The internet as a disinformation superhighway? In *Electronic Library*, 14, 1996, 509–514.

môže poškodiť zdravie. Vedie tiež k nedôvere v zdravotnícke orgány a podkopáva verejnosť reakciu v oblasti zdravia.[37]

Slovo dezinformácia pochádza z ruského jazyka, kde sa udomácnilo počas fungovania Sovietskeho zväzu.[38] *Dezinformatsiya* v tomto pôvodnom ruskom znení znamenala *„nepravdivé, chybné alebo zavádzajúce informácie v úmyselnom, vedomom alebo účelovom úsilí uviesť do omylu, klamať alebo zmiasť."*[39] Svoje využitie nachádzali primárne pri štátnej propagande.[40] Slovník cudzích slov definuje dezinformáciu ako *„nesprávnu, vedome skreslenú informáciu."*[41] Slovník súčasného slovenského jazyka pristupuje k definícií iným spôsobom. Podľa tohto slovníka je dezinformácia *„nepravdivá, vedome skreslená informácia, ktorej cieľom je ovplyvniť určitú skupinu ľudí, prípadne celú populáciu."*[42]

Dezinformácie môžu mať rozmanitú podobu. Fallis[43] uvádza 6 podôb dezinformácií, ktoré kategorizuje nasledovným spôsobom:

1. Dezinformácie šírené štátom alebo ako vojenská aktivita;
2. Dezinformácie ako vopred plánovaná sofistikovaná operácia;
3. Šírenie dezinformácií prostredníctvom médií, ktoré preberajú nepravdivé tlačové správy;
4. Šírenie dezinformačných obrázkov ako sú mapy alebo manipulované fotografie;
5. Cielené šírenie dezinformácií na konkrétnu skupinu ľudí;
6. Dezinformácie cielené na oklamanie automatizovaného systému.[44]

Z prvotných doktrinálnych analýz pojmu dezinformácia z filozofie či informačnej vedy vyberáme diela Floridiho, Fetzera, Fallisa a Skyrmsa. Tieto konceptuálne analýzy pojmu poskytujú historický náhľad vo vývoj interpretácie predmetného termínu, ktorý výrazne

---

[37] WORLD HEALTH ORGANIZATION. Infodemic. WHO Website, 2021. Dostupné na: https://www.who.int/health-topics/infodemic#tab=tab_1.
[38] https://www.etymonline.com/word/disinformation
[39] FETZER, J. Disinformation: The Use of False Information. In *Minds and Machines*, 14(2), 2014, s. 231.
[40] HRČKOVÁ, A. - SRBA, I. - MÓRO, R. - BLAHO, R. - ŠIMKO, J. - NÁVRAT, P. - BIELIKOVÁ, M. Unravelling the basic concepts and intents of misbehavior in post-truth society. In *Bibliotecas. Anales de Investigación*; 15(3), 2019, s. 421-428. Dostupné na: http://revistas.bnjm.cu/index.php/BAI/article/view/109/110.
[41] *Slovník cudzích slov*. Dezinformácia. 2015. Dostupné na: https://slovnik.juls.savba.sk/?w=dezinform%C3%A1cia+&s=exact&c=B04a&cs=&d=scs#.
[42] *Slovník súčasného slovenského jazyka*. Dezinformácia. 2015. Dostupné na: https://slovnik.juls.savba.sk/?w=dezinformacia+&s=exact&c=a31c&cs=&d=sssj#.
[43] FALLIS, D. A Conceptual Analysis of Disinformation. In *iConference 2009 Papers*. Dostupné na: https://www.ideals.illinois.edu/items/15210.
[44] Tamže.

ovplyvnil vývoj informačných technológií. Floridi sa pojmu dezinformácia venoval v rámci troch štúdií publikovaných v rozsahu dvadsiatich rokov. V roku 1996 uviedol, že dezinformácie vznikajú vtedy, ak je proces informovania chybný.[45] Fallis kritizuje, že takto koncipovaná definícia zahŕňa aj náhodné klamstvá – úprimné chyby bez úmyslu zavádzať.[46] V roku 2005 Floridi svoju koncepciu dezinformácie upravil takým spôsobom, že za dezinformáciu považuje nesprávne informácie, ktorých zdroj je si nesprávnosti vedomý.[47] Problémom tohto konceptu je, že za dezinformácie považuje aj vtipy alebo sarkastické komentáre, o ktorých zdroj vie, že sú nesprávne, ale nemali by byť považované za dezinformácie.[48] Posledným Floridiho pokusom definovať dezinformácie je charakteristika tohto termínu z roku 2011 ako nesprávnych informácií, ktorých zdroj má v úmysle uviesť príjemcu do omylu.[49] Fallis k tejto definícií uvádza, že je príliš široká, nakoľko v sebe obsahuje aj nedôveryhodné (nereálne) klamstvá a pravdivé dezinformácie, a zároveň príliš úzka, keďže tento pojem v sebe nesubsumuje prípady bez úmyslu uviesť príjemcu do omylu.[50] O posledný prípad by išlo v prípade, ak by sa nesprávne informácie šírili za účelom vývoja kritického myslenia a vzdelania. Filozof Fetzer uvádza, že dezinformácia by mala byť vnímaná rovnako ako klamstvo. Podľa neho sú dezinformácie tvrdenia, o ktorých sa pôvodca domnieva, že sú nepravdivé, a ich cieľom je uviesť do omylu.[51] Takáto definícia už nezahŕňa vtipy a sarkastické komentáre. Na druhej strane však zahŕňa aj náhodné pravdy a nezahŕňa inú formu dezinformácií ako tvrdenia napríklad obrázky, videá alebo zvukové nahrávky.[52] Fallis v roku 2009 definoval dezinformácie ako *„zavádzajúce informácie, ktoré majú byť (alebo sa aspoň predpokladá, že budú) byť zavádzajúce."*[53] Túto neskoršiu koncepciu vo svojej ďalšej tvorbe označil ako príliš širokú, nakoľko zahŕňa aj jemné formy humoru ako satiru.[54] Zároveň uvádza, že dezinformácie sa môžu šíriť aj bez úmyslu zavádzať.[55] Skyrms pri výskume zavádzajúcich signálov u niektorých živočíšnych druhov skúma podobný koncept ako dezinformácie v biológií. V tomto kontexte by sme za dezinformácie

[45] FLORIDI, L. Brave.net.world: The internet as a disinformation superhighway? In *Electronic Library*, 14, 1996, 509.
[46] FALLIS, D. A Conceptual Analysis of Disinformation. In *iConference 2009 Papers*. Dostupné na: https://www.ideals.illinois.edu/items/15210.
[47] FLORIDI, L. Semantic conceptions of information. In *Stanford Encyclopedia of Philosophy*, 2015. Dostupné na: http://plato.stanford.edu/entries/information-semantic.
[48] FALLIS, D. A Conceptual Analysis of Disinformation. In *iConference 2009 Papers*. Dostupné na: https://www.ideals.illinois.edu/items/15210.
[49] Pozri FLORIDI, L. *The philosophy of information*. New York: Oxford University Press, 2011.
[50] FALLIS, D. A Conceptual Analysis of Disinformation. In *iConference 2009 Papers*. Dostupné na: https://www.ideals.illinois.edu/items/15210.
[51] FETZER, J. H. Disinformation: The use of false information. In *Minds and Machines*, 2(14), 2014 s. 231–240.
[52] FALLIS, D. A Conceptual Analysis of Disinformation. In *iConference 2009 Papers*. Dostupné na: https://www.ideals.illinois.edu/items/15210.
[53] Tamže.
[54] Tamže.
[55] Tamže.

označili zavádzajúce informácie, ktoré systematicky zvýhodňuje zdroj na úkor príjemcu.[56] Takto koncipovaná definícia by nezahŕňala aj tzv. altruistické dezinformácie t.j. také, z ktorých benefituje príjemca.[57] Podobne definuje pojem dezinformácie Wardle a Derakshan: *„informácie, ktoré sú zámerne nepravdivé, s úmyslom poškodiť ľudí ako sociálnu skupinu, alebo spoločnosť."*[58] Fallis uvádza tri znaky dezinformácie: (i) informácia, ktorá je (ii) nenáhodne (iii) zavádzajúca.[59] Pojem informácia z hľadiska informačnej bezpečnosti, práva či filozofie sme diskutovali vyššie. Druhým znakom je, že dezinformácia musí byť *nenáhodne* zavádzajúca. To znamená, že sa predpokladá určitý úmysel šíriť nepravdivú informáciu. Ide tak o iný princíp a koncept ako sú napríklad satira alebo úprimná chyba.[60] Kritérium zavádzania spočíva v tom, že šírenie takejto informácie má potenciál vytvárať falošné presvedčenie.[61] Fallis zároveň zvýrazňuje, že základnou funkciou dezinformácie je zavádzať.[62] Túto funkciou môže dezinformácia získať dvoma spôsobmi. Prvým je úmysel pôvodcu dezinformácie. Druhým spôsobom je systematický zvýhodňovanie pôvodcu dezinformácie napríklad pri šírení konšpiračných teórií.[63]

Z pohľadu právnej literatúry Van Hoboken a kolektív definujú štyri atribúty všeobecne akceptovanej definície dezinformácie a to konkrétne: pravdivosť alebo zavádzajúci charakter informácií, spoločenskú škodlivosť, úmysel aktéra a ekonomický zisk.[64] Bayer a kolektív k týmto atribútom pridáva aj to, že dezinformácia sa musí týkať veci verejného záujmu a je strategicky rozširovaná.[65] Zavádzajúci charakter dezinformácie sme diskutovali vyššie. Spoločenská škodlivosť dezinformácie môže spočívať v potenciálnej ujme pre jednotlivca, ale aj skupinu ľudí alebo štát. Najširším konceptom môže byť „verejná ujma," ktorá cieli na demokraciu a jej hodnoty.[66] Ekonomický úžitok ako atribút dezinformácie môže byť daný alternatívne práve s úmyselným zavádzaním verejnosti alebo spôsobením verejnej ujmy.[67]

---

[56] Pozri napríklad SKYRMS, B. *Signals: Evolution, Learning, and Information*. Oxford: Oxford University Press, 2010.
[57] FALLIS, D. A Conceptual Analysis of Disinformation. In *iConference 2009 Papers*. Dostupné na: https://www.ideals.illinois.edu/items/15210.
[58] WARDLE, C. – DERAKSHAN, H. *Information Disorder: Toward an interdisciplinary framework for research and policy making*. Council of Europe, report DGI (2017) 09, 2017, s. 20.
[59] FALLIS, D. What is Disinformation? In *Library Trends*, Volume 63, Number 3, Winter 2015, s. 404 – 406.
[60] Tamže, s. 406.
[61] Tamže.
[62] Tamže, s. 413.
[63] Tamže.
[64] VAN HOBOKEN, J. - Ó FATHAIGH, R. Regulating Disinformation in Europe: Implications for Speech and Privacy. In *UC Irvine Journal of International, Transnational, and Comparative Law*, 2021, 6, s. 9–36.
[65] BAYER, J. et al. *Disinformation and propaganda: impact on the functioning of the rule of law and democratic processes in the EU and its Member States - 2021 update*. Dostupné na: https://www.europarl.europa.eu/thinktank/en/document/EXPO_STU(2021)653633.
[66] Ó FATHAIGH, R. - HELBERGER, N. - APPELMAN, N. The perils of legally defining disinformation. In *Internet Policy Review*, 2021, 10(4). https://doi.org/10.14763/2021.4.1584, s. 5.
[67] Tamže, s. 9.

Dezinformácia je pojem častokrát zamieňaný s inými konceptami ako falošné správy (*fake news*), hoax, nepodložená správa (*rumor*), misinformácia, názorový spam (*opinion spam*) alebo satira. Prehľadová štúdia v počítačových vedách uvádza stručnú definíciu dezinformácie ako *„úmyselne klamlivé informácie s vopred definovaným zámerom*"[68] s cieľom prezentovania určitého presvedčenia alebo myšlienky, finančného profitu alebo pošpinenia verejnej mienky o konkrétnej osobe.[69] Na rozlíšenie pojmov informácia, dezinformácia a misinformácia doktrína využíva 5 faktorov, ktoré vyhodnocuje. Konkrétne pravdivosť, presnosť, úplnosť, aktuálnosť a klamlivosť.[70] K týmto faktorom odborná literatúra ďalej pridáva médium, úmysel a analyzovateľnú jednotku.[71] Práve úmysel zavádzať alebo klamať je kľúčovým pre rozlíšenie medzi dezinformáciou a misinformáciou. Pri dezinformácií je úmysel zavádzať alebo klamať prítomný. Naopak, pri misinformáciach absentuje.[72] Tento aspekt sa zvýrazňuje aj v odbornej literatúre z počítačových vied.[73] Misinformácie vznikajú organicky, ľudskou chybou.

Ďalším často zamieňaným pojmom sú falošné správy. Gelfert falošné správy klasifikuje ako druh dezinformácií a definuje ich ako *„úmyselné vydávanie (typicky) falošných alebo zavádzajúcich tvrdení za spravodajstvo, pričom tvrdenia sú schválne zavádzajúce.*"[74] Determinantom je vydávanie informácií za autentické spravodajstvo.[75]

Dezinformácie sú voľne interpretované v právnej literatúre na základe troch perspektív:

- Perspektíva obsahu sa zaoberá klasifikáciou nepravdivých alebo zavádzajúcich informácií, čo je oblasť, ktorá je významne regulovaná;

[68] MEEL, P. - VISHWAKARMA, D. K. Fake news, rumor, information pollution in social media and web: A contemporary survey of state-of-the-arts, challenges and opportunities. In *Expert Systems with Applications*. 2020. Vol. 153, s. 112986. DOI 10.1016/j.eswa.2019.112986.
[69] Tamže.
[70] KARLOVA, N. – FISHER, K. A social diffusion model of misinformation and disinformation for understanding human information behaviour. In *Information Research 18.1* (2013).
[71] HRČKOVÁ, A. - SRBA, I. - MÓRO, R. - BLAHO, R. - ŠIMKO, J. - NÁVRAT, P. - BIELIKOVÁ, M. Unravelling the basic concepts and intents of misbehavior in post-truth society. In *Bibliotecas. Anales de Investigación*; 15(3), 2019, s. 421-428. Dostupné na: http://revistas.bnjm.cu/index.php/BAI/article/view/109/110.
[72] MEEL, P. - VISHWAKARMA, D. K. Fake news, rumor, information pollution in social media and web: A contemporary survey of state-of-the-arts, challenges and opportunities. In *Expert Systems with Applications*. 2020. Vol. 153, s. 112986. DOI 10.1016/j.eswa.2019.112986.
[73] KUMAR, S. - SHAH, N. *False information on web and social media: A survey*. arXiv preprint. 2021. Dostupné na: arXiv:1804.08559.
[74] GELFERT, A. Fake News: A Definition. In *Informal Logic*, Vol.38, No.1, 2018, s. 84–117. Preklad prevzatý z MESARČÍK, M. a kol. *Analysis of selected regulations proposed by the European Commission and technological solutions in relation to the dissemination of disinformation and the behaviour of online platforms*. 2022. Dostupné na: https://kinit.sk/sk/publikacia/dissemination-of-disinformation-and-the-behaviour-of-online-platforms/.
[75] Zhodne MEEL, P. - VISHWAKARMA, D. K. Fake news, rumor, information pollution in social media and web: A contemporary survey of state-of-the-arts, challenges and opportunities. In *Expert Systems with Applications*. 2020. Vol. 153, s. 112986. DOI 10.1016/j.eswa.2019.112986.

- Perspektíva účastníkov reflektuje dezinformácie z hľadiska subjektov, ktoré ich šíria, ako napríklad tretie krajiny, ktoré majú záujem o destabilizáciu demokratického systému;
- Tretí pohľad sa zameriava na šírenie a rôzne techniky, ktoré zvyšujú efektivitu distribúcie dezinformácií.[76]

Dezinformácie nemusia spôsobovať škodu priamo, ale môžu mať aj nepriame negatívne vplyvy. Ide predovšetkým o prípady erózie dôvery, ktorá narušuje schopnosť jednotlivcov vymieňať si informácie navzájom.[77]

V tomto kontexte považujeme za nevyhnutné spomenúť aj informačné operácie s cieľom ovplyvniť spoločnosť vykonávané tretími krajinami a zasahovanie zo zahraničia. Pojem *„informačné operácie pokrýva široké spektrum aktivít a spôsobov, ktoré slúžia na zber a šírenie potenciálne škodlivých informácií. Na dosiahnutie týchto cieľov slúžia napr. dezinformácie, využívanie falošných identít a manipulatívnych techník na internete či zneužívanie technológií."*[78]

Operácie s cieľom ovplyvniť spoločnosť bývajú koordinované s cieľom ovplyvniť publikum v konkrétnej krajine prostredníctvom nelegitímnych a klamlivých prostriedkov za účelom posilniť pozitívnu väzbu voči tretej krajine.[79] Dezinformácie sú častokrát jedným z takýchto prostriedkov. Zasahovanie zo zahraničia je o stupeň invazívnejšie a predstavuje nátlakové, klamlivé prípadne netransparentné snahy tretej krajiny alebo jeho zástupcov s cieľom narušiť slobodné formovanie a vyjadrenie politickej vôle napríklad vo voľbách alebo krízových situáciách.[80] V tomto nastavení už môžeme hovoriť o hybridnej hrozbe. Hybridné hrozby je široký zastrešujúci pojem,[81] ktorý zahŕňa mnoho typov aktivít od narušovania,

[76] HOBOKEN VAN, J. - Ó FATHAIGH, R. Regulating Disinformation in Europe: Implications for Speech and Privacy. In *UC Irvine Journal of International, Transnational, and Comparative Law*. Volume 6 Symposium: The Transnational Legal Ordering of Privacy and Speech. Article 3, 2021, s. 13.
[77] FALLIS, D. What is Disinformation? In *Library Trends*, Volume 63, Number 3, Winter 2015, s. 402.
[78] ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY. *Koordinovaný mechanizmus odolnosti Slovenskej republiky voči informačným operáciám*, s. 5.
[79] PAMMENT, J. *The EU's Role in Fighting Disinformation: Taking Back the Initiative*. Carnegie Endowment for International Peace, 2020, s. 16-17.
[80] Tamže.
[81] Národný bezpečnostný úrad definuje hybridné hrozby ako *„Súbor nátlakových a podvratných činností, konvenčných a nekonvenčných, vojenských a nevojenských metód, ktoré môžu štátne aj neštátne subjekty koordinovaným spôsobom využívať na dosiahnutie konkrétnych cieľov bez formálneho vyhlásenia vojny. Hybridná hrozba je charakteristická simultánnym použitím viacerých nástrojov koordinovaným spôsobom s cieľom využiť zraniteľnosti (slabé miesta) protivníka a následne oslabiť jeho rozhodovacie procesy pri zachovaní určitého stupňa hodnoverného popretia. Strategickým cieľom týchto hrozieb je oslabenie dôvery verejnosti v demokratické inštitúcie, prehĺbenie nezdravej polarizácie na národnej a medzinárodnej úrovni, spochybnenie základných hodnôt demokratických spoločností, zisk geopolitického vplyvu a moci prostredníctvom poškodzovania ostatných a ovplyvňovania demokratických rozhodovacích procesov."* NÁRODNÝ BEZPEČNOSTNÝ ÚRAD. *Krátky slovník hybridných hrozieb*. Dostupné na: https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/kratky-slovnik-hybridnych-hrozieb/index.html.

budovania vplyvu, operácií, rôznych kampaní a vojny. Koncepcia pre boj Slovenskej republiky s hybridnými hrozbami tento pojem definuje ako *„súbor nátlakových a podvratných činností, konvenčných a nekonvenčných, vojenských a nevojenských metód, ktoré môžu štátne aj neštátne subjekty koordinovaným spôsobom využívať na dosiahnutie konkrétnych cieľov bez formálneho vyhlásenia vojny a pod prahom zvyčajnej reakcie."*[82]

Všetky tieto činnosti možno považovať za nežiaduce zásahy do vnútorného priestoru štátu. Pojem hybridné hrozby, tak ako je vnímaný v západnej kultúre je používaný na diskusiu o bezpečnostných dilemách, ktorej čelia štáty a ktoré majú buď demokratický systém, alebo sú v fáze demokratizácie.[83] Prirodzene, nie všetky dezinformácie sú súčasťou snáh o ovplyvnenie nálad alebo politickej vôle smerujúcich z tretích krajín. Aspekt dezinformácií ak súčasti hybridnej vojny však nemôžeme pri analýze právnych nástrojov opomenúť, nakoľko šírenie dezinformácií je možne považovať za hybridnú hrozbu z toho dôvodu, že *„podrývajú dôveru občanov v demokratické inštitúcie a demokratické procesy a šíria nenávistnú ideológiu."*[84]

1.2. Dezinformácie v právnych a strategických dokumentoch na úrovni EÚ

Absencia účinnej legálne definície pojmu dezinformácie ale neznamená, že neexistujú politické alebo odborné definície dezinformácie. Ak sa pozrieme do politických deklarácií a dokumentov na úrovní EÚ, môžeme v nich nájsť viacero definícií pojmu dezinformácia.

Európska komisia v roku 2018 vydala oznámenie týkajúce sa európskeho prístupu k boju s dezinformáciami, kde tento termín definuje nasledovne: *„Za dezinformáciu sa považuje overiteľne nepravdivá alebo zavádzajúca informácia, ktorá je vytvorená, prezentovaná a šírená na účely hospodárskeho zisku alebo zámerného zavádzania verejnosti, a môže poškodiť verejný záujem. Poškodenie verejného záujmu zahŕňa ohrozenie demokratických procesov a procesy tvorby politiky, ako aj verejných statkov, ako napr. ochrany zdravia občanov EÚ, životného prostredia alebo bezpečnosti. Medzi dezinformácie nepatria chyby v spravodajstve, satira a*

[82] *Koncepcia pre boj Slovenskej republiky proti hybridným hrozbám* schválená uznesením vlády SR č. 345 zo dňa 11. júla 2018.
[83] EUROPEAN COMMISSION, JOINT RESEARCH CENTRE, GIANNOPOULOS, G., SMITH, H., THEOCHARIDOU, M., THE LANDSCAPE OF HYBRID THREATS : A CONCEPTUAL MODEL : PUBLIC VERSION, GIANNOPOULOS, G.(EDITOR), SMITH, H.(EDITOR), THEOCHARIDOU, M.(EDITOR). Publications Office of the European Union, 2021. Dostupné na: https://data.europa.eu/doi/10.2760/44985.
[84] IVANČÍK, R. Dezinformácie ako hybridná hrozba. In MEDELSKÝ, J., LACA, N. 2022. *Dezinformácie a právo (úlohy a postavenie bezpečnostných zložiek).* Zborník príspevkov. Bratislava. Akadémia Policajného zboru v Bratislave, s. 58.

paródie, ani správy a komentáre naklonené jednej strane, ktoré sú takto zreteľne označené."[85] Predmetnú definíciu preberá aj Akčný plán Európskej komisie pre boj s dezinformáciami.[86]

Podobne definuje pojem dezinformácia aj Správa expertnej skupiny na vysokej úrovni o falošných správach a dezinformáciách v online prostredí. Za dezinformáciu správa považuje nepravdivé, nepresné alebo zavádzajúce informácie navrhnuté, prezentované a propagované s cieľom úmyselne spôsobiť spoločenskú škodu alebo za účelom zisku.[87] Definíciu dezinformácie v pozitívnom a negatívnom zmysle upravuje aj Kódex nakladania s dezinformáciami.[88] Predmetný kódex dezinformáciu definuje ako *„overiteľne nepravdivú alebo zavádzajúcu informáciu."*[89] Na naplnenie definície musia byť prítomné ešte ďalšie dva atribúty. Prvý sa týka požiadavky hospodárskeho zisku alebo zámerného zavádzania verejnosti, ktoré sú účelom ich vytvorenia, prezentovania alebo šírenia. Druhý atribút vyžaduje poškodenie verejného záujmu,[90] *„keďže jej ciele zahŕňajú „ohrozenie demokratických procesov a procesy tvorby politiky, ako aj verejných statkov, ako napr. ochrany zdravia občanov EÚ, životného prostredia alebo bezpečnosti."*[91] Negatívna definícia dezinformácie vymedzuje, čo nezahŕňame pod daný pojem. Konkrétne ide o *„klamlivú reklamu, chyby v spravodajstve, satiru a paródie ani správy a komentáre naklonené jednej strane, ktoré sú takto zreteľne označené, a nemá vplyv na platné právne predpisy, samoregulačné kódexy v oblasti reklamy a normy týkajúce sa klamlivej reklamy."*[92] Revidovaná verzia kódexu z roku 2022 už iba odkazuje na definíciu z Akčného plánu Európskej komisie pre boj s dezinformáciami.

1.3. Dezinformácie v právnych a strategických dokumentoch na úrovni SR

V rámci Slovenskej republiky sa opätovne musíme oprieť iba o strategické dokumenty politického charakteru. Koordinovaný mechanizmus odolnosti Slovenskej republiky voči informačným operáciám obsahuje nasledovnú definíciu: *"Dezinformácia – označuje nepravdivú*

---

[85] EURÓPSKA KOMISIA. *Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a výboru regiónov. Boj proti dezinformáciám na internete: európsky prístup*. COM/2018/236 final. Dostupné na: https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX%3A52018DC0236.

[86] EURÓPSKA KOMISIA. *Spoločné oznámenie Európskemu parlamentu, Európskej rade, Rade, Európskemu hospodárskemu a sociálnemu výboru a výboru regiónov. Akčný plán proti dezinformáciám*. JOIN/2018/36 final. Dostupné na: https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX%3A52018JC0036.

[87] HIGH LEVEL GROUP ON FAKE NEWS AND ONLINE DISINFORMATION. *A multi-dimensional approach to disinformation. Report of the independent High level Group on fake news and online disinformation*. 2018, s. 10. Originálne znenie: *"...false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit."* Dostupné na: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=50271.

[88] *Kódex nakladania s dezinformáciami*. 2018. Dostupné na: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=59125.

[89] Tamže, s. 1.

[90] K pojmu verejný záujem pozri VRABKO, M. a kol. *Správne právo hmotné*. 2. vydanie. Praha: C.H. Beck, 2018.

[91] *Kódex nakladania s dezinformáciami*. 2018, s. 1. Dostupné na: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=59125.

[92] Tamže.

alebo zmanipulovanú informáciu, ktorá je šírená zámerne s cieľom zavádzať a uškodiť. Dezinformácie môžu mať podobu nepravdivého alebo zmanipulovaného textu, obrázku, videa alebo zvuku, pričom môžu byť použité na podporu konšpirácií, šírenie pochybností a diskreditáciu pravdivých informácií či jednotlivcov a organizácií. Aj pravdivú informáciu môžeme považovať za dezinformáciu, ak je podaná manipulatívnym spôsobom. Medzi dezinformácie nepatria neúmyselné chyby v spravodajstve, satira, paródia ani správy a komentáre naklonené jednej strane, ktoré sú takto zreteľne označené."[93] Bezpečnostná stratégia Slovenskej republiky[94] či Koncepcia Slovenskej republiky pre boj proti hybridným hrozbám[95] síce šírenie dezinformácií výslovne spomínajú na viacerých miestach, ale samotný termín nedefinujú. Krátky slovník Národného bezpečnostného úradu SR dezinformáciu definuje ako *„overiteľne nepravdivú, zavádzajúcu alebo manipulatívne podanú informáciu, ktorá je zámerne vytvorená, prezentovaná a šírená s jednoznačným úmyslom klamať alebo zavádzať, spôsobiť nejakú ujmu alebo zabezpečiť nejaký zisk (napríklad hospodársky či politický). Dezinformácia často obsahuje element, ktorý je zjavne pravdivý, čo jej dodáva na dôveryhodnosti a môže tak skomplikovať jej odhalenie. Medzi dezinformácie nepatria neúmyselné chyby v spravodajstve, satira a paródie, ani správy a komentáre naklonené jednej strane, ktoré sú takto zreteľne označené."*[96]

Pre komplexnosť je potrebné uviesť, že slovenský Trestný zákon obsahuje viacero pojmov, ktoré sa s dezinformáciami častokrát zamieňajú. Ako príklad možno uviesť termíny nepravdivá informácia, nepravdivý údaj alebo poplašná správa. Trestný čin ohrozenia bezpečnosti vzdušného dopravného prostriedku a lode upravuje skutkovú podstatu, v zmysle ktorej *„kto oznámi **nepravdivú informáciu**, ktorá môže ohroziť bezpečnosť alebo prevádzku vzdušného dopravného prostriedku za letu alebo lode za plavby, potrestá sa odňatím slobody až na tri roky."*[97] S pojmom nepravdivá informácia operuje aj trestný čin teroristického útoku: *„kto v úmysle poškodiť ústavné zriadenie alebo obranyschopnosť štátu, narušiť alebo zničiť základnú politickú, hospodársku alebo spoločenskú štruktúru štátu alebo medzinárodnej organizácie, závažným spôsobom zastrašiť obyvateľstvo alebo donútiť vládu štátu alebo iný orgán verejnej moci alebo medzinárodnej organizácie, aby niečo konala, opomenula alebo strpela... zmocní sa lietadla, lode, iného prostriedku osobnej dopravy alebo...**oznámi nepravdivú informáciu**, čím*

[93] *Koordinovaný mechanizmus odolnosti Slovenskej republiky voči informačným operáciám*. Dostupné na slov-lex.sk.
[94] *Bezpečnostná stratégia Slovenskej republiky*. Dostupné na: https://www.nbu.gov.sk/wp-content/uploads/urad/Bezpecnostna-strategia-SR-2021.pdf.
[95] *Koncepcia pre boj Slovenskej republiky proti hybridným hrozbám*. Dostupné na: https://www.nbu.gov.sk/wp-content/uploads/PHHD/Koncepcia-boja-SR-proti-hybridnym-hrozbam.pdf.
[96] NÁRODNÝ BEZPEČNOSTNÝ ÚRAD SR. *Krátky slovník hybridných hrozieb*. Dostupné na: https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/kratky-slovnik-hybridnych-hrozieb/index.html.
[97] Trestný zákon, § 292.

ohrozí život alebo zdravie ľudí, bezpečnosť takého dopravného prostriedku."[98] Pojem nepravdivá informácia komentárová literatúra definuje ako akúkoľvek informáciu, *„ktorá nezodpovedá skutočnosti alebo informácia skreslená do takej miery, že je spôsobilá ohroziť bezpečnosť alebo prevádzku vzdušného dopravného prostriedku za letu alebo lode za plavby.*"[99]

Ďalším príkladom je trestný čin šírenia poplašnej správy: *„kto úmyselne spôsobí nebezpečenstvo vážneho znepokojenia aspoň časti obyvateľstva nejakého miesta tým, že rozširuje poplašnú správu, ktorá je nepravdivá, alebo sa dopustí iného obdobného konania spôsobilého vyvolať také nebezpečenstvo, potrestá sa odňatím slobody až na dva roky.*"[100] Za poplašnú správu komentárová literatúra považuje takú správu, *„ktorá nezodpovedá realite, je zavádzajúca a nezakladá sa na pravde, pričom je schopná vyvolať paniku, pocit strachu, neistoty a pod.*"[101] Trestný čin ohovárania zasa operuje s termínom nepravdivý údaj: *„kto o inom oznámi nepravdivý údaj, ktorý je spôsobilý značnou mierou ohroziť jeho vážnosť u spoluobčanov, poškodiť ho v zamestnaní, v podnikaní, narušiť jeho rodinné vzťahy alebo spôsobiť mu inú vážnu ujmu, potrestá sa odňatím slobody až na dva roky.*"[102] Za nepravdivé údaje možno považovať *„také tvrdenie páchateľa, ktoré je objektívne v rozpore s realitou, t. j. nezhoduje sa so skutočnosťou.*"[103]

Zákon o kybernetickej bezpečnosti ustanovoval možnosť Národného bezpečnostného úradu SR blokovať webové sídla, ktoré obsahovali škodlivý obsah. Rozhodnutia o blokovaní strácali platnosť 30. septembra 2022. Medzi škodlivý obsah právna úprava zaraďovala aj „závažné dezinformácie."[104] Právna úprava nedefinovala tento pojem a dôvodová správa taktiež neobsahuje žiadny návod, ako pri výklade pojmu závažná dezinformácia postupovať.

1.3.1 Návrhy právnych úprav

V Slovenskej republike boli v ostatnom období prezentované viaceré návrhy zákonov, ktoré operujú s pojmami dezinformácia prípadne súvisiacimi termínmi. V rámci novely Trestného zákona mala byť zakotvená skutková podstata trestného činu šírenia nepravdivých informácií.[105] Cieľom zákonodarcu bolo reagovať na zamorenie informačného priestoru

[98] Trestný zákon, § 419 .
[99] STRÉMY, T. – KURILOVSKÁ, L. *Trestný zákon. Komentár Zväzok II*. Wolters Kluwer, 2022, s. 896.
[100] Trestný zákon, § 361.
[101] STRÉMY, T. – KURILOVSKÁ, L. *Trestný zákon. Komentár Zväzok II*. Wolters Kluwer, 2022, s. 1219.
[102] Trestný zákon, § 373
[103] STRÉMY, T. – KURILOVSKÁ, L. *Trestný zákon. Komentár Zväzok II*. Wolters Kluwer, 2022, s. 1245.
[104] § 27b ods. 3 Zákona o kybernetickej bezpečnosti. *„Škodlivým obsahom sa rozumie 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.*"
[105] *LP/2021/744*. Zákon, ktorým sa mení a dopĺňa zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov a o zmene a doplnení niektorých zákonov.

dezinformáciami počas pandémie COVID-19.[106] Návrh právnej úpravy pojem nepravdivá informácia nedefinoval. Na základe navrhovanej skutkovej podstaty tohto trestného činu (ktorá bude predmetom analýzy v osobitnej kapitole) sa domnievame, že tu absentovalo kritérium konkrétneho úmyslu dezinformácie, najmä v podobe finančného zisku alebo spoločenskej škody. V zmysle navrhovanej úpravy postačí spôsobilosť vyvolania nebezpečenstva vážneho znepokojenia, ovplyvnenie obyvateľstva pri jeho rozhodovaní i závažných otázkach celospoločenského významu alebo ohrozenie zdravia a života ľudí. Takto koncipovaná skutková podstata je výrazne širšia a nezahŕňala by iba dezinformácie, ale aj misinformácie, keďže osobitne upravuje aj nedbanlivostné zavinenie.[107]

Na druhej strane, návrh zákona o opatreniach na zvýšenie bezpečnosti a dôveryhodnosti platforiem v on-line prostredí obsahuje priamo legálnu definíciu dezinformácie v § 2 ods. 1: *„Dezinformáciou sa na účely tohto zákona rozumie celkom zjavne nepravdivá informácia, ktorá je vytvorená, prezentovaná a šírená s cieľom klamať verejnosť, alebo určitú skupinu osôb a má, alebo môže mať za následok spôsobenie škody, alebo ujmy alebo zabezpečenie prospechu.*" Oproti definíciám uvedených v predchádzajúcich statiach, slovenský zákonodarca vyžaduje „zjavnosť" nepravdivej informácie. Predmetná požiadavka môže naraziť na rôzne interpretácie pri správnych alebo súdnych konaniach. Politické dokumenty na úrovni EÚ v niektorých prípadoch vyžadujú splnenie požiadavky „overiteľnosti." Táto formulácia sa javí ako vhodnejšia a zároveň reflektuje ciele zákonodarcu.[108] Navrhovaná právna úprava zároveň definuje aj dezinformačnú aktivitu ako vytváranie, prezentovanie alebo šírenie dezinformácií.[109]

Ako však uviedol špeciálny spravodajca Organizácie spojených národov pre slobodu prejavu, z hľadiska legálneho definovania dezinformácie ide o mimoriadne ťažko legálne definovateľný pojem, ktorý môže orgánom verejnej moci poskytnúť vysokú mieru voľnosti pri určovaní toho, čo je dezinformácia, čo je omyl a čo je pravda.[110]

---

[106] *Dôvodová správa k zákonu, ktorým sa mení a dopĺňa zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov a o zmene a doplnení niektorých zákonov*. Dostupné na: https://www.slov-lex.sk/legislativne-procesy/-/SK/dokumenty/LP-2021-744.

[107] *LP/2021/744*. Zákon, ktorým sa mení a dopĺňa zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov a o zmene a doplnení niektorých zákonov.

[108] Tamže. *„Definícia dezinformácie na účely návrhu zákona sa navrhuje založiť na troch podmienkach. Prvou je charakter informácie – musí ísť o informáciu celkom zjavne nepravdivú, bude sa teda skúmať pravdivosť informácie.*"

[109] Návrh dezinfo zákona, § 2 ods. 2.

[110] JOINT DECLARATION ON FREEDOM OF EXPRESSION AND "FAKE NEWS", DISINFORMATION AND PROPAGANDA. Organization for Security and Co-operation in Europe. 2017. Dostupné na: https://www.osce.org/fom/302796.

1.3.1 Pojem dezinformácia v judikatúre slovenských súdov

S úsvitom súdnych konaní, ktoré sa týkajú ohovárania, nenávistných prejavov či šírenia nepravdivých informácií začala s pojmom dezinformácia pracovať aj judikatúra slovenských súdov. Túto rovinu nemôžeme v práci opomenúť, nakoľko aj súdna prax výrazne pomáha formovať interpretáciu právnych noriem.

Z metodologického hľadiska sme zvolil výskum cez webový portál judikaty.info, ktorý v sebe integruje súdne rozhodnutia Najvyššieho súdu SR, Najvyššieho správneho súdu SR, Ústavného súdu SR a krajských súdov SR. Rozhodnutia okresných súdov sme hľadali prostredníctvom portálu obcan.justice.sk, ktorý prevádzkuje Ministerstvo spravodlivosti Slovenskej republiky. Po zadaní kľúčového slova „dezinformácia" portál vyhľadával aj jazykové odvodeniny daného slova v súdnych rozhodnutiach vyššie uvedených súdov. Výsledky sú nasledujúce:[111]

Súd	Počet nájdených rozhodnutí
Najvyšší súd SR	17
Najvyšší správny súd SR	1
Ústavný súd SR	11
Krajské súdy	77
Okresné súdy	207

Tabuľka: Výsledky vyhľadávania súdnych rozhodnutí obsahujúcich pojem dezinformácia na portály judikaty.info.
Zdroj: judikaty.info a obcan.justice.sk.

Nie všetky vyššie uvedené rozhodnutia súdov však definujú alebo pracujú so samotným pojmom dezinformácia. Vo väčšine prípadov sa dezinformácie spomínajú skôr ako súčasť skutkovej podstaty prejednávaného prípadu bez hlbšej analýzy predmetného pojmu. Napriek tomu poskytuje judikatúra slovenských súdov zaujímavé závery.

Ústavný súd SR vo svojom rozhodnutí III. ÚS 288/2017[112] rozlišuje medzi dezinformáciami a nepravdami. V rozhodnutí týkajúcom sa moratória na zverejňovanie prieskumov verejnej mienky badať rozlišovanie medzi dezinformáciami a účelovými informáciami.[113] V totožnom rozhodnutí aj Ústavný súd upozorňuje na absenciu legálnej definície dezinformácie.[114] Rozhodnutia Najvyššieho súdu SR a Najvyššieho správneho súdu neposkytujú analytickejšiu

[111] Údaje sú aktuálne k 30.6.2023.
[112] Nález Ústavného súdu SR, sp. zn. III. ÚS 288/ zo dňa 05.12.2017.
[113] Nález Ústavného súdu SR, sp. zn. PL. ÚS 26/2019 zo dňa 26.05.2021.
[114] Tamže, bod 107.

sondu do termínu dezinformácia a súvisiacich pojmov. Identifikované rozhodnutia krajských súdov SR sa definíciou dezinformácie taktiež nezaoberali. Skúmané rozhodnutia okresných súdov sa k pojmu dezinformácia taktiež nevyjadrujú.

1.4. Metodika posudzovania škodlivosti dezinformácií

Napriek tomu, že právny poriadok explicitne nevymedzuje pojem dezinformácie, v strategických dokumentoch SR možno nájsť návrhy metodických prístupov k hodnotenie prvkov informačných operácií, kde možno dezinformácie s určitosťou zaradiť. Koordinovaný mechanizmus odolnosti Slovenskej republiky voči informačným operáciám stanovuje 14 kritérií, ktoré by orgány verejnej moci mali vyhodnocovať v kontexte šírenia dezinformácií. Konkrétne ide o:[115]

Kritérium	Charakteristika kritéria
Potenciál spôsobiť škodu	Manipulatívnosť, polarizácia spoločnosti, ľudské zdravie, hospodárske škody, princípy právneho štátu, dôveryhodnosť štátu),
Existencia potenciálu vyvolať akciu	Nenásilná, násilná, masový nepokoj
Veľkosť skupiny, ktorá by mohla byť prvkom informačnej operácie ovplyvnená	Jednotlivec, malá skupina, veľká skupina, celá populácia
Pôvodca prvku informačnej operácie	Jednotlivec, skupina, riziková skupina, neštátna organizácia, štátna organizácia, štátny predstaviteľ
Významnosť vplyvu statusu adresáta, potenciál amplifikácie	Bežný občan, člen rizikovej skupiny, všeobecne uznávaná osobnosť, štátny úradník, štátny predstaviteľ
Miera pravdepodobnosti ovplyvnenia adresáta, na ktorého je prvok informačnej operácie zameraný	Obsahová kvalita PIO - spôsobilosť presvedčiť adresáta
Dôveryhodnosť prvku informačnej operácie	Nízka, stredná alebo vysoká. Podrobnosti ustanovuje Príloha č. 1 Koordinovaného mechanizmus odolnosti Slovenskej republiky voči informačným operáciám
Koordinácia šírenia prvku informačnej operácie	Neorganizovaná/organizovaná

[115] ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY. *Koordinovaný mechanizmus odolnosti Slovenskej republiky voči informačným operáciám*, s. 11 – 12.

Kanál prvku informačnej operácie z hľadiska presvedčivosti	Ústny, sociálne siete, webové sídlo, printové médium, audio vizuálne médium
Šíriteľ prvku informačnej operácie	Jednotlivec, skupina, riziková skupina, neštátna organizácia, štátna organizácia, štátny predstaviteľ
Geografický zdroj prvku informačnej operácie	Zahraničný, domáci
Charakteristika konania vykazujúceho znaky trestného činu	Ohováranie, šírenie poplašnej správy, podnecovanie rasovej, náboženskej alebo inej neznášanlivosti
Existencia neutralizačných mechanizmov	Existuje/neexistuje možnosť prijať protiopatrenia
Iné významné okolnosti	Načasovanie, súbeh s inými prvkami hybridných hrozieb a pod.

Tabuľka: Kritéria posudzovania vplyvu informačnej operácie.
Zdroj: Koordinovaný mechanizmus odolnosti Slovenskej republiky voči informačným operáciám.

Následne, po vykonaní kvalitatívnej a kvantitatívnej analýzy nebezpečnosti dezinformácie je determinovaná úroveň vplyvu prvku informačnej operácie. Vplyv môže byť nepatrný, znepokojujúci, vysoký alebo kritický:[116]

Vplyv	Príklad
Nepatrný	Pravdepodobnosť akýchkoľvek dôsledkov z prvku informačnej operácie je mizivá, môže dochádzať k neúmyselným chybám, nedorozumeniam v komunikácii. Šíreniu prvkov informačnej operácie možno zamedziť faktami.
Znepokojujúci	Hrozia nepriaznivé následky alebo vytváranie priestoru pre šírenie prvkov informačnej operácie, môže hroziť poškodenie zdravia jednotlivcov alebo skupín, ohrozenie osobnej dôstojnosti a vážnosti, riziko porušenia právneho poriadku. Často dochádza k neorganizovanej koordinácii pri ich šírení.
Vysoký	Šíriteľom je zväčša známa osoba, verejný činiteľ, veľká skupina osôb. Existuje vysoká pravdepodobnosť pre vznik nepriaznivej udalosti s negatívnym dopadom na dôveryhodnosť štátnych orgánov.
Kritický	Vysoká koncentrácia šírenia prvkov informačnej operácie, šíriteľom je verejný činiteľ, štátna inštitúcia. Vysoká

[116] Tamže, s. 12.

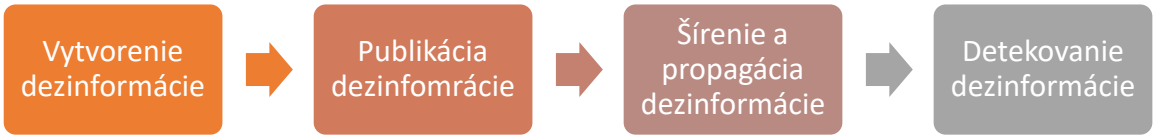
	pravdepodobnosť negatívnych dôsledkov vrátane ohrozenia bezpečnosti štátu, významného strategického záujmu štátu vysoké hospodárske škody, ohrozená je zvrchovanosť, územná celistvosť, princípy demokracie a právneho štátu. Prvok informačnej operácie sa šíri v celej populácií.

Tabuľka: Posudzovanie vplyvu informačnej operácie.
Zdroj: Koordinovaný mechanizmus odolnosti Slovenskej republiky voči informačným operáciám.

1.5. Životný cyklus dezinformácie

Pred pochopením jednotlivých faktorov, ktoré šírenie dezinformácií ovplyvňujú považujeme za nevyhnutné aspoň v stručnej miere načrtnúť životný cyklus dezinformácie. Tento cyklus možno charakterizovať prostredníctvom 4 štádií:

1. Vytvorenie dezinformácie
2. Publikácia dezinformácie
3. Šírenie a propagácia dezinformácie
4. Detekovanie dezinformácie.[117]



V prvej fáze je dezinformácia vytvorená, pričom na jej tvorbe sa môže podieľať niekoľko subjektov. Môže ísť o jednotlivca, ale aj o koordinovanú spoluprácu subjektov vrátane štátnych aparátov. Dezinformácia môže mať rôznu podobu ako text, obrázok alebo audiovizuálna nahrávka.

Druhá fáza predstavuje nasadenie dezinformácie do informačného priestoru. Najefektívnejšie sa dezinformácie šíria prostredníctvom sociálnych médií, kde ich prezentuje alebo propaguje buď konkrétny jednotlivec prostredníctvom svojho osobného profilu alebo stránka (napríklad dezinformačné médium), ktorá už má svoje publikum. Motív nasadenia

[117] JARRAHI, A. - SAFARI, L. Evaluating the effectiveness of publishers' features in fake news detection on social media. In *Multimedia Tools and Applications*. 2022. 82. 10.1007/s11042-022-12668-8.

dezinformácie môže byť rôzny, od získania politickej moci, skrývanie chýb zo strany vlády, polarizovanie spoločnosti zahraničnými subjektami až po finančné záujmy.[118]

V tretej fáze dochádza k šíreniu a propagácie dezinformácie. Táto fáza výrazne závisí od správania užívateľov a ich interakcií s dezinformáciou. Správania užívateľov ovplyvňuje úspešnosť šírenia. Literatúra všeobecne rozlišuje tri typy užívateľov, ktorí dezinformácie zdieľajú. V prvom rade ide o zlomyseľné subjekty, ktoré dezinformácie zdieľajú a šíria cielene a úmyselne, pričom si uvedomujú, že ide o dezinformačný obsah. Druhým typom sú uvedomelí užívatelia, ktorí sa snažia kriticky pristupovať k zdieľaniu informácií, avšak môže sa im stať, že v ojedinelých situáciách si informáciu vyhodnotia nesprávne. Posledným typom užívateľov sú naivní užívatelia, ktorí dezinformácie zdieľajú z dôvodu pomýlenosti prostredníctvom konfirmačného skreslenia (pozri nižšie) alebo sociálneho nátlaku svojej skupiny.[119] Samotná dezinformácia môže byť zvýraznená prostredníctvom platenej reklamy. Dezinformácie sa šíria prostredníctvom rôznych techník. Spomenúť môžeme využívanie tzv. platených trolých fariem, potemkinove osoby (produkovanie pravdivého a neskôr dezinformačného obsahu), využitie umelej inteligencie na generovanie zmanipulovaných videí či súkromných skupinových kanáloch[120] a zosobňovanie tradičných mainstreamových médií.[121]

V poslednej, štvrtej fáze je dezinformácia detekovaná. To znamená, že je vyvrátená jej pravdivosť a môžeme ju označovať za dezinformáciu.[122]

1.6. Faktory ovplyvňujúce šírenie dezinformácií v online priestore

Dezinformácie nefungujú vo vákuu. Ich šírenie a vplyv na jednotlivcov alebo verejnú mienku ovplyvňuje rad faktorov od psychologických, sociologických, ekonomických či technických.[123] Cieľom tejto state je načrtnúť a vysvetliť tieto faktory. Tento krok považujeme za osobitne dôležitý v kontexte potenciálnej regulácie, ktorá by mala rešpektovať poznatky

[118] HARRISON, R. *Tackling Disinformation in Times of Crisis: The European Commission's Response to the Covid-19 Infodemic and the Feasibility of a Consumer-centric Solution*. 17(3) Utrecht Law Review, 2021 s. 18–33. DOI: https://doi.org/10.36633/ulr.675.
[119] Tamže.
[120] K tomu pozri BAYER, J. et al. *Disinformation and propaganda: impact on the functioning of the rule of law and democratic processes in the EU and its Member States - 2021 update*. Dostupné na: https://www.europarl.europa.eu/thinktank/en/document/EXPO_STU(2021)653633.
[121] EUROPEAN PARLIAMENT, DIRECTORATE-GENERAL FOR EXTERNAL POLICIES OF THE UNION, COLOMINA, C., SÁNCHEZ MARGALEF, H., YOUNGS, R. *The impact of disinformation on democratic processes and human rights in the world, European Parliament*. 2021. Dostupné na: https://data.europa.eu/doi/10.2861/59161.
[122] Tamže.
[123] Zhodne SAURWEIN, F. - SPENCER-SMITH, CH. *Combating Disinformation on Social Media: Multilevel Governance and Distributed Accountability in Europe, Digital Journalism*. 2021. Dostupné na: 10.1080/21670811.2020.1765401.

z technických, humanitných, ekonomických či spoločenských vied pri koncipovaní záväzných pravidiel správania sa.

1.6.1 Psychologické a sociologické faktory

Šírenie dezinformácií prostredníctvom nových technológií v online priestore má dôležité psychologické a sociologické súvislosti. Prostredie online platforiem totiž vytvorilo bezprecedentnú infraštruktúru na šírenie informácií, vrátane dezinformácií. Na jednej strane síce filtruje vhodné informácie pre jednotlivých užívateľov, na strane druhej im však môže ukazovať práve informácie, ktoré chcú vidieť, zdieľať alebo je predpoklad, že o nich majú na základe psychologického profilu záujem.[124] Zároveň, rozlišovanie medzi pravdivými a nepravdivými informáciami môže byť pre jednotlivcov náročné, ak je im ponúkaný obsah, ktorý ich názory a vieru reflektuje. Ide o fenomén tzv. uzavretých komôr s ozvenou (*echo chamber*) alebo filtračných bublín, ktoré sú však v akademickej debate podrobené kritike.[125]

Čo sú teda primárne faktory dôvery v jednotlivcov v dezinformácie? Ecker a kol. vo svojej štúdií uvádzajú nasledujúce faktory:

- Kognitívne faktory
  - Intuitívne premýšľanie
  - Kognitívne zlyhania
  - Iluzórna pravda
- Sociálne afektívne faktory
  - Zdroj informácie
  - Emócia
  - Názor a viera adresáta. [126]

Prvým kognitívnym faktorom je, že jednotlivci uprednostňujú predtuchu alebo pocity pred kritickým zamyslením sa nad konkrétnou informáciou.[127] Druhým kognitívnym faktorom

[124] K tomu pozri napríklad ACERBI, A. Cognitive attraction and online misinformation. In *Palgrave Commun*. 5, 15, 2019 alebo KOZYREVA, A. - LEWANDOWSKY, S. - HERTWIG, R. Citizens versus the internet: confronting digital challenges with cognitive tools. In *Psychol. Sci. Public Interest*. 21, s. 103–156 (2020).
[125] GARRETT, R. K. The echo chamber distraction: disinformation campaigns are the problem not audience fragmentation. In *J. Appl. Res. Mem. Cogn*. 6, 370–376 (2017).
[126] ECKER, U.K.H. - LEWANDOWSKY, S. - COOK, J. et al. The psychological drivers of misinformation belief and its resistance to correction. In *Nat Rev Psychol* 1, 13–29 (2022). https://doi.org/10.1038/s44159-021-00006-y.
[127] BRASHIER, N. M. - MARSH, E. J. Judging truth. Annu. In *Rev. Psychol*. 71, 499–515 (2020).

je, že jednotlivci zanedbajú overenie identity a kredibility zdroja informácie alebo ho prípadne úplne ignorujú.[128] Zároveň vzniká efekt tzv. iluzórnej pravdy, z toho dôvodu, že jednotlivci používajú a vnímajú periférne podnety, ako je známosť informácie (s danou správou sa už stretli), plynulosť spracovania (informácia je buď zakódovaná, alebo sa bez námahy vyvoláva), a súdržnosť (informácie majú odkazy v pamäti, ktoré sú vnútorne konzistentné) intenzívnejšie ako signály pravdivosti, pričom sila periférnych signálov sa zvyšuje s opakovaním. Opakovanie taktiež zvyšuje dôveru v dezinformácie a tento stav môže pretrvávať mesiace bez ohľadu na kognitívne schopnosti a napriek vystaveniu jednotlivca protiargumentom.[129] Dezinformácie sú zároveň príťažlivé, pretože ponúkajú zjednodušené videnie sveta a atraktívne príbehy, ktorým sa jednoducho dá rozumieť.[130]

Pre pochopenie kognitívnych faktorov je nevyhnutné aj pochopenie tzv. kognitívnych skreslení. Kognitívne skreslenie (*cognitive bias*) je systematické odchyľovanie sa od normy alebo racionality v usudzovaní.[131] Skúmanie kognitívnych skreslení je doménou kognitívnej vedy, sociálnej psychológie alebo behaviorálnej ekonomiky. V kontexte dezinformácií hrá významnú rolu tzv. potvrdzovacie skreslenie (*confirmation bias*). Ide o tendenciu vyhľadávať alebo interpretovať informácie spôsobom, ktorý potvrdzuje vlastné názory a úvahy, a ignorovať informácie, ktoré nepotvrdzujú pôvodný názor.[132] V súvislosti s dezinformáciami[133] to znamená, že ak je človek súčasťou bubliny alebo skupiny ľudí s podobnými názormi a je vystavený podobným informáciám, potvrdzovacie skreslenie jednotlivca utvrdí o svojej pravde. Osobitne dôležitý je aj tzv. *priming bias*, ktorého účinok spočíva v tom, že ak je jednotlivec vystavený pôvodnej informácií, túto si osvojí bez ohľadu na jej pravdivosť.[134]

Efekt viery v dezinformácie ovplyvňujú aj ďalšie kognitívne faktory, ktoré súvisia s fungovaním pamäte, kde sa informácie ukladajú ako prepojená sieť. Keď je dezinformácia

[128] ECKER, U.K.H. - LEWANDOWSKY, S. - COOK, J. et al. The psychological drivers of misinformation belief and its resistance to correction. In *Nat Rev Psychol* 1, 13–29 (2022). https://doi.org/10.1038/s44159-021-00006-y.
[129] Tamže.
[130] BAYER, J. et al. Disinformation and propaganda: impact on the functioning of the rule of law and democratic processes in the EU and its Member States - 2021 update. Dostupné na: https://www.europarl.europa.eu/thinktank/en/document/EXPO_STU(2021)653633.
[131] HASELTON M.G. – NETTLE, D. – ANDREWS, P.W. The evolution of cognitive bias. In BUSS, D.M. (ed.). *The Handbook of Evolutionary Psychology*. Hoboken, NJ, US: John Wiley & Sons Inc., 2005, s. 724–746.
[132] MAHONEY, M.J. Publication prejudices: An experimental study of confirmatory bias in the peer review system. In *Cognitive Therapy and Research*, 1997, 1 (2), s. 161–175. Zhodne BAYER, J. et al. *Disinformation and propaganda: impact on the functioning of the rule of law and democratic processes in the EU and its Member States - 2021 update*. Dostupné na: https://www.europarl.europa.eu/thinktank/en/document/EXPO_STU(2021)653633.
[133] K tomu pozri napríklad KIM, A. - DENNIS, A. R. Says who? The effects of presentation format and source rating on fake news in social media. In *MIS Quarterly: Management Information Systems*, 43(3), 2019, s. 1025–1039. https://doi.org/10.25300/MISQ/2019/15188.
[134] BARGH, J.A. – CHARTRAND, T.L. Studying the Mind in the Middle: A Practical Guide to Priming and Automaticity Research". In REIS H., JUDD C. (EDS.). *Handbook of Research Methods in Social Psychology*. New York, NY: Cambridge University Press, 2000, s. 1–39.

zakódovaná do pamäte a následne sa objavia nové informácie, ktoré ju vyvracajú, pôvodná dezinformácia automaticky nezmizne, ale čaká na svoju aktiváciu[135] napríklad prostredníctvom opakovania alebo príbuznosti.[136]

Sociálne afektívne faktory sú nemenej dôležité ako tie kognitívne. Výskumy ukazujú, že odborníci a politické elity sú dôveryhodnejšie ako ostatné zdroje a majú potenciál formovať verejnú mienku.[137] Ďalším výrazným faktorom sú emócie, konkrétne v dvoch rovinách. V prvom rade je nevyhnutné vyhodnotiť emocionálny stav adresáta dezinformácie. Vyvolávanie emócií prostredníctvom informácií môže spôsobiť, že ľudia budú náchylní na klamstvo a povzbudzovanie ľudí, aby sa spoliehali sa na svoje emócie zvyšuje ich zraniteľnosť voči dezinformáciám.[138] Ako dôležitý faktor sa ukazuje hnev.[139] Sociálne vylúčenie, vyvolávajúce negatívnu náladu, môže zvýšiť náchylnosť dôvery v dezinformačný obsah.[140] V druhom rade je nevyhnutné analyzovať emóciu samotnej informácie alebo dezinformácie. Emocionálny obsah zdieľaných informácií ovplyvňuje aj vytváranie falošných presvedčení a zavádzajúci obsah ktorý sa na internete šíri virálne často obsahuje apel na emócie, čo môže zvýšiť presvedčivosť predmetnej informácie.[141] Tretím sociálno-afektívnym faktorom je názor a dôvera adresáta. Celková viera v spravodajské informácie je vyššia, ak tieto informácie dopĺňajú názory čitateľa.[142] Politická stranícka príslušnosť môže tiež prispieť k falošným predstavám týkajúcich sa škandálov obľúbených politických elít.[143] Výskumy ukazujú, že vyvracanie dezinformácií, ktorým jednotlivec dôveruje v dôsledku svojej viery a názorov je náročné.[144]

Zo sociologického hľadiska existujú viaceré výskumy prezentujúce faktory, ktoré výrazne ovplyvňujú úspech šírenia dezinformácií nie len v online priestore.[145] Tieto faktory analyzujeme

---

[135] SHTULMAN, A. - VALCARCEL, J. Scientific knowledge suppresses but does not supplant earlier intuitions. In *Cognition* 124, 209–215 (2012).
[136] YONELINAS, A. P. The nature of recollection and familiarity: Aa review of 30 years of research. In *J. Mem. Lang*. 46, 441–517 (2002).
[137] BRULLE, R. J. - CARMICHAEL, J. - JENKINS, J. C. Shifting public opinion on climate change: an empirical assessment of factors influencing concern over climate change in the U.S. 2002–2010. In *Clim. Change* 114, 169–188 (2012).
[138] MARTEL, C. - PENNYCOOK, G. - RAND, D. G. Reliance on emotion promotes belief in fake news. In *Cognit. Res. Princ. Implic*. 5, 47 (2020).
[139] WEEKS, B. E. Emotions, partisanship, and misperceptions: how anger and anxiety moderate the effect of partisan bias on susceptibility to political misinformation. In *J. Commun*. 65, 699–719 (2015).
[140] GRAEUPNER, D. - COMAN, A. The dark side of meaning-making: how social exclusion leads to superstitious thinking. In *J. Exp. Soc. Psychol*. 69, 218–222 (2017).
[141] ECKER, U.K.H. - LEWANDOWSKY, S. - COOK, J. et al. The psychological drivers of misinformation belief and its resistance to correction. In *Nat Rev Psychol* 1, 13–29 (2022). https://doi.org/10.1038/s44159-021-00006-y.
[142] PENNYCOOK, G. - RAND, D. G. The psychology of fake news. In *Trends Cognit. Sci*. 25, 388–402 (2021).
[143] PENNYCOOK, G. - RAND, D. G. Lazy, not biased: susceptibility to partisan fake news is better explained by lack of reasoning than by motivated reasoning. In *Cognition* 188, 39–50 (2019).
[144] NYHAN, B. - REIFLER, J. When corrections fail: the persistence of political misperceptions. In *Political Behav*. 32, 303–330 (2010).
[145] Napríklad LEWANDOWSKY, S. - ECKER, U. K. H. - COOK, J. Beyond misinformation: Understanding and coping with the "post-truth" era. In *Journal of Applied Research in Memory and Cognition*, 2017, 6(4), s. 353–369. Dostupné

aj v prostredí EÚ a Slovenskej republiky. Ako dôležité sociologické faktory možno spomenúť predovšetkým:

- Úbytok sociálneho kapitálu
- Nárast nerovnosti
- Zvyšujúcu sa polarizáciu spoločnosti
- Nedôverou vo vedu
- Evolúciu mediálneho prostredia.[146]

Sociálny kapitál reflektuje prevalenciu faktorov ako empatia, dôvera a dobrá vôľa medzi jednotlivcami, dôveru vo verejné inštitúcie či angažovanie sa občianskej spoločnosti.[147] Výskumy z európskeho prostredia ukazujú, že zvýšený sociálny kapitál môže zlepšiť nakladanie s peniazmi chudobnejších domácností a súvisí so zvýšenou úrovňou šťastia v danej krajine.[148] Trend znižovania dôvery voči inštitúciám alebo jednotlivcom je evidentný aj v Slovenskej republike. Počas pandémie COVID-19 klesla od apríla 2020 do februára 2022 dôvera verejnosti voči všetkým orgánom verejnej moci. Dôvera vláde klesla zo 47 % na 11 %, prezidentke z 54 % na 21 %, vedeckým inštitúciám z 65 % na 31 % a zdravotníctvu zo 73 % na 33 %.[149] Nedávny prieskum dôvery Slovákov v demokraciu odhalil, že iba 18 % ľudí je spokojných s fungovaním demokracie na Slovensku. Naopak, až 55 % respondentov vyjadrilo nespokojnosť.[150] Hodnota medziľudskej dôvery sa za ostatných 30 rokov v Slovenskej republike nezmenila a drží sa na hodnote 23 %.[151] V roku 2023 prieskum ukazoval takmer 36 % dôveru Slovákov prezidentke,

---

na: https://doi.org/10.1016/j.jarmac.2017.07.008 alebo VAN DER LINDEN, S. - LEISEROWITZ, A. - ROSENTHAL, S. - - MAIBACH, E. Inoculating the public against misinformation about climate change. In *Global Challenges*, 2017, 1, 1600008. Dostupné na: http://dx.doi.org/10.1002/gch2.201600008.

[146] Lewandovsky a kolektív k týmto faktorom zaradzuje aj vnímanie informácií na základe politickej afiliácie. Tento faktor je však založený na skúmaní systému tvoreného z prevažne dvoch veľkých politických strán v USA a nemusí byť preto aplikovateľný aj v prostredí EÚ alebo Slovenskej republiky. LEWANDOWSKY, S. - ECKER, U. K. H. - COOK, J. Beyond misinformation: Understanding and coping with the "post-truth" era. In *Journal of Applied Research in Memory and Cognition*, 2017, 6(4), s. 353–369. Dostupné na: https://doi.org/10.1016/j.jarmac.2017.07.008.

[147] K tomi pozri bližšie ALDRICH, D. P. - MEYER, M. A. Social capital and community resilience. In *American Behavioral Scientist*, 59, 2015, s. 254–269. Dostupné na: http://dx.doi.org/10.1177/0002764214550299.

[148] GUAGNANO, G. - SANTARELLI, E. - SANTINI, I. Can social capital affect subjective poverty in Europe? An empirical analysis based on a generalized ordered logit model. In *Social Indicators Research*, 2016 128, s. 881–907. Dostupné na: http://dx.doi.org/10.1007/s11205-015-1061-z a RODRÍGUEZ-POSE, A. - VON BERLEPSCH, V. Social capital and individual happiness in Europe. In *Journal of Happiness Studies*, 15, s. 357–386. Dostupné na: http://dx.doi.org/10.1007/s10902-013-9426-y.

[149] *Ako sa máte Slovensko? Dôvera v inštitúcie*. Dostupné na: https://www.akosamateslovensko.sk/tema/dovera-v-institucie/.

[150] KINIT. *Prieskum CEDMO odhalil nízku dôveru Slovákov v demokraciu*. Dostupné na: https://kinit.sk/sk/prieskum-cedmo-odhalil-nizku-doveru-slovakov-v-demokraciu/.

[151] DEKK. *TRENDY [NE]DÔVERY 2023. Správa o stave [ne]dôvery na Slovensku*. Dostupné na: https://www.dekk.institute/trendy-ne-dovery-2023/.

22,6 % ľudí dôveruje vláde, 22,5 % politickým stranám a 18,8 % parlamentu.[152] 24,7 % obyvateľov Slovenska považuje za najväčší problém stav politiky a kvalitu demokracie.[153]

Druhým výrazným faktorom je zvyšovanie nerovnosti medzi obyvateľstvom. Príjmy najbohatších vrstiev spoločnosti rástli exponenciálne, čo sa však už nedá povedať o chudobnejších domácnostiach.[154] Totožné konštatovanie možno uviesť v kontexte pohlaví.[155] Negatívna sociálna situácia výrazne ovplyvňuje dôveru v dezinformácie, ako ukazujú prieskumy spomenuté v predchádzajúcich častiach tejto kapitoly. Jednotlivci zažívajúci stres zo života sú náchylnejší veriť dezinformáciám oproti jednotlivcom s pohodlným životom.[156]

Tretím faktorom je zvyšujúca sa polarizácia spoločnosti. Jednotlivci prirodzene vyhľadávajú ľudí s podobnými názormi a následne sa uzatvárajú do svojich názorových bublín.[157] Predmetný trend je viditeľný aj v Slovenskej republike, či už prostredníctvom postoja obyvateľstva k témam ako príslušnosť k NATO, EÚ, vojna na Ukrajine alebo manipulovanie volebných procesov.[158]

Štvrtým faktorom prospievajúcim k šíreniu dezinformácií je slabá dôvera vo výskum a vedecké poznanie.[159] Dôvera vo vedecké inštitúcie klesla aj v rámci Slovenskej republiky, napriek tomu, že vedecké inštitúcie stále patria medzi jedny z najdôveryhodnejších subjektov medzi obyvateľmi Slovenska (takmer 65 %).[160]

---

[152] Tamže, s. 13.
[153] Tamže, s. 22.
[154] *Income inequality across Europe in 2021*. Eurostat. Dostupné na: https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20230113-1.
[155] HAMUĽÁK, J. – FREEL, L. – NEVICKÁ, D. The comparative analysis of women's status in labor relations in modern Slovakia and the Czech Republic. In *Danube*. Roč. 11, č. 3 (2020), s. 214-227 alebo NEVICKÁ, D. Rovnaké zaobchádzanie a ochrana práce. In *Legislatívny rámec a prípadové štúdie k Pracovnému právu 2*. 1. vyd. Bratislava : Wolters Kluwer SR, 2020, s. 43-59 prípadne HAMUĽÁK, J. – NEVICKÁ, D. Breastfeeding as a (non)exclusive right of women in labor relations - the European approach. In *European studies : the review of European law, economics and politics*. Roč. 7. 1. vyd. Praha : Wolters Kluwer, 2020, s. 273-282.
[156] BAYER, J. et al. *Disinformation and propaganda: impact on the functioning of the rule of law and democratic processes in the EU and its Member States - 2021 update*. Dostupné na: https://www.europarl.europa.eu/thinktank/en/document/EXPO_STU(2021)653633.
[157] MOTYL, M. - IYER, R. - OISHI, S. - TRAWALTER, S. - NOSEK, B. A. How ideological migration geographically segregates and polarizes groups. In *Journal of Experimental Social Psychology*, 2014, 51, s. 1–14.
[158] GLOBSEC. *Nový prieskum GLOBSEC-u: Slovensko zaznamenalo výrazný prepad v prozápadných postojoch*. Dostupné na: https://www.globsec.org/what-we-do/press-releases/novy-prieskum-globsec-u-slovensko-zaznamenalo-vyrazny-prepad-v.
[159] LEWANDOWSKY, S. - ECKER, U. K. H. - COOK, J. Beyond misinformation: Understanding and coping with the "post-truth" era. In *Journal of Applied Research in Memory and Cognition*, 2017, 6(4), s. 353–369. Dostupné na: https://doi.org/10.1016/j.jarmac.2017.07.008.
[160] DEKK. *TRENDY [NE]DÔVERY 2023. Správa o stave [ne]dôvery na Slovensku*. Dostupné na: https://www.dekk.institute/trendy-ne-dovery-2023/.

Ďalším výrazným faktorom je evolúcia mediálneho prostredia,[161] ktoré sa z prostredia tlače presunulo do digitálneho priestoru.[162] Je evidentné, že diskutovaná transformácia vzhľadom na jednoduchosť šírenia informácií prispela k post-faktuálnej ére spoločnosti, v ktorej hrajú významnú rolu dezinformácie.[163] K tomuto faktoru prispela aj možnosť jednotlivcov nechať sa uzavrieť do názorových bublín, ktoré hlavne sociálne média ponúkajú.[164] Medzi ďalšie akcelerátory mediálnej technologickej zmeny patria väčší výber médií z pohľadu jednotlivca - spotrebiteľa či psychologická vzdialenosť medzi jednotlivcami, ktorá prispieva k agresívnejším prejavom.[165]

Zo sociologického pohľadu môže mať šírenie dezinformácií rôzny vplyv na spoločnosť. Šírenie dezinformácie môže ovplyvniť dôveru v informácie, „unaviť" spoločnosť, ktorá už nebude vedieť rozlišovať čo je pravdivé a čo nie alebo podávať mylný obraz o svete prostredníctvom elít.[166]

1.6.2 Ekonomické faktory

Šírenie dezinformácií má aj ekonomické faktory, ktoré častokrát vo verejnosti nerezonujú. Zároveň je potrebné poznamenať, že ekonomické faktory fungujú v tesnej symbióze s technickým nastavením fungovania sociálnych médií a súvisiacimi psychologickými a sociologickými faktormi.

Z hľadiska ekonomických faktorov považujeme za nevyhnutné zdôrazniť ľudskú pozornosť, ako súčasť ekonomiky pozornosti (*attention economy*) a s tým súvisiaci koncept kapitalizmu dohľadu (*surveillance capitalism*).

Ľudská pozornosť je dnes trhovou komoditou. Pod pozornosťou možno rozumieť mozgový „kurzor," ktorý určuje aké informácie sa dostávajú do mozgu. Inými slovami, ide

[161] SAURWEIN, F. - SPENCER-SMITH, CH. *Combating Disinformation on Social Media: Multilevel Governance and Distributed Accountability in Europe, Digital Journalism*. 2021. Dostupné na: 10.1080/21670811.2020.1765401.
[162] K tomu pozri napríklad DEUZE, M. - WITSCHGE, T. Beyond journalism: Theorizing the transformation of journalism. In *Journalism*, 2017. Dostupné na: http://dx.doi.org/10.1177/1464884916688550.
[163] LEWANDOWSKY, S. - ECKER, U. K. H. - COOK, J. Beyond misinformation: Understanding and coping with the "post-truth" era. In *Journal of Applied Research in Memory and Cognition*, 2017, 6(4), s. 353–369. Dostupné na: https://doi.org/10.1016/j.jarmac.2017.07.008.
[164] GARRETT, R. K. - WEEKS, B. E. - NEO, R. L. Driving a wedge between evidence and beliefs: How online ideological news exposure promotes political misperceptions. In *Journal of Computer-Mediated Communication*, 21, s. 331–348. Dostupné na: http://dx.doi.org/10.1111/jcc4.12164, alebo PARISER, E. *The filter bubble: What the internet is hiding from you*. New York: Penguin Press, 2011.
[165] LORENZO-DUS, N. - BLITVICH, G.-C. - BOU-FRANCH, P. On-line polylogues and impoliteness: The case of postings sent in response to the Obama Reggaeton YouTube video. In *Journal of Pragmatics*, 2011, 43, 2578–2593. Dostupné na: http://dx.doi.org/10.1016/j.pragma.2011.03.005.
[166] ENGLER, A. *Fighting deepfakes when detection fails*, The Brookings Institute. Dostupné na: https://www.brookings.edu/articles/fighting-deepfakes-when-detection-fails/.

o určitú formu uzurpácie mysle[167] alebo koncentrácie povedomia na určité stimuly, pričom ostatné sú z koncentrácie vylúčené.[168] Pozornosť je veľmi dôležitá, nakoľko jednotlivec počas svojho limitovaného času čelí množstvu informácií a stimulov a preto nám pozornosť filtruje skutočnosti a informácie, ktoré prijímame.[169] Na alokáciu pozornosti má ľudský mozog prostriedky, pomocou ktorých sa rozhoduje, ktorým prúdom informácií, sa bude venovať alebo spracúvať.[170] Z týchto dôvodov je ľudská pozornosť vzácnym zdrojom, o ktorý sa zvádza na trhu boj.

Rôzne subjekty sa snažia ľudskú pozornosť monetizovať a to takým, spôsobom, aby bolo jednotlivcom zobrazené čo najväčšie množstvo reklamy, ktoré upútavajú ich pozornosť. Firmy oceňujú reklamu pre jej schopnosť ovplyvňovať dopyt - vytvárať alebo ovplyvňovať dopyt a zároveň potenciálne potláčať dopyt po konkurenčných výrobkoch. Inými slovami, ide o vytvorenie túžby alebo želania po produkte alebo službe, ktoré predtým v ľudskej mysli neexistovala.[171] Práve tieto aspekty mali vplyv na kreovanie tzv. ekonomiky pozornosti a teda trhu, ktorý sa zameriava na udržanie jednotlivca pri určitom obsahu z dôvodu zvýšenia ziskov za zobrazovanú reklamu. Tento model prešiel od novín do komerčného vysielania a svoje najväčšie uplatnenie našiel na internete prostredníctvom vyhľadávačov alebo sociálnych sietí, ktoré sú zadarmo.[172] Užívatelia však „platia" za tieto služby prostredníctvom svojej pozornosti a prevádzkovatelia platforiem za to získavajú profity z predaja reklamného priestoru.[173]

S konceptom ekonomiky pozornosti imanentne súvisí aj téza kapitalizmu dohľadu. Ide o koncept, ktorý vytvorila profesorka Shoshana Zuboff vo svojej vedeckej spisbe.[174] Kapitalizmus dohľadu je pojem v politickej ekonómii, ktorý označuje rozsiahle zhromažďovanie a komodifikáciu osobných údajov korporáciami. Tento fenomén sa líši od sledovania štátom, hoci sa môžu navzájom posilňovať. Koncept kapitalizmu dohľadu, ako ho opisuje Shoshana Zuboff, je poháňaný motiváciou vytvárať zisk a vznikol, keď reklamné spoločnosti na čele s

[167] Bližšie k definícií pozornosti pozri napríklad JAMES, W. *The Principles of Psychology*. Vol. 1. New York: Henry Holt, 1890, s. 403–404.
[168] *Attention*. Britannica. Dostupné na: https://www.britannica.com/science/attention.
[169] SARTER, M. - GEHRING, J.W. - KOZAK, R. More attention must be paid: The neurobiology of attentional effort. In *Brain Research Reviews*, Volume 51, Issue 2, 2006, s. 145-160, ISSN 0165-0173. Dostupné: https://doi.org/10.1016/j.brainresrev.2005.11.002.
[170] K tomu pozri BUSCHMAN, T.J. – MILLER, E.K. Top-down versus bottom-up control of attention in the prefrontal and posterior parietal cortices. In *Science.* 2007 Mar 30;315(5820):1860-2.
[171] K tomu pozri napríklad GALBRAITH, J.K. *The affluent society*. Houghton Mifflin Harcourt, 1998.
[172] WU, T. *The attention merchants: the epic scramble to get inside our Heads*. Knopf, 2016.
[173] K tomu pozri napríklad CLEMENT, J. *Facebook's Average Revenue per User (ARPU) from 2012 to 2020*. Statista. Dostupné na: https://www.statista.com/statistics/234056/facebooks-average-advertisingrevenue-per-user/.
[174] ZUBOFF, S. Surveillance Capitalism and the Challenge of Collective Action. In *New Labor Forum*. 28 (1): s. 10–29. doi:10.1177/1095796018819461. ISSN 1095-7960. S

Google AdWords videli možnosti využitia osobných údajov na presnejšie zacielenie reklamy na spotrebiteľov.[175] Predmetný koncept stojí na štyroch kľúčových aspektoch:

- Snaha o čoraz rozsiahlejšie získavanie a analýzu údajov,
- Vývoj nových zmluvných foriem s využitím počítačového monitorovania a automatizácie,
- Snaha o personalizáciu a prispôsobenie služieb ponúkaných používateľom digitálnych platforiem,
- Využívanie technologickej infraštruktúry na vykonávanie neustálych experimentov na svojich používateľoch a spotrebiteľoch.[176]

Vyššie uvedené aspekty významne prispievajú k tomu, že na online médiách sa šíri aj škodlivý obsah vrátane dezinformácií. Niektorí autori dokonca uvádzajú, že šírenie dezinformácií je „funkciou" pre ekonomické zisky digitálnych platforiem.[177]

Osobitným aspektom je výnosnosť reklamy pri tzv. dezinformačných webov. Reklamu ako zdroj príjmu využíva 47 % dezinformačných webov.[178] Odhadované maximálne potenciálne príjmy z reklamy sú na najnavštevovanejších dezinformačných weboch v desiatkach tisícoch eur.[179]

1.6.3 Technické faktory

Sociálne siete sú jedným z kľúčových médií, prostredníctvom ktorých sa šíria informácie vrátane dezinformácií. Až 22 % ľudí získava spravodajské informácie prostredníctvom webov alebo aplikácií.[180] Najpopulárnejšou sociálnou sieťou ostáva Facebook, avšak ostatné sociálne siete, predovšetkým Youtube a TikTok si zachovávajú solídne čísla užívateľov, predovšetkým

[175] Tamže.
[176] Zuboff sa pri analýze týchto faktorov odvoláva na štúdiu od Hala Variana. VARIAN, H. Computer Mediated Transactions. In *American Economic Review: Papers and Proceedings*. 100 (2): s. 1–10.
[177] OLDENBOURG, A. Digital Freedom and Corporate Power in Social Media'. In *Critical Review of International Social and Political Philosophy*. 2022. Dostupné na: https://doi.org/10.1080/13698230.2022.2113229.
[178] DUBÓCZI, P. – FRIEDL, M. – RUŽIČKOVÁ, M. *DEZINFORMÁCIE A PROPAGANDA AKO BIZNIS. Mapovanie finančného a organizačného pozadia dezinformačných webov na Slovensku*. 2023. Dostupné na: https://infosecurity.sk/dezinfo/dezinformacie-a-propaganda-ako-biznis-mapovanie-financneho-a-organizacneho-pozadia-dezinformacnych-webov-na-slovensku/.
[179] Tamže, s. 12.
[180] REUTERS. *Reuters Institute Digital News Report 2023*. 2023. Dostupné na: https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2023-06/Digital_News_Report_2023.pdf.

medzi mladšou generáciou.[181] Pri preberaní správ, respondenti výskumu uviedli, že zvýšenú pozornosť venujú kanálom a stránkam celebrít, influencerom či iným osobnostiam.[182]

V Slovenskej republike patrí medzi najpoužívanejšie sociálne siete stále Facebook.[183]

Online platforma	Využitie za účelom získania spravodajstva	Využitie za iným účelom
Facebook	48 %	71 %
Youtube	25 %	63 %
Facebook messanger	15 %	49 %
Instagram	11 %	32 %
WhatsApp	9 %	33 %
Telegram	5 %	11 %

Tabuľka: Konzumácia správ pri využívaní online platforiem.
Zdroj: Reuters.

Ako už bolo uvedené pri diskusií ohľadom ekonomických faktorov šírenia dezinformácií, online platformy fungujú na modely udržiavania pozornosti za účelom zobrazovania reklám a následného zisku. Nemenej dôležité je zvýrazniť technické aspekty fungovania predmetného modelu, ktorý vedie k personalizácií obsahu pre jednotlivých užívateľov.[184] Personalizácia obsahu znamená, že obsah je užívateľovi zoradené podľa odhadovanej preferencie alebo relevantnosti pre konkrétneho užívateľa. Online platforma automaticky vyberá príspevky od užívateľov a kanálov, ktoré užívateľ sleduje na základe jeho interakcií, ako sú napríklad tlačidlá *Pačí sa mi to* alebo *Zdieľať*. Rovnako obsahuje príspevky od iných užívateľov a z kanálov, ktoré algoritmus platformy považuje za potenciálne zaujímavé pre daného užívateľa. Poradie príspevkov môže byť ovplyvnené aj tým, či sú príspevky sponzorované alebo obsahujú platenú reklamu.[185] Personalizáciu obsahu zabezpečujú tzv. odporúčacie systémy.

Odporúčacie systémy používajú sofistikované, distribuované modely strojového učenia, ako napríklad hlboké neurónové siete, na identifikáciu, usporiadanie a prezentovanie menšieho výberu zo všetkých dostupných informácií. Tento výber je navrhnutý tak, aby bol relevantný

[181] Tamže.
[182] Tamže.
[183] Tamže, s. 97.
[184] Zhodne JERÓNIMO, P. - ESPARZA, M.S. *Disinformation at a Local Level: An Emerging Discussion*. Publications 2022, 10, 15. Dostupné na: https://doi.org/10.3390/publications10020015.
[185] MESARČÍK, M. a kol. *Analysis of selected regulations proposed by the European Commission and technological solutions in relation to the dissemination of disinformation and the behaviour of online platforms*. 2022. Dostupné na: https://kinit.sk/sk/publikacia/dissemination-of-disinformation-and-the-behaviour-of-online-platforms/.

pre každého používateľa na základe pravdepodobnosti, že používateľ naňho zareaguje, či už zobrazením, kliknutím, lajkom, zdieľaním alebo inými spôsobmi interakcie.

Aby boli tieto predpovede zapojenia presné a prispôsobené konkrétnemu používateľovi v danom okamihu, tieto algoritmické odporúčacie systémy sú trénované na základe obrovského množstva údajov získaných z predchádzajúcich aktivít používateľa a záujmov vrátane záujmov iných podobných používateľov. Tieto algoritmy sa taktiež prispôsobujú špecifickému kontextu, ako je čas dňa, alebo používané zariadenie. Odporúčacie systémy sú kľúčovým nástrojom na podporu a udržiavanie zapojenia používateľov. Spoločnosti zdôrazňujú, že ich odporúčacie systémy majú za cieľ spojiť používateľov s obsahom a ľuďmi, ktorí sú pre nich relevantní. Avšak, kritici tvrdia, že obchodný model týchto systémov často uprednostňuje obsah, ktorý priláka používateľov na stránky a udržiava ich tam čo najdlhšie, bez ohľadu na to, či je tento obsah kontroverzný, škodlivý alebo nízkej kvality.[186]

Samotný proces odporúčania má dve hlavné fázy:

1. Generovanie kandidátov (*candidate generation*), pri ktorom sa analyzujú milióny informácií a následne sa automatizovane vyberie užšia množina relevantná pre konkrétneho užívateľa, tzv. kandidátske príspevky,

2. Poradie (*ranking*) kde sa ďalej analyzujú vlastnosti kandidátskych príspevkov a história aktivít používateľov s cieľom vyhodnotiť príspevky na základe predpokladaného zapojenia používateľov a nakoniec vybrať niekoľko desiatok príspevkov, ktoré sa nakoniec zobrazia používateľovi pri otvorení alebo obnovení aplikácie.[187]

Jedným z najväčších nedostatkov využívania odporúčacích systémov je ich nedostatočná vysvetliteľnosť a transparentnosť, keď ani vývojári častokrát nevedia fungovanie systému vysvetliť v plnej miere.[188] Niektorí akademici odporúčajú väčšiu kontrolu odporúčacích systémov zo strany užívateľov.[189]

[186] BUSTAMENTE, C. et al. *Technology Primer: Social Media Recommendation Algorithms*. Edited by Ariel Higuchi. Belfer Center for Science and International Affairs, Harvard Kennedy School, August 25, 2022.
[187] Tamže, s. 6.
[188] VOOSE, P. How AI Detectives Are Cracking Open the Black Box of Deep Learning. In *Science*, July 06, 2017. Dostupné na: https://www.science.org/content/article/how-ai-detectives-arecracking-open-black-box-deep-learning.
[189] WOLFRAM, S. *Testifying at the Senate about AI-Selected Content on the Internet*. Stephen Wolfram Writings blog, June 25, 2019. Dostupné na: https://writings.stephenwolfram.com/2019/06/testifying-at-the-senate-about-a-i-selected-content-on-the-internet/.

Odporúčanie konkrétneho obsahu výrazne ovplyvňuje, akému typu informácií jednotlivci venujú pozornosť, čo vedie k uzavretej slučke v ktorej algoritmus zobrazuje jednotlivcom obsah, ktorý upúta ich pozornosť, a jednotlivci venujú väčšiu pozornosť tomu, čo im algoritmus ukazuje.[190] Posilňovanie zobrazovania podobného obsahu prostredníctvom odporúčacích systémov zároveň spôsobuje, že niekoľko kliknutí na kontroverzný obsah môže mať za následok ďalšie odporúčania kontroverzného obsahu, ktoré je ťažké prestať prijímať a ktoré môžu ovplyvniť jednotlivca v jeho nazeraní na svet a prijímaní informácií.[191] Ako príklad možno uviesť vyšetrovanie denníka *Wall Street Journal* týkajúce sa sociálnej siete TikTok, na ktorej nasadili umelých používateľov (botov), ktorí simulovali prezeranie odporúčaných videí so smutným kontextom dlhšie ako iné videá. Následne po tridsiatich minútach odporúčací systém užívateľovi zobrazoval videá, z ktorých 93 % bolo depresívnej povahy.[192]

Osobitným problémom je preferencia zobrazovania ofenzívneho, urážlivého alebo extrémistického obsahu. Pri takýchto informáciách alebo príspevkov je totiž pravdepodobnejšie zapojenie a interakcia užívateľov prostredníctvom klikov, lajkov, komentárov alebo zdieľaní. To ukazuje, že senzačný a problematický obsah je pre priemerného používateľa sociálnych médií lákavý.[193] Na sociálnych sieťach sa zároveň informácie vrátane dezinformácií šíria rýchlejšie ako prostredníctvom iných médií,[194] k čomu prispieva aj nastavenie odporúčacích systémov. Ďalšie šírenie dezinformácií užívateľmi je o 70 % pravdepodobnejšie ako šírenie pravdivých informácií.[195]

S odporúčacími systémami súvisí aj problematika tzv. filtračných bublín, ktoré reflektujú situáciu, v ktorej je užívateľ prostredníctvom generovaných odporúčaní uzavretý do skupín, v ktorých sa určité informácie (vrátane dezinformácií) opakujú, potvrdzujú a posilňujú.[196] Technologická filtračná bublina znamená prostredie, v ktorom sa znižuje rozmanitosť odporúčaní používateľa v priebehu a v čase, v akejkoľvek dimenzii rozmanitosti,

---

[190] KALIMERIS, D. et al. Preference Amplification in Recommender Systems. In *Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining* (New York: Association for Computing Machinery, 2021): s. 805–15. Dostupné na: https://doi.org/10.1145/3447548.3467298.

[191] *Algorithms and Amplification: How Social Media Platforms' Design Choices Shape Our Discourse and Our Minds, Subcommittee on Privacy, Technology, and the Law* (April 27, 2021) (statement by Joan Donovan, Research Director, Shorenstein Center on Media, Politics and Public Policy, Harvard Kennedy School). Dostupné na: https://www.judiciary.senate.gov/imo/media/doc/Donovan%20Testimony%20(updated).pdf.

[192] WSJ SRAFF. *Inside TikTok's Algorithm: A WSJ Video Investigation*. Wall Street Journal, July 21, 2021. Dostupné na: https://www.wsj.com/articles/tiktok-algorithm-video-investigation-11626877477.

[193] K tomu pozri napríklad BRADY, W. et al. Emotion Shapes the Diffusion of Moralized Content in Social Networks. In *Proceedings of the National Academy of Sciences* 114, no. 28 (2017): 7313–8.

[194] VOSOUGHI, S. - ROY, D. - ARAL, S. The Spread of True and False News Online. In *Science* 359, no. 6380 (2018): 1146–51. Dostupné na: https://www.science.org/doi/full/10.1126/science.aap9559.

[195] Tamže.

[196] ZUIDERVEEN BORGESIUS, F.L. et al. Should We Worry about Filter Bubbles? In *Internet Policy Review* (March 2016).

vyplývajúci z výberu rôznych odporúčaní zainteresovaných strán.[197] Filtračné bubliny v kontexte dezinformácií znamenajú, že užívateľovi je vo výrazne zvýšenej miere ponúkaný dezinformačný obsah a ocitá sa tak v stave intelektuálnej izolácie vo falošných presvedčeniach alebo manipulovanom vnímaní reality.[198] Dezinformačné filtračné bubliny možno považovať za špeciálny prípad zníženia názorovej diverzity, v ktorom sú názory preukázateľne nepravdivé. Zároveň dezinformačné filtračné bubliny možno charakterizovať vysokou homogenitou odporúčaní alebo výsledkov vyhľadávania, ktoré majú spoločný rovnaký pozitívny postoj k dezinformáciám. Inými slovami, obsah adaptívne prezentovaný používateľovi v dezinformačnej bubline podporuje jedno alebo viacero nepravdivých tvrdení.[199]

Problémom a faktorom pre šírenie dezinformácií sú aj automatizované spôsoby ich šírenia, napríklad prostredníctvom umelo vytvorených účtoch na digitálnych službách, ktoré sa tvária ako reálne osoby. Ich jediným cieľom je však šíriť dezinformačný obsah a zvýrazňovať ho v informačnom priestore.[200] Automatizované generovanie dezinformačného obsahu je taktiež novou metódou a problémom pre boj s takýmto obsahom.[201]

[197] MICHIELS, L. What Are Filter Bubbles Really? A Review of the Conceptual and Empirical Work. In *Adjunct Proceedings of the 30th ACM Conference on User Modeling, Adaptation and Personalization* (UMAP '22 Adjunct). Association for Computing Machinery, New York, NY, USA, s. 274–279. Dostupné na: https://doi.org/10.1145/3511047.3538028

[198] SRBA, I. et al. Auditing YouTube's Recommendation Algorithm for Misinformation Filter Bubbles. In *ACM Transactions on Recommender Systems*. 1, 1, Article 6 (March 2023), Dostupné na: 10.1145/3568392.

[199] K tomu pozri napríklad COALITION TO FIGHT DIGITAL DECEPTION. T*rained for Deception: How Artificial Intelligence Fuels Online Disinformation A Report from the Coalition to Fight Digital Deception. Technical Report*. 2022.

[200] DUMBRAVA, C. *Key social media risks to democracy. Risks from surveillance, personalisation, disinformation, moderation and microtargeting*. EPRS | European Parliamentary Research Service alebo CHAKRABORTY, T. Dynamics of Fake News Diffusion. In: CHAKRABORTY, T., LONG, C., SANTHOSH, K. G. (ed.). *Data Science for Fake News*. Switzerland: Springer. 2021, s. 101–127.

[201] BONTRIDDER, N. - POULLET, Y. The role of artificial intelligence in disinformation. In *Data & Policy*, 2021 3, E32. Dostupné na: 10.1017/dap.2021.20.

2. KAPITOLA

BOJ PROTI DEZINFORMÁCIÁM V EURÓPSKEJ ÚNII A SLOVENSKEJ REPUBLIKE

Boj proti dezinformáciám v podobe prijímania konkrétnych záväzkov, opatrení a regulácií je stabilnou súčasťou európskych a slovenských politík. V rámci tejto kapitoly analyzujeme pozície pre boj s dezinformáciami v rámci EÚ a Slovenskej republiky. Politické deklarácie a pozície poskytujú nevyhnutný kontext pre prijatie regulačných opatrení pre boj s dezinformáciami online.

2.1 Európska únia

Šírenie dezinformácií môže mať celý rad škodlivých následkov ako ohrozenie demokracií, polarizáciu diskusií a ohrozenie zdravia, bezpečnosti a životného prostredia občanov EÚ. Rozsiahle dezinformačné kampane predstavujú pre Európu veľkú výzvu a vyžadujú si koordinovanú reakciu členských štátov, inštitúcií EÚ, online platforiem, spravodajských médií a občanov EÚ. Európska komisia vypracovala niekoľko iniciatív na boj proti dezinformáciám.[202] V januári 2018 bola zriadená skupina na vysokej úrovni pre falošné správy a online dezinformácie zložená z odborníkov v oblasti médií, akadémie, overovateľov faktov, občianskej spoločnosti a platforiem, ktorá vypracovala a v tom istom roku predložila záverečnú správu s odporúčaniami.[203] Okrem potreby preferencie používania pojmu dezinformácia namiesto falošnej správy obsahuje správa viacero odporúčaní, ktoré oscilujú okolo piatich pilierov:

- zvýšiť transparentnosť online spravodajstva, vrátane primeraného zdieľania údajov o systémoch, ktoré umožňujú ich šírenie online, v súlade s ochranou súkromia;
- podporovať mediálnu a informačnú gramotnosť s cieľom bojovať proti dezinformáciám a pomôcť používateľom orientovať sa v prostredí digitálnych médií;
- vyvinúť nástroje na posilnenie postavenia používateľov a novinárov v boji proti dezinformáciám a na podporu pozitívneho vzťahu k rýchlo sa vyvíjajúcim informačným technológiám;

[202] EURÓPSKA KOMISIA. *Tackling online disinformation*. Dostupné na: https://digital-strategy.ec.europa.eu/en/policies/online-disinformation.
[203] *Final report of the High Level Expert Group on Fake News and Online Disinformation.* Dostupné na: https://digital-strategy.ec.europa.eu/sk/node/3245.

- chrániť rozmanitosť a udržateľnosť ekosystému európskych spravodajských médií a
- podporovať pokračujúci výskum vplyvu dezinformácií v Európe s cieľom vyhodnotiť opatrenia prijaté rôznymi aktérmi a neustále upravovať potrebné reakcie.[204]

Pre prehĺbenie kontextu boja s dezinformáciami, osobitne v online prostredí budeme v tejto kapitole analyzovať strategické dokumenty, ktoré nadväzujú na záverečnú správu uvedenú vyššie, konkrétne:

- Oznámenie komisie európskemu parlamentu, rade, európskemu hospodárskemu a sociálnemu výboru a výboru regiónov Boj proti dezinformáciám na internete: európsky prístup z roku 2018,[205]
- Spoločné Oznámenie Európskemu Parlamentu, Európskej Rade, Rade, Európskemu Hospodárskemu A Sociálnemu Výboru A Výboru Regiónov Akčný plán proti dezinformáciám z roku 2018,[206]
- Oznámenie Komisie Európskemu Parlamentu, Rade, Európskemu Hospodárskemu A Sociálnemu Výboru A Výboru Regiónov o akčnom pláne pre európsku demokraciu z roku 2020.[207]

2.1.1 Boj proti dezinformáciám na internete: európsky prístup

Oznámenie komisie európskemu parlamentu, rade, európskemu hospodárskemu a sociálnemu výboru a výboru regiónov Boj proti dezinformáciám na internete: európsky prístup z roku 2018 (ďalej len ako „Oznámenie") je prvým strategickým dokumentom na úrovní EÚ, ktorý reflektuje problematiku dezinformácií.

Oznámenie vymedzuje tri hlavné príčiny tvorby a šírenia dezinformácií. Prvou príčinou sú všeobecné javy, ktoré výrazne ovplyvňujú spoločnosť ako hospodárska neistota, nárast extrémizmu a kultúrne zmeny vyvolávajúce strach a neistotu.[208] Druhou príčinou je prebiehajúca transformácia mediálneho sektora, kde tradičnú úlohu printových médií postupne

[204] Tamže.
[205] *OZNÁMENIE KOMISIE EURÓPSKEMU PARLAMENTU, RADE, EURÓPSKEMU HOSPODÁRSKEMU A SOCIÁLNEMU VÝBORU A VÝBORU REGIÓNOV Boj proti dezinformáciám na internete: európsky prístup*. COM/2018/236 final. Dostupné na: https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX%3A52018DC0236.
[206] *SPOLOČNÉ OZNÁMENIE EURÓPSKEMU PARLAMENTU, EURÓPSKEJ RADE, RADE, EURÓPSKEMU HOSPODÁRSKEMU A SOCIÁLNEMU VÝBORU A VÝBORU REGIÓNOV Akčný plán proti dezinformáciám*. JOIN/2018/36 final. Dostupné na: https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX%3A52018JC0036.
[207] *OZNÁMENIE KOMISIE EURÓPSKEMU PARLAMENTU, RADE, EURÓPSKEMU HOSPODÁRSKEMU A SOCIÁLNEMU VÝBORU A VÝBORU REGIÓNOV o akčnom pláne pre európsku demokraciu*. COM/2020/790 final. Dostupné na: https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=COM%3A2020%3A790%3AFIN&qid=1607079662423.
[208] Oznámenie, časť 2.2.

nahrádza trh s digitálnymi médiami.[209] Treťou príčinou je nastavenie a fungovanie sociálnych médií, ktorému sa venujeme v osobitnej časti.[210]

Komisia v Oznámení definuje štyri všeobecné zásady a ciele pre boj s dezinformáciami. Prvou prioritou je zvýšiť transparentnosť pôvodu informácií a spôsobu, akým sú tieto informácie vytvárané, financované, šírené a cielené. Cieľom tohto kroku je umožniť verejnosti posúdiť obsah, ktorý konzumujú na internete, a identifikovať pokusy o manipuláciu verejných názorov. Druhým dôležitým aspektom je podpora rozmanitosti informácií, čo umožní občanom robiť informované rozhodnutia na základe kritického myslenia. Predmetný cieľ možno dosiahnuť podporou kvalitnej novinárskej práce, zvyšovaním mediálnej gramotnosti a zabezpečením rovnováhy medzi tvorcami a distribútormi informácií. Tretím krokom je zvýšiť dôveryhodnosť informácií prostredníctvom ich označovania a zlepšením sledovateľnosti informačných zdrojov, a to aj prostredníctvom overovania a hodnotenia dôveryhodných poskytovateľov informácií. Štvrtým bodom je podpora inkluzívnych riešení. Efektívne dlhodobé riešenia vyžadujú zvýšenie povedomia verejnosti, posilnenie mediálnej gramotnosti, aktívnu účasť rôznych zainteresovaných strán a spoluprácu verejných orgánov, online platforiem, reklamných agentúr, dôveryhodných informačných zdrojov, novinárov a médií.[211]

Z hľadiska transparentnosti Oznámenie explicitne spomína podporu online platforiem v adaptácii na zodpovednejšie správanie, vytvorenie informačného ekosystému zameraného na zodpovednosť, rozvoj lepších schopností overovania faktov, rozšírenie kolektívnych znalostí o dezinformáciách a využívanie inovatívnych technológií na zlepšenie procesov produkcie a šírenia informácií na internete.[212] Európska komisia apeluje na online platformy vytvoriť zodpovedné a bezpečné prostredie, hlavne v kontexte politickej reklamy a sponzorovaného obsahu.[213] Overovatelia faktov sú v Oznámení vnímaní ako silný prvok pri dôveryhodnosti a overovaní faktov.[214] Oznámenie zvýrazňuje, že je nevyhnutné sledovať zdroj dezinformácie v celom procese jej šírenia, aby sme mohli identifikovať zodpovedné strany a zvýšiť dôveru voči identifikovateľným informačným zdrojom. Týmto spôsobom môžeme povzbudiť zodpovednejšie správanie na internete. Napríklad používatelia by sa mohli rozhodnúť komunikovať iba s tými ľuďmi na online platformách, ktorí odhalili svoju totožnosť.[215]

[209] Tamže.
[210] Tamže.
[211] Tamže, bod 3.
[212] Tamže, bod 3.1.
[213] Tamže, bod 3.1.1.
[214] Tamže, bod 3.1.2.
[215] Tamže, bod 3.1.3.

Technológie ako umelá inteligencia je v zmysle Oznámenia dôležitá pri overovaní, označovaní a identifikácií dezinformácií.[216]

Európska komisia osobitne zdôrazňuje, že zabezpečenie volebných procesov, ktoré predstavujú základ našej demokracie, vyžaduje špeciálnu pozornosť. V dnešnej dobe dezinformácie predstavujú iba jednu z mnohých taktík používaných na manipuláciu volebnými procesmi, spolu s činnosťami, ako je hackovanie, znefunkčnenie webových stránok alebo získavanie prístupu k osobným údajom politikov s následným ich zverejnením. Kybernetické operácie môžu slúžiť na narušenie dôveryhodnosti verejných informácií a sťažovať identifikáciu zdrojov dezinformácií. Táto problematika je nesmierne dôležitá počas volebných kampaní, pretože môže byť ťažšie odhaliť dezinformácie a reagovať na ne včas.[217]

Podpora vzdelávania a mediálnej gramotnosti je taktiež jedným z opatrení prezentovaných v oznámení.[218] Kvalitné médiá, vrátane verejnoprávnych, a novinárska práca zohrávajú dôležitú úlohu v poskytovaní občanom informácií vysokej kvality. Kreovaním pluralitného a rozmanitého mediálneho prostredia majú schopnosť odhaliť dezinformácie, konfrontovať ich a rozptýliť. V dnešnom neustále sa meniacom digitálnom prostredí je nevyhnutné investovať do kvalitného žurnalizmu, obnoviť dôveru v kritickú spoločenskú a demokratickú úlohu kvalitných novinárov na internete a v tlači a podporiť kvalitné novinárske zdroje pri vytváraní inovatívnych foriem žurnalistiky.[219] Komunikácia a zvyšovanie informovanosti orgánmi verejnej moci sú neoddeliteľnou súčasťou úsilia v boji proti dezinformáciám. Okrem zhromažďovania a analýzy údajov vyžaduje strategická komunikácia aj vhodné osvetové aktivity, ktoré majú za cieľ konfrontovať nepravdivé argumenty.[220]

2.1.2 Akčný plán proti dezinformáciám

Spoločné Oznámenie Európskemu Parlamentu, Európskej Rade, Rade, Európskemu Hospodárskemu A Sociálnemu Výboru A Výboru Regiónov Akčný plán proti dezinformáciám z roku 2018 (ďalej len „Akčný plán") nadväzuje na Oznámenie a ustanovuje štyri konkrétne piliere koordinovanej reakcie na dezinformácie:

- zlepšovanie schopností inštitúcií EÚ, pokiaľ ide o detekciu, analýzu a odhaľovanie dezinformácií,

[216] Tamže, bod 3.1.4.
[217] Tamže, bod 3.2.
[218] Tamže, bod 3.3.
[219] Tamže, bod 3.4.
[220] Tamže, bod 3.5.

- posilňovanie koordinovaných a spoločných reakcií na dezinformácie,
- mobilizácia súkromného sektora pri boji proti dezinformáciám,
- zvyšovanie informovanosti a zlepšovanie odolnosti spoločnosti.[221]

Pre efektívne zvládnutie hrozby dezinformácií je potrebné posilniť špeciálne strategické komunikačné jednotky Európskej služby pre vonkajšiu činnosť, delegácie EÚ a stredisko EÚ pre hybridné hrozby. Táto posilnenie môže zahŕňať pridelenie dodatočných špecializovaných pracovníkov, napríklad odborníkov na spracovávanie a analýzu dát, ktorí pomôžu spracovávať relevantné informácie. Rovnako dôležité je využívať služby viacerých monitorovacích agentúr médií na zabezpečenie pokrytia rôznych zdrojov a jazykov a na vykonávanie ďalšieho výskumu a analýz vplyvu dezinformácií. Okrem toho by mala byť pozornosť venovaná investíciám do analytických nástrojov, ako je špeciálny softvér na získavanie, usporadúvanie a zhromažďovanie veľkého množstva digitálnych údajov.[222] Akčný plán predpokladá implementáciu systému rýchleho varovania, ktorý bude okamžite identifikovať dezinformačné kampane a bude závisieť na špecializovanej technologickej infraštruktúre. To umožní jednoduchú výmenu údajov, spoločné hodnotenie situácie, koordinované pridelenie a reakcie, a efektívne využitie času a zdrojov.[223] V boji proti problému dezinformácií majú online platformy, inzerenti a reklamný priemysel kľúčovú úlohu, pretože rozsah problému priamo závisí od schopnosti týchto platforiem umožňovať, cieliť a šíriť dezinformácie. Vzhľadom na to, že tieto subjekty v minulosti neadekvátne riešili tento problém, Európska komisia aktívne podniká kroky pre riešenie tohto problému.[224] *„Online platformy by navyše mali spolupracovať s národnými orgánmi na reguláciu audiovizuálnych médií a s nezávislými overovateľmi faktov a výskumníkmi s cieľom odhaľovať dezinformačné kampane a upozorňovať na ne – najmä počas volebných období – a zabezpečiť, aby bol overený obsah viditeľnejší a rozšírenejší.*"[225] Pre dosiahnutie väčšej odolnosti spoločnosti voči hrozbám, ktoré predstavujú dezinformácie, je esenciálne zvyšovať informovanosť verejnosti. Kľúčovým prvkom je lepšie pochopenie zdrojov dezinformácií, ich úmyslov, nástrojov a cieľov, ako aj našej vlastnej zraniteľnosti voči nim. Identifikácia hlavných slabých miest vo všetkých členských štátoch by mohla profitovať zo

[221] Akčný plán, bod 3.
[222] Tamže, 1. pilier.
[223] Tamže, 2. pilier.
[224] Tamže, 3. pilier.
[225] Tamže.

spoľahlivej vedeckej metodiky. Je dôležité pochopiť, prečo občania, a niekedy aj celé komunity, podľahli dezinformačnej rétorike, a vypracovať komplexnú reakciu na tento fenomén.[226]

2.1.3 Akčný plán pre európsku demokraciu

EÚ v úvode Oznámenia Komisie Európskemu Parlamentu, Rade, Európskemu Hospodárskemu A Sociálnemu Výboru A Výboru Regiónov o akčnom pláne pre európsku demokraciu z roku 2020 (ďalej len „AP pre demokraciu") uvádza, že zoskupenie je vybudované na demokracií, právnom štáte a rešpektovaní základných práv.[227] Online priestor a digitálna transformácia však umožnila ohrozenie týchto hodnôt prostredníctvom šírenia dezinformácií a koordinovaných dezinformačných kampaní. Z tohto dôvodu je jedným z prostriedkov posilňovania demokratickej odolnosti aj boj s dezinformáciami.[228]

AP pre demokraciu reflektuje na potrebu boja proti dezinformáciám v súvislosti s volebnými procesmi.[229] Dokument zdôrazňuje slobodu a pluralitu médií *„v boji proti dezinformáciám a manipulácii demokratickej diskusie tým, že poskytujú verejnosti spoľahlivé informácie."*[230]

Samotnému boju proti dezinformáciám sa osobitne venuje štvrtá časť AP pre demokraciu. Diskutovaná stať prezentuje tri okruhy opatrení:

- Zlepšovanie kapacít EÚ a členských štátov pri boji proti dezinformáciám,
- Viac povinností a zodpovednosť online platforiem,
- Posilnenie postavenia občanov, aby vedeli prijímať informované rozhodnutia.

Efektívna reakcia na dezinformácie, bez ohľadu na to, či ide o izolované prípady alebo súčasť širšieho ovplyvňovania informácií a zahraničného zasahovania, si vyžaduje dôkladné pochopenie súvisiacich výziev. Dezinformácie, ktoré zahŕňajú šírenie evidentne nepravdivých informácií, sú iba jednou z mnohých techník - ďalšie zahŕňajú skresľovanie informácií, zavádzanie verejnosti a manipulatívne taktiky, ako napríklad falošné profily a falošné interakcie, ktoré majú za cieľ umelo posilňovať odkazy týkajúce sa konkrétnych politických otázok a využívať existujúce spoločenské rozdiely. Vzhľadom na nové hrozby je potrebná ešte tesnejšia spolupráca medzi inštitúciami EÚ, občianskou spoločnosťou, akademickou obcou, a

[226] Tamže, 4. pilier.
[227] AP pre demokraciu, 1. úvod.
[228] Tamže.
[229] Tamže, bod 2.3.
[230] Tamže, bod 3.

súkromným sektorom, a medzinárodnými partnermi. Tieto ciele reflektuje zahraničná spolupráca v bezpečnostných politikách a otvorenie systému včasného varovanie pre zahraničných partnerov. Okrem systému včasného varovania pracuje európska sieť pre spoluprácu v oblasti volieb na vypracovaní efektívnych reakcií na dezinformácie v prípade, že sú súčasťou širšieho hybridného ohrozenia. Inštitúcie EÚ zabezpečia lepšiu vnútornú koordináciu v boji proti dezinformáciám a vypracujú jasné postupy na rýchlu výmenu informácií a zdrojov na riešenie konkrétnych situácií. Členské štáty budú povzbudené k investíciám do príslušných sietí a k zabezpečeniu koherentnej spolupráce medzi svojimi zástupcami na rôznych fórach. [231]

Šírenie dezinformácií na online platformách môže byť podporované manipuláciou systémov, ako sú klasifikačné a odporúčacie algoritmy, ktoré usmerňujú prístup občanov k relevantným informáciám, najmä prostredníctvom súčinnosti neautentických operácií. Pre zvýšenie porozumenia a riešenia takýchto problémov je dôležité, aby platformy uskutočňovali dôkladné audity svojich systémov a boli skutočne transparentné voči svojim používateľom. Tieto problémy vrátane dezinformácií boli predmetom nedávneho hodnotenia Kódexu postupov proti šíreniu dezinformácií (do ktorého sa platformy a iné zúčastnené strany dobrovoľne zapojili). Komisia však považuje za potrebné pristupovať k boju proti dezinformáciám dôslednejšie, zakladať ho na jasných záväzkoch a podrobiť ho vhodným regulačným dohľadom. Reakciou na vznikajúce riziká bude návrh horizontálneho rámca pre reguláciu, zodpovednosť a transparentnosť online priestoru v rámci Aktu o digitálnych službách. [232]

V boji proti dezinformáciám hrá podľa AP pre demokraciu každý jednotlivec svoju úlohu. Mediálna gramotnosť, vrátane kritického myslenia, je kľúčová pre občanov všetkých vekových skupín, pretože im umožňuje lepšie sa orientovať v informáciách, rozpoznávať rôzne médiá a ich fungovanie a kriticky hodnotiť sociálne siete. Vďaka mediálnej gramotnosti občania dokážu preveriť informácie, pochopiť ich zdroje, ciele a dôveryhodnosť, a to ešte predtým, ako tieto informácie začnú zdieľať. Digitálna gramotnosť zase umožňuje ľuďom rozumne, bezpečne a eticky sa zapájať do online prostredia. Pre účinné zapojenie do spoločnosti a demokratických procesov je kľúčové bojovať proti dezinformáciám a nenávistným prejavom pomocou

[231] Tamže, bod 4.1.
[232] Tamže, bod 4.2.

vzdelávania a odbornej prípravy, ako aj podporovať otvorené politické diskusie. To je dôležitou prioritou v akčnom pláne digitálneho vzdelávania.[233]

2.2 Slovenská republika

Podobne ako na úrovní EÚ, aj Slovenská republika vo svojich strategických dokumentoch uvedomuje zásadnú rolu dezinformácií a ich potenciál ohroziť bezpečnosť a demokraciu štátu. Na nasledujúcich riadkoch preto budeme analyzovať strategické dokumenty, ktoré spomínajú dezinformácie, konkrétne:

- Koncepcia pre boj Slovenskej republiky proti hybridným hrozbám z roku 2018,
- Bezpečnostnú stratégiu Slovenskej republiky z roku 2021,
- Obrannú stratégiu Slovenskej republiky z roku 2021,
- Koordinovaný mechanizmus odolnosti Slovenskej republiky voči informačným operáciám z roku 2019,
- Akčný plán koordinácie boja proti hybridným hrozbám 2022 – 2024
- Koncepcia strategickej komunikácie Slovenskej republiky z roku 2023.

2.2.1 Koncepcia pre boj Slovenskej republiky proti hybridným hrozbám

Koncepcia pre boj Slovenskej republiky proti hybridným hrozbám bola prijatá v roku 2018.[234] Dokument má len koncepčný charakter a nadväzuje na neho akčný plán, ktorý rozoberáme nižšie. Dezinformácie spomína koncepcia iba na jednom mieste a to konkrétne pri východiskách pre vypracovanie koncepcie hybridných hrozieb. Koncepcia uznáva vplyv dezinformačných kampaní *„o údajných politických a ekonomických problémoch vyplývajúcich z členstva v EÚ a NATO vytváraním falošného obrazu o nevýhodách obmedzenia suverenity národných štátov v prospech európskeho integračného projektu, vstupu do schengenského priestoru a prijatia spoločnej európskej meny."*[235] Takéto kampane majú následne potenciál oslabiť dôveru vo verejné inštitúcie a demokraciu.[236]

[233] Tamže, bod 4.3
[234] NÁRODNÝ BEZPEČNOSTNÝ ÚRAD. *Koncepcia pre boj Slovenskej republiky proti hybridným hrozbám*. Dostupné na: https://www.nbu.gov.sk/wp-content/uploads/PHHD/Koncepcia-boja-SR-proti-hybridnym-hrozbam.pdf.
[235] Tamže, s. 3.
[236] Tamže.

2.2.2 Bezpečnostná stratégia Slovenskej republiky

Bezpečnostná stratégia Slovenskej republiky bola prijatá v roku 2021 a predstavuje strategický dokument v súvislosti s obranou štátu, ktorý reflektuje princípy a východiská štátu v oblasti bezpečnostnej politiky.[237] Medzi strategické bezpečnostné záujmy zaraďuje stratégia aj *„pripravenosť štátu a spoločnosti efektívne a koordinovane reagovať na hybridné hrozby vrátane dezinformácií."*[238] Dezinformácie a propagandu stratégia označuje za jednu za najväčších bezpečnostných hrozieb namierenú voči rozhodovacím procesom v štáte a s cieľom ovplyvniť verejnú mienku.[239]Osobitne sa dezinformácie spomínajú aj ako súčasť hybridných hrozieb cudzích mocností.[240]

Vzhľadom na vyššie uvedené výzvy kladie stratégia dôraz na vytvorenie koordinovaného národného mechanizmu pre zvyšovanie odolnosti voči dezinformáciám a informačným operáciám. *„Cieľom je posilniť štruktúry a rozhodovacie procesy skorej identifikácie, vyhodnotenia a reakcie na vplyvové a dezinformačné pôsobenie, ako aj realizáciu systémových opatrení."*[241] Spolu s týmto opatrením stratégia zdôrazňuje aj rozvoj kritického myslenia, strategickú komunikáciu[242] a boj proti dezinformáciám prostredníctvom reforiem v oblasti vzdelávania.[243]

2.2.3 Obranná stratégia Slovenskej republiky

Ďalším dôležitým strategickým dokumentom týkajúcim sa obrany štátu je Obranná stratégia Slovenskej republiky prijatá v roku 2021.[244] Predmetný dokument definuje základné prístupy SR k zabezpečovaniu svojej obrany.[245] V kontexte politicko-vojenských záverov z hodnotenia bezpečnostného prostredia, má zásadný vplyv na zabezpečenie obrany štátu aj *„šírenie propagandy a dezinformačných aktivít, ktoré môžu negatívne ovplyvňovať súdržnosť a akcieschopnosť NATO a EÚ"*[246] a narúšať demokratické procesy vo vnútri štátu.[247]

---

[237] *Bezpečnostná stratégia Slovenskej republiky*. 2021. Dostupné na: https://www.mosr.sk/data/files/4263_210128-bezpecnostna-strategia-sr-2021.pdf.
[238] Tamže, s. 2.
[239] Tamže, s. 5.
[240] Tamže, s. 7.
[241] Tamže, s. 11.
[242] Tamže.
[243] Tamže, s. 20.
[244] *Obranná stratégia Slovenskej republiky*. 2021. Dostupné na: https://www.mosr.sk/data/files/4286_obranna-strategia-sr-2021.pdf.
[245] Tamže, s. 6.
[246] Tamže, s. 9.
[247] Tamže.

Vzhľadom na vyššie uvedenú identifikovanú hrozbu Obranná stratégia Slovenskej republiky zavádza opatrenia v podobe prípravy obyvateľstva a vzdelávania. Od poskytovania relevantných informácií si stratégia sľubuje zvýšenie odolnosti voči dezinformáciám.[248]

2.2.4 Koordinovaný mechanizmus odolnosti Slovenskej republiky voči informačným operáciám

Koordinovaný mechanizmus odolnosti Slovenskej republiky voči informačným operáciám bol predložený do medzirezortného pripomienkového konania v roku 2020, avšak do dnešného dňa nie je schválený.[249] Navrhovaný dokument hneď v úvode niekoľkokrát spomína dezinformácie a ich masívne šírenie ako súčasť širšieho rámca informačných operácií.[250] Dokument rozlišuje medzi dezinformáciami a inými formami informačných operácií.[251] Mechanizmus obšírne opisuje inštitucionálny rámec pre boj Slovenskej republiky s informačnými operáciami prostredníctvom vlády SR a ústredných orgánov štátnej správy. Osobitné úlohy by mali byť pridelené Situačnému centru Slovenskej republiky a Národnému bezpečnostnému analytickému centru.[252] Dokument zároveň obsahuje podrobnú metodiku analýzy a hodnotenia vplyvu prvkov informačnej operácie vrátane dezinformácií vrátane možných opatrení.

2.2.5 Akčný plán koordinácie boja proti hybridným hrozbám 2022 – 2024

Akčný plán koordinácie boja proti hybridným hrozbám 2022 – 2024 nadväzuje na koncepciu boja proti hybridným hrozbám a navrhuje konkrétne opatrenia vo viacerých oblastiach.[253] Jednou z oblastí obsahujúcich konkrétne opatrenia je aj strategická komunikácia a dezinformácie.[254] Za jeden z hlavných nástrojov boja proti dezinformáciám akčný plán vymedzuje strategickú komunikáciu a jej koordináciu.[255]

Akčný plán predpokladá 9 konkrétnych opatrení pre boj s dezinformáciami a to:

- Vznik útvaru pre strategickú komunikáciu na Úrade vlády SR,

[248] Tamže, s. 23.
[249] *LP/2020/507 Koordinovaný mechanizmus odolnosti Slovenskej republiky voči informačným operáciám*. Dostupné na: https://www.slov-lex.sk/legislativne-procesy/-/SK/LP/2020/507.
[250] ÚRAD VLÁDY SR. *Koordinovaný mechanizmus odolnosti Slovenskej republiky voči informačným operáciám*, s. 3.
[251] Tamže, s. 5.
[252] Tamže, s. 10.
[253] MINISTERSTVO OBRANY SR. *Akčný plán koordinácie boja proti hybridným hrozbám 2022 – 2024*. Dostupné na: https://www.nbu.gov.sk/wp-content/uploads/2022/08/AKCNY-PLAN-KOORDINACIE-BOJA-PROTI-HYBRIDNYM-HROZBAM.pdf.
[254] Tamže, s. 11 – 13.
[255] Tamže, s. 11.

- Vznik odboru pre hybridné hrozby a strategickú komunikáciu na MO SR
- Vznik špecializovaných útvarov pre hybridné hrozby a hrozby a strategickú komunikáciu na MV SR
- Doplnenie strategickej komunikácie do organizačného poriadku pre všetky ministerstvá a ÚV
- Vytvorenie Koncepcie strategickej komunikácie Slovenskej republiky
- Komplexná analýza možností stransparentnenia informačného priestoru
- Implementácia výsledkov a odporúčaní
- Vyhodnotenie právnej odolnosti trestného zákona a trestnoprávnej zodpovednosti v kontexte hybridných hrozieb
- Analýza účinného postihovania produkcie a šírenia dezinformácií.[256]

2.2.6 Koncepcia strategickej komunikácie Slovenskej republiky

V nadväznosti na úlohy v akčnom pláne prijala vláda Slovenskej republiky na jeseň 2023 Koncepciu strategickej komunikácie Slovenskej republiky.[257] Koncepcia v úvode uvádza potrebu strategickej komunikácie štátu v kontexte produkovania polarizujúceho alebo nepravdivého obsahu aj na digitálnych platformách.[258] Šírenie dezinformácií je aj dôsledkom nedostatočnej a nesystémovej komunikácie štátu.[259] Koncepcia si dáva dva hlavné ciele. Po prvé je to zvýšenie dôvery občanov v demokratické inštitúcie aj prostredníctvom zamedzenia dezinformácií prostredníctvom strategickej komunikácie.[260] Druhým hlavným cieľom je zvýšenie informovanosti a podpory verejnosti pre dlhodobé strategické záujmy Slovenskej republiky, ktorý možno dosiahnuť taktiež zmenšením priestoru pre dezinformačné kampane.[261] Jedným z kľúčových tém strategického významu je aj zachovanie demokratického zriadenia Slovenskej republiky, ktoré je dlhodobo terčom dezinformačných kampaní.[262] Pre úspešnú krízovú komunikáciu sú kľúčové štyri princípy a to včasnosť, transparentnosť, presnosť a zrozumiteľnosť. *„Krízová situácia si vyžaduje včasné informovanie občanov, pretože informačné*

[256] Tamže, s. 12 – 13.
[257] ÚRAD VLÁDY SR. *Koncepcia strategickej komunikácie Slovenskej republiky*. 2023. Dostupné na: https://www.slov-lex.sk/legislativne-procesy/-/SK/LP/2023/56.
[258] Tamže, s. 3.
[259] Tamže, s. 4.
[260] Tamže, s. 7.
[261] Tamže.
[262] Tamže, s. 10.

vákuum má predpoklad vyvolať chaos a zároveň predstavuje priestor na šírenie dezinformácií, či neprávd s cieľom vyvolať a rozširovať v spoločnosti strach a paniku."[263]

[263] Tamže, s. 14.

3. KAPITOLA

NÁSTROJE VEREJNÉHO PRÁVA PRE BOJ S DEZINFORMÁCIAMI V ONLINE PROSTREDÍ

V rámci tretej kapitoly analyzujeme konkrétne nástroje verejného práva pre boj s dezinformáciami v online priestore. Nezameriavame sa však iba na charakteristiku predmetných nástrojov, ale pozornosť zameriavame aj na potenciálne aplikačné problémy prípadne problematické legislatívne vyjadrenie. Metodologicky predstavujeme pôsobnosť daného právneho aktu respektíve nástroja a následne špecifické inštitúty relevantné pre šírenie dezinformácií.

Samotné nástroje môžeme deliť podľa viacerých kritérií. Dezinformácie sa nešíria vo vákuu, ale v konkrétnom prostredí prostredníctvom konkrétnych nástrojov. Právo má teda viacero možností pre úpravu legislatívnych nástrojov pre boj s dezinformáciami. Prvým z možných delení predmetných nástrojov je delenie na **priame a nepriame**. Kritériom (ne)priamosti je, či daný nástroj reguluje dezinformácie ako systémový fenomén alebo umožňuje v konkrétnych prípadoch priamy zásah voči konkrétnemu obsahu. Uvedieme stručný prehľad daných nástrojov.

Medzi **priame nástroje** boja s dezinformáciami môžeme zahrnúť:

- nástroje trestného práva, a
- nástroje správneho práva.

Nástrojmi trestného práva sú predovšetkým zakotvenia skutkových podstát trestných činov šírenia dezinformácií. Aj v krajinách EÚ máme členské štáty, ktoré sa rozhodli šírenie dezinformácií sankcionovať prostredníctvom noriem trestného práva.[264] V Slovenskej republike sa taktiež zvažovalo zakotvenie trestného činu šírenia dezinformácií, avšak tieto snahy neboli úspešné.[265]

Oveľa bežnejšími pre boj s dezinformáciami sú nástroje správneho práva. Tieto možno bližšie diferencovať na preventívne opatrenia a opatrenia na zamedzenie šírenia dezinformácií. Preventívne opatrenia zahŕňajú napríklad legislatívne zakotvené obsahové požiadavky na

[264] Pre prehľad pozri napríklad HOBOKEN VAN, J. - Ó FATHAIGH, R. Regulating Disinformation in Europe: Implications for Speech and Privacy. In *UC Irvine Journal of International, Transnational, and Comparative Law. Volume 6 Symposium: The Transnational Legal Ordering of Privacy and Speech*. Article 3, 2021.

[265] HOSPODÁRSKE NOVINY. *Ministerstvo spravodlivosti z návrhu Trestného zákona vyškrtlo trestný čin šírenia nepravdivej informácie*. Dostupné na: https://hnonline.sk/slovensko/9604690-ministerstvo-spravodlivosti-z-navrhu-trestneho-zakona-vyskrtlo-trestny-cin-sirenia-nepravdivej-informacie.

rozvoj kritického myslenia alebo finančné stimuly pre osvetu. Opatrenia na zamedzenie šírenia predstavujú široký diapazón nástrojov. Spomenúť možno blokovanie webstránok, špecifické správne konanie o nelegálnom obsahu či iné opatrenia na zvýšenie transparentnosti a zodpovednosti platforiem. Iné opatrenia na zamedzenie šírenia dezinformácií prostriedkami správneho práva môžu zahŕňať požiadavky na zvýšenie transparentnosti alebo zodpovednosti. Opomenúť nemožno ani priestupkové právo. Špecifické nástroje môže ponúknuť aj oblasť ochrany osobných údajov reprezentovaná všeobecným nariadením o ochrane údajov (známe pod skratkou GDPR).

Systematickejšie riešenie šírenia dezinformácií ale ponúkajú **nepriame nástroje.** Ide o legislatívnu úpravu:

- prostredia, v ktorom sa dezinformácie šíria, a
- konkrétnych nástrojov, ktoré dezinformácie napomáhajú šíriť.

Čo sa týka prostredia, dezinformácie sa výrazne šíria na sociálnych sieťach a iných médiách. Nasvedčuje tomu aj ekonomický model online platforiem založený na monetizácii pozornosti užívateľov prostredníctvom zobrazenej reklamy.[266] Z tohto dôvodu je kľúčová legislatíva upravujúca prostredie sociálnych sietí. Európska únia prijala v tomto smere novú právnu úpravu v podobe Aktu o digitálnych službách (ďalej len „DSA" ako *Digital Services Act*),[267] ktorá obsahuje požiadavky náležitej starostlivosti aplikovateľné aj na veľmi veľké online platformy, vrátane najväčších poskytovateľov sociálnych sietí.[268] Druhým kľúčovým systémovým riešením je regulácia nástrojov, konkrétne systémov umelej inteligencie (AI). Je to z toho dôvodu, že práve systémy AI v podobe odporúčacích systémov a nastavenie ich parametrov výrazne prispievajú k šíreniu škodlivého obsahu na internete.[269] EÚ aj v tomto smere predstavila návrh legislatívy, ktorý sa bude zaoberať požiadavkami na systémy AI vysokého rizika a praktikami, ktoré budú na európskom kontinente zakázané.[270]

---

[266] ZUBOFF, S. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs, 1. vydanie, 2019.

[267] Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2065 z 19. októbra 2022 o jednotnom trhu s digitálnymi službami a o zmene smernice 2000/31/ES (akt o digitálnych službách). OJ L 277, 27.10.2022, s. 1–102.

[268] K základnému rámcu DSA pozri napríklad HUSOVEC, M. – ROCHE LAGUNA, I. *Digital Services Act: A Short Primer* (July 5, 2022). Dostupné na https://ssrn.com/abstract=4153796.

[269] Pozri napríklad HAGEY, K. - HORWITZ, J. *Facebook Tried to Make Its Platform a Healthier Place. It Got Angrier Instead*. The Wall Street Journal, 2021. Dostupné na: https://www.wsj.com/articles/facebook-algorithm-change-zuckerberg-11631654215. PARISER, E. *The filter bubble: What the internet is hiding from you*. New York: Penguin Press, 2011.

[270] Tzv. Akt o umelej inteligencií. Návrh nariadenia Európskeho parlamentu a Rady, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie (Akt o umelej inteligencií) a menia niektoré legislatívne akty únie. COM/2021/206 final.

Ďalším možným delením je delenie na nástroje systémové a individuálne. Deliacim kritériom je, či si konkrétny nástroj musí uplatniť konkrétna dotknutá osoba alebo ide o systémov riešenie, ktoré cieli na riešenie šírenia dezinformácií ako systémového rizika. Individuálny nástroj predstavuje napríklad uplatnenie práva dotknutej osoby podľa GDPR alebo návrh na začatie priestupkového konania, či trestné oznámenie. Systémovým nástrojom sú napríklad povinnosti transparentnosti pre online platformy alebo požiadavky na optimalizáciu systémov AI prostredníctvom verejnoprávnej regulácie.

3.1 Regulácia online prostredia a nástrojov

Ako sme uviedli vyššie, dezinformácie sa najčastejšie šíria v online prostredí. Z tohto dôvodu považujeme za nevyhnutné analyzovať právnu úpravu, ktorí sa týka sociálnych médií vrátane sociálnych sietí a taktiež nástrojov umelej inteligencie. Práve tieto nástroje a ich vzájomná interakcia spôsobujú amplifikovanie dezinformačného obsahu a jeho úspešné šírenie v širšom rozsahu.

3.1.1 Regulácia online platforiem

Na sklonku roka 2020 predstavila Európska Komisia návrh nariadenia o digitálnych službách známeho pod skratkou DSA („*Digital Services Act*“). Základným motívom bola revízia dvadsať rokov platného právneho rámca zodpovednosti online platforiem v podobe smernice o elektronickom obchode. Zároveň zákonodarca reflektoval vývoj digitálneho trhu a narastajúcej ekonomickej sily online platforiem, čo podnietilo diskusie o možných rizikách a regulácii. Európska komisia identifikovala niekoľko dôvodov, ktoré viedli k navrhovanej legislatíve. V prvom rade ide o nárast rizík v súvislosti s používaním a správaním online platforiem v podobe sociálnych a ekonomických rizík a možnej ujmy pre jednotlivcov a ich základné práva a slobody. Druhým dôvodom bol nedostatočný dohľad a spolupráca pri digitálnych službách, čo spôsobovalo eróziu jednotného trhu EÚ v kontexte poskytovania digitálnych služieb. Tretím dôvodom bolo odstránenie bariér pre menšie spoločnosti pri poskytovaní digitálnych služieb vzhľadom na pozíciu veľkých online platforiem.[271] Tieto dôvody sú následne prenesené do konkrétnych požiadaviek v DSA. V kontexte dezinformácií aj akademická literatúra upozorňuje na to, že model fungovania sociálnych médií zneužívajú štátni ale aj neštátni hráči na šírenie propagandy a dezinformácií.[272]

[271] EURÓPSKA KOMISIA. *Impact assessment accompanying the document proposal for a regulation of the european parliament and of the council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC.* SWD(2020) 348 final.
[272] L LEISER, M. *Reimagining Digital Governance: The EU's Digital Service Act and the Fight Against Disinformation* 2023. Dostupné na: https://ssrn.com/abstract=4427493.

DSA bol v októbri 2022 finálne prijatý. Prirodzene, nie všetky navrhované zmeny zo strany inštitúcií EÚ sa premietli aj do finálneho znenia právneho predpisu. DSA má rozdielnu účinnosť diferencovanú podľa typu subjektu, na ktorý sa vzťahuje. Na sprostredkovateľské služby, hostingové služby a online platformy (pre vysvetlenie týchto pojmov pozri nižšie) bude DSA účinný od 17. februára 2024.[273] Pre veľmi veľké online platformy, na ktorých sa dezinformácie šíria najviac, je DSA účinný od štyroch mesiacov po oznámení dotknutému poskytovateľovi Európskou komisiou, že predstavuje veľmi veľkú online platformu. K oznámeniu došlo 23. apríla 2023.[274]

3.1.1.1 Pôsobnosť právneho predpisu

DSA upravuje dve oblasti relevantné z hľadiska hmotnoprávnych požiadaviek na sprostredkovateľské služby. Prvou oblasťou je právny rámec pre podmienené výnimky zo zodpovednosti poskytovateľov sprostredkovateľských služieb. Inými slovami ide o režim tzv. bezpečných prístavov pri zodpovednosti sprostredkovateľských služieb za obsah pridaný tretími stranami. Ide o relevantný režim pre šírenie dezinformácií tretími stranami na sociálnych médiách. Predmetná časť DSA upravuje podmienky, za akých sprostredkovateľské služby sú a nie sú zodpovedné za obsah pridaný tretími stranami. Podotýkame, že tento režim neprešiel zásadnejšími zmenami oproti predošlej právnej úprave v smernici o elektronickom obchode, transponovanou do slovenského zákona č. 22/2004 Z. z. o elektronickom obchode a o zmene a doplnení zákona č. 128/2002 Z. z. o štátnej kontrole vnútorného trhu vo veciach ochrany spotrebiteľa a o zmene a doplnení niektorých zákonov v znení zákona č. 284/2002 Z. z.

Druhou veľkou oblasťou sú požiadavky tzv. náležitej starostlivosti (požiadavky *due dilligence)* pre sprostredkovateľské služby. Práve tieto predstavujú nóvum v legislatíve EÚ a viaceré inštitúty považujeme za vysoko relevantné pre šírenie dezinformácií online.

Z hľadiska vecnej pôsobnosti je potrebné upozorniť na jeden zásadný limit. DSA sa vzťahuje v drvivej miere na nezákonný obsah. Za nezákonný obsah sa považuje *„akákoľvek informácia, ktorá sama osebe alebo tým, že odkazuje na nejakú činnosť vrátane predaja výrobkov alebo poskytovania služieb, nie je v súlade s právnymi predpismi Únie alebo niektorého členského štátu, a to bez ohľadu na presný predmet alebo povahu týchto právnych predpisov.*"[275] DSA v recitálovej časti vyžaduje široký význam interpretácie daného pojmu.[276] Ako príklady

[273] DSA, článok 93 ods. 2.
[274] EURÓPSKA KOMISIA. *Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines*. Dostupné na: https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2413.
[275] DSA, článok 2 písm. h).
[276] DSA, recitál 12.

nezákonného obsahu DSA uvádza nezákonné nenávistné prejavy alebo teroristický obsah, nezákonný diskriminačný obsah, obrázky sexuálneho zneužívania detí, zdieľanie súkromných snímok bez súhlasu, online prenasledovanie, predaj nevyhovujúcich alebo falšovaných produktov, predaj produktov alebo poskytovanie služieb v rozpore s právnymi predpismi o ochrane spotrebiteľa, nepovolené používanie materiálu chráneného autorským právom, nezákonná ponuka ubytovacích služieb alebo nezákonný predaj živých zvierat.[277] Zároveň, je potrebné zvýrazniť, že nezákonný obsah si definujú samotné členské štáty vo svojich právnych poriadkoch resp. ho definuje legislatíva EÚ. Takýto prístup bude prirodzene znamenať fragmentáciu. Túto fragmentáciu môžu svojim nastavením preklenúť aj adresáti právnych noriem – samotné sprostredkovateľské služby. Ak sa vnútroštátne predpisy budú odlišovať iba okrajovo, sprostredkovateľské služby môžu určiť spoločného menovateľa pre určenie nezákonnosti obsahu napríklad v prípade zákazu násilného obsahu vo viacerých členských štátoch, ale s odlišným prístupom k nezákonnosti takéhoto obsahu.[278] Ťažšie prípady môžu nastať, ak členské štáty majú odlišný pohľad na zákonnosť alebo nezákonnosť určitého obsahu ako sú napríklad interrupčné tabletky.[279] Z hľadiska definície nezákonného obsahu budú najťažšie situácie, ak požiadavky na určitý obsah budú kontradiktórne to znamená v priamom rozpore. Ilustrovať to možno na situácií ak zverejnenie určitých informácií je v jednom členskom štáte povinné a v inom nezákonné.[280]

Ak dáme vyššie uvedené do kontextu dezinformácií, v rôznych členských štátoch sa môžeme dopracovať k odlišným záverom. Existujú členské štáty EÚ, kde dezinformácie v určitom kontexte predstavujú nezákonný obsah. Ako príklad možno uviesť Poľsko alebo Maďarsko, kde je trestné šírenie dezinformácií o nebezpečne nákazlivej chorobe COVID-19. V iných prípadoch budú dezinformácie považované „iba" za škodlivý obsah a väčšina ustanovení DSA sa na takýto druh obsahu nebude vzťahovať. Výnimkou je inštitút posudzovania a zmierňovania rizík, ktorý má všeobecnejšiu pôsobnosť.[281] Zároveň, samotné sprostredkovateľské služby sa môžu nad rámec právneho systému rozhodnúť, aký obsah budú klasifikovať ako nezákonný a zahrnúť do neho aj dezinformácie.

[277] Tamže.
[278] HUSOVEC, M. – ROCHE LAGUNA, I. *Digital Services Act: A Short Primer* (July 5, 2022). Dostupné na https://ssrn.com/abstract=4153796.
[279] Tamže.
[280] Tamže.
[281] DSA, článok 34 a 35.

DSA z hľadiska osobnej pôsobnosti rozlišuje štyroch aktérov, na ktorých sa vzťahujú konkrétne právne požiadavky. V zásade ide o niekoľko množín vzťahov. DSA rozlišuje:

- Sprostredkovateľské služby;
- Hostingové služby;
- Online platformy; a
- Veľmi veľké online platformy.[282]

Najväčšou množinou aktérov sú **sprostredkovateľské služby**, ktoré návrh DSA delí na služby typu obyčajný prenos, kešing a hosting.[283] Služby typu obyčajný prenos zahŕňajú poskytovateľov internetového pripojenia alebo prevádzkovateľov otvorenej wifi siete. Podstatou služieb kešingu je dočasné a prechodné uloženie informácií s cieľom zefektívnenia služby.

Dôležitou množinou z hľadiska šírenia dezinformácií sú služby typu **hosting**. V zásade ide o služby webhostingu, cloudových služieb, úložísk, sociálnych sietí alebo online inzercií.

Podmnožinou služieb hosting sú **online platformy**, ktoré DSA definuje *ako „hostingová služba, ktorá na žiadosť príjemcu služby uchováva a verejne šíri informácie, pokiaľ táto činnosť nie je nepodstatným a čisto vedľajším prvkom inej služby alebo nepodstatnou funkciou hlavnej služby, ktorý z objektívnych a technických dôvodov nemožno použiť bez tejto inej služby, a začlenenie tohto prvku alebo funkcie do inej služby nie je prostriedkom na obchádzanie uplatniteľnosti tohto nariadenia."*[284]

Špecifická pozornosť a právne požiadavky sú zamerané aj na poslednú množinu aktérov - **veľmi veľké online platformy**. Tieto priamo definované v DSA nie sú, avšak nariadenie obsahuje návod na ich klasifikáciu. V zmysle článku 33 ods. 1 DSA veľkými online platformami možno rozumieť tých sprostredkovateľov, *„ktorí majú priemerný mesačný počet aktívnych príjemcov služby v Únii, ktorý sa rovná 45 miliónom alebo je vyšší."* Zároveň je potrebné dodať, že

[282] Navyše, DSA definuje a upravuje povinnosti aj pre veľmi veľké online vyhľadávače. Tie sa však zásadne nelíšia od povinností pre veľmi veľké online platformy.

[283] DSA, článok 2 písm. g): *„sprostredkovateľská služba je jedna z týchto služieb informačnej spoločnosti:*
i) služba „obyčajný prenos" pozostávajúca z prenosu informácií poskytovaných príjemcom služby v komunikačnej sieti alebo z poskytovania prístupu ku komunikačnej sieti,
ii) služba „kešing" pozostávajúca z prenosu informácií poskytovaných príjemcom služby v komunikačnej sieti, pri ktorom sa tieto informácie automaticky, dočasne a prechodne uchovávajú, vykonávaná výlučne na účely zefektívnenia ďalšieho prenosu informácií k iným príjemcom na ich žiadosť,
iii) služba „hosting" pozostávajúca z uchovávania informácií poskytovaných príjemcom služby na jeho žiadosť."

[284] DSA, článok 2 písm. i).

veľmi veľkú platformu musí dezignovať Európska komisia.[285] Ako upozorňuje Husovec, či konkrétna služba spadá pod DSA bude nutné posudzovať z mikroskopického hľadiska, nakoľko sa môže stať, že nie všetky služby konkrétnej platformy budú pod DSA spadať.[286] Veľmi veľké online platformy predstavujú špecifikum aj v prípade dohľadu. Exkluzívnu právomoc nad týmito subjektami má Európska komisia.

Požiadavky kladené DSA na vyššie uvedených aktérov sa líšia a je preto vždy dôležité správne klasifikovať sprostredkovateľa služieb.[287] Najväčší „balík" povinností prirodzene prislúcha veľmi veľkým online platformám, ktoré musia spĺňať vyššie požiadavky na transparentnosť, nastavenia odporúčacích systémov, transparentnosti cielenia reklamy či vypracovania krízových protokolov.

Povinnosti v zmysle DSA môžeme rozdeliť na univerzálne, základné, dodatočné a špeciálne. Univerzálne povinnosti platia pre všetky typy sprostredkovateľských služieb. Univerzálne a základné pre sprostredkovateľské služby a služby typu hosting. Univerzálne, základné a dodatočné povinnosti platia pre online platformy. Pre veľmi veľké online platformy budú platiť všetky uvedené typy povinností. Nižšie uvádzame prehľad konkrétnych inštitútov aplikovateľných na jednotlivé subjekty:

Vrstva (stupeň)	Typ služby	Požiadavky
Univerzálne	Sprostredkovateľská služba	• Kontaktné miesto v EÚ • Všeobecné obchodné podmienky • Správy o transparentnosti
Základné	Hosting	• Mechanizmy oznamovania a prijímania opatrení • Oznamovanie podozrení z trestných činov
Dodatočné	Online platforma	• Vnútorný systém vybavovania sťažností • Mimosúdne riešenie sporov • Dôveryhodní nahlasovatelia • Opatrenia a ochrana proti zneužitiu • Dizajn platforiem • Dodatočné parametre Správy o transparentnosti

[285] DSA, článok 33 ods. 4.
[286] HUSOVEC, M. *The DSA's Scope Briefly Explained*. 2023. Dostutpné na: https://ssrn.com/abstract=4365029.
[287] Pozri EURÓPSKA KOMISIA. *Digital Services Act*. Dostupné na: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en.

		• Koncepcia a organizácia online rozhrania • Reklama na online platformách • Transparentnosť odporúčacieho systému • Ochrana maloletých • Opatrenia na ochranu spotrebiteľov
Špecifické	Veľmi veľká online platforma	• Posudzovanie a zmierňovanie rizík • Auditovanie • Mechanizmus reakcie na krízu • Dodatočné požiadavky na odporúčacie systémy • Dodatočná transparentnosť online reklamy • Dodatočné parametre Správy o transparentnosti • Prístup k údajom a ich kontrola

Tabuľka: Pôsobnosť DSA.
Zdroj: Text DSA a zdroj v poznámke pod čiarou č. 286.

Vzhľadom na to, že kľúčové pre šírenie dezinformácií sú veľmi veľké online platformy, budeme sa pri analýze konkrétnych požiadaviek sústrediť práve na tieto typy služieb.

3.1.1.2 Inštitúty relevantné pre šírenie dezinformácií

Ako je evidentné zo zoznamu požiadaviek vyššie, DSA upravuje množstvo nových inštitútov a povinností pre sprostredkovateľské služby. Poukázali sme na to, že dezinformácie budú v zmysle väčšiny právnych poriadkov členských štátov EÚ považované za škodlivý obsah a preto sa v zmysle DSA na takýto obsah nebude väčšina požiadaviek vzťahovať. Považujeme za vhodné ale upozorniť aj na povinnosti sprostredkovateľských služieb v kontexte nezákonného obsahu, nakoľko dezinformácie sa môžu za nezákonný obsah považovať ak tak ustanovuje právo členského štátu EÚ, právny systém EÚ alebo sa samotná platforma rozhodne k určitému typu obsahu správať analogicky ako k nezákonnému. Diskutovať preto budeme požiadavky na posudzovanie a zmierňovanie rizík, auditovanie, odporúčacie systémy, požiadavky na transparentnosť a samotný dizajn platforiem. Pozornosť ďalej zameriame na transparentnosť reklamy, zodpovednosť za cudzí obsah a inštitúty občianskej spoločnosti.

Posudzovanie a zmierňovanie rizík

Články 34 a 35 DSA upravujú povinnosť posudzovania a zmierňovania rizík pre veľmi veľké online platformy (VVOP). Predmetná povinnosť spočíva v identifikovaní, analýze a posúdenia všetkých systémových rizík v EÚ, ktoré vyplývajú z návrhu alebo fungovania ich služby a jej príslušných systémov vrátane algoritmických systémov, alebo z využívania ich služieb.[288] Povinnosť vykonať posúdenie rizík majú VVOP raz ročne alebo pri každom nasadení nových funkcionalít s kritickým vplyvom na fungovanie platformy.[289] Zvýrazňujeme, že predmetná požiadavka sa netýka iba šírenia nezákonného obsahu, ale aj zvýrazniť, že predmetná požiadavka sa netýka iba nezákonného obsahu, ale aj posúdenia: "***akýchkoľvek negatívnych účinkov na výkon základných práv*** *na rešpektovanie súkromného a rodinného života, slobody prejavu a práva na informácie, zákazu diskriminácie a práv dieťaťa, ako sú zakotvené v článkoch 7, 11, 21 a 24 charty; a* ***úmyselnej manipulácie ich služieb****, a to aj prostredníctvom neautentického používania alebo automatizovaného využívania služby, so skutočným alebo predvídateľným negatívnym vplyvom na ochranu verejného zdravia, maloletých osôb a občianskej diskusie alebo skutočnými alebo predvídateľnými účinkami súvisiacimi s volebnými procesmi a verejnou bezpečnosťou."*[290] Recitály 80 až 83 DSA diferencujú medzi štyrmi kategóriami systémových rizík a to konkrétne:

- riziká spojené so šírením nezákonného obsahu (nenávistné prejavy, materiály obsahujúce sexuálne zneužívanie detí),[291]
- skutočné alebo predvídateľné vplyvy služby na uplatňovanie základných ľudských práv a slobôd,[292]
- negatívne účinky na demokratické procesy, občiansku diskusiu a volebné procesy, ako aj na verejnú bezpečnosť,[293]
- obavy týkajúce sa modelu fungovania, a to aj prostredníctvom manipulácie, VVOP so skutočným alebo predvídateľným negatívnym vplyvom na ochranu verejného zdravia, maloletých a s vážnymi negatívnymi dôsledkami na telesnú a duševnú

[288] DSA, článok 34 ods. 1.
[289] Tamže.
[290] Tamže.
[291] DSA, recitál 80.
[292] DSA, recitál 81.
[293] DSA, recitál 82.

pohodu osoby alebo na rodovo motivované násilie vrátane dezinformačných kampaní.[294]

Inými slovami, predmetná požiadavka sa týka identifikácie systémových rizík, medzi ktoré možno zaradiť aj šírenie dezinformačného obsahu. Konkrétnejšie možno uviesť šírenie dezinformácií prostredníctvom falošných účtov, umelých subjektov (botov) alebo iných prostriedkov, ktoré využívajú model fungovania platforiem na efektívnejšie šírenie neželaného obsahu.[295] Posudzovanie rizika preto nevyhnutne bude musieť zahŕňať aj šírenie dezinformácií na veľmi veľkých online platformách. Osobitne tomu nasvedčuje ustanovenie článku 34 ods. 2 DSA, ktoré vyžaduje špecificky skúmať *"ako systémy moderovania obsahu,* ***odporúčacie systémy a systémy na výber a zobrazovanie reklamy*** *ovplyvňujú ktorékoľvek zo systémových rizík uvedených článku 34 ods. 1 vrátane možného neautentického používania alebo automatizovaného využívania služby, ako aj amplifikáciou a potenciálne rýchlym a rozsiahlym šírením nezákonného obsahu a informácií, ktoré nie sú zlučiteľné s obchodnými podmienkami platformy."*[296] Podklady z takéhoto posúdenia sú VVOP povinné uchovávať tri roky po ich vykonaní a poskytujú ich Európskej komisií alebo určenému národnému dozornému orgánu. Dozor na národnej úrovní vykonávajú tzv. koordinátori digitálnych služieb (KDS).

Ak VVOP identifikovala riziká, je povinná voči nim zaviesť vhodné, primerané a účinné zmierňujúce opatrenia.[297] V rámci opatrení musia zohľadniť vplyv na základné ľudské práva a slobody.[298] DSA zároveň obsahuje demonštratívny výpočet týchto opatrení. Pre šírenie dezinformácií sa ako relevantné javia úpravy algoritmov vrátane odporúčacích systémov, úpravy zobrazovania reklamy, dezignovanie nových dozorných mechanizmov pre dohľad nad systémovými rizikami, opatrenia na zvýšenie informovanosti či informovanie o vytvorenom alebo zmanipulovanom obsahu.[299] Najčastejšie vyskytujúce sa riziká monitoruje Európska komisia a Európsky výbor pre digitálne služby zriadený podľa DSA a tieto orgány v spolupráci raz ročne zverejňujú správu s identifikáciou najvýznamnejších a opakujúcich sa rizík komunikovaných VVOP spolu s odporúčaniami najlepších postupov pre ich zmiernenie.[300] Nakoľko dezinformácie možno jednoznačne označiť za systémové riziko, môže ísť o významný

[294] DSA, recitál 83.
[295] K tomu pozri napríklad LEISER, M. *Reimagining Digital Governance: The EU's Digital Service Act and the Fight Against Disinformation* 2023. Dostupné na: https://ssrn.com/abstract=4427493, s. 6-7.
[296] Zhodne SAVIN, A. The EU Digital Services Act: Towards a More Responsible Internet. In *Copenhagen Business School Law Research Paper Series No. 21-04*. Dostupné na: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3786792.
[297] DSA, článok 35 ods. 1.
[298] Tamže.
[299] Tamže.
[300] DSA, článok 35 ods. 2 a 3.

nástroj pre zmiernenie ich šírenia. Práve odlišné nastavenie prioritizácie obsahu a fungovania algoritmov sociálnych médií býva označované za kľúčové pre boj so šírením dezinformácií v online priestore.[301]

Auditovanie

Auditovanie je dnes bežnou súčasťou procesov, či už vo verejnej správe alebo v súkromnom sektore. Fenomén auditovania je prítomný aj v digitálnej regulácii, pričom ilustrovať to možno na legislatíve na ochranu osobných údajov[302] alebo kybernetickej bezpečnosti.[303] Teória auditu diferencuje medzi auditmi prvej strany, druhej strany a tretej strany. Audit prvej strany znamená, že kontrola je vykonávaná interným tímom v rámci auditovaného subjektu. Audit druhej strany reflektuje situáciu, keď si kontrolu objednal auditovaný subjekt u iného subjektu. Audity tretej strany vykonávajú nezávislé tretie strany bez zmluvného vzťahu s auditovanou osobou.[304]

Jedným z kľúčových systémových nástrojov pre externú kontrolu VVOP v kontexte nezákonného obsahu je práve výkon auditov. VVOP sa musia minimálne raz do roka podrobiť nezávislému auditu, v rámci ktorého audítor bude posudzovať dodržiavanie požiadaviek DSA (vrátane posúdenia a minimalizácie rizík) a súladu s kódexami správania, ak je VVOP ich signatárom.[305] V zmysle vyššie uvedeného teoretického delenia auditov by tak išlo o audit druhej strany. Audit nemôže vykonať akýkoľvek subjekt. DSA stanovuje presné požiadavky,

[301] LEISER, M. *Reimagining Digital Governance: The EU's Digital Service Act and the Fight Against Disinformation* 2023. Dostupné na: https://ssrn.com/abstract=4427493, s. 6.
[302] GDPR, článok 35 predpisuje posúdenie vplyvu na ochranu údajov pre určité spracovateľské operácie.
[303] Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti upravuje v § 29 auditovanie kybernetickej bezpečnosti v zmysle predmetného zákona.
[304] COSTANZA-CHOCK, S. - DEBORAH RAJI, I. - BUOLAMWINI, J. Who Audits the Auditors? Recommendations from a Field Scan of the Algorithmic Auditing Ecosystem. In *2022 ACM Conference on Fairness, Accountability, and Transparency* (FAccT '22: 2022 ACM Conference on Fairness, Accountability, and Transparency, Seoul Republic of Korea: ACM, 2022), s. 1571–83. Dostupné na: https://doi.org/10.1145/3531146.3533213.
[305] DSA, článok 37 ods. 1.

ktorými sú nezávislosť,[306] odborné znalosti v oblasti riadenia rizík[307] a sú objektívne.[308] Prirodzenie, VVOP sú povinné audítorom poskytnúť plnú súčinnosť, dáta a vstup do potrebných priestorov za zohľadnenia dôvernosti a ochrany informácií auditovaného subjektu.[309] Z každého auditu musí byť vyhotovená správa, ktorej náležitosti upravuje DSA.[310] V prípade, ak audítor nemohol posúdiť určité aspekty, v správe uvedenie z akých dôvodov tak nemohol urobiť.[311] Samotná audítorská správa môže byť kladná alebo negatívna s odporúčaniami pre VVOP. Platformy sú následne povinné tieto odporúčania implementovať, avšak predmetná povinnosť neplatí absolútne. VVOP môžu od prijatia opatrení upustiť ak stanovia alternatívne opatrenia na riešenie identifikovaných negatív.[312] Proces auditu bude predmetom úpravy delegovaného nariadenia, pričom Európska komisia už predstavila jeho návrh.[313]

Odporúčacie systémy

Jedným z hlavných nástrojov, cez ktoré sa šíri obsah na sociálnych médiách sú personalizované algoritmy – odporúčacie systémy. Základným účelom odporúčacích systémov je zobrazenie konkrétneho obsahu pre konkrétneho užívateľa, ktorý je šitý na mieru záujmom alebo potenciálnym záujmom užívateľa. Práve tieto nástroje zvýrazňujú a uľahčujú šírenie škodlivého alebo nezákonného obsahu širokému publiku. Z tohto dôvodu DSA neopomína reguláciu odporúčacích systémov.

---

[306] *„Organizácie sú nezávislé od poskytovateľa dotknutých veľmi veľkých online platforiem alebo veľmi veľkých internetových vyhľadávačov a akejkoľvek právnickej osoby prepojenej s uvedeným poskytovateľom a nie sú s nimi v žiadnom konflikte záujmov; najmä:*
i) počas 12 mesiacov pred začatím auditu neposkytovali dotknutému poskytovateľovi veľmi veľkej online platformy alebo veľmi veľkého internetového vyhľadávača a žiadnej právnickej osobe prepojenej s uvedeným poskytovateľom žiadne neaudítorské služby súvisiace so záležitosťami, ktoré sú predmetom auditu, a zaviazala sa, že im do 12 mesiacov od ukončenia auditu takéto služby nebude poskytovať;
ii) neposkytovali audítorské služby podľa tohto článku dotknutému poskytovateľovi veľmi veľkej online platformy alebo veľmi veľkého internetového vyhľadávača a žiadnej právnickej osobe prepojenej s uvedeným poskytovateľom v období dlhšom ako 10 po sebe nasledujúcich rokov;
iii) nevykonávali audit výmenou za poplatky, ktoré závisia od výsledku auditu." DSA, článok 37 ods. 3 písm. a).

[307] Organizácia majú *„preukázateľné odborné znalosti v oblasti riadenia rizík, technickú spôsobilosť a spôsobilosti.*" DSA, článok 37 ods. 3 psím. b).

[308] Organizácie majú *„preukázanú objektívnosť a profesionálnu etiku, najmä na základe dodržiavania kódexov postupov alebo vhodných noriem.*" DSA, článok 37 ods. 3 psím. c).

[309] Tamže.

[310] DSA, článok 37 ods. 4.

[311] DSA, článok 37 ods. 5.

[312] DSA, článok 37 ods. 6. *„Poskytovatelia veľmi veľkých online platforiem alebo veľmi veľkých internetových vyhľadávačov, ktorí dostanú správu z auditu a táto správa nie je „kladná", náležite zohľadnia operatívne odporúčania, ktoré im boli určené, a prijmú potrebné opatrenia na ich vykonanie. Do jedného mesiaca od prijatia odporúčaní prijmú správu o vykonávaní odporúčaní auditu, v ktorej uvedené opatrenia stanovia. V prípadoch, keď operatívne odporúčania nevykonajú, uvedú v správe o vykonávaní odporúčaní auditu dôvody, prečo ich nevykonali, a stanovia alternatívne opatrenia, ktoré prípadne prijali na riešenie akýchkoľvek zistených prípadov nesúladu.*"

[313] Pozri EURÓPSKA KOMISIA. *Digital Services Act. Conducting independent audits*. Dostupné na: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13626-Digital-Services-Act-conducting-independent-audits_en.

DSA obsahuje legálnu definíciu odporúčacích systémov ako *„úplne alebo čiastočne automatizovaný systém, ktorý online platforma používa na odporúčanie konkrétnych informácií príjemcom služby vo svojom online rozhraní alebo na uprednostňovanie uvedených informácií, a to aj v dôsledku vyhľadávania iniciovaného príjemcom služby alebo iného určenia relatívneho poradia alebo významnosti zobrazovaných informácií.*"[314] Samotné odporúčacie systémy výrazne závisia od voľby ich architektúry a preferencie konkrétnych parametrov ako sú obmedzenia zdieľaného obsahu, užívateľské správanie a interakcia medzi užívateľom a obsahom.[315]

Požiadavky kladené na odporúčacie systémy sú predmetom úpravy pre VVOP a online platformy. Pre VVOP platí, že odporúčací systém musí pre užívateľov obsahovať možnosť personalizáciu obsahu vypnúť.[316]

Okrem toho, online platformy (vrátane VVOP) sú povinné zabezpečiť transparentnosť odporúčacích systémov. Transparentnosť v tomto ohľade spočíva v komunikovaní hlavných parametrov, ktoré odporúčacie systémy využívajú a poskytnutie možnosti na užívateľskú úpravu predmetných systémov.[317] Hlavné parametre musia minimálne obsahovať informácie o (i) kritériách, ktoré sú najvýznamnejšie pri určovaní informácií navrhovaných príjemcovi služby a (ii) dôvodoch relatívneho významu týchto parametrov.[318] Poradie zobrazenia informácií si budú môcť užívatelia zmeniť a upraviť fungovanie odporúčacieho systému pre seba.[319]

Transparentnosť

DSA upravuje viaceré požiadavky týkajúce sa transparentnosti, či už v podobe podávania verejne dostupných správ, reklamy alebo odporúčacích systémov (viď diskusia vyššie). Obsah právnych požiadaviek na transparentnosť sa líši podľa toho, či ide o všeobecne sprostredkovateľov služieb, online platformy alebo VVOP. Práve otázky transparentnosti boli identifikované ako kľúčové odbornou komunitou pre získanie poznatkov o metódach a dôvodoch efektívneho šírenia dezinformácií.[320] Najvšeobecnejšia povinnosť transparentnosti

---

[314] DSA, článok 3 písm. s).
[315] EVANS, S. et al. Explicating Affordances: A Conceptual Framework for Understanding Affordances in Communication Research. In *Journal of Computer-Mediated Communication* 22, no. 1 (2017), s. 35–52. Dostupné na: https://doi.org/10.1111/jcc4.12180.
[316] DSA, článok 38. *„Okrem požiadaviek stanovených v článku 27 poskytovatelia veľmi veľkých online platforiem a veľmi veľkých internetových vyhľadávačov, ktorí používajú odporúčacie systémy, pre každý zo svojich odporúčacích systémov poskytnú aspoň jednu možnosť,* ***ktorá nie je založená na profilovaní*** *v zmysle vymedzenia článku 4 bodu 4 nariadenia (EÚ) 2016/679.*"
[317] DSA, článok 27 ods. 1.
[318] DSA, článok 27 ods. 2.
[319] DSA, článok 27 ods. 3.
[320] *Report of the independent High level Group on fake news and online disinformation. A Multi-Dimensional Approach to Disinformation*, s. 22. Dostupné na: https://op.europa.eu/sk/publication-detail/-/publication/6ef4df8b-4cea-11e8-be1d-01aa75ed71a1.

sa nachádza v článku 14 DSA týkajúcom sa všeobecných obchodných podmienok sprostredkovateľských služieb. Tie okrem iného musia obsahovať aj informácie o *"všetkých politikách, postupoch, opatreniach a nástrojoch používaných na účely moderovania obsahu vrátane algoritmického rozhodovania a ľudskej kontroly."*[321]

Pozornosť oprávnene vzbudzuje požiadavka pravidelne podávať správy o transparentnosti. Takúto správu musia zverejňovať sprostredkovateľské služby, ktoré nie sú mikropodniky alebo malé podniky, najmenej raz ročne.[322] Totožná povinnosť platí aj pre online platformy[323] s dodatočnými požiadavkami. VVOP taktiež musia zverejňovať správy o transparentnosti obohatené o informácie o vykonaných auditoch či analýzach rizík každých 6 mesiacov,[324] pričom prvú správu musia zverejniť do dvoch mesiacov od dezignovania VVOP Európskou komisiou.

VVOP sú povinné zverejňovať najrozsiahlejšie správy o transparentnosti. Tieto správy musia zahŕňať informácie o:

- *„**počte príkazov prijatých od orgánov členských štátov** vrátane príkazov vydaných v súlade s článkami 9 a 10 rozdelených podľa druhu dotknutého nezákonného obsahu, o členskom štáte, ktorý príkaz vydal, a mediáne času potrebnom na informovanie orgánu, ktorý príkaz vydal, alebo akéhokoľvek iného orgánu uvedeného v príkaze o jeho prijatí a na vykonanie príkazu;*
- *počte oznámení predložených v súlade s článkom 16 rozdelených podľa druhu dotknutého údajne nezákonného obsahu, **počte oznámení predložených dôveryhodnými nahlasovateľmi**, akýchkoľvek opatreniach prijatých na základe týchto oznámení rozlíšených podľa toho, či sa opatrenie prijalo na základe zákona alebo obchodných podmienok poskytovateľa, počte oznámení spracovaných výlučne automatizovanými prostriedkami a o mediáne času potrebnom na prijatie opatrení;*
- ***zmysluplné a zrozumiteľné informácie o moderovaní obsahu z vlastnej iniciatívy** poskytovateľov vrátane používania automatizovaných nástrojov, opatrení prijatých na poskytovanie odbornej prípravy a pomoci osobám zodpovedným za moderovanie obsahu, počtu a druhu prijatých opatrení, ktoré ovplyvňujú dostupnosť, viditeľnosť a prístupnosť informácií poskytovaných príjemcami služby, a schopnosti príjemcov*

[321] DSA, článok 14 ods. 1.
[322] DSA, článok 15 ods. 1.
[323] DSA, článok 24 ods. 1.
[324] DSA, článok 42 ods. 1.

poskytovať informácie prostredníctvom služby, ako aj o iných súvisiacich obmedzeniach služby; poskytnuté informácie sa delia podľa druhu nezákonného obsahu alebo porušenia obchodných podmienok poskytovateľa služieb, podľa metódy detekcie a druhu uplatneného obmedzenia;

- ***počte sťažností prijatých prostredníctvom vnútorných systémov vybavovania sťažností*** *v súlade s obchodnými podmienkami poskytovateľa a okrem toho v prípade poskytovateľov online platforiem v súlade s článkom 20, základe týchto sťažností, rozhodnutiach prijatých v súvislosti s týmito sťažnosťami, mediáne času potrebnom na prijatie týchto rozhodnutí a počte prípadov, v ktorých boli tieto rozhodnutia zrušené;*

- ***akomkoľvek použití automatizovaných prostriedkov na účely moderovania obsahu*** *vrátane kvalitatívneho opisu, špecifikácie presných účelov, ukazovateľov presnosti a možnej chybovosti automatizovaných prostriedkov použitých pri plnení týchto účelov a akýchkoľvek uplatnených záruk.*

- ***počte sporov predložených orgánom mimosúdneho riešenia sporov*** *uvedeným v článku 21, výsledky riešenia sporov a medián času potrebný na dokončenie postupov riešenia sporov, ako aj podiel sporov, v prípade ktorých poskytovateľ online platformy vykonal rozhodnutia orgánu;*

- ***počte pozastavení*** *uložených podľa článku 23, rozčlenených na pozastavenia uložené za poskytovanie zjavne nezákonného obsahu, predkladanie zjavne neopodstatnených oznámení a podávanie zjavne neopodstatnených sťažností.*

- ***ľudské zdroje, ktoré poskytovateľ veľmi veľkých online platforiem venuje moderovaniu obsahu v súvislosti so službou poskytovanou v Únii****, pre každý uplatniteľný úradný jazyk členských štátov vrátane dodržiavania povinností stanovených v článkoch 16 a 22, ako aj dodržiavania povinností stanovených v článku 20;*

- *kvalifikáciu a jazykové znalosti osôb vykonávajúcich činnosti* [uvedené alebo v predchádzajúcom bode]*, ako aj odbornú prípravu a podporu pre takýchto pracovníkov;*

- *ukazovatele presnosti a súvisiace informácie uvedené v článku 15 ods. 1 písm. e) podľa každého úradného jazyka členských štátov;*

- *priemernom mesačnom počte príjemcov služby za každý členský štát."*[325]

Ak sa VVOP rozhodne z dôvodov dôvernosti určitých informácií niektoré z nich verejnosti nekomunikovať, správu o transparentnosti v celistvosti predkladá KDS a Európskej komisii.[326]

Dizajn platforiem

Článok 25 DSA, podobne ako článok 25 GDPR upravuje povinnosť koncepcie a organizácie online rozhrania pre online platformy vrátane VVOP. V zmysle predmetného ustanovenia *„poskytovatelia online platforiem nesmú navrhovať, organizovať ani prevádzkovať svoje online rozhrania tak, aby zavádzali alebo manipulovali s príjemcami ich služieb alebo tak, aby podstatne narúšali alebo obmedzovali schopnosť príjemcov ich služieb prijímať slobodné a informované rozhodnutia."*[327] Európska komisia k diskutovanej povinnosti môže vydávať usmernenia.[328]

Táto povinnosť dopĺňa článok 25 GDPR,[329] ktorý upravuje inštitút špecificky navrhnutej a štandardnej ochrany osobných údajov a cieli na elimináciu tzv. temných vzorov (*dark patterns*) alebo manipulatívnych praktík online služieb. Podobne ako pri GDPR, analogicky aj pri DSA možno za manipulatívne prvky označiť „rozhrania a používateľské skúsenosti zakomponované do platforiem sociálnych médií, ktoré používateľov nútia robiť nezamýšľané, nedobrovoľné a potenciálne škodlivé rozhodnutia týkajúce sa spracúvania ich osobných údajov. To ovplyvňuje správanie používateľov a ich schopnosť účinne chrániť svoje osobné údaje."[330] Temným vzorom sa venoval aj expertný panel Organizácie pre ekonomickú spoluprácu a obchod.[331] Za takéto praktiky sa napríklad považuje nútenie užívateľa interagovať s veľkým množstvom informácií, notifikácií a možností, pričom cieľom je uviesť ho do stavu „odklikávania" a súhlasu s rôznymi praktikami. Iným príkladom je vizuálne prívetivejšie zobrazenia invazívnejšej možnosti pre užívateľa či schovávanie nastavenia parametrov v nastaveniach služby.[332]

[325] DSA, článok 15, 24 ods. 1 a 42 ods. 2.
[326] DSA, článok 42 ods. 5.
[327] DSA, článok 25 ods. 1.
[328] DSA, článok 25 ods. 3.
[329] Pozri LEISEER, M. Dark patterns': The case for regulatory pluralism between the European Union's consumer and data protection regimes. In KOSTA, E. et al. *Research Handbook on EU Data Protection Law*, Eward Elgar 2022.
[330] EUROPEAN DATA PROTECTION BOARD. *Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them*. Dostupné na: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en.
[331] OECD. *Dark Commercial Patterns*. OECD Digital Economy Papers October 2022 No. 336. Dostupné na:. https://www.oecd.org/digital/dark-commercial-patterns-44f5e846-en.htm.
[332] Tamže.

Napriek tomu, že tento inštitút si zatiaľ nevyžiadal hlbšiu akademickú diskusiu,[333] môže ísť o jeden z výrazných prvkov pri boji s dezinformáciami online. Pri viacerých inštitútoch DSA sa totiž vyžaduje aktivita užívateľa a ten by mal byť schopný urobiť relevantné a uvedomelé rozhodnutia bez podprahového ovplyvnenia.

Zobrazovanie reklamy

Zobrazovanie platených inzercií s dezinformačný obsahom je citlivou regulačnou a politickou témou. DSA upravuje pozitívne a negatívne požiadavky pre online platformy a VVOP v kontexte platených reklám. V zmysle článku 26 ods. 1 DSA musia užívatelia jednoznačným spôsobom vedieť identifikovať, že zobrazovaný obsah je reklamou, aká osoba sa ňou prezentuje a kto reklamu platí. Dôležitým aspektom je, že užívateľovi sa musia poskytnúť informácie aj o hlavných parametroch použitých na určenie príjemcu, ktorému sa reklama prezentuje, a prípadne o tom, ako tieto parametre zmeniť.[334] Inými slovami, každému užívateľovi online platformy musí byť jasné, z akých dôvodov je mu určitá reklama zobrazená a akým spôsobom môžu personalizáciu reklamy zmeniť. Za osobitne dôležitý taktiež považujeme zákaz zobrazovanie reklamy na základe profilovania z citlivých osobných údajov.[335] Tým pádom nebudú môcť online platformy zobrazovať cielenú reklamu na základe údajov o zdravotnom stave alebo sexuálnej orientácií. V kontexte lekcií zo šírenia dezinformácií počas pandémie COVID-19 to môže predstavovať výrazný limit pre šírenie dezinformácií, ktoré môžu byť zdravie alebo život ohrozujúce.

Okrem požiadaviek diskutovaných vyššie sú VVOP navyše povinné spravovať a zverejňovať repozitár (archív) zobrazovanej reklamy spolu s informáciami[336] o inzerentovi.[337]

---

[333] Výnimkou je výborná komparácia regulačných požiadaviek na temné vzory správania v online priestore z pohľadu práva EÚ. GRAEF, I. *The EU Regulatory Patchwork for Dark Patterns: An Illustration of an Inframarginal Revolution in European Law?* (April 3, 2023). Forthcoming as a book chapter in Ramsi A. Woodcock, Toward an Inframarginal Revolution: Markets as Wealth Distributors, Cambridge University Press 2023, TILEC Discussion Paper No. 2023-07, Tilburg Law School Research Paper. Dostupné na: http://dx.doi.org/10.2139/ssrn.4411537.

[334] DSA, článok 26 ods. 1.

[335] DSA, článok 26 ods. 3.

[336] DSA, článok 39 ods. 2: *„Archív musí obsahovať minimálne všetky tieto informácie:*

a) obsah reklamy vrátane názvu produktu, služby alebo značky a predmetu reklamy;
b) fyzickú alebo právnickú osobu, v mene ktorej sa reklama zobrazuje;
c) fyzickú alebo právnickú osobu, ktorá za reklamu zaplatila, ak je to osoba iná ako uvedená v písmene b);
d) obdobie, počas ktorého bola reklama zobrazovaná;
e) informácie o tom, či sa reklama mala zobrazovať osobitne jednej alebo viacerým konkrétnym skupinám príjemcov služby, a ak áno, hlavné parametre použité na tento účel vrátane prípadných hlavných parametrov použitých na vylúčenie jednej alebo viacerých takýchto konkrétnych skupín;
f) komerčné oznámenia zverejňované na veľmi veľkých online platformách a identifikované podľa článku 26 ods. 2;
g) *celkový počet oslovených príjemcov služby a prípadne súhrnné počty rozčlenené podľa členských štátov za skupinu alebo skupiny príjemcov, ktorým bola reklama konkrétne určená.*"

[337] DSA, článok 39 ods. 1.

Negatívnou povinnosťou je, aby repozitár neobsahoval žiadne osobné údaje príjemcov reklamy.[338]

Inštitúty občianskej spoločnosti

Požiadavky na jednotlivé atribúty fungovania online platforiem a dohľad nad nimi zo strany národných štátov alebo Európskej komisie nie sú jedinými mechanizmami, ktoré DSA ponúka na boj s dezinformáciami online. Na tomto mieste považujeme za vhodné aspoň stručne načrtnúť možnosti angažovanej občianskej spoločnosti pri moderovaní obsahu na platformách či vykonávaní kontroly.

Jedným z nových prvkov pri moderovaní obsahu na online platformách vrátane VVOP je privilegované postavenie tzv. dôveryhodných nahlasovateľov (*trusted flaggers*). O štatútu dôveryhodného nahlasovateľa môže požiadať akýkoľvek subjekt, pričom o udelení alebo neudelení tohto statusu rozhodujú KDS.[339] Dôveryhodným nahlasovateľom musí preukázať požiadavky na odbornosť na účely odhaľovania, identifikácie a oznamovania nezákonného obsahu, nezávislosť od poskytovateľov online platforiem a činnosť vykonávanú s cieľom predkladania objektívnych a presných oznámení online platformám.[340] Oznámenia dôveryhodných oznamovateľov musí platforma riešiť prednostne a bez zbytočného odkladu.[341] Subjekty, ktoré získali štatútu dôveryhodného nahlasovateľa budú uvedené vo verejne prístupnej databáze spravovanej Európskou komisiou.[342] Nakoľko štát nemusí mať vždy dostatočné personálne kapacity na nahlasovanie obsahu na online platformách, občianska spoločnosť prostredníctvom inštitútu dôveryhodných nahlasovateľov môže výrazne ovplyvniť kvalitu oznámení nezákonného obsahu a ich následné riešenie zo strany platforiem.

Ďalším zaujímavým inštitútom je prístup k dátam. Jedným z problémov online platforiem je ich nedostatočná možnosť kontroly[343] a prístup k informáciám zo strany vedeckých inštitúcií. Napriek tomu, že niektoré platformy poskytovali prístup vedeckým tímom k informáciám, išlo skôr o ojedinelé prípady a výrazne pod kontrolou a za podmienok určených platformou. Alternatívou bolo obchádzania všeobecných obchodných podmienok jednotlivých platforiem. DSA preto v článku 40 zakotvuje mechanizmus prístupu k údajom pre preverených

[338] Tamže.
[339] DSA, článok 22 ods. 2.
[340] Tamže.
[341] DSA, článok 22 ods. 1.
[342] DSA, článok 22 ods. 5.
[343] Pozri napríklad GORWA, R. - GARTON ASH, T. *Democratic transparency in the platform society*. SOC. MEDIA DEMOCR. STATE FIELD PROSPECTS REFORM 286 (2020).

výskumných pracovníkov (*vetted researchers*).[344] Požiadavka sa aplikuje na VVOP a samotnú žiadosť platforme musí zaslať KDS. Prístup preverených vedeckých pracovníkov je možné získať iba za účelom výskumu, ktorý prispieva k odhaľovaniu, identifikácii a pochopeniu systémových rizík v EÚ.[345] Ako sme uviedli vyššie, za systémové riziko možno jednoznačne považovať aj šírenie dezinformácií v online priestore. Podobne ako pri dôveryhodných nahlasovateľoch, previereným výskumníkom nemôže byť každý, ale DSA ustanovuje precízne požiadavky, za akých možno štatút previereného výskumníka získať.[346] Opätovne, o udelení alebo neudelení štatútu rozhoduje národný dozorný orgán podľa DSA.[347] VVOP môže žiadosť KDS na prístup k údajom pre preverených výskumníkov odmietnuť iba na základe taxatívne vymenovaných dôvodov a to ak k údajom nemajú prístup alebo poskytnutie prístupu k údajom by viedlo k vzniku významných zraniteľností z hľadiska bezpečnosti ich služby alebo ochrany dôverných informácií, najmä obchodného tajomstva.[348] Zároveň, ale VVOP musí navrhnúť alternatívu, ktorá adekvátne substituuje zamietnutú žiadosť.[349] Konečné slovo pri rozhodovaní má KDS. Práve aplikácia tejto výnimky otestuje efektívnosť inštitútu v aplikačnej praxi.

Preverení výskumníci môžu žiadať prístup k rôznych kategóriám dát. DSA uvádza napríklad údaje potrebné na posúdenie rizík a možných škôd spôsobených systémami VVOP, údaje o presnosti, fungovaní a testovaní algoritmických systémov na moderovanie obsahu, odporúčacích systémov alebo reklamných systémov, v prípade potreby vrátane trénovacích údajov a algoritmov, alebo údaje o postupoch a výstupoch moderovania obsahu alebo vnútorných systémov vybavovania sťažností v zmysle DSA.[350]

[344] DSA, článok 40 ods. 4.
[345] Tamže.
[346] Výskumní pracovníci musia preukázať, že:
„a) sú členmi výskumnej organizácie vymedzenej v článku 2 ods. 1 smernice (EÚ) 2019/790;
b) sú nezávislí od obchodných záujmov;
c) v ich žiadosti sa uvádza financovanie výskumu;
d) sú schopní splniť osobitné požiadavky na bezpečnosť a dôvernosť údajov súvisiace s každou žiadosťou, ochrániť osobné údaje a vo svojej žiadosti opísali vhodné technické a organizačné opatrenia, ktoré na tento účel zaviedli;
e) ich žiadosť preukazuje, že ich prístup k požadovaným údajom a časovým rámcom je potrebný a primeraný účelu ich výskumu a že očakávané výsledky uvedeného výskumu prispejú k účelom stanoveným v odseku 4;
f) plánované výskumné činnosti sa budú vykonávať na účely stanovené v odseku 4;
zaväzujú sa verejnosti bezplatne sprístupniť výsledky svojho výskumu v primeranej lehote po ukončení výskumu, s prihliadnutím na práva a záujmy príjemcov dotknutých služieb, v súlade s nariadením (EÚ) 2016/679." DSA, článok 40 ods. 8.
[347] DSA, článok 40 ods. 8.
[348] DSA, článok 40 ods. 5.
[349] Tamže.
[350] DSA, recitál 96.

Prirodzene preverení výskumníci po schválenej žiadosti musia dodržiavať povinnosti týkajúce sa zachovania dôvernosti informácií, práv duševného vlastníctva, bezpečnosti či ochrany osobných údajov.[351]

Aspekt kontroly zo strany preverených výskumníkov je v DSA koncipovaný veľmi výrazne, nakoľko tieto subjekty môžu vyhodnocovať aj opatrenia na zmiernenie rizík prijatých VVOP. Možno zhrnúť, že diskutovaný inštitútu má dve kľúčové funkcie a to (i) porozumieť fungovaniu platforiem a (ii) kontroly vhodnosti prijatých opatrení na riešenie systémových rizík.[352]

Vyššie uvedené inštitúty sú relevantné pre občiansku spoločnosť a poskytujú ďalšie významné nástroje mimo horizontálnych požiadaviek na online platformy, ktoré môže vyšetrovať a prípadne sankcionovať KDS alebo Európska komisia. V tomto smere je ale potrebné upozorniť, že aby predmetné inštitúty fungovali, sú potrebné investície štátu do občianskej spoločnosti.[353]

Zodpovednosť za obsah tretích strán

Základnou otázkou pri boji s dezinformáciami je stanoviť zodpovednosť kľúčových aktérov v procese šírenia dezinformácií, najmä VVOP, cez ktoré sa dezinformácie šíria najrýchlejšie. Je nevyhnutné diskutovať o možnostiach zodpovednosti za obsah, ktorý na tieto platformy pridávajú užívatelia. Z pohľadu slovenského práva ide o situáciu, kde dochádza k spolupôsobeniu pri páchaní deliktov vo forme účastníctva, použitia osoby na spáchanie deliktu alebo nezakročenia na ochranu práv inej strany.[354] Tento režim je tiež predmetom úpravy v DSA.

Vzhľadom na zameranie tejto práce sa zameriame na otázky zodpovednosti za cudzí obsah služieb "hosting," nakoľko práve do tohto typu služieb spadajú online platformy a veľmi veľké online platformy vrátane sociálnych sietí. Podobne ako pri predchádzajúcej právnej úprave, DSA zachováva koncept tzv. "bezpečného prístavu", a teda podmienok, ktoré ak

[351] Bližšie k týmto požiadavkám pozri EDELSON, L. - GRAEF, I. - LANCIERI, F. *Access to Data and Algorithms: For an Effective DMA and DSA Implementation*. (CERRE, March 2023), Dostupné na: https://cerre.eu/publications/access-to-data-and-algorithms-for-an-effective-dma-and-dsaimplementation.
[352] VERMEULEN, M. Researcher Access to Platform Data: European Developments. In *Journal of Online Trust and Safety*, 1(4), 2022. Dostupné na: https://doi.org/10.54501/jots.v1i4.84.
[353] HUSOVEC, M. *Will the DSA work? On money and effort*. Verfassungsblog. Dostupné na: https://verfassungsblog.de/dsa-money-effort/.
[354] HUSOVEC, M. Digitálny trh EÚ a zodpovednosť poskytovateľov služieb. In HUSOVEC, M. - MESARČÍK, M. - ANDRAŠKO, J. *Právo informačných a komunikačných technológií I*. TINCT, 2021, s. 128 a nasl.

hostingová služba splní, nie je zodpovedná za obsah tretích strán. DSA tieto podmienky upravuje v článku 6 ods. 1 a bezpečný prístav poskytovateľ služby má, ak

- *„nemá skutočnú vedomosť o nezákonnej činnosti alebo nezákonnom obsahu a vzhľadom na nároky na náhradu škody si nie je vedomý skutočností alebo okolností, z ktorých by bolo zrejmé, že ide o nezákonnú činnosť alebo nezákonný obsah alebo*
- *po získaní takejto vedomosti alebo povedomia urýchlene koná, aby nezákonný obsah odstránil alebo k nemu znemožnil prístup.*"

Podmienkou pre dosiahnutie bezpečného prístavu a vyhnutie sa zodpovednosti je pasivita poskytovateľa hostingovej služby. Filtrovanie a zobrazovanie konkrétneho obsahu určeného pre jednotlivých užívateľov sa považuje za technickú a pasívnu súčasť fungovania platforiem.[355] Avšak, toto tvrdenie sa stáva predmetom diskusie vzhľadom na aktivity platforiem zameraných na udržanie pozornosti a algoritmické rozhodovanie o zobrazovanom obsahu.[356] Rakúsky najvyšší súd sa v prípade predloženom na riešenie aj Súdnemu dvoru Európskej Únie zaoberal otázkou, či online platformy ostávajú neutrálne, ak optimalizujú zobrazovanie svojho obsahu.

Rakúsky najvyšší súd sa priklonil k interpretácii, že takéto konanie je tradičný obchodný model a štruktúrovanie vyhľadávania by stále malo byť považované za pasívne správanie platformy.[357] Zároveň je dôležité, aby prevádzkovateľ hostingovej služby nijako nenavádzal priamo ani nepriamo na spáchanie deliktu, pretože ak tak urobí, stráca svoj štatút bezpečného prístavu a nesie zodpovednosť za danú činnosť.[358] V prípade, že prevádzkovateľ získa reálnu (napríklad na základe oznámenia) alebo konštruktívnu vedomosť (napríklad z vlastnej činnosti)[359] o nezákonnej činnosti alebo obsahu, je povinný prijať opatrenia s cieľom odstrániť takýto obsah alebo znemožniť prístup k nemu. DSA poskytuje presný opis mechanizmu na oznamovanie nezákonného obsahu zo strany užívateľov alebo iných subjektov (tzv. notice and action mechanism). Ak tieto oznámenia spĺňajú požiadavky stanovené nariadením, považujú

[355] BUITEN, M. *The Digital Services Act: From Intermediary Liability to Platform Regulation*. Working Paper. Dostupné na https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3876328, s. 15. Zhodne EURÓPSKA KOMISIA. *Impact assessment accompanying the document proposal for a regulation of the european parliament and of the council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*. SWD(2020) 348 final, s. 159.

[356] BUITEN, M. *The Digital Services Act: From Intermediary Liability to Platform Regulation.* Working Paper. Dostupné na https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3876328, s. 15.

[357] *Handelsgericht Wien*. Puls 4 TV GmbH & Co. KG v YouTube LLC and Google Austria GmbH, prípad č. 4 R 119/18a, s. 10.

[358] DSA, článok 6 ods. 2.

[359] K tomu pozri napríklad rozhodnutie Súdneho dvora EÚ č. C-324/09 vo veci z 12. júla 2011 L'Oréal SA a iní proti eBay International AG a iní alebo spojené veci C-236/08 až C-238/08 z 23. marca 2010 Google.

sa za dostatočne presné, aby prevádzkovatelia mohli vyhodnotiť skutočnú vedomosť o nelegálnom obsahu a následne musia rýchlo konať a proti takémuto obsahu zakročiť.

Článok 7 DSA zároveň výslovne podporuje dobrovoľné vyšetrovania zo strany platforiem. Pri aktivitách zameraných na odhaľovanie, identifikáciu a odstraňovanie nezákonného obsahu alebo znemožnenie prístupu k nemu alebo prijímania potrebných opatrení na dosiahnutie súladu s právnymi požiadavkami sa môžu spoľahnúť na výnimku zo zodpovednosti uvedenej vyššie.[360] Zjednodušene, ak platforma vykonáva dobrovoľné šetrenie svojho obsahu, nemusí to automaticky z pohľadu práva znamenať nadobudnutie objektívnej vedomosti o nelegálnom obsahu. Platforma sa stále môže spoľahnúť na podmienky bezpečného prístavu.

DSA podobne ako predchádzajúca právna úprava obsahuje zákaz všeobecnej povinnosti monitorovania.[361] Súdny dvor EÚ opakovane vo svojej judikatúre uvádza, že všeobecná povinnosť monitorovať obsah by pre prevádzkovateľov znamenala výrazný zásah do práva na podnikanie a v dlhodobom horizonte limity pre vývoj inovácií.[362] Azda najlepšie to vyjadril generálny advokát v prípade Youtube/Cyando v kontexte ochrany autorského práva.[363] Jeho závery je ale analogicky možné aplikovať aj na povinnosť kontroly akéhokoľvek obsahu pred publikovaním na platformách: *"Požiadavka, aby prevádzkovatelia platforiem s cieľom vyhľadávania akéhokoľvek porušenia autorských práv* ***všeobecným a abstraktným spôsobom kontrolovali všetky súbory****, ktoré majú ich používatelia v úmysle zverejniť, ešte pred ich nahraním na internet, by pritom* ***predstavovala značné riziko zásahu do týchto rôznych základných práv****. Vzhľadom na potenciálne obrovské množstvo ukladaného obsahu by totiž jednak bolo nemožné manuálne vykonávať takúto predbežnú kontrolu, a jednak riziko spojené so zodpovednosťou by bolo pre týchto prevádzkovateľov neúmerné. V praxi by hrozilo, že najmenší prevádzkovatelia by túto zodpovednosť nezvládli, a* ***tí, ktorí majú dostatočné zdroje, by boli nútení pristúpiť k všeobecnému filtrovaniu obsahu svojich používateľov bez súdneho preskúmania, čo by viedlo k následnému riziku „nadmerného odstraňovania" tohto obsahu."*** [364]

[360] Ide o klauzulu tzv. Dobrého samaritána. Pozri viac KUCZERAWY, A. *The Good Samaritan that wasn't: voluntary monitoring under the (draft) Digital Services Act*. Dostupné na: https://verfassungsblog.de/good-samaritan-dsa/.
[361] DSA, článok 8: *„Poskytovateľom sprostredkovateľských služieb sa neukladá všeobecná povinnosť monitorovať informácie, ktoré títo poskytovatelia prenášajú alebo uchovávajú, ani povinnosť aktívne zisťovať skutočnosti alebo okolnosti naznačujúce nezákonnú činnosť."*
[362] Pozri napríklad rozhodnutie Súdneho dvora EÚ C-360/10 zo dňa 16. Februára 2012 vo veci SABAM v Netlog.
[363] Rozhodnutie Súdneho dvora EÚ C-682/18 zo dňa 22. júna 2021 Frank Peterson proti Google LLC a i. a Elsevier Inc. proti Cyando AG.
[364] Tamže, bod 242.

3.1.1.3 Kódexy správania a Kódex nakladania s dezinformáciami z roku 2022

Osobitnou možnosťou boja proti dezinformáciám v intenciách DSA je prijatie kódexov správania (*Codes of conduct)*, ktoré predstavujú samoregulačný nástroj pre trhových aktérov. DSA v článku 35 upravuje apel na Európsku komisiu a Výbor pre digitálne služby podporovať vypracovanie takýchto kódexov.[365] Pri významných systémových rizikách, ktorým šírenie dezinformácií nepochybne je, Európska komisia môže VVOP vyzvať na zapojenie do prípravy takýchto kódexov, ktoré by mali obsahovať konkrétne opatrenia na zmiernenie rizík a záväzok tieto opatrenia dodržiavať.[366] Kódexy musia obsahovať merateľné ukazovatele na dosahovanie vytýčených cieľov.[367] Následne Európska komisia posudzuje a vyhodnocuje dodržiavanie kódexov správania.[368]

Na preklenutie legislatívnej medzery bola v roku 2018 prijatá prvá verzia Kódexu nakladania s dezinformáciami (ďalej len „Kódex"), ktorého signatármi sa okrem iných stali aj Facebook, Google, Twitter či Mozilla.[369] Po vyhodnotení jeho účinnosti bola následne v roku 2022 prijatá posilnená verzia Kódexu.

Samotný Kódex je založený na dodržiavaní slobody prejavu a základných ľudskoprávnych štandardoch.[370] Jeho účelom je zaviesť opatrenia na zvládanie výziev spojených s fenoménom dezinformácií. Predmetné opatrenia boli vypracované s cieľom zlepšiť informačné prostredie a minimalizovať šírenie nepravdivých informácií. Účel kódexu zároveň načrtáva aj čiastkové ciele, ktoré reflektujú konkrétne opatrenia a záväzky signatárov. Prvým cieľom je zameranie na implementáciu záruk, ktoré by mali zabrániť šíreniu dezinformácií. Druhým cieľom je dôraz na reguláciu umiestňovania reklamy s cieľom znížiť príjmy tých, ktorí šíria dezinformácie. Ciele zdôrazňujú potrebu transparentnosti v oblasti politických reklám a reklám týkajúcich sa aktuálnych problémov. Ďalším cieľom je implementácia politík na potlačenie skreslenia skutočnosti a zabezpečenie presnosti informačného obsahu. Signatári Kódxu by sa taktiež mali snažiť o detekciu a odhalenie falošných účtov a tzv. botov, ktoré šíria dezinformácie. Pri implementácií konkrétnych opatrení Kódex zvýrazňuje potrebu ochrany integrity služieb, ktorých cieľom je šíriť dezinformácie, pričom je nutné dodržiavať zásady ľudských práv. Ďalší ciel upriamuje pozornosť na využívanie technologických prostriedkov,

[365] DSA, článok 35 ods. 1.
[366] DSA, článok 35 ods. 2.
[367] DSA, článok 35 ods. 3.
[368] DSA, článok 35 ods. 4.
[369] *Kódex nakladania s dezinformáciami*. Dostupné na: https://digital-strategy.ec.europa.eu/en/news/code-practice-disinformation.
[370] Kódex, preambula.

ktoré by mali v algoritmoch vyhľadávania prednostne zobrazovať relevantné, autentické, presné a dôveryhodné informácie. Dôležité je aj zachovanie slobody prejavu a neskĺznuť k vymazávaniu legálneho obsahu alebo obmedzovanie prístupu na základe subjektívneho označenia informácií za "nepravdivé". Ďalší ciel zdôrazňuje potrebu transparentnosti, ktorá umožní používateľom identifikovať pôvod politických reklám a overiť dôveryhodnosť zdrojov obsahu. Viditeľnosť dôveryhodného obsahu na internete by mala byť zvýšená a používatelia by mali mať k dispozícií nástroje, ktoré umožnia personalizovaný prístup k objavovaniu rôznych zdrojov. Posledným cieľom je dôležitosť zabezpečenia prístupu k údajom, ktoré by mohli byť využité na overovanie faktov a výskumné účely za zachovania ochrany súkromia.[371]

Konkrétne záväzky signatárov sú diferencované do piatich oblastí:

- Kontrola umiestňovania reklám
- Politická reklama a reklama zameraná na aktuálne problémy
- Integrita služieb
- Posilnenie postavenia spotrebiteľov
- Posilnenie výskumnej obce.
- Posilnený Kódex z roku 2022 osobitne upravuje aj posilnenie komunity na overovanie faktov a kreovanie centra transparentnosti či stálej pracovnej skupiny.

Kontrola umiestňovania reklám zahŕňa záväzok signatárov, že prijmú opatrenia na obmedzenie reklamných a monetizačných stimulov, ktoré by mohli povzbudiť nežiaduce správanie, ako je skresľovanie dôležitých informácií o sebe alebo svojich aktivitách. Tieto opatrenia môžu zahŕňať obmedzenie reklamných služieb alebo platobných umiestnení, prípadne spoluprácu s organizáciami pre overovanie faktov.[372] V oblasti politickej reklamy sa signatári zaväzujú dodržiavať platné právne predpisy EÚ a národné právne úpravy týkajúce sa povinnosti zreteľne oddeliť reklamu od redakčného obsahu, vrátane spravodajstva, bez ohľadu na jej formu a médium, na ktorom sa zobrazuje. Reklama musí byť jednoznačne a ľahko rozpoznateľná ako platená komunikácia alebo by mala byť vhodne označená. Taktiež sa signatári zaväzujú umožniť zverejnenie politických reklám, ktoré môžu obsahovať informácie o skutočnej totožnosti sponzora a finančných prostriedkoch vynaložených na takéto reklamy. Signatári sa zaväzujú prijať primerané kroky na zverejnenie „reklamy zameranej na aktuálne

[371] Kódex, I. Účely.
[372] Kódex, II. A.

problémy".[373] Integritu služieb zabezpečuje záväzok signatárov implementovať transparentné politiky týkajúce sa identifikácie a potláčania zneužívania automatizovaných botov v rámci svojich služieb.[374] V oblasti posilnenia práv spotrebiteľov sa signatári Kódexu zaväzujú investovať do rozhraní, ktoré umožnia lepšie informované rozhodnutia používateľov, preferenciu autentických správ či jednoduché vyhľadávanie alternatívnych zdrojov informácií.[375] Výskumná obec by mala byť posilnená v podpore výskumu dezinformácií na platformách a organizácia konferencií.[376]

Posilnený Kódex z roku 2022 obsahuje 43 konkrétnych opatrení, pričom pridáva oblasti ako posilnenie spolupráce, koordinácia s overovateľmi faktov, či kreovanie centra transparentnosti pre overovanie súladu s Kódexom. Z hľadiska formulácia jednotlivých záväzkov a opatrení je v mnohom špecifickejší a detailnejší, ako pôvodná verzia Kódexu.

Meranie záväzkov uvedených vyššie prebieha prostredníctvom vypracovania ročnej správy.[377] Zaujímavosťou je, že dodržiavanie Kódexu správania môže Európska komisia vyhodnotiť ako jeden z faktorov na zmierňovanie rizík v zmysle DSA.

3.1.2 Regulácia umelej inteligencie

Európska komisia v apríli 2021 po niekoľko-mesačných snahách predstavila prvý komplexný návrh regulácie umelej inteligencie na svete – návrh nariadenia o umelej inteligencií (*Artificial Intelligence Act*, AIA). Nadviazala tak na dlhoročnú prácu expertných skupín a požiadaviek orgánov Európskej únie v podobe stanovísk či odporúčaní.[378] V decembri 2022 publikovala svoju pozíciu (všeobecné smerovanie) k AIA Rada EÚ.[379] Dlho očakávaná pozícia Európskeho parlamentu bola schválená v júny 2023[380] a v ten istý mesiac začali trialógy. Konečné znenie AIA je v súčasnosti predmetom diskusie. V rámci analýzy tohto právneho rámca budeme vychádzať z pôvodného návrhu Európskej komisie, upozorníme aj na návrhy a doplnenia od Rady EÚ a Európskeho parlamentu, ktoré majú relevanciu pre šírenie dezinformácií v online priestore.[381]

---

[373] Kódex, II. B.
[374] Kódex, II. C.
[375] Kódex, II. D.
[376] Kódex, II. E.
[377] Kódex, III. Meranie a monitorovanie účinností Kódexu.
[378] Napríklad EXPERTNÁ SKUPINA NA VYSOKEJ ÚROVNI PRE UMELÚ INTELIGENCIU. *Etické Usmernenia Pre Dôveryhodnú Umelú Inteligenciu*. Dostupné na: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.
[379] Pozícia je dostupná online na https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf.
[380] Pozícia je dostupná online na https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html.
[381] Pri referenciách na pozície Rady EÚ a Európskeho parlamentu budeme vždy v poznámke pod čiarou uvádzať, že ide o takúto pozíciu. Ak informácia chýba, reflektujeme na pôvodný návrh Európskej komisie z roku 2021.

Dopadová štúdia k návrhu AIA uvádza 6 dôvodov pre prijatie regulácie umelej inteligencie (AI) na úrovní EÚ, konkrétne:

- Využívanie AI predstavuje zvýšené riziko pre bezpečnosť jednotlivcov,
- Využívanie AI predstavuje zvýšené riziko porušovania základných ľudských práv a slobôd,
- Dozorné orgány nemajú právomoci, procesné rámce a zdroje na zabezpečenie a monitorovanie súlad vývoja a používania umelej inteligencie s platnými pravidlami,
- Právna neistota ohľadom uplatnenia súčasného právneho rámca na systémy AI,
- Nedôvera k AI by znížila inovatívnosť a konkurecieschopnosť EÚ v globálnom meradle
- Fragmentované opatrenia predstavujú prekážky pre ďalší vývoj jednotného digitálneho trhu a suverenity.[382]

Práve riziko v podobe negatívneho vplyvu na základné ľudské práva a slobody má vysokú relevanciu pre šírenie dezinformácií online. Ako uvádza dopadová štúdia, otázky manipulácie osôb vrátane zraniteľných osôb prostredníctvom AI sú relevantné z hľadiska práva na ľudskú dôstojnosť a osobnej autonómie.[383]

AIA si za cieľ kladie harmonizovať pravidlá systémov AI pri uvádzaní a používaní v EÚ, zakázať určité systémy AI, upraviť špecifické požiadavky pre vysokorizikové systémy AI, zakotviť požiadavky transparentnosti pre špecifické systémy AI a harmonizovať pravidlá dohľadu a monitorovania trhu.[384]

AIA je formulovaná ako produktová regulácia a porovnať to možno s požiadavkami na produkty ako napríklad zdravotnícke pomôcky alebo elektronické výrobky pri uvedení na trh. To znamená, že určuje špecifické vlastnosti a požiadavky na systémy AI, ktoré musia byť splnené pri uvedení na trh a veľkú zodpovednosť ponecháva na samotných prevádzkovateľoch týchto systémov prostredníctvom inštitútu posúdenia zhody (*conformity assessment*).

[382] EURÓPSKA KOMISIA. *Commission staff working document impact assessment accompanying the proposal for a regulation of the european parliament and of the council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts*. {COM(2021) 206 final} - {SEC(2021) 167 final} - {SWD(2021) 85 final}.
[383] Tamže, s. 20 – 21.
[384] AIA, článok 1.

AIA je horizontálna regulácia založená na skúmaní rizika. To prakticky znamená, že vymedzuje systémy AI v kontexte rôznych typov rizík pre základné ľudské práva a slobody[385] a následne upravuje špecifické právne požiadavky pre tieto systémy v danej kategórií. AIA rozlišuje systémy AI, ktoré predstavujú:

- Neakceptovateľné riziko (zakázané praktiky),
- Vysoké riziko,
- Nízke riziko,
- Žiadne riziko.

Takmer vôbec sa regulácia netýka systémov AI nízkeho resp. minimálneho rizika, kde ustanovuje iba strohé požiadavky na transparentnosť a odporúčanie prijatia kódexov správania, ktoré výrobcovia a prevádzkovatelia takýchto AI systémov budú dodržiavať.

Zaujímavosťou sú aj sankcie za porušenie AIA. Tie sú upravené ešte striktnejšie ako pri GDPR. Za porušenie ustanovení AIA bude možné uložiť pokutu až do výšky 30 000 000 EUR, alebo ak je porušiteľom spoločnosť, až do výšky 6 % jej celkového svetového ročného obratu za predchádzajúci účtovný rok, podľa toho, ktorá suma je vyššia za porušenie zakázaných praktík a nesúlad s požiadavkami na správu údajov. Ďalej AIA umožňuje správne pokuty do výšky 20 000 000 EUR a 10 000 000 EUR.[386] Návrhy Rady EÚ a Európskeho parlamentu tieto sankcie znižujú.

AIA ustanovuje povinnosť pre členské štáty kreovať alebo určiť dozorný orgán, ktorý bude vykonávať štátny dozor. Na úrovní EÚ zároveň vznikne Európska rada pre umelú inteligenciu. Európsky parlament navrhuje silnejšiu rolu Úradu pre umelú inteligenciu (*AI Office*). Zároveň bude musieť každý členský štát dezignovať národný dozorný orgán.

3.1.2.1 Pôsobnosť právneho predpisu

Kľúčovou definíciou regulácie je pojem systémy AI. Ten je definovaný ako *„softvér vyvinutý s jednou alebo viacerými technikami a prístupmi uvedenými v prílohe I, ktorý môže pre daný súbor cieľov vymedzených človekom vytvárať výstupy, ako je obsah, predpovede,*

[385] Napríklad AIA, recitál 15: *„Využívanie umelej inteligencie má síce mnoho výhod, túto technológiu však možno zneužiť a môže sa stať zdrojom nových a výkonných nástrojov umožňujúcich manipulatívne a zneužívajúce praktiky a praktiky v oblasti sociálnej kontroly. Takéto praktiky sú mimoriadne škodlivé a mali by sa zakázať, pretože sú v rozpore s hodnotami Únie týkajúcimi sa **rešpektovania ľudskej dôstojnosti, slobody, rovnosti, demokracie a právneho štátu a základných práv Únie vrátane práva na nediskrimináciu, ochranu údajov a súkromia a práv dieťaťa.***"

[386] AIA, článok 71.

odporúčania alebo rozhodnutia ovplyvňujúce prostredie, s ktorým sú v interakcii."[387] Príloha I AIA následne uvádza konkrétne techniky spadajúce pod pojem AI.[388] Predmetná definícia je rozsiahlo kritizovaná technologickým sektorom, ale aj akademickou obcou pre svoju všeobecnosť a širokosť.[389] Rada EÚ vo svojej pozície navrhuje definíciu zúžiť a doplniť jej vysvetlenie v recitálovej časti. Európsky parlament navrhuje v regulácií zakotviť definíciu systému AI, ktorá vychádza z dokumentov na úrovni Organizácia pre hospodársku spoluprácu a rozvoj (OECD). Systém AI je v návrhoch Európskeho parlamentu definovaný ako *„strojový systém, ktorý je navrhnutý tak, aby fungoval s rôznou úrovňou autonómie a ktorý môže pre explicitné alebo implicitné ciele vytvárať výstupy, ako sú predpovede, odporúčania alebo rozhodnutia, ktoré ovplyvňujú fyzické alebo virtuálne prostredie.*"[390]

AIA by sa mala vzťahovať na poskytovateľov systémov AI bez ohľadu na to, či sú v EÚ usadení alebo nie, postačí, ak je splnené kritérium, že budú systémy AI uvádzať na trhu alebo prevádzkovať v rámci EÚ.[391] Nariadenie sa ďalej bude vzťahovať na používateľov systémov AI nachádzajúcich sa v EÚ. V zmysle pôvodného návrhu však nejde o fyzické osoby ako jednotlivcov, ktorých práva, záujmy a slobody môžu byť ohrozené, ale o skôr o *business users*.[392] Extra-teritoriálna pôsobnosť AIA je zvýraznená aj tým, že sa bude vzťahovať na poskytovateľov používateľov systémov AI z tretích krajín, ak výstupy tvorené ich systémami sa využívajú v EÚ.[393] AIA sa bude vzťahovať na tie systémy, ktoré budú uvedené na trhu po nadobudnutí účinnosti. Súčasné používané vysokorizikové systémy AI budú musieť spĺňať požiadavky AIA iba v prípade, ak prejdú „zásadnou zmenou," pričom tento pojem v regulácií nie je definovaný.[394] Vytváranie takejto dvojkoľajnosti je predmetom kritiky a tento prístup môže ešte zákonodarca upraviť.

Z hľadiska negatívnej pôsobnosti sa AIA nevzťahuje na systémy umelej inteligencie vyvinuté alebo používané výlučne na vojenské účely a na produkty v rámci právnych aktov

[387] AIA, článok 3 bod 1.
[388] Konkrétne
„a)prístupy strojového učenia vrátane učenia s učiteľom, bez učiteľa a učenia posilňovaním pomocou širokého spektra metód vrátane hĺbkového učenia;
b)prístupy založené na logike a poznatkoch vrátane reprezentácie poznatkov, induktívneho (logického) programovania, vedomostných základní, inferenčných a deduktívnych mechanizmov, (symbolického) uvažovania a expertných systémov;
c)štatistické prístupy, bayesovský odhad, metódy vyhľadávania a optimalizácie."
[389] Napríklad SCHUETT, J. *Defining the Scope of AI Regulations*. Forthcoming in Law, Innovation and Technology, Legal Priorities Project Working Paper Series No. 9. Dostupné na: https://ssrn.com/abstract=3453632.
[390] Pozícia Európskeho parlamentu k AIA, článok 3 bod 1.
[391] AIA, článok 2 ods. 1 písm. a).
[392] AIA, článok 2 ods. 1 písm. b) v spojitosti článkom 3 bodom 4.
[393] AIA, článok 2 ods. 1 písm. c).
[394] AIA, článok 83.

výslovne vymenovaných v článku 2 ods. 2 AIA. Návrhy Rady EÚ z pôsobnosti AIA vynímajú aj systémy AI využívané na účely národnej bezpečnosti a bezpečnosti členských štátov.[395] Európsky parlament vo svojej pozícií bude negociovať vylúčenie vývoja a výskumu systémov AI a taktiež open-source systémy AI, ktoré nepredstavujú vysoké riziko z pôsobnosti AIA.[396]

3.1.2.2 Inštitúty relevantné pre boj s dezinformáciami online

AIA predstavuje pomerne komplexnú reguláciu, ktorá reflektuje prístup založený na skúmaní rizika jednotlivých systémov AI. Ak chceme posúdiť relevantnosť jednotlivých inštitútov pre boj s dezinformáciami online, musíme v prvom rade analyzovať, či niektoré z činností primárne odporúčacích systémov na sociálnych médiách nespadajú pod zakázané praktiky alebo vysokorizikové systémy AI. Následne môžeme pristúpiť k diskusií o jednotlivých požiadavkách na vysokorizikové systémy AI. Diskusiu nemožno obmedziť iba na odporúčacie systémy, ale taktiež na tzv. generatívnu umelú inteligenciu a teda systémy, ktoré na základe pokynov jednotlivcov generujú obsah. Nie je nutné hlbšie rozoberať, že takýto obsah môže mať aj dezinformačnú kvalitu. Z tohto dôvodu považujeme za nevyhnutné analyzovať požiadavky na generatívny systémy AI a taktiež na transparentnosť z pohľadu interakcie systémov AI a ich výstupov s človekom.

Zakázané praktiky

Na vrchole pyramídovej regulácie sú systémy AI, ktoré predstavujú neprijateľné riziko a zákonodarca sa ich rozhodol zakázať. Ide o systémy AI, ktoré predstavujú neakceptovateľné riziko pre bezpečnosť, zdravie a základné ľudské práva a slobody. Článok 5 AIA, ktorý upravuje tieto zákazy do istej miery reflektuje diskusiu o tzv. červených čiarach pri systémoch AI.[397] Ide o 4 zakázané praktiky, pričom posledná z nich obsahuje aj niekoľko výnimiek. AIA výslovne zakazuje:

1) *„uvádzanie na trh, uvádzanie do prevádzky alebo používanie systému umelej inteligencie, ktorý s cieľom podstatne narušiť správanie osoby* ***využíva podprahové techniky mimo vedomia osoby*** *tak, že tejto alebo inej osobe spôsobí alebo by mohol*

[395] Pozícia Rady EÚ, článok 2.
[396] Pozícia Európskeho parlamentu, článok 2 ods. 5d a 5e.
[397] K tomu pozri napríklad EDRI. *Civil society calls for AI red lines in the European Union's Artificial Intelligence proposal*. Dostupné na: https://edri.org/our-work/civil-society-call-for-ai-red-lines-in-the-european-unions-artificial-intelligence-proposal/. UNITED NATIONS – HUMAN RIGHTS, OFFICE OF THE HIGH COMMISSIONER. *New and emerging technologies need urgent oversight and robust transparency: UN experts*. Dostupné na: https://www.ohchr.org/en/press-releases/2023/06/new-and-emerging-technologies-need-urgent-oversight-and-robust-transparency.

spôsobiť fyzickú alebo psychickú ujmu."[398] Ako príklad takéhoto systému možno uviesť využívanie zvukových podprahových techník, ktoré udržia zamestnancov vo vyššej výkonnosti s potenciálom škody na mentálnom[399] alebo fyzickom zdraví;

2) *„uvádzanie na trh, uvádzanie do prevádzky alebo používanie systému umelej inteligencie, ktorý* ***s cieľom podstatne narušiť správanie osoby patriacej do konkrétnej skupiny osôb využíva ktorúkoľvek zo zraniteľností*** *tejto skupiny osôb vyplývajúcich z ich veku, fyzického alebo duševného postihnutia tak, že tejto alebo inej osobe spôsobí alebo by mohol spôsobiť fyzickú alebo psychickú ujmu.*"[400] Pod tento zákaz možno zaradiť napríklad hračky pre deti, ktoré maloletých budú nútiť do nebezpečných aktivít ako bábika hovoriaca maloletým užívateľom o pozitívnom účinku tvrdej drogy;

3) *„uvádzanie na trh, uvádzanie do prevádzky alebo používanie systémov umelej inteligencie* ***orgánmi verejnej moci alebo v ich mene na účely hodnotenia alebo klasifikácie dôveryhodnosti fyzických osôb*** *počas určitého obdobia na základe ich spoločenského správania alebo známych či predpokladaných osobných alebo osobnostných charakteristík, pričom takto získané sociálne skóre vedie k jednému alebo obidvom z týchto výsledkov: (i)* ***škodlivé alebo nepriaznivé zaobchádzanie*** *s určitými fyzickými osobami alebo celými skupinami fyzických osôb* ***v sociálnych kontextoch****, ktoré* ***nesúvisia*** *s kontextmi, v ktorých boli údaje pôvodne generované alebo zhromaždené a/alebo (ii) škodlivé alebo nepriaznivé zaobchádzanie s určitými fyzickými osobami alebo celými skupinami fyzických osôb, ktoré je* ***neodôvodnené alebo neprimerané*** *ich spoločenskému správaniu alebo jeho závažnosti.*"[401] Predmetný zákaz reflektuje situáciu, ak by orgány verejnej moci zaviedli systém hodnotenia občanov, ktorý by im podľa získaných bodov (ne)umožňoval využívať hromadnú dopravu, diaľkové spoje alebo sociálne služby. Podobný systém funguje v niektorých ázijských krajinách.[402]

---

[398] AIA, článok 5 ods. 1 písm. a).

[399] K otázke rešpektovania duševného zdravia zamestnanca pozri napríklad LADIVEROVÁ, E. – NEVICKÁ, D. Práca z domu a domácka práva. In *Bratislavské právnické fórum 2021: Realizácia sociálnych práv v období pandémie*. 1. vyd. Bratislava : Právnická fakulta UK, 2021, s. 83-87 alebo LADIVEROVÁ, E. – NEVICKÁ, D. Pružný pracovný čas v home office – súmrak flexibilných foriem zamestnávania. In *Bratislavské právnické fórum 2022: raison ď être pracovného práva a práva sociálneho zabezpečenia na Slovensku - 100 rokov vývoja a vyhliadky do budúcnosti.* 1. vyd. IBratislava : Právnická fakulta UK, 2022, s. 80-86.

[400] AIA, článok 5 ods. 1 písm. b).

[401] AIA, článok 5 ods. 1 písm. c).

[402] K tomu pozri KASL, F. Surveillance in digitalized society: the chinese social credit system from a european perspective. In *The Lawyer Quarterly*, Vol 9, No 4 (2019).

4) *„používanie systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva"*[403] s výnimkou špecifických prípadov a podmienok, keď orgány presadzovania práva (napríklad orgány činné v trestnom konaní) môžu systémy diaľkovej biometrickej identifikácie (kamery s funkciou rozpoznávania tváre) použiť. Mohlo by sa tak stať napríklad pri hľadaní detí alebo pri predchádzaní teroristických útokov. AIA ale zároveň vyžaduje splnenie viacerých požiadaviek, ak by sa členské štáty rozhodli takýto systém nasadiť. Predovšetkým ide o požiadavku nezávislého dohľadu resp. povolenia súdneho alebo iného orgánu s využitím takýchto metód.[404] Zároveň musí byť zachovaná proporcionalita nasadenia takéhoto systému AI.[405]

Rada EÚ navrhuje rozšíriť zákaz hodnotenia jednotlivcov na základe ich spoločenského správania alebo známych či predpokladaných osobných alebo osobnostných charakteristík aj na súkromný sektor. Zároveň pozícia Rady EÚ obsahuje doplnenia zraniteľnosti jednotlivcov o ich sociálnu alebo ekonomickú situáciu. Využitie systémov vzdialenej biometrickej identifikácie navrhuje pozícia ešte viac limitovať, aby jeho využívanie bolo iba v naozaj výnimočných situáciách.[406]

Európsky parlament vo svojej pozícií navrhuje spresniť zákaz využívania systémov AI, ktoré podprahovo ovplyvňujú vedomie jednotlivcov s tým, že nariadenie bude alternatívne stanovovať nielen využitie podprahových techník, ale aj zámerné manipulatívne alebo klamlivé techniky, čím sa zákaz rozšíri. Výnimku zo zákazu budú mať systémy AI na terapeutické účely s informovaným súhlasom pacientov. Podobne ako Rada EÚ, aj Európsky parlament navrhuje doplniť zákaz zneužívania zraniteľností osôb o sociálne a ekonomické faktory s tým, že môže ísť o nielen známu zraniteľnosť, ale aj predpokladanú (predikovanú). Totožne ako Rada EÚ, aj Európsky parlament navrhuje rozšíriť zákaz profilovania na súkromných aktérov. Pozícia Európskeho parlamentu ale obsahuje doplňujúce zakázané praktiky, konkrétne:

- používanie biometrických kategorizačných systémov, ktoré kategorizujú fyzické osoby podľa citlivých alebo chránených atribútov alebo charakteristík alebo na základe odvodenia týchto atribútov alebo charakteristík. Výnimka sa navrhuje pre terapeutické účely po informovanom súhlase pacienta,

[403] AIA, článok 5 ods. 1 písm. d) v spojení s odsekmi 2-4.
[404] AIA, článok 5 ods. 3.
[405] AIA, článok 5 ods. 2 – 4.
[406] Pozícia Rady EÚ, článok 5.

- vykonávanie hodnotenia rizík fyzických osôb alebo ich skupín s cieľom posúdiť riziko fyzickej osoby, že spácha trestný čin alebo opakovane spácha trestný čin, alebo na predvídanie výskytu alebo opakovaného výskytu skutočného alebo potenciálneho trestného činu alebo správneho deliktu na základe profilovania fyzickej osoby alebo na základe posúdenia osobnostných vlastností a charakteristík vrátane miesta pobytu osoby alebo predchádzajúceho trestného konania fyzických osôb alebo skupín fyzických osôb,
- používanie systémov umelej inteligencie, ktoré vytvárajú alebo rozširujú databázy rozpoznávania tváre prostredníctvom necieleného získavania obrazov tváre z internetu alebo záznamov priemyselných kamier,
- používanie systémov umelej inteligencie na odvodzovanie emócií fyzickej osoby v oblasti presadzovania práva, riadenia hraníc, na pracovisku a vo vzdelávacích inštitúciách.[407]

Využívanie systémov diaľkovej biometrie Európsky parlament podmieňuje povoleniu zo strany nezávislého orgánu a s odkazom na politiky EÚ vymedzujúce konkrétne trestné činy.[408]

V kontexte šírenia dezinformácií považujeme za vhodné diskutovať dva zákazy uvedené vyššie. Prvým je využívanie systémov AI s technikami podprahovej manipulácie, ktoré môžu spôsobiť jednotlivcovi fyzickú alebo psychologickú ujmu. Odôvodnenie zákazu takýchto systémov naznačuje dopadová štúdia. V súvislosti s technikami podprahovej manipulácie odkazuje na odporúčania Rady Európy[409] a vplyvom na autonómiu rozhodovania jednotlivca. Vyššie uvedené odporúčania spomínajú aj negatívne vplyvy na demokraciu a informačné toky smerom k jednotlivcom.[410] Dopadová štúdia zároveň uvádza, že nezakázala iné využitie systémov AI s podobným negatívnym vplyvom prostredníctvom techník podprahovej manipulácie a to konkrétne mikro-targeting a profilovanie za účelom zneužitia,[411] nakoľko tieto aspekty reguluje DSA. Zároveň, dopadová štúdia pri praktických príkladoch pre zakotvenie

[407] Pozícia Európskeho parlamentu, článok 5 ba), da), db), dc).
[408] Pozícia Európskeho parlamentu, článok 5 de).
[409] *Council of Europe, Declaration on the manipulative capabilities of algorithmic processes*, 13 February 2019, Recommendation CM/Rec(2020).
[410] Tamže, body 4 – 6, 8 – 9.
[411] EURÓPSKA KOMISIA. *Commission staff working document impact assessment accompanying the proposal for a regulation of the european parliament and of the council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts*. {COM(2021) 206 final} - {SEC(2021) 167 final} - {SWD(2021) 85 final}, s. 47.

diskutovaného zákazu uvádza manipulácie prostredníctvom digitálnych asistentov[412] a hračiek. Vzhľadom na vyššie uvedené preto nič nenasvedčuje tomu, že diskutovaný zákaz by mal byť mierený na odporúčacie systémy online platforiem. Toto konštatovanie uvádzame napriek tomu, že pri bližšom skúmaní by sme vedeli nájsť náznaky, na základe ktorých by sme odporúčacie systémy šíriace dezinformácie vedeli pod daný zákaz subsumovať. Na konci bude záležať na výklade predmetného zákazu súdnymi orgánmi.

Druhým zákazom hodným diskusie je zákaz hodnotenia alebo klasifikácie dôveryhodnosti fyzických osôb počas určitého obdobia na základe ich spoločenského správania alebo známych či predpokladaných osobných alebo osobnostných charakteristík pre súkromných aktérov, ako navrhuje Rada EÚ a Európsky parlament. Nakoľko Európska komisia pôvodne tento zákaz navrhovala iba pre orgány verejnej moci alebo využívanie systémov AI v ich mene, dopadová štúdia rozšírenie pre súkromný sektor nepokrýva. Doplnenie recitálovej časti v návrhoch Rady EÚ naznačuje, že predmetný zákaz by sa mal týkať iba situácií, ak boli systémy AI využívaní pre iné účely, ako pôvodné a viedli by k nespravodlivému konaniu voči jednotlivcom. Samotný zákaz by sa nemal vzťahovať na vyhodnocovanie v súlade s právnym poriadkom.[413] Európsky parlament vo svojich návrhoch dokonca zakotvuje definíciu sociálneho hodnotenia a sociálneho správania. Sociálne hodnotenie definuje ako *„hodnotenie alebo klasifikáciu fyzických osôb na základe ich sociálneho správania, sociálno-ekonomického postavenia alebo známych alebo predpokladaných osobných alebo osobnostných charakteristík."*[414] Spoločenské správanie *„znamená spôsob, akým fyzická osoba spolupracuje s inými fyzickými osobami alebo spoločnosťou a ovplyvňuje ich."*[415] Podmienka analýzy spoločenského správania by na sociálnych sieťach bola splnená, keďže základom zbierania informácií zo strany sociálnych médií je práve analýza a predikcia správania užívateľov na základe ich vzájomnej interakcie, osobných informácií a navštívených lokalitách. Problematický aspektom zaradenia vplyvu odporúčacích systémov na jednotlivcov v kontexte diskutovaného zákazu môžu byť podmienky v podobe škodlivého alebo nepriaznivého zaobchádzania s určitými fyzickými osobami alebo celými skupinami fyzických osôb v sociálnych kontextoch, ktoré nesúvisia s pôvodnými súvislosťami zberu údajov alternatívne škodlivého alebo nepriaznivého zaobchádzania s určitými fyzickými osobami alebo skupinami, ktoré je neodôvodnené alebo neprimerané. Personalizácia obsahu je pomerne široký kontext,

[412] STUCKE, E. M. – EZRACHI, A. *The Subtle Ways Your Digital Assistant Might Manipulate You*. The Wired. November 2016. Dostupné na: https://www.wired.com/2016/11/subtle-ways-digital-assistant-might-manipulate/.
[413] Pozícia Rady EÚ, Recitál 17.
[414] Pozícia Európskeho parlamentu, článok 3 bod 44k.
[415] Pozícia Európskeho parlamentu, článok 3 bod 44l.

ktorý stojí a padá na zbere a analýze údajov. Ak sociálne siete transparentne komunikujú takúto súčasť služby (a zároveň aj špecifický účel spracúvania osobných údajov), profilovanie už nemusia vykonávať na iný účel alebo kontext ako tento pôvodný. Diskutovaný zákaz naozaj mieri na situácie, ak by napríklad štát využíval údaje a profily svojich občanov získané na účely sociálneho poistenia na to, aby občanom dovolil alebo nedovolil využiť služby národného železničného dopravcu. Problematickým môže byť aj subsumovanie podmienky neodôvodneného alebo neprimeraného zaobchádzania, i keď zaradenie jednotlivca do filtračnej bubliny môže mať vplyvom dezinformácií škodlivé účinky a môže sa javiť ako neprimerané voči ostatným užívateľom. Podobne ako pri prvom diskutovanom zákaze bude záležať na interpretácií zákazu v praxi.

Vysokorizikové systémy

AIA sa automaticky nevzťahuje na všetky systémy AI v zmysle definície uvedenej vyššie. Požiadavky kladené týmto nariadením sa budú aplikovať na tzv. vysokorizikové systémy AI. Či je systém AI vysokorizikový alebo nie upravuje článok 6. Klasifikovať systém AI ako vysokorizikový možno na základe dvoch alternatívnych zdrojov. Prvým zdrojom je odkaz na špecifickú reguláciu prostredníctvom prílohy II AIA. Ide o prípady, ak systém AI *„je určený na používanie ako bezpečnostný komponent výrobku, na ktorý sa vzťahujú harmonizačné právne predpisy Únie uvedené v prílohe II, alebo je sám osebe takýmto výrobkom.*"[416] Alternatívne totožné konštatovanie platí, ak *„výrobok, ktorého bezpečnostným komponentom je systém umelej inteligencie, alebo samotný systém umelej inteligencie ako výrobok sa musí podrobiť posúdeniu zhody treťou stranou s cieľom uviesť daný výrobok na trh alebo do prevádzky podľa harmonizačných právnych predpisov Únie uvedených v prílohe II .*"[417] Príloha II pre tieto výrobky uvádza nasledujúce regulácie:

- nariadenie o strojníckych výrobkoch[418]
- smernica o bezpečnosti hračiek[419]
- smernica o rekreačných plavidlách a skútroch[420]

[416] AIA, článok 6 ods. 1 písm. a).
[417] AIA, článok 6 ods. 1 písm. b).
[418] Nariadenie Európskeho parlamentu a Rady (EÚ) 2023/1230 zo 14. júna 2023 o strojových zariadeniach a o zrušení smernice Európskeho parlamentu a Rady 2006/42/ES a smernice Rady 73/361/EHS.
[419] Smernica Európskeho parlamentu a Rady 2009/48/ES z 18. júna 2009 o bezpečnosti hračiek.
[420] Smernica Európskeho parlamentu a Rady 2013/53/EÚ z 20. novembra 2013 o rekreačných plavidlách a vodných skútroch a o zrušení smernice 94/25/ES.

- smernica o harmonizácii právnych predpisov členských štátov týkajúcich sa výťahov a bezpečnostných komponentov do výťahov[421]
- smernica o harmonizácii právnych predpisov členských štátov týkajúcich sa zariadení a ochranných systémov určených na použitie v potenciálne výbušnej atmosfére[422]
- smernica o harmonizácii právnych predpisov členských štátov týkajúcich sa sprístupňovania rádiových zariadení na trhu[423]
- smernica o harmonizácii právnych predpisov členských štátov týkajúcich sa sprístupňovania tlakových zariadení na trhu[424]
- nariadenie o lanovkových zariadeniach a zrušení smernice 2000/9/ES[425]
- nariadenie o osobných ochranných prostriedkoch[426]
- nariadenie o spotrebičoch spaľujúcich plynné palivá[427]
- nariadenie o zdravotníckych pomôckach[428]
- nariadenie o diagnostických zdravotníckych pomôckach in vitro[429]
- nariadenie o spoločných pravidlách v oblasti bezpečnostnej ochrany civilného letectva[430]

[421] Smernica Európskeho parlamentu a Rady 2014/33/EÚ z 26. februára 2014 o harmonizácii právnych predpisov členských štátov týkajúcich sa výťahov a bezpečnostných komponentov do výťahov.
[422] Smernica Európskeho parlamentu a Rady 2014/34/EÚ z 26. februára 2014 o harmonizácii právnych predpisov členských štátov týkajúcich sa zariadení a ochranných systémov určených na použitie v potenciálne výbušnej atmosfére.
[423] Smernica Európskeho parlamentu a Rady 2014/53/EÚ zo 16. apríla 2014 o harmonizácii právnych predpisov členských štátov týkajúcich sa sprístupňovania rádiových zariadení na trhu, ktorou sa zrušuje smernica 1999/5/ES.
[424] Smernica Európskeho parlamentu a Rady 2014/68/EÚ z 15. mája 2014 o harmonizácii právnych predpisov členských štátov týkajúcich sa sprístupňovania tlakových zariadení na trhu.
[425] Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/424 z 9. marca 2016 o lanovkových zariadeniach a zrušení smernice 2000/9/ES.
[426] Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/425 z 9. marca 2016 o osobných ochranných prostriedkoch a o zrušení smernice Rady 89/686/EHS.
[427] Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/426 z 9. marca 2016 o spotrebičoch spaľujúcich plynné palivá a zrušení smernice 2009/142/ES.
[428] Nariadenie Európskeho parlamentu a Rady (EÚ) 2017/745 z 5. apríla 2017 o zdravotníckych pomôckach, zmene smernice 2001/83/ES, nariadenia (ES) č. 178/2002 a nariadenia (ES) č. 1223/2009 a o zrušení smerníc Rady 90/385/EHS a 93/42/EHS.
[429] Nariadenie Európskeho parlamentu a Rady (EÚ) 2017/746 z 5. apríla 2017 o diagnostických zdravotníckych pomôckach in vitro a o zrušení smernice 98/79/ES a rozhodnutia Komisie 2010/227/EÚ.
[430] Nariadenie Európskeho parlamentu a Rady (ES) č. 300/2008 z 11. marca 2008 o spoločných pravidlách v oblasti bezpečnostnej ochrany civilného letectva a o zrušení nariadenia (ES) č. 2320/2002.

- nariadenie o schvaľovaní a dohľade nad trhom dvoj- alebo trojkolesových vozidiel a štvorkoliek[431]
- nariadenie o schvaľovaní poľnohospodárskych a lesných vozidiel a o dohľade nad trhom s týmito vozidlami[432]
- smernica o vybavení námorných lodí[433]
- smernica o interoperabilite železničného systému v Európskej únii[434]
- nariadenie o schvaľovaní motorových vozidiel a ich prípojných vozidiel, ako aj systémov, komponentov a samostatných technických jednotiek určených pre takéto vozidlá[435]
- nariadenie o spoločných pravidlách v oblasti civilného letectva, ktorým sa zriaďuje Agentúra Európskej únie pre bezpečnosť letectva.[436]

Ak je AI súčasťou alebo samostatným produktom pri niektorej z uvedených produktových regulácií, vzťahuje sa na nich kľúčová časť AIA, ktorá obsahuje drvivú väčšinu povinností pre systémy AI.

Ak systém AI nespadá pod osobitnú reguláciu, adresáti povinností sú povinní reflektovať prílohu III AIA, ktorá ustanovuje oblasti AI vysokého rizika, na ktoré sa následne nariadenie

[431] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 168/2013 z 15. januára 2013 o schvaľovaní a dohľade nad trhom dvoj- alebo trojkolesových vozidiel a štvorkoliek.
[432] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 167/2013 z 5. februára 2013 o schvaľovaní poľnohospodárskych a lesných vozidiel a o dohľade nad trhom s týmito vozidlami.
[433] Smernica Európskeho parlamentu a Rady 2014/90/EÚ z 23. júla 2014 o vybavení námorných lodí a o zrušení smernice Rady 96/98/ES.
[434] Smernica Európskeho parlamentu a Rady (EÚ) 2016/797 z 11. mája 2016 o interoperabilite železničného systému v Európskej únii.
[435] Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/858 z 30. mája 2018 o schvaľovaní motorových vozidiel a ich prípojných vozidiel, ako aj systémov, komponentov a samostatných technických jednotiek určených pre takéto vozidlá a o dohľade nad trhom s nimi, ktorým sa menia nariadenia (ES) č. 715/2007 a (ES) č. 595/2009 a zrušuje smernica 2007/46/ES (Ú. v. EÚ L 151, 14.6.2018, s. 1); 3. nariadenie Európskeho parlamentu a Rady (EÚ) 2019/2144 z 27. novembra 2019 o požiadavkách na typové schvaľovanie motorových vozidiel a ich prípojných vozidiel a systémov, komponentov a samostatných technických jednotiek určených pre tieto vozidlá, pokiaľ ide o ich všeobecnú bezpečnosť a ochranu cestujúcich vo vozidle a zraniteľných účastníkov cestnej premávky, ktorým sa mení nariadenie Európskeho parlamentu a Rady (EÚ) 2018/858 a ktorým sa zrušujú nariadenia Európskeho parlamentu a Rady (ES) č. 78/2009, (ES) č. 79/2009 a (ES) č. 661/2009 a nariadenia Komisie (ES) č. 631/2009, (EÚ) č. 406/2010, (EÚ) č. 672/2010, (EÚ) č. 1003/2010, (EÚ) č. 1005/2010, (EÚ) č. 1008/2010, (EÚ) č. 1009/2010, (EÚ) č. 19/2011, (EÚ) č. 109/2011, (EÚ) č. 458/2011, (EÚ) č. 65/2012, (EÚ) č. 130/2012, (EÚ) č. 347/2012, (EÚ) č. 351/2012, (EÚ) č. 1230/2012 a (EÚ) 2015/166
[436] Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1139 zo 4. júla 2018 o spoločných pravidlách v oblasti civilného letectva, ktorým sa zriaďuje Agentúra Európskej únie pre bezpečnosť letectva a ktorým sa menia nariadenia Európskeho parlamentu a Rady (ES) č. 2111/2005, (ES) č. 1008/2008, (EÚ) č. 996/2010, (EÚ) č. 376/2014 a smernice Európskeho parlamentu a Rady 2014/30/EÚ a 2014/53/EÚ a zrušujú nariadenia Európskeho parlamentu a Rady (ES) č. 552/2004 a (ES) č. 216/2008 a nariadenie Rady (EHS) č. 3922/91, pokiaľ ide o projektovanie a výrobu lietadiel uvedených v článku 2 ods. 1 písm. a) a b) a ich umiestňovanie na trh, ak sa týka bezpilotných vzdušných prostriedkov a ide o ich motory, vrtule, súčasti a vybavenie na ich diaľkové ovládanie.

taktiež aplikuje. Príloha III upravuje oblasti a konkrétne aplikácie oblastí vysokého rizika. Konkrétne:

Oblasť	Aplikácia
Biometrická identifikácia a kategorizácia fyzických osôb	systémy umelej inteligencie určené na používanie na diaľkovú biometrickú identifikáciu fyzických osôb „v reálnom čase" a „následne".
Riadenie a prevádzka kritickej infraštruktúry	systémy umelej inteligencie, ktoré sa majú používať ako bezpečnostné komponenty pri riadení a prevádzke cestnej premávky a pri dodávkach vody, plynu, tepla a elektriny.
Vzdelávanie a odborná príprava	• systémy umelej inteligencie, ktoré sa majú používať na určovanie prístupu fyzických osôb do inštitúcií vzdelávania a odbornej prípravy alebo na ich priradenie k týmto inštitúciám • systémy umelej inteligencie, ktoré sa majú používať na hodnotenie študentov vo vzdelávacích inštitúciách a inštitúciách odbornej prípravy a na hodnotenie účastníkov skúšok, ktoré sa bežne vyžadujú na prijatie do vzdelávacích inštitúcií
Zamestnanosť, riadenie pracovníkov a prístup k samostatnej zárobkovej činnosti	• systémy umelej inteligencie určené na nábor alebo výber fyzických osôb, najmä na inzerovanie voľných pracovných miest, preverovanie alebo filtrovanie žiadostí, hodnotenie uchádzačov počas pohovorov alebo skúšok • systémy umelej inteligencie, ktoré sa majú používať pri rozhodovaní o postupe v zamestnaní a ukončení zmluvných pracovných vzťahov, pri prideľovaní úloh a monitorovaní a hodnotení výkonnosti a správania osôb v rámci takýchto vzťahov
Prístup k základným súkromným a verejným službám a dávkam a ich využívanie	• systémy umelej inteligencie, ktoré sa majú používať orgánmi verejnej moci alebo v ich mene na hodnotenie oprávnenosti fyzických osôb na dávky a služby verejnej pomoci, ako aj na poskytovanie, zníženie či zrušenie takýchto dávok a služieb alebo na žiadosti o ich vrátenie • systémy umelej inteligencie, ktoré sa majú používať na hodnotenie úverovej bonity fyzických osôb alebo stanovenie ich bodového hodnotenia kreditného rizika, s výnimkou

	systémov umelej inteligencie prevádzkovaných malými poskytovateľmi na vlastnú potrebu • systémy umelej inteligencie určené na vysielanie záchranných služieb prvej reakcie vrátane hasičov a zdravotníckej pomoci alebo na stanovovanie priority ich vysielania
Presadzovanie práva	• systémy umelej inteligencie, ktoré majú používať orgány presadzovania práva na individuálne posúdenie rizika fyzických osôb s cieľom posúdiť riziko, ktoré fyzická osoba predstavuje z hľadiska (opakovaného) páchania trestnej činnosti, alebo riziko pre potenciálne obete trestných činov • systémy umelej inteligencie, ktoré majú používať orgány presadzovania práva, ako napríklad detektory lži a podobné nástroje, alebo na zisťovanie emocionálneho stavu fyzickej osoby; • systémy umelej inteligencie, ktoré majú používať orgány presadzovania práva na odhaľovanie prípadov tzv. deepfake, ako sa uvádza v článku 52 ods. 3; • systémy umelej inteligencie, ktoré majú používať orgány presadzovania práva na hodnotenie spoľahlivosti dôkazov v priebehu vyšetrovania alebo stíhania trestných činov; • systémy umelej inteligencie, ktoré majú používať orgány presadzovania práva na predvídanie výskytu alebo opakovaného výskytu skutočného alebo potenciálneho trestného činu na základe profilovania fyzických osôb uvedeného v článku 3 bode 4 smernice (EÚ) 2016/680, alebo na posúdenie osobnostných a povahových rysov alebo trestnej činnosti fyzických osôb alebo skupín v minulosti; • systémy umelej inteligencie, ktoré majú orgány presadzovania práva používať na profilovanie fyzických osôb uvedené v článku 3 bode 4 smernice (EÚ) 2016/680 v priebehu odhaľovania, vyšetrovania alebo stíhania trestných činov; • systémy umelej inteligencie, ktoré sa majú používať pri analýze trestnej

	činnosti týkajúcej sa fyzických osôb, čo orgánom presadzovania práva umožní prehľadávať zložité súvisiace aj nesúvisiace veľké súbory údajov dostupné v rôznych dátových zdrojoch alebo v rôznych dátových formátoch s cieľom identifikovať v údajoch neznáme vzorce alebo odhaliť medzi nimi skryté vzťahy.
Migrácia, azyl a riadenie kontroly hraníc	• systémy umelej inteligencie, ktoré majú používať príslušné orgány verejnej moci, ako napríklad detektory lži a podobné nástroje, alebo na zisťovanie emocionálneho stavu fyzickej osoby; • systémy umelej inteligencie, ktoré majú používať príslušné orgány verejnej moci na posúdenie rizika vrátane bezpečnostného rizika, rizika nelegálneho prisťahovalectva alebo zdravotného rizika, ktoré predstavuje fyzická osoba, ktorá má v úmysle vstúpiť na územie členského štátu alebo naň už vstúpila; • systémy umelej inteligencie, ktoré majú používať príslušné orgány verejnej moci na overovanie pravosti cestovných dokladov a podpornej dokumentácie fyzických osôb a odhaľovanie nepravých dokladov kontrolou ich ochranných prvkov; • systémy umelej inteligencie určené na pomoc príslušným orgánom verejnej moci pri posudzovaní žiadostí o azyl, víza a povolení na pobyt a súvisiacich sťažností týkajúcich sa oprávnenosti fyzických osôb žiadajúcich o určitý status.
Výkon spravodlivosti a demokratické procesy	systémy umelej inteligencie určené na pomoc súdnemu orgánu pri skúmaní a interpretácii faktov a práva a pri uplatňovaní práva na konkrétny súbor skutočností

Tabuľka: Vysokorizikové systémy AI podľa prílohy III AIA.
Zdroj: Príloha III AIA.

Vzhľadom na dynamický vývoj AI nariadenie predpokladá dopĺňanie prílohy III prostredníctvom delegovaných aktov Európskej komisie. Na doplnenie musia byť splnené dve podmienky. Prvou je, že systémy AI sú určené na nasadenie v niektorej z oblasti uvedenej

v Prílohe III AIA.[437] Druhá podmienka spočíva v tom, že *„systémy umelej inteligencie predstavujú riziko poškodenia zdravia a bezpečnosti alebo riziko nepriaznivého vplyvu na základné práva, ktoré je vzhľadom na svoju závažnosť a pravdepodobnosť výskytu prinajmenšom rovnocenné riziku poškodenia alebo nepriaznivého vplyvu.*"[438] AIA zároveň ustanovuje kritéria, ktoré Európska komisia posudzuje pri prijímanie doplnenia Prílohy III.[439] Už na základe uvedeného je zjavný nedostatok v tom, že Európska komisia síce môže dopĺňať konkrétne aplikácie vysokorizikových systémov AI, avšak nemá kompetenciu pridávať oblasti vysokého rizika. Inými slovami, musí vysokorizikové systémy AI subsumovať pod jednu z uvedených oblastí. Tento prístup môže pri dynamickom vývoji AI razantne zúžiť možnosti regulácie. Rada EÚ vo svojich návrhoch zastáva pozíciu, aby Európska komisia mohla za presne stanovených podmienok zoznam meniť výmazom.[440]

Rada EÚ navrhuje, aby sa za vysokorizikové systémy AI nepovažovali také systémy, ktoré síce napĺňajú literu konkrétnej aplikácie v Prílohe III, ale ich výstupy nemajú negatívny vplyv na zdravie, bezpečnosť a základné ľudské práva a slobody.[441] Až návrhy Európskeho parlamentu zohľadňujú vyššie uvedený nedostatok pôvodného návrhu, v zmysle ktorého by Európska komisia mohla dopĺňať aj oblasti v Prílohe III.[442] Taktiež Európsky parlament vo svojej pozícií navrhuje pridať kritérium, aby sa za systémy vysokého rizika klasifikovali iba také, ktoré predstavujú významné riziko poškodenia zdravia a bezpečnosti alebo nepriaznivého vplyvu na základné práva, životné prostredie alebo demokraciu a právny štát a toto riziko je z hľadiska

[437] AIA, článok 7 ods. 1 písm. a).
[438] AIA, článok 7 ods. 1 písm. b).
[439] AIA, článok 7 ods. 2: *„a) zamýšľaný účel systému umelej inteligencie;*
b) rozsah, v akom sa systém umelej inteligencie používa alebo sa pravdepodobne bude používať;
c) rozsah, v akom používanie systému umelej inteligencie už spôsobilo poškodenie zdravia a bezpečnosti alebo nepriaznivý vplyv na základné práva, alebo vyvolalo vážne obavy v súvislosti s naplnením takéhoto poškodenia alebo nepriaznivého vplyvu, preukázaný správami alebo zdokumentovanými tvrdeniami predloženými príslušným vnútroštátnym orgánom;
d) potenciálny rozsah takéhoto poškodenia alebo nepriaznivého vplyvu, najmä pokiaľ ide o jeho intenzitu a schopnosť zasiahnuť značný počet osôb;
e) rozsah, v akom sú potenciálne poškodené alebo nepriaznivo ovplyvnené osoby závislé od výsledku vytvoreného systémom umelej inteligencie, najmä preto, že z praktických alebo právnych dôvodov nie je odôvodnene možné sa na tomto výsledku nepodieľať;
f)rozsah, v akom sú potenciálne poškodené alebo nepriaznivo ovplyvnené osoby vo vzťahu k používateľovi systému umelej inteligencie v zraniteľnom postavení, najmä v dôsledku nerovnováhy moci, znalostí, hospodárskych alebo sociálnych okolností alebo veku;
g) rozsah, v akom sa výsledok vytvorený systémom umelej inteligencie dá ľahko zvrátiť, pričom výsledky, ktoré majú vplyv na zdravie alebo bezpečnosť osôb, sa nepovažujú za také, ktoré sa dajú ľahko zvrátiť;
h) rozsah, v akom sa v existujúcich právnych predpisoch Únie stanovujú:
i)účinné nápravné opatrenia v súvislosti s rizikami, ktoré systém umelej inteligencie predstavuje, s výnimkou nárokov na náhradu škody;
ii)účinné opatrenia na predchádzanie týmto rizikám alebo ich podstatnú minimalizáciu."
[440] Pozícia Rady EÚ, článok 7 ods. 3 a 4.
[441] Pozícia Rady EÚ, článok 6 ods. 3.
[442] Pozícia Európskeho parlamentu, článok 7 ods. 1.

závažnosti a pravdepodobnosti výskytu rovnaké alebo väčšie ako riziko ujmy alebo nepriaznivého vplyvu, ktoré predstavujú vysokorizikové systémy umelej inteligencie uvedené v Prílohe III.[443] Zároveň, faktory doplnenia zoznamu zo strany Európskej komisie dopĺňa o zohľadnenie aspektov vplyvu na demokraciu, právny štát, životné prostredie, možnosti ľudského dohľadu či potenciálne zneužitie systémov AI.[444]

Prirodzene, o tom, ktorá oblasť a aplikácia má byť súčasťou Prílohy III prebieha čulá akademická a politická diskusia. Svoje pozície už deklarovali aj Rada EÚ a Európsky parlament. Rada EÚ navrhuje vymazať z oblasti presadzovania práva systémy AI na detekciu tzv. deepfakes, analýzu trestných činov a overenie pravosti cestovných dokumentov. Zároveň navrhuje pridať aplikácie systémov AI v kritickej digitálnej infraštruktúre (do oblasti riadenia a prevádzky kritickej infraštruktúry) a životného a zdravotného poistenia (do oblasti prístup k základným súkromným a verejným službám a dávkam a ich využívanie).

Európsky parlament vo svojej pozícií navrhuje pridať viacero konkrétnych aplikácií:

- systémy umelej inteligencie určené na vyvodzovanie záverov o osobných charakteristikách fyzických osôb na základe biometrických alebo údajov vrátane systémov na rozpoznávanie emócií okrem zakázaných systémov podľa článku 5,
- pridanie oblastí dodávok vody, plynu, tepla a elektriny do oblasti manažmentu kritickej infraštruktúry a rozšírenie aplikácií o AI systémy na manažment železničnej a leteckej dopravy, ak nie sú pokryté harmonizačnými predpismi na úrovni EÚ,
- systémy umelej inteligencie určené na použitie ako bezpečnostné prvky pri riadení a prevádzke dodávok vody, plynu, tepla, elektriny a kritickej digitálnej infraštruktúry,
- systémy umelej inteligencie, ktoré sa majú používať na účely posúdenia vhodnej úrovne vzdelania pre jednotlivca a podstatné ovplyvňujú úrovne vzdelania a odbornej prípravy, ktorú tento jednotlivec získa alebo ku ktorej bude mať prístup,
- systémy umelej inteligencie určené na monitorovanie a odhaľovanie zakázaného správania študentov počas testov v rámci inštitúcií vzdelávania a odbornej prípravy
- spresnenie aplikácií v oblasti zamestnanosti,

[443] Tamže.
[444] Pozícia Európskeho parlamentu, článok 7 ods. 2.

- systémy umelej inteligencie určené na rozhodovanie alebo podstatné ovplyvňovanie rozhodnutí o oprávnenosti fyzických osôb na zdravotné a životné poistenie,
- systémy umelej inteligencie určené na používanie príslušnými orgánmi verejnej moci alebo agentúrami, úradmi alebo orgánmi Únie v oblasti riadenia migrácie, azylu a kontroly hraníc alebo v ich mene na monitorovanie, sledovanie alebo spracovanie údajov v súvislosti s činnosťami riadenia hraníc na účely odhaľovania, rozpoznávania alebo identifikácie fyzických osôb,
- systémy umelej inteligencie určené na používanie príslušnými verejnými orgánmi alebo v ich mene alebo agentúrami, úradmi alebo orgánmi Únie v oblasti riadenia migrácie, azylu a kontroly hraníc na prognózovanie alebo predpovedanie trendov súvisiacich s migračným pohybom a prekračovaním hraníc,
- systémy AI určené na ovplyvňovanie výsledkov volieb alebo referenda alebo správania sa fyzických osôb pri hlasovaní vo voľbách alebo referende. Nepatria sem systémy UI, ktorých výstupom nie sú fyzické osoby priamo vystavené, ako sú nástroje používané na organizáciu, optimalizáciu a štruktúru politických kampaní z administratívneho a logistického hľadiska,
- systémy umelej inteligencie určené na používanie platformami sociálnych médií, ktoré boli označené za veľmi veľké online platformy v zmysle článku 33 nariadenia EÚ 2022/2065 (Akt o digitálnych službách), v ich odporúčacích systémoch na odporúčanie obsahu generovaného inými užívateľmi príjemcovi služby.[445]

V kontexte šírenia dezinformácií prostredníctvom odporúčacích systémov by sme len s veľkou dávkou fantázie vedeli zaradiť tieto systémy AI do niektorej z pôvodných oblastí a aplikácií vysokého rizika podľa Prílohy III. Prirodzeným „favoritom" by bola oblasť výkonu spravodlivosti a demokratické procesy, avšak táto oblasť je v pôvodnom návrhu Európskej komisie zúžená na súdne procesy. Z tohto dôvodu vítame návrhy Európskeho parlamentu, ktorý chce do tejto oblasti explicitne zahrnúť odporúčacie systémy VVOP. Ak sa daná aplikácia pretaví aj do konečného znenia AIA, odporúčacie systémy na najväčších platformách sa budú považovať za vysokorizikové systémy AI a budú musieť spĺňať požiadavky na ne kladené týmto právnym aktom.

[445] Pozícia Európskeho parlamentu, Príloha III.

Požiadavky na vysokorizikové systémy AI

Drvivá väčšina požiadaviek v AIA sa zameriava na regulácie systémov AI vysokého rizika. Ak bude chcieť výrobca uviesť vysoko-rizikový systém AI na trh a následne do praxe, bude musieť v zmysle požiadaviek AIA splniť niekoľko krokov. Je nutné poznamenať, že AIA dáva dôraz na splnenie požiadaviek pred uvedením na trh (*ex ante*), aby sa minimalizovali riziká AI z hľadiska zdravia, bezpečnosti a rešpektovania základných ľudských práv pri jej používaní.

Prvým krokom je vykonanie tzv. posudzovania zhody (*conformity assessment*), čo je proces známy aj z iných regulácií, či ako súčasť auditovacích mechanizmov.[446] Rôzne nástroje a metódy auditu systémov AI nie sú nové a v kontexte AIA môžu plniť rôzne funkcie. Nástroje auditu sa môžu použiť na hodnotenie dodržiavania právnych noriem zo strany regulačných a dozorných orgánov, na zmiernenie rôznych druhov rizík zo strany poskytovateľov a vývojárov systémov AI alebo na prijímanie informovaných rozhodnutí zo strany verejnosti a zainteresovaných subjektov.[447]

Samotné posúdenie zhody má legálnu definíciu v AIA: *„posudzovanie zhody je postup overovania, či boli splnené požiadavky stanovené v hlave III kapitole 2 tohto nariadenia týkajúce sa systému umelej inteligencie.*"[448] Jeho zmyslom je, aby výrobca systémov AI sám dbal na dodržiavanie požiadaviek AIA, ktoré mu nariadenie ustanovuje a reflektoval zásadu zodpovednosti (*accountability*).

Väčšina poskytovateľov vysokorizikových systémov AI sa bude riadiť postupom pre posúdenie zhody založenom na vnútornej kontrole, keďže externá kontrola je povinná len v obmedzenom počte prípadov.[449] Dôvodom povinnosti vykonávať posúdenie zhody interne na strane poskytovateľa je, že poskytovatelia systémov AI majú viac skúseností a rozumejú špecifikám svojich systémov.[450] Externá kontrola a teda vykonanie posúdenia zhody treťou stranou sa vyžaduje iba v prípade systémov AI, ktoré budú využívať biometrickú identifikáciu

[446] Pozri napríklad ŠIMKO, J a kol. Towards Continuous Automatic Audits of Social Media Adaptive Behavior and its Role in Misinformation Spreading. In *29th ACM Conference on UMAP'21*.
[447] BROWN, S. - DAVIDOVIC, J. - HASAN, A. The algorithm audit: Scoring the algorithms that score us. In *Big Data & Society*, 8(1), 2021.
[448] AIA, článok 3 bod 20.
[449] VEALE, M. - ZUIDERVEEN BORGESIUS, F. Demystifying the Draft EU Arti ficial Intelligence Act — Analysing the good, the bad, and the unclear elements of the proposed approach. In *Computer Law Review International*, vol. 22, no. 4, 2021.
[450] AIA, recitál 64.

ľudí.[451] Rozsah externej kontroly vysokorizikových systémov AI pred uvedením na trhu je tak značne obmedzený.[452]

Obsahové náležitosti posúdenia zhody je možné derivovať z kapitoly 2 hlavy III AIA. Tieto požiadavky sú koncipované s cieľom efektívne zmierniť riziká pre zdravie, bezpečnosť a základné ľudské práva a slobody v kontexte účelu posudzovaného systému AI.[453] Tieto požiadavky zahŕňajú:

- zriadenie, zavedenie a dokumentácia systému riadenia rizík[454]
- zavedenie procesov pre správu údajov[455]
- koncipovanie technickej dokumentácie[456]
- uchovávania záznamov[457]
- zachovanie transparentnosti a poskytovanie informácií používateľom[458]
- zavedenie ľudské dohľadu[459]
- požiadavky na presnosť, spoľahlivosť a kybernetickú bezpečnosť.[460]

Z pohľadu rizík a kvality vysokorizikových systémov AI najrelevantnejšie požiadavky na odporúčacie systémy na sociálnych médiách predstavujú ustanovenia týkajúce sa kvality a správy údajov, presnosti a ľudské dohľadu. Požiadavky na správu údajov obsahuje článok 10 AIA, ktorý ustanovuje kvalitatívne požiadavky pre súbory trénovacích, validačných a testovacích údajov.[461] Tieto údaje musia byť dostatočne relevantné, reprezentatívne, bezchybné a úplné.[462] Zároveň musia byť pre tieto datasety zavedené postupy zberu údajov, posúdenia vhodnosti a dostupnosti či preskúmania z hľadiska možných skreslení (*bias*).[463] *„Súbory trénovacích, validačných a testovacích údajov musia, pokiaľ si to vyžaduje zamýšľaný*

[451] AIA, článok 43 ods. 1 v spojitosti s Prílohou III, bod 1.
[452] HAATAJA, M. - BRYSON, J. J. *What costs should we expect from the EU's AI Act?* 2021. Dostupné na: https://doi.org/10.31235/osf.io/8nzb4.
[453] AIA, recitál 43.
[454] AIA, článok 9.
[455] AIA, článok 10.
[456] AIA, článok 11.
[457] AIA, článok 12.
[458] AIA, článok 13.
[459] AIA, článok 14.
[460] AIA, článok 15.
[461] AIA, článok 10 ods. 1.
[462] AIA, článok 10 ods. 3.
[463] AIA, článok 10 ods. 2.

účel, zohľadňovať vlastnosti alebo prvky, ktoré sú špecifické pre konkrétne geografické, behaviorálne alebo funkčné podmienky, v ktorých sa má vysokorizikový systém umelej inteligencie používať."[464] Vyššie uvedené požiadavky neplatia iba pre AI systémy, ktoré je potrebné natrénovať, ale pre vysokorizikové systémy AI vo všeobecnosti.[465]

Tieto atribúty pre údaje a správu údajov výrazne ovplyvňujú kvalitu výstupov a samotné fungovanie systému AI. V prípade odporúčacích systémov je dôležité, aby nezobrazovali obsah na základe skreslení, to znamená s určitými predsudkami. Ilustrovať to možno na príklade, ak by človeku, ktorý je súčasťou určitej sociálnej alebo ekonomickej skupiny zobrazoval dezinformačný obsah, ktorý sledujú ďalší členovia danej skupiny. Požiadavku na kvalitu a dostatočnú reprezentáciu údajov je tak nutné vnímať ako dôležité aj v tomto kontexte. Zároveň, organizačné postupy pre správu údajov by mali zahŕňať aj postupy, ktoré by takéto fungovanie odhalilo a mohlo byť zmiernené. S tým súvisí aj požiadavka na uchovávania záznamov (*logov*), z ktorých možno vysledovať potenciálne riziká a zasiahnuť.[466] Požiadavky na kvalitu údajov je ale potrebné vnímať v tom zmysle, že poskytovateľ alebo prevádzkovateľ vysokorizikového AI systému je povinný urobiť všetko pre to, aby datasety boli čo najkvalitnejšie.

Aby však bolo možné pri nesprávnom alebo škodlivom fungovaní vysokorizikového systému AI zasiahnuť, proces nemôže byť plne automatizovaný. Z tohto dôvodu po vzore viacerých politických alebo etických dokumentov či deklarácií zakotvuje požiadavku na ľudský dohľad: *„Vysokorizikové systémy umelej inteligencie musia byť koncipované a vyvinuté tak, aby nad nimi počas obdobia používania systému umelej inteligencie mohli fyzické osoby vykonávať účinný dohľad, a to aj pomocou vhodných nástrojov rozhrania človek – stroj.*"[467] Požiadavka praktický znamená, že vysokorizikové systémy AI musia byť dizajnované takým spôsobom, aby umožnili dohľad človeka nad jeho fungovaním. Tento dohľad by sa mal zameriavať na *„prevenciu alebo minimalizáciu rizík pre zdravie, bezpečnosť alebo základné práva, ktoré môžu vzniknúť pri používaní vysokorizikového systému umelej inteligencie v súlade so zamýšľaným účelom alebo za podmienok logicky predvídateľného nesprávneho použitia.*"[468] Samotný ľudský dohľad má uvedené požiadavky na jeho kvalitu. Osoba vykonávajúca dohľad musí rozumieť

[464] AIA, článok 10 ods. 4.
[465] AIA, článok 10 ods. 6.
[466] AIA, článok 12 ods. 1: *„Vysokorizikové systémy umelej inteligencie musia byť koncipované a vyvinuté tak, aby boli počas svojej prevádzky schopné automaticky zaznamenávať udalosti („logy"). Tieto schopnosti logovania musia byť v súlade s uznávanými normami alebo spoločnými špecifikáciami*" a článok 12 ods. 2: *„Schopnosťami logovania sa počas celého životného cyklu systému umelej inteligencie zabezpečí úroveň vysledovateľnosti jeho fungovania, ktorá je primeraná zamýšľanému účelu systému.*"
[467] AIA, článok 14 ods. 1.
[468] AIA, článok 14 ods. 2.

kapacitám a obmedzeniam dohladovaného vysokorizikového systému AI a efektívne ho monitorovať.[469] Ľudský dohľad zároveň musí vedieť správne interpretovať výstupy systému[470] a rozhodovať o zásahoch do jeho fungovania.[471] Osobitnou požiadavkou je, aby ľudský dohľad umožňoval vysokorizikový systém AI vypnúť.[472] Koncepcia ľudského dohľadu zahŕňa aj požiadavku na uvedomenie si potenciálneho automatizovaného skreslenia.[473] To prakticky znamená, že osoba, ktorá nad vysokorizikovým systémom AI vykonáva dohľad by mala vedieť o možnosti prílišného sa spoliehania na automatizované procesy bez kontroly, čo môže spôsobiť prehliadnutie rizík, chýb a omylov.[474]

Veľkú diskusiu spôsobili požiadavky AIA na presnosť, spoľahlivosť a kybernetickú bezpečnosti.[475] Tieto požiadavky zvýrazňujú atribúty odolnosti voči chybám, poruchám a nezrovnalostiam.[476] *„Vysokorizikové systémy umelej inteligencie, ktoré sa po uvedení na trh alebo do prevádzky ďalej učia, sa musia vyvíjať tak, aby sa zabezpečilo, že prípadné skreslené výstupy v dôsledku výstupov používaných ako vstup pre budúce operácie („slučky spätnej väzby") budú náležite riešené vhodnými zmierňujúcimi opatreniami."*[477] Zároveň, musia byť tieto systémy odolné voči útokom a pokusom neoprávnených tretích strán o manipuláciu.[478]

Rada EÚ v rámci svojej pozície precizovala niektoré požiadavky na vysokorizikové systémy AI a zakotvila požiadavky na ich plnenie nielen pre poskytovateľov takýchto systémov, ale aj používateľov alebo iné subjekty zapojené do ich vývoja. Významných zmien sa však vo svojej pozícií dožaduje Európsky parlament. Vysokorizikové systémy AI by sa nemali posudzovať iba v kontexte rizík pre bezpečnosť, zdravie a základné ľudské práva a slobody, ale aj demokraciu a právny štát či životné prostredie.[479] Medzi požiadavky na správu údajov pridáva povinnosť transparentne zverejniť zdroje údajov.[480] Zároveň, podobne ako Rada EÚ špecifikuje

[469] AIA, článok 14 ods. 4 písm. a).
[470] AIA, článok 14 ods. 4 písm. c).
[471] AIA, článok 14 ods. 4 písm. d).
[472] AIA, článok 14 ods. 4 písm. e).
[473] AIA, článok 14 ods. 4 písm. b): *„Opatrenia uvedené v odseku 3 musia osobám, ktorým je zverený ľudský dohľad, umožniť, aby podľa okolností... si boli neustále vedomé možnej tendencie automatického spoliehania sa alebo nadmerného spoliehania sa na výstupy vytvorené vysokorizikovým systémom umelej inteligencie („automatizačné skreslenie"), a to najmä v prípade vysokorizikových systémov umelej inteligencie používaných na poskytovanie informácií alebo odporúčaní pre rozhodnutia, ktoré majú prijať fyzické osoby."*
[474] K tomu napríklad SKITKA, L. J. - MOSIER, K. L. - BURDICK, M. Does automation bias decision-making? In *International Journal of Human-Computer Studies*, 1999, 51, 991-1006.
[475] AIA, článok 15 ods. 1: *„Vysokorizikové systémy umelej inteligencie musia byť koncipované a vyvinuté tak, aby vzhľadom na svoj zamýšľaný účel dosahovali primeranú úroveň presnosti, spoľahlivosti a kybernetickej bezpečnosti a aby v týchto ohľadoch konzistentne fungovali počas celého svojho životného cyklu."*
[476] AIA, článok 15 ods. 3.
[477] AIA, článok 15 ods. 3.
[478] AIA, článok 15 ods. 4.
[479] Pozícia Európskeho parlamentu, článok 9 ods. 2 písm. a).
[480] Pozícia Európskeho parlamentu, článok 10 ods. 2 písm. aa).

niektoré požiadavky a zakotvuje povinností aj pre iné subjekty ako napríklad entity, ktoré vysokorizikové systémy AI nasadzujú a používajú.[481] Dôraz kladie Európsky parlament aj na zverejňovanie uhlíkovej stopy, záznamy o spotrebe energie s cieľom dbať na životné prostredie.

Zaujímavým návrhom v rámci pozície Európskeho parlamentu je povinné vykonanie tzv. posúdenie vplyvu na základné ľudské práva a slobody (*Fundamental rights impact assessment*, skrátene FRIA) pre vysokorizikové systémy AI.[482] Predmetná povinnosť by sa nevzťahovala na systémy AI využívané v oblasti kľúčovej a kritickej infraštruktúry.[483] Posúdenie vplyvu na základné ľudské práva a slobody by okrem iného malo zahŕňať aj vypracovanie plánu na zmiernenie rizík pre základné ľudské práva a slobody pri nasadení a využívaní vysokorizikového systému AI, zohľadnenie vplyvu na marginalizované skupiny či zapojenie zainteresovaných subjektov do vypracovania tohto dokumentu.[484] Ak poskytovateľ takéhoto systému nebude vedieť vypracovať plán na zmiernenie rizík pre základné ľudské práva a slobody pri nasadení a využívaní vysokorizikového systému AI, nemal by ho nasadiť a informovať o tom dozorný orgán.[485] V prípade, ak poskytovateľ má povinnosť vykonať posúdenie vplyvu na ochranu údajov podľa článku 35 GDPR (viď diskusia nižšie), posúdenie vplyvu na ľudské práva môže vykonať v úzkej nadväznosti na posúdenie vplyvu podľa GDPR. Posúdenie vplyvu na ochranu údajov by malo tvoriť verejne dostupnú prílohu celkového posúdenia.[486]

Súlad s požiadavkami pre vysokorizikové systémy AI je možné realizovať aj odlišným spôsobom, ako priamym plnením povinností v zmysle AIA. Návrh nariadenia obsahuje aj prezumpciu plnenia požiadaviek, ak vysokorizikové systémy AI spĺňajú príslušné harmonizované normy - štandardy.[487] Môže ísť o prípad dodržiavania povinností v oblasti kybernetickej bezpečnosti, keď bolo poskytovateľovi vysokorizikových systémov AI vydané vyhlásenie o zhode podľa schémy kybernetickej bezpečnosti podľa osobitného nariadenia EÚ.[488] Významnú úlohu organizácií rozvíjajúcich normy v zmysle AIA kritizovala akademická obec pre obavy súvisiace s ochranou základných práv a procesnými aspektmi preskúmavania

[481] Napríklad Pozícia Európskeho parlamentu, článok 10 ods. 6.
[482] Pozícia Európskeho parlamentu, článok 29a.
[483] Tamže.
[484] Pozícia Európskeho parlamentu, článok 29a ods. 1 a 4.
[485] Tamže, článok 29a ods. 2.
[486] Tamže, článok 29a ods. 6.
[487] AIA, články 40 a 42.
[488] Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti). Ú. v. EÚ L 151, 7.6.2019, s. 15 – 69.

týchto noriem z pohľadu nezávislých orgánov.[489] Napriek tomu Európska komisia očakáva prijatie takýchto noriem ešte pred prijatím samotného nariadenia.[490]

Samotné posúdenie zhody je potrebné vykonať pred uvedením vysokorizikového systému AI na trh EÚ[491] alebo pred uvedením vysokorizikového systému AI do prevádzky.[492] Okrem toho sa posúdenie vplyvu vykoná aj v prípadoch, keď sú vysokorizikové systémy AI podstatne zmenenia. Toto je prípad zmeny ovplyvňujúcej súlad s nariadením alebo modifikácia zamýšľaného účelu. Neustále učenie sa systémov AI sa nepovažuje za podstatnú zmenu.[493]

Členské štáty EÚ sa môžu odchýliť od postupov posudzovania zhody na území príslušných členských štátov *„z výnimočných dôvodov verejnej bezpečnosti alebo ochrany života a zdravia osôb, ochrany životného prostredia a ochrany kľúčových priemyselných a infraštruktúrnych aktív."*[494] Výnimka je však prísne obmedzená a posúdenie zhody by sa malo vykonať počas uplatňovania výnimky.[495]

Druhým krokom po úspešnom posúdení zhody je registrácia systému AI v databáze EÚ pre samostatné vysokorizikové systémy AI.[496] Túto databázu bude spravovať samotná Európska komisia spolu s členskými štátmi. Databáza bude verejne dostupná a tak si každý užívateľ môže overiť, či je systém AI registrovaný a prešiel posúdením zhody.

EÚ následne pre registrovaný vysokorizikový AI systém vydá tzv. vyhlásenie o zhode.[497] Zároveň výrobca označenie zhody umiestni tak, aby bolo viditeľné, čitateľné a neodstrániteľné.[498]

[489] Napríklad VEALE, M. - ZUIDERVEEN BORGESIUS, F. Demystifying the Draft EU Arti ficial Intelligence Act — Analysing the good, the bad, and the unclear elements of the proposed approach. In *Computer Law Review International*, vol. 22, no. 4, 2021, s. 105.
[490] EURÓPSKA KOMISIA. Commission staff working document impact assessment accompanying the proposal for a regulation of the european parliament and of the council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts. {COM(2021) 206 final} - {SEC(2021) 167 final} - {SWD(2021) 85 final}.
[491] Uvedenie na trh definuje AIA v článku 3 bode 9: *„uvedenie na trh je prvé sprístupnenie systému umelej inteligencie na trhu Únie."*
[492] Uvedenie do prevádzky definuje AIA v článku 3 bode 11: *„uvedenie do prevádzky je dodanie systému umelej inteligencie na prvé použitie priamo používateľovi alebo na vlastné použitie na trhu Únie na zamýšľaný účel."*
[493] AIA, recitál 66.
[494] AIA, článok 47 ods. 1.
[495] Tamže.
[496] AIA, článok 60.
[497] AIA, článok 48.
[498] AIA, článok 49.

Tretím krokom je *ex post* monitorovanie systémov AI po uvedení na trh. Prakticky to znamená výkon dohľadu a monitorovania vysokorizikových systémov AI. Po vzore iných právnych úprav je zakotvený inštitút nahlasovania incidentov pri využívaní systémov AI.[499]

Samotný dozor budú vykonávať príslušné vnútroštátne orgány.

Požiadavky na generatívne systémy AI

Osobitnou kategóriou systémov AI, ktoré považujeme za vhodné diskutovať z hľadiska regulačných požiadaviek na nich kladených sú tzv. generatívne systémy AI. Ide o pojem súvisiaci s termínmi základné modely (*foundation models*)[500] prípadne veľké jazykové modely.[501] Generatívne systémy AI predstavujú pokročilé modely strojového učenia, ktoré sú trénované na generovanie nových údajov, ako je text, obrázky alebo zvuk, pričom to ich odlišuje od iných modelov určených na vytváranie predpovedí, klasifikácií alebo iné špecifické funkcie.[502] Inými slovami, generatívne systémy AI „vedia" nachádzať vzorce a vzťahy medzi dátami sami od seba. Následne tieto systémy generujú nový obsah podobný tomu, na ktorom boli natrénované.[503] Vzhľadom na to, že predmetné systémy vedia generovať nový obsah v dobrej kvalite a veľkou rýchlosťou, manuálna kontrola generovaného obsahu je v podstate nemožná. Jednotlivci tak majú k dispozícií silný nástroj na generovanie dezinformácií, napriek tomu, že poskytovatelia generatívnej AI vyvíjajú snahu, aby sa ich produkt nezneužil týmto spôsobom.[504]

Pôvodný návrh Európskej komisie tento fenomén vôbec neriešil. Návrhy Rady EÚ smerujú iba k regulácií tzv. AI na všeobecné účely (*general-purpose AI*), ktorá môže, ale nemusí[505] zahŕňať aj generatívnu AI, ktorú definuje ako systémy *„umelej inteligencie, ktorých cieľom je s rôznymi úrovňami autonómie vytvárať obsah, ako je komplexný text, obrázky, audio alebo video."*[506] S komplexným návrhom regulácie generatívnej AI prišiel Európsky parlament vo svojej pozícií. Európsky parlament navrhuje špecificky regulovať generatívne systémy AI v rámci požiadaviek pre základné modely. Základné modely definuje návrh Európskeho parlamentu ako *„model systému umelej inteligencie, ktorý je trénovaný na rozsiahlom súbore*

[499] AIA, článok 62.
[500] K tomu pozri napríklad BOMMASANI, R. et al. *On the opportunities and risks of foundation models*. arXiv preprint arXiv:2108.07258 (2021).
[501] GANGULI, D. Predictability and surprise in large generative models. *ACM Conference on Fairness, Accountability, and Transparency* (2022), 1747-1764.
[502] HACKER, P. et al. *Regulating ChatGPT and other Large Generative AI Models*. FAccT '23, June 12-15, 2023, Chicago, IL, USA.Dostupné na: https://arxiv.org/abs/2302.02337.
[503] Tamže.
[504] K možnostiam obídenia limitov pozri napríklad ZOU, A. et al. *Universal and Transferable Adversarial Attacks on Aligned Language Models*. Dostupné na: https://arxiv.org/abs/2307.15043.
[505] K tomu pozri UUK, R. et al. *Operationalising the Definition of General Purpose AI Systems: Assessing Four Approaches*. 2023. Dostupné na: https://ssrn.com/abstract=4471151.
[506] Pozícia Európskeho parlamentu, článok 28b ods. 4.

údajov, je navrhnutý na všeobecný charakter výstupov a možno ho prispôsobiť širokému spektru osobitných úloh."[507] Na tieto modely sú naviazané nasledujúce požiadavky:

- identifikovať a zmierňovať dôvodne predpokladané riziká pre zdravie, bezpečnosť, základné práva, životné prostredie a demokraciu a právny štát pred vývojom a počas neho napríklad prostredníctvom zapojenia externých odborníkov,
- využívať predovšetkým vhodné údaje
- navrhnúť a vyvíjať základný model s cieľom dosiahnuť počas celého jeho životného cyklu primeranú úroveň výkonnosti, predvídateľnosti, interpretovateľnosti, korigovateľnosti, bezpečnosti a kybernetickej bezpečnosti
- zaznamenávať a znižovať negatívny vplav základného modelu na životné prostredie,
- vypracovať technickú dokumentáciu a návod,
- vytvoriť systém riadenia kvality,
- registrácia základného modelu v databáze vedenej EÚ.[508]

Nad rámec vyššie uvedených požiadaviek musia poskytovatelia systémov generatívnej AI spĺňať ďalšie povinnosti. Konkrétne ide o dodržiavanie povinnosti transparentnosti podľa článku 52 ods. 1 AIA v zmysle návrhov Európskeho parlamentu,[509] ktoré diskutujeme nižšie. Kľúčovou navrhovanou požiadavkou je *„trénovať a prípadne navrhnúť a rozvíjať základný model takým spôsobom, aby sa zabezpečili primerané záruky na predchádzanie vytváraniu obsahu v rozpore s právnymi predpismi Únie v súlade so všeobecne uznávaným stavom techniky a bez toho, aby boli dotknuté základné práva vrátane slobody prejavu.*"[510] Toto ustanovenie tak v sebe ukrýva povinnosť pre poskytovateľov generatívnej AI zabezpečiť, aby systémy negenerovali nenávistný obsah, detskú pornografiu alebo extrémistické materiály. Podobne ako pri DSA, dezinformácie nemusia predstavovať obsah, ktorý je v rozpore s právnymi predpismi EÚ.

Treťou požiadavkou navyše je dokumentácia a zverejňovanie zhrnutia používania údajov z odbornej prípravy chránených podľa autorského práva.[511] Inými slovami, ak poskytovatelia

[507] Pozícia Európskeho parlamentu, článok 3 bod 1c.
[508] Pozícia Európskeho parlamentu, článok 28b ods. 2.
[509] Pozícia Európskeho parlamentu, článok 28b ods. 4 písm. a).
[510] Pozícia Európskeho parlamentu, článok 28b ods. 4 písm. b).
[511] Pozícia Európskeho parlamentu, článok 28b ods. 4 písm. c).

generatívnej AI natrénujú model na dielach chránených autorských zákonom, sú povinní túto skutočnosť transparentne komunikovať, aby si držitelia práv vedeli uplatniť svoje nároky.[512]

Transparentnosť systémov AI

Transparentnosť systémov AI je vo všeobecnosti jednou z veľkých tém súčasnosti.[513] Zároveň je nutné uviesť, že pri systémoch AI má transparentnosť viaceré modality. Preto je nevyhnutné medzi týmito modalitami rozlišovať. Diferencovať ich možno na:

1) Povedomie (*awaraness*);

2) Vysvetliteľnosť (*explainability*); a

3) Dosledovateľnosť rozhodnutí (*logging*).

Otázky povedomia sa týkajú poskytovania informácií o systéme AI. Táto vedomosť by sa nemala limitovať iba na binárne zistenie, či sa takýto proces využíva alebo nie, ale zároveň by mal jednotlivec mať možnosť pochopiť, v čom proces rozhodovania systémom AI spočíva a aký to má vplyv na jeho výsledok.

Vysvetliteľnosť môže byť všeobecná (*ex ante*) alebo špecifická (*ex post*). Všeobecná vysvetliteľnosť znamená, že ešte predtým, ako je o jednotlivcovi rozhodnuté systémom AI, má k dispozícii všeobecné informácie o fungovaní tejto technológie.[514] Predmetná modalita je veľmi blízka otázke povedomia. Na druhej strane rozoznávame vysvetliteľnosť *ex post* v konkrétnych prípadoch s konkrétnym rozhodnutí a vplyvom na jednotlivca. To prakticky znamená, že jednotlivec by mal vedieť a pochopiť, prečo v jeho konkrétnom prípade bolo rozhodnuté systémom AI určitým spôsobom.

Poslednou modalitou transparentnosti je dosledovateľnosť rozhodnutí. To znamená, že prevádzkovateľ AI systému je schopný identifikovať, prečo bolo konkrétne rozhodnutie urobené výsledným spôsobom a na základe akých parametrov. Tieto informácie sa najčastejšie získavajú z tzv. logov (záznamov) systému AI. Uchovávanie a spracúvanie predmetných záznamov vo významnej miere môže pomôcť pri hlbšom sledovaní algoritmov a zároveň slúži

[512] K tomu pozri QUINTAIS, J. P. *Generative AI, Copyright and the AI Act*. Kluwer Copyright Blog. Dostupné na: https://copyrightblog.kluweriplaw.com/2023/05/09/generative-ai-copyright-and-the-ai-act/.
[513] GOHEL, P. – SINGH, P. – MOHANTY, M. *Explainable AI: current status and future directions*. Dostupné na: https://arxiv.org/abs/2107.07045.
[514] WACHTER, S. – MITTLESTADT, B. – FLORIDI, L. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. In *International Data Privacy Law*, Volume 7, Issue 2, May 2017, s. 76–99.

ako prevencia pred diskriminačnými rozhodnutiami či inými negatívnymi dôsledkami využívania systémov AI, ako je uvedené vyššie.

Pôvodný návrh AIA z dielne Európskej komisie reflektoval v zásade všetky modality transparentnosti. Dosledovateľnosť sme diskutovali vyššie z pohľadu povinnosti uchovávať záznamy. Vysvetliteľnosť vo všeobecnej rovine odzrkadľujú požiadavky pre vysokorizikové systémy AI v článku 13 AIA (transparentnosť a poskytovanie informácií používateľom). V kontexte šírenia dezinformácií je ale najviac relevantné povedomie. Konkrétne v prípadoch, kde ide o obsah manipulovaný systémami AI, ktorého cieľom je pôsobiť ako realita, tzv. deepfakes[515] a systémoch AI určených na interakciu s človekom. Vo všeobecnosti AIA klasifikuje systémy generujúce deepfakes ako nízko rizikové, avšak to platí iba v prípadoch, ak nie sú využívané v oblastiach vysokého rizika. Návrhy Európskeho parlamentu obsahujú aj definíciu deepfakes ako *„zmanipulovaný alebo syntetický zvukový, obrazový alebo video obsah, ktorý sa falošne javí ako autentický alebo pravdivý a ktorý obsahuje zobrazenia osôb, ktoré zdanlivo hovoria alebo robia veci, ktoré nepovedali alebo neurobili, vytvorený pomocou techník umelej inteligencie vrátane strojového učenia a hĺbkového učenia."*[516]

Samotná požiadavka transparentnosti pre systémy AI určené na interakciu s človekom je ustanovená nasledovným spôsobom: *„Poskytovatelia zabezpečia, aby systémy umelej inteligencie určené na interakciu s fyzickými osobami boli koncipované a vyvinuté tak, aby boli fyzické osoby informované o tom, že komunikujú so systémom umelej inteligencie, pokiaľ to nie je zrejmé z okolností a kontextu používania."*[517] V prípade takýchto systémov, ktoré vytvárajú obrazové, zvukové alebo obrazovo-zvukové obsahy, ktoré sa zjavne podobajú existujúcim osobám, predmetom, miestam, subjektom alebo udalostiam, používatelia predmetných systémov musia zabezpečiť informácie o tom, že upravený obsah bol umelo vytvorený alebo zmanipulovaný.[518] Pri dezinformáciách šírených prostredníctvom zvukov, obrazov alebo videí za podmienky ich úpravy alebo manipulácie systémami AI by tak užívateľ mal mať vedomosť o tom, že takýto obsah bol umelo generovaný. Rada EÚ vo svojej pozícií navrhuje, aby predmetné informácie boli poskytnuté najneskôr v momente prvej interakcie človeka so systémom AI alebo obsahom.[519] Európsky parlament navrhuje pridať aj informácie o tom, ktoré *„funkcie sú umožnené umelou inteligenciou, ak existuje ľudský dohľad, a kto je zodpovedný za*

[515] K tomu viac SAMPLE, I. *What are deepfakes – and how can you spot them?* The Guardian. Dostupné na: https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them.
[516] Pozícia Európskeho parlamentu, článok 3 bod 44d.
[517] AIA, článok 52 ods. 1.
[518] AIA, článok 52 ods. 3.
[519] Pozícia Rady EÚ, článok 52 ods. 3a.

rozhodovací proces, ako aj existujúce práva a postupy, ktoré podľa práva Únie a vnútroštátneho práva umožňujú fyzickým osobám alebo ich zástupcom namietať proti uplatňovaniu takýchto systémov vo vzťahu k nim a domáhať sa súdneho prostriedku nápravy v prípade rozhodnutí prijatých systémami umelej inteligencie alebo ujmy nimi spôsobenej vrátane ich práva požiadať o vysvetlenie."[520] Pri deepfakes Európsky parlament navrhuje rozšíriť obsah o obsah textový a povinnosť informovať o osobe, ktorá obsah vytvorila.[521] Rozšírenie pôsobnosti týchto povinností o textový obsah môže výrazne posilniť boj s dezinformáciami online, nakoľko väčšina dezinformácií má textovú podobu.

Európsky parlament vo svojich návrhoch ohľadom transparentnosti ide ešte ďalej a navrhuje zakotvenie práva na vysvetlenie individuálnych rozhodnutí vysokorizikových systémov AI.[522] Na právo na vysvetlenie má každá dotknutá osoba nárok vtedy, ak výstup vysokorizikového systému AI v podobe rozhodnutia má právne účinky na ňu alebo podobne významný negatívny vplyv na zdravie, základné práva, sociálno-ekonomický blahobyt alebo akékoľvek iné práva vyplývajúce z povinností stanovených v AIA.[523] Dotknutá osoba by mala následne dostať zmysluplné vysvetlenie ohľadom úlohy systému AI v rozhodovacom procese, hlavných parametroch prijatého rozhodnutia čo súvisiacich vstupných údajov.[524] V kontexte odporúčacích systémov na sociálnych sieťach tak môže ísť o ďalší z nástrojov, ktoré si môže individuálne jednotlivec uplatniť. Toto právo môžu členské štáty alebo EÚ v právnom poriadku obmedziť.[525]

3.2 Špecifické nástroje verejného práva

3.2.1 Konanie vo veci zamedzenia šírenia nelegálneho obsahu

Zákon o mediálnych službách upravuje osobitné správne konanie vo veci zamedzenia šírenia nelegálneho obsahu. Predmetné konanie posilňuje kompetencie Rady pre mediálne služby v oblastí vymáhania práv v online priestore a v prípade, ak dezinformácie dosahujú kvalitu nezákonnosti, môže byť tento nástroj významný dielom skladačky pre boj s dezinformáciami online.

§ 151 ods. 2 Zákona o mediálnych službách definuje nelegálny obsah ako obsah, ktorý:

[520] Pozícia Európskeho parlamentu, článok 52 ods. 1.
[521] Pozícia Európskeho parlamentu, článok 52 ods. 3.
[522] Pozícia Európskeho parlamentu, článok 68c ods. 1.
[523] Tamže.
[524] Tamže.
[525] Pozícia Európskeho parlamentu, článok 68c ods. 2.

„ a)napĺňa znaky detskej pornografie alebo extrémistického materiálu,

b) podnecuje ku konaniu, ktoré napĺňa znaky niektorého z trestných činov terorizmu,

c) schvaľuje konanie, ktoré napĺňa znaky niektorého z trestných činov terorizmu, alebo

d) napĺňa znaky trestného činu popierania a schvaľovania holokaustu, zločinov politických režimov a zločinov proti ľudskosti, trestného činu hanobenia národa, rasy a presvedčenia alebo trestného činu podnecovania k národnostnej, rasovej a etnickej nenávisti."

Konanie sa môže začať na podnet podaný písomne alebo elektronicky[526] alebo *ex offo*, ak vec neznesie odklad.[527] Samotné konanie vedú trojčlenné senáty Rady pre mediálne služby a podnety prerokúvajú najneskôr do 45 dní od zaevidovanie podnetu.[528]

Na začatie konania je nevyhnutné, aby nelegálny obsah bol prítomný na platforme na zdieľanie obsahu[529] alebo obsahovej služby[530] nevyžadujúcej oprávnenie podľa tohto zákona, najmä v elektronickej periodickej publikácii, na spravodajskom webovom portáli alebo v agentúrnom servise.[531] Rada pre mediálne služby konanie začne za splnenia dvoch podmienok. Prvou podmienkou je, *„že ide o potenciálne nelegálny obsah, ktorého šírením môže byť ohrozený verejný záujem alebo predstavuje značný zásah do individuálnych práv či oprávnených záujmov osoby v pôsobnosti právneho poriadku Slovenskej republiky.*"[532] Druhou podmienkou je, že ešte pred podaním podnetu bol poskytovateľ obsahovej služby preukázateľne informovaný o nelegálnom obsahu na svojej službe a oznámenie ignoroval,[533] obsah neodstránil[534] alebo oznámil podávateľovi, že obsah neplánuje odstrániť.[535] Samotné začatie konanie je Rada pre mediálne služby povinná oznámiť dotknutému poskytovateľovi obsahovej služby s identifikáciou nelegálneho obsahu a odôvodnením nelegálnosti obsahu.[536] Poskytovateľ obsahovej služby musí Rade pre mediálne služby poskytovať súčinnosť, minimálne vo forme

[526] Zákon o mediálnych službách, § 151 ods. 1.
[527] Zákon o mediálnych službách, § 152 ods. 3.
[528] Zákon o mediálnych službách, § 152 ods. 1.
[529] Platforma na zdieľanie obsahu je definovaná v Zákone o mediálnych službách v § 9 ods. 1 ako *„služba informačnej spoločnosti, ktorej hlavným účelom alebo jedným z jej hlavných účelov alebo ktorej zásadnou funkciou je ukladať veľký počet diel a iných predmetov ochrany podľa osobitného predpisu4) nahrávaných jej užívateľmi a šíriť ich podľa osobitného predpisu.*" Medzi platformy na zdieľanie obsahu nepatria on-line encyklopédie a vzdelávacie a vedecké úložisko, ktorých účelom nie je dosahovanie zisku; platformy na vývoj a zdieľanie počítačových programov s otvoreným zdrojovým kódom a on-line trhovisko, medzipodniková cloudová služba a cloudová služba, ktoré užívateľom umožňujú nahrať obsah pre vlastnú potrebu alebo potreby štátu. Zákon o mediálnych službách, § 9 ods. 2.
[530] Obsahovú službu definuje Zákon o mediálnych službách v § 13 pozitívnym a negatívnym spôsobom.
[531] Zákon o mediálnych službách, § 152 ods. 2.
[532] Tamže.
[533] Zákon o mediálnych službách, § 152 ods. 2 písm. a).
[534] Zákon o mediálnych službách, § 152 ods. 2 písm. b).
[535] Zákon o mediálnych službách, § 152 ods. 2 písm. c).
[536] Zákon o mediálnych službách, § 152 ods. 4.

zdieľania informácií a vytvorením mechanizmu na efektívnu komunikáciu medzi Radou pre mediálne služby a poskytovateľom služby.[537]

Ak senát Rady pre mediálne služby preukáže, že prejedávaný obsah spĺňa parametre nelegálnosti, vydá rozhodnutie o zamedzení šírenia nelegálneho obsahu. Poskytovateľ obsahovej služby je následne povinný predmetný obsah odstrániť a zamedziť jeho šíreniu.[538] Samotné rozhodnutia sú zverejňované prostredníctvom webového sídla Rady pre mediálne služby.[539] *„Voči rozhodnutiu podľa odseku 1 môže podať námietku každý, kto sa cíti jeho účinkami dotknutý na svojich právach; podanie námietky nemá odkladný účinok a nevzťahujú sa naň ustanovenia správneho poriadku."*[540] Ak Rada pre mediálne služby uzná námietku v plnej alebo čiastočnej miere, vydá upravené rozhodnutie.[541]

Nakoľko sú rozhodnutia Rady pre mediálne služby verejne dostupné na jej webovom sídle,[542] vykonali sme analýzu rozhodnutí v časovom rámci od nadobudnutia účinnosti právnej úpravy (1.8.2022) do 10.11.2023. Vo vymedzenom období posudzovali senáty celkovo 53 podnetov na nelegálny obsah, z toho správne konanie začali iba v dvoch prípadoch.[543]

Zasadnutie rady	Počet	Rozhodnutie o zamedzení šírenia	Rozhodnutie o odložení
Zasadnutie RpMS č. 1/2022	0	0	0
Zasadnutie RpMS č. 2/2022	0	0	0
Zasadnutie RpMS č. 3/2022	0	0	0
Zasadnutie RpMS č. 4/2022	0	0	0
Zasadnutie RpMS č. 5/2022	9	0	9
Zasadnutie RpMS č. 6/2022	3	0	3
Zasadnutie RpMS č. 7/2022	5	0	5
Zasadnutie RpMS č. 8/2022	2	0	2
Mimoriadne zasadnutie RpMS č. 9/2022	0	0	0
Zasadnutie RpMS č. 10/2022	2	1	1

[537] Zákon o mediálnych službách, § 152 ods. 8.
[538] Zákon o mediálnych službách, § 153 ods. 1.
[539] Zákon o mediálnych službách, § 153 ods. 3.
[540] Zákon o mediálnych službách, § 153 ods. 4.
[541] Zákon o mediálnych službách, § 153 ods. 5.
[542] RADA PRE MEDIÁLNE SLUŽBY. *Zasadnutia Rady pre mediálne služby*. Dostupné na: https://rpms.sk/o-nas/zasadnutia/zasadnutia-rady.
[543] To nevylučuje začatie konania *ex offo*.

Zasadnutie RpMS č. 11/2022	1	0	1
Zasadnutie RpMS č. 1/2023	1	0	1
Zasadnutie RpMS č. 2/2023	5	1	4
Zasadnutie RpMS č. 3/2023	2	0	2
Zasadnutie RpMS č. 4/2023	2	0	2
Zasadnutie RpMS č. 5/2023	7	0	7
Zasadnutie RpMS č. 6/2023	3	0	3
Zasadnutie RpMS č. 7/2023	3	0	3
Zasadnutie RpMS č. 8/2023	0	0	0
Zasadnutie RpMS č. 9/2023	0	0	0
Zasadnutie RpMS č. 10/2023	1	0	1
Zasadnutie RpMS č. 11/2023	1	0	1
Zasadnutie RpMS č. 12/2023	3	0	3
Zasadnutie RpMS č. 13/2023	1	0	1
Zasadnutie RpMS č. 14/2023	0	0	0
Zasadnutie RpMS č. 15/2023	1	0	1
Zasadnutie RpMS č. 16/2023	0	0	0
Zasadnutie RpMS č. 17/2023	0	0	0
Zasadnutie RpMS č. 18/2023	0	0	0
Zasadnutie RpMS č. 19/2023	1	0	1
Zasadnutie RpMS č. 15/2023	1	0	1
SPOLU	**53**	**2**	**50**

Tabuľka: Rozhodnutia Rady pre mediálne služby vo veci nelegálneho obsahu.
Zdroj: Web Rady pre mediálne služby.

Ak sa pozrieme bližšie na dôvody odloženia podnetu, Rada pre mediálne služby podnety najčastejšie podnety odložila z dôvodu neopodstatnenosti (27) a absencie povinných náležitostí (9). Medzi menej časté dôvody odloženia podnetov boli nedostupnosť obsahu, na ktorý smeroval podnet (8) a zjavná neodôvodnenosť alebo zjavná neopodstatnenosť podnetu (2).

Zasadnutie Rady	Počet rozhodnutí o odložení	Neopodstatnenosť	Absencia povinných náležitostí	Zjavne neôdovodnený / neopodstatnený	Vymazanie obsahu
Zasadnutie RpMS č. 5/2022	9	3	6	0	0

Zasadnutie RpMS č. 6/2022	3	3	0	0	0
Zasadnutie RpMS č. 7/20221	2	1	0	1	0
Zasadnutie RpMS č. 10/2022	1	0	0	0	1
Zasadnutie RpMS č. 11/2022	1	1	0	0	0
Zasadnutie RpMS č. 1/2023	1	0	1	0	0
Zasadnutie RpMS č. 2/2023	4	1	0	0	3
Zasadnutie RpMS č. 3/2023	2	1	0	1	0
Zasadnutie RpMS č. 4/2023	2	2	0	0	0
Zasadnutie RpMS č. 5/2023	7	7	0	0	0
Zasadnutie RpMS č. 6/2023	3	1	1	0	1
Zasadnutie RpMS č. 7/2023	3	1	1	0	1
Zasadnutie RpMS č. 10/2023	1	1	0	0	0
Zasadnutie RpMS č. 11/2023	1	1	0	0	0
Zasadnutie RpMS č. 12/2023	3	2	0	0	1
Zasadnutie RpMS č. 13/2023	1	0	0	0	1
Zasadnutie RpMS č. 15/2023	1	1	0	0	0
Zasadnutie RpMS č. 19/2023	1	1	0	0	0
Zasadnutie RpMS č. 20/2023	0	0	0	0	0
SPOLU	**46**	**27**	**9**	**2**	**8**

Tabuľka: Odložené rozhodnutia Rady pre mediálne služby vo veci nelegálneho obsahu.
Zdroj: Web Rady pre mediálne služby.

Ak sa bližšie pozrieme na rozhodnutia, v ktorých Rada pre mediálne služby začala správne konanie, možno konštatovať, že išlo o výrazne intenzívny nelegálny obsah.

Prvé analyzované rozhodnutia sa týka blogového príspevku, zverejneného na portáli hlavespravy.sk, ktoré spochybňuje počet obetí holokaustu a zároveň obsahuje nenávistné komentáre pretkané konšpiráciami o príslušníkoch židovskej národnosti a ich úlohe v globálnom meradle.[544] Na základe ustanovení Trestného zákona Rada pre mediálne služby analyzovaný blog vyhodnotila ako obsahujúci nelegálny obsah a začala správne konanie.

Druhé analyzované rozhodnutie sa týka komentára pod videom na platforme na zdieľanie videí YouTube na kanály spravodajstva z krajského mesta. Video sa týka vyhodenia príslušníkov rómskeho etnika z vozidla mestskej hromadnej dopravy. Pod týmto videom sa objavil nenávistný komentár apelujúci na likvidáciu tejto etnickej menšiny.[545] Opätovne s odkazmi na relevantné ustanovenia Trestného zákona týkajúce sa podnecovania k národnostnej, rasovej a etnickej nenávisti Rada pre mediálne služby začala správne konanie. Z mediálnych vyjadrení je zjavné, že poskytovateľ služby na zdieľanie videí YouTube komentáre po začatí správneho konania odstránil.[546]

V oboch vyššie uvedených prípadoch Rada pre mediálne služby upozornila orgány činné v trestnom konaní.

Zásadné obmedzenie konaní o obmedzení nelegálneho obsahu je práve ich úzka pôsobnosť. Ako uvádza Rada pre mediálne služby vo väčšine svojich rozhodnutí *„vo veci zamedzenia šírenia nelegálneho obsahu podľa § 152 zákona o mediálnych službách, v jej kompetenciách nie je posudzovať kontroverzné, šokujúce či hanlivé tvrdenia a obsahy, ak zároveň nenapĺňajú definíciu nelegálneho obsahu – t.j. ak nenapĺňajú znaky detskej pornografie, extrémistického materiálu alebo trestných činov uvedených v § 152 ods. 2 zákona o mediálnych službách alebo posudzovať pravdivosť či opodstatnenosť existencie takzvaných „konšpirácií" či „konšpiračných teórií", t. j. tvrdení/teórií, ktoré nie sú podložené vedeckými dôkazmi či inými faktami."*[547] Ak by dezinformácie predstavovali nezákonný obsah, Rada pre mediálne služby by sa nimi mohla zaoberať. V opačnom prípade by došlo k odloženiu podnetu.

Takýto postup Rada pre mediálne služby zvolila pri preverovaní podnetu, ktorý sa týkal videa obsahujúceho vojnovú dezinformačnú propagandu z Ruskej federácie na sociálnej sieti. Ako sa v rozhodnutí uvádza: *„Za daných okolností a vychádzajúc z obsahu videa sa Kancelária*

---

[544] *Pracovný materiál Kancelárie Rady na rokovanie Rady dňa 7. 12. 2022, podnet týkajúci sa nelegálneho obsahu č.: AO-RPMS/2022/00254*.
[545] *Pracovný materiál Kancelárie Rady na rokovanie Rady dňa 25. 1. 2023, Podnet týkajúci sa nelegálneho obsahu č.: AO-RPMS/2023/00143*.
[546] DENNÍK N. *Minúta po minúte zo dňa 7. februára 2023 11:05*. Dostupné na: https://dennikn.sk/minuta/3227529/.
[547] *Pracovný materiál Kancelárie Rady na rokovanie Rady dňa 22. 2. 2023, Podnet týkajúci sa nelegálneho obsahu č.: AO-RPMS/2022/00139*.

domnieva, že predmetné informácie obsiahnuté vo videu môžu obsahovať prvky konšpiračných teórií, dezinformácií či vyfabulovaných informácií, ktoré nie je možné nezávisle overiť. Video totiž okrem iného obsahuje vyjadrenia o údajných tajných bunkroch a údajných sprisahaniach médií a „elít". Tieto informácie však nie sú podložené relevantnými zdrojmi. Zároveň sú bez náležitého celkového kontextu manipulatívne spájané časti vyjadrení a informácií takým spôsobom, aby u príjemcu navodili pocit, že sa vo videu deklarované udalosti a reálie (tajné bunkre a plánované sprisahania) aj skutočne reálne odohrali."[548] Vzhľadom na to, že išlo síce o dezinformačný obsah, ale nie o nelegálny obsah, Rada pre mediálne služby správne konanie nezačala a odložila podnet ako neopodstatnený.

3.2.2 Špecifické opatrenia na zvýšenie transparentnosti a zodpovednosti v online priestore

Ako sme uviedli vyššie, niektoré štáty upravujú boj s dezinformáciami alebo nelegálnym obsahom aj prostredníctvom špecifických právnych úprav.[549] Najznámejším príkladom je Nemecko, konkrétne známy nemecký zákon *Netzwerkdurchsetzungsgesetz*, v skratke NetzDG.[550] V zmysle tejto právnej úpravy sa sociálnym sieťam ukladajú povinnosti zaviesť efektívny manažment sťažností kvôli obsahu či podávanie správ o transparentnosti. Za porušenie zákona hrozia sankcie až do výšky 50 miliónov eur.[551] Kľúčovou požiadavkou NetzDG je povinné zavedenie mechanizmov na odstránenie zjavne nelegálneho obsahu u sociálnych sietí s viac ako 2 miliónmi užívateľmi v Nemecku do 24 hodín od upozornenia. Na odstránenie nelegálneho obsahu majú platformy 7 dní. Nezákonný obsah NetzDG definuje prostredníctvom odkazu na skutkové podstaty trestných činov v nemeckom trestnom zákonníku. Prevádzkovatelia sociálnych sietí musia v zmysle tejto legislatívy určiť kontaktnú osobu v Nemecku na prijímanie sťažností a podnetov.[552]

Francúzsko v roku 2018 zaviedlo právnu úpravu, ktorá sa týka šírenia dezinformácií počas volieb. Zákon umožňuje v období troch mesiacov pred voľbami orgánom verejnej moci

---

[548] *Pracovný materiál Kancelárie Rady na rokovanie Rady dňa 22. 2. 2023, Podnet týkajúci sa nelegálneho obsahu č.: AO-RPMS/2023/01084*.

[549] Podkladom pre vypracovanie tejto kapitoly je príspevok prezentovaný na konferencii Míľniky práva v stredeurópskom priestore 2023. MESARČÍK, M. Ale prečo? predbežná analýza návrhu zákona o opatreniach na zvýšenie bezpečnosti a dôveryhodnosti platforiem v on-line prostredí. In ŤAŽKÁ, V. (ed). *Míľniky práva v stredoeurópskom priestore 2023*. Bratislava : Právnická fakulta Univerzity Komenského v Bratislave., 2023, s. 122 – 133.

[550] *Netzwerkdurchsetzungsgesetz*. Dostupné na: https://www.bmj.de/DE/Themen/FokusThemen/NetzDG/NetzDG_EN_node.html;jsessionid=0012EB9BAA0F22E45E36BA0E408CB648.2_cid297.

[551] ANDRES, R. - SLIVKO, O: *Content Regulation on Social Media: Evidence from NetzDG*. ZEW - Centre for European Economic Research Discussion Paper No. 21-103. 2021. Dostupné na: https://ssrn.com/abstract=4013662 or http://dx.doi.org/10.2139/ssrn.4013662.

[552] NIKOLAS GUGGENBERGER. *The Network Enforcement Act*. Dostupné na: https://wilmap.stanford.edu/entries/network-enforcement-act.

odstraňovať obsah a dokonca aj blokovať konkrétne webové sídla, ak sa na nich šíria falošné správy.[553] Samotný zákon konkrétne zavádza nové predbežné konanie, ktoré umožňuje sudcom prijať primerané a nevyhnutné opatrenia voči poskytovateľom internetových služieb a službám typu hosting s cieľom zastaviť šírenie nepresných alebo zavádzajúcich tvrdení alebo podozrení o skutočnosti. Francúzska audiovizuálna rada zároveň dostala nové právomoci, konkrétne aby mohla zabrániť, pozastaviť alebo ukončiť vysielanie televíznych služieb kontrolovaných cudzím štátom v prípade porušenia základných záujmov krajiny. Zákon taktiež zaviedol povinnosti pre služby typu hosting a poskytovateľov internetových služieb umožňujúce používateľom upozorniť na informácie, ktoré považujú za falošné a informovať orgány verejnej moci.[554] Ústavnosť diskutovaného zákona bola potvrdená aj francúzskym ústavným súdom.[555]

Z nemeckej právnej úpravy si berie inšpiráciu aj slovenský pokus o podobnú legislatívu. Na jar 2023 predstavilo Ministerstvo investícií, regionálneho rozvoja a informatizácie návrh zákona o opatreniach na zvýšenie bezpečnosti a dôveryhodnosti platforiem v on-line prostredí (ďalej len „Návrh dezinfo zákona"), ktorý už prešiel medzirezortným pripomienkovým konaním.

Navrhovaná právna úprava deklaruje niekoľko cieľov, konkrétne:

- rozšírenie definície nezákonného obsahu v zmysle Zákona o mediálnych službách,
- sprísnenie sankcií za šírenie dezinformácií,
- zakotvenie právneho rámca na zásahy štátu voči dezinformáciami, a
- obmedzenie anonymity v online diskusiách.[556]

Už z vyššie deklarovaných cieľov je zjavné, že slovenská právna úprava sa nevyhnutne dotkne aj oblasti, ktorú upravuje DSA. Konkrétne pri zakotvení rámca pre zásahy štátu voči nezákonnému či škodlivému obsahu ide o oblasť, ktorú v určitej miere upravuje aj právo EÚ.

---

[553] YOUNG, Z. *French Parliament passes law against 'fake news.'* Politico. Dostupné na: https://www.politico.eu/article/french-parliament-passes-law-against-fake-news/. Text zákona vo francúzštine dostupný na: https://www.assemblee-nationale.fr/dyn/15/textes/l15b0799_proposition-loi.

[554] Text zákona vo francúzštine dostupný na: https://www.assemblee-nationale.fr/dyn/15/textes/l15b0799_proposition-loi.

[555] Rozhodnutie dostupné na: https://www.conseil-constitutionnel.fr/decision/2018/2018773DC.htm.

[556] *Dôvodová správa k Návrhu dezinfo zákona*.

Návrh dezinfo zákona obsahuje legálnu definíciu dezinformácie v § 2 ods. 1, ktorej aspekty v kontexte definícií dezinformácie z pohľadu vedeckého výskumu a politických dokumentov sme už analyzovali v prvej kapitole predkladanej práce.

Ako bolo uvedené vyššie, Návrh dezinfo zákona rozširuje legálnu definíciu nezákonného obsahu. V súčasnosti platná definícia v zmysle Zákona o mediálnych službách obsahuje iba štyri skutkové podstaty (viď diskusia vyššie).[557] Navrhovaná právna úprava rozširuje definíciu nezákonného obsahu o bezmála 25 skutkových podstát. Podľa tohto návrhu by definícia nelegálneho obsahu vyzerala nasledovným spôsobom:

„Nelegálnym obsahom je na účely tohto zákona obsah, ktorý

a) obsahuje znaky niektorého z nasledovných trestných činov:

1. sexuálne zneužívanie,

2. trestné činy podvodu,

3. trestné činy spojené s neoprávneným zásahom alebo prístupom do počítačového programu alebo údaja,

4. založenie, zosnovanie a podporovanie zločineckej alebo teroristickej skupiny,

5. vlastizrada,

6. sabotáž, vyzvedačstvo,

7. ohrozenie utajovanej skutočnosti,

8. násilie proti skupine obyvateľov,

9. nebezpečné vyhrážanie,

10. nebezpečné prenasledovanie,

11. nebezpečné elektronické obťažovanie,

12. šírenie poplašnej správy,

13. trestné činy detskej pornografie,

14. podpora a propagácia sexuálnych patologických praktík,

[557] Zákon o mediálnych službách, § 151 ods. 1.

15. spolupráca s nepriateľom,

16. ohrozenie mieru,

17. genocídium,

18. trestné činy terorizmu,

19. založenie, podpora a propagácia hnutia smerujúceho k potlačeniu základných práv a slobôd,

20. prejav sympatie k hnutiu smerujúcemu k potlačeniu základných práv a slobôd,

21. trestné činy spojené s extrémistickým materiálom,

22. popieranie a schvaľovanie holokaustu, zločinov politických režimov a zločinov proti ľudskosti,

23. hanobenie národa, rasy a presvedčenia,

24. podnecovanie k národnostnej, rasovej a etnickej nenávisti,

25. vojnové bezprávie.

b) napĺňa znaky detskej pornografie alebo extrémistického materiálu,

c) je verejným podnecovaním na šírenie alebo uskutočnenie obsahu podľa písmen a) alebo b), alebo verejným schvaľovaním obsahu podľa písmen a) alebo b),

d) je označený ako nezákonný osobitným predpisom,

e) je šírený alebo dostupný verejne, ak je verejné šírenie alebo dostupnosť takého obsahu zakázané podľa osobitného predpisu."[558]

Prakticky tak „spúšťa" povinnosti súladu a požiadaviek náležitej starostlivosti v zmysle DSA v oveľa väčšom rozsahu pre online platformy a zároveň rozširuje rozsah možných správnych konaní vo veci zamedzenia šírenia nelegálneho obsahu, ktoré vedie Rada pre mediálne služby.

Gro Návrhu dezinfo zákona tvorí demonštratívny výpočet preventívnych a aktívnych opatrení pre boj s dezinformáciami. Tieto opatrenia môžu prijímať orgány verejnej moci, ak majú negatívny vplyv na základné práva a slobody veľkého počtu osôb.[559] Preventívne

[558] Návrh dezinfo zákona, článok 2 bod 12.
[559] Tamže, § 3 ods. 1.

opatrenia slúžia na posilňovanie vedomostnej a informačnej úrovne v oblastiach, ktoré sú náchylné čeliť dezinformáciám, alebo v prípadoch hrozby koordinovaných dezinformačných aktivít ako napríklad monitorovanie dezinformačných trendov a naratívov či vzdelávanie.[560] Aktívne opatrenia budú môcť orgány verejnej moci prijímať v reakcii na existujúce dezinformácie, alebo koordinované dezinformačné aktivity ako analýzy, detekcie či návrhy opatrení na zabránenie šírenia dezinformácií.[561] Práve tieto časti navrhovanej právnej úpravy sa môžu dostať do konfliktu s DSA. Recitál 9 DSA ustanovuje: *„Týmto nariadením **sa v plnej miere harmonizujú pravidlá uplatniteľné na sprostredkovateľské služby** na vnútornom trhu s cieľom zaistiť bezpečné, predvídateľné a dôveryhodné online prostredie, riešiť šírenie nezákonného obsahu na internete a spoločenské riziká, ktoré môžu vyplynúť zo šírenia dezinformácií alebo iného obsahu, a v rámci ktorého sú účinne chránené základné práva zakotvené v charte a uľahčujú sa inovácie. **Členské štáty by preto nemali prijímať ani trvať na dodatočných vnútroštátnych požiadavkách týkajúcich sa záležitostí, ktoré patria do rozsahu pôsobnosti tohto nariadenia**, pokiaľ sa to v ňom výslovne neustanovuje, keďže by to malo vplyv na priame a jednotné uplatňovanie plne harmonizovaných pravidiel uplatniteľných na poskytovateľov sprostredkovateľských služieb v súlade s cieľmi tohto nariadenia."* Vzhľadom na to, že DSA sa v určitej miere týka aj škodlivého obsahu a po klasifikovaní dezinformácií ako nezákonného obsahu by sa aplikovalo v plnej miere, je na mieste uviesť, že Návrh dezinfo zákona nebude v súlade s cieľmi DSA, ktoré predstavuje harmonizáciu pravidiel pre sprostredkovateľské služby.

Osobitne, problematické otázky regulácie sa týkajú aj dohľadu. Kľúčovú úlohu podľa navrhovanej právnej úpravy zohráva Úrad vlády Slovenskej republiky, ktorý by mal koordinovať orgány verejnej moci, ktoré sú súčasťou národného systému v prijímaní opatrení proti dezinformáciám.[562] Táto požiadavka naráža na viaceré aspekty regulácie digitálnych služieb. Prvým je, že dohľad nad veľmi veľkými online platformami (ako Facebook, Instagram alebo Twitter) vykonáva výlučne Európska komisia.[563] Slovenské orgány preto nebudú môcť prijímať opatrenia pre boj s dezinformáciami voči týmto platformám. Zároveň, každý členský štát musí v zmysle DSA ustanoviť nezávislého koordinátora digitálnych služieb, ktorý je poverený dohľadom v danej krajine.[564] Predmetné orgány musia spĺňať kritérium nezávislosti.[565] Toto

[560] Tamže, § 5 ods. 2
[561] Tamže, § 5 ods. 3.
[562] Tamže, § 3 ods. 2.
[563] DSA, článok 56 ods. 3.
[564] DSA, článok 49 ods. 1.
[565] DSA, článok 50 ods. 2. *„Pri plnení svojich úloh a výkone svojich právomocí podľa tohto nariadenia konajú koordinátori digitálnych služieb úplne nezávisle. Nesmú podliehať žiadnemu vonkajšiemu vplyvu, či už priamemu alebo nepriamemu, a nesmú žiadať ani prijímať pokyny od žiadneho iného verejného orgánu ani od žiadneho súkromného subjektu."*

kritérium by nebolo naplnené, ak by Úrad vlády Slovenskej republiky disponoval koordinačným a nadrezortným postavením voči takýmto orgánom dohľadu. Zároveň, aj Rada pre mediálne služby, ktorá má právomoc viesť konanie vo veci zamedzenia šírenia nelegálneho obsahu musí napĺňať kritéria nezávislosti v zmysle špecifickej legislatívy EÚ. Takýmto spôsobom koncipovaný dohľad naráža na mantinely práva EÚ.

Návrh dezinfo zákona ustanovuje aj povinnosť de-anonymizácie v online diskusiách. V zmysle navrhovanej právnej úpravy *„Poskytovateľ platformy na zdieľanie videí [a aj obsahu] je povinný prijať vhodné opatrenia na overenie totožnosti užívateľa služby a zabezpečiť, aby funkcie služby, ktoré slúžia na priamu komunikáciu medzi užívateľmi, ako aj funkcie, ktoré slúžia na zverejnenie reakcie, odpovede, či názoru na obsah zverejnený iným užívateľom alebo poskytovateľom služby boli dostupné len užívateľovi služby, ktorého totožnosť je úspešne overená."*[566] Napriek tomu, že dôvodová správa vyvracia povinnosť plošného overovania identít, dôsledkom takto navrhovanej právnej úpravy bude práve povinnosť mať na platformách iba užívateľov, ktorých totožnosť je overená. Takto koncipovaná povinnosť však môže naraziť na limity slobody prejavu. Európsky súd pre ľudské práva v rozhodnutí *Standard Verlagsgesellschaft* uviedol, že právo na slobodu prejavu v určitej miere zaručuje anonymitu prejavov v online priestore. Predmetné konštatovanie neplatí absolútne.[567] Nie je jasné, či predkladateľ návrhu pri príprave zákona zohľadnil dané rozhodnutie a limity obmedzovania prejavu v online priestore.

Navrhovaná právna úprava, zapadá do širšieho rámca regulácie nástrojov boja proti dezinformáciám v online priestore. Ambicióznosť sa návrhu zákona nedá uprieť, avšak podľa nášho názoru je návrh vo výraznom konflikte s právom EÚ a taktiež slovenskou legislatívou. Už samotná navrhovaná definícia dezinformácie nereflektuje súčasný stav poznania a charakteristiky predmetného pojmu v dostupných akademických či politických dokumentoch. Zásadným problémom navrhovaného zákona môže byť konflikt s DSA, ktorý harmonizuje pravidlá pre sprostredkovateľské služby vrátane online platforiem v rámci EÚ. Nešťastným spôsobom je podľa nášho názoru koncipovaný aj dohľad, ktorý opätovne naráža na limity práva EÚ, osobitne kritéria nezávislosti. Požiadavka na de-anonymizáciu diskusií v online priestore si zaslúži hlbšiu dopadovú štúdiu v kontexte nedávneho rozhodnutia Európskeho súdu pre ľudské práva.

[566] Návrh dezinfo zákona, článok II bod 3.
[567] Rozhodnutie Európskeho súdu pre ľudské práva. Sťažnosť č. 39378/15. STANDARD VERLAGSGESELLSCHAFT MBH v. AUSTRIA (č. 3) zo dňa 7 decembra 2022, body 74 – 79.

3.2.3 Blokovanie webstránok

Blokovanie webstránok je ďalším zo špecifických inštitútov, ktoré môžu štátu a jednotlivcom chrániť informačný ekosystém. Napriek tomu, tento inštitút sa v prevažnej miere využíva pri ochrane autorských práv,[568] svoje uplatnenie nachádza aj pri obsahovo iných reguláciách ako napríklad regulácia online hazardných hier. Blokovanie sa vykonáva primárne prostredníctvom súdnych príkazov (*blocking injunctions*), ktoré vyžaduje od poskytovateľa internetovej siete alebo iného subjektu, aby zaviedol technické opatrenia zamerané na zabránenie alebo znemožnenie prístup na konkrétne miesto na webe.[569] Okrem tohto typu blokovania existuje aj dynamické blokovanie, ktoré je flexibilnejšie a umožňuje automatizované blokovanie určitého obsahu alebo webu aj do budúcnosti.[570] Z technického hľadiska sú možné viaceré spôsoby výkonu samotného blokovania. Najčastejšie využívanými sú blokovanie webov na základe konkrétnej IP adresy alebo domény.[571] Okrem súdnych príkazov je možné, aby príkazy na blokovanie vydávali aj správne orgány. Takúto možnosť využívajú aj viaceré členské štáty EÚ.[572]

Prirodzene, blokovanie webstránok má potenciál zasiahnuť do základných ľudských práv a slobôd. Viaceré prípady pred Európskym súdom pre ľudské práva týkajúce sa blokovania webstránok zvýrazňujú právo na informácie a slobodu prejavu. Každý zásah štátu do tohto práva musí byť opatrne vyvážený a proporcionálny. Nevyvážený by bol taký postup, ktorý by zablokoval celé webové stránky prípadne všetky webové stránky sídliace na tej istej IP adrese. Bol by to analogický prípad ako v prípade, ak by bola zablokovaná celá televízna stanica alebo noviny z dôvodu jednej reportáže alebo článku. Je nevyhnutné pri blokovaní rozlišovať medzi legálnym a nelegálnym obsahom.[573] V kontexte slobody prejavu a práva na informácie by súdy v zmysle judikatúry Európskeho súdu pre ľudské práva mali zohľadňovať minimálne 5 kritérií.

---

[568] K tomu napríklad HUSOVEC, M. Injunctions against Innocent Third Parties: The Case of Website Blocking. In 4(2) *JIPITEC* 116, 2013 alebo MOSTERT, F. - LAMBERT, J. *Study on IP Enforcement Measures, Especially Anti-Piracy Measures in the Digital Environment*. WIPO/ACE/14/7 (2019).

[569] FROSIO, G. - BULAYENKO, O. Website Blocking Injunctions in Flux: Static, Dynamic, and Live. In 16(3) *Journal of Intellectual Property Law and Practice* (2021). Dostupné na: https://ssrn.com/abstract=3848063

[570] *„Sú to súdne príkazy, ktoré možno vydať napríklad v prípadoch, keď sa v podstate tá istá webová lokalita ihneď po vydaní súdneho príkazu sprístupní s inou IP alebo URL adresou, a ktoré sú naformulované tak, aby sa týkali aj nových IP adries alebo URL adries bez toho, aby bolo potrebné nové súdne konanie na získanie nového súdneho príkazu.*" 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.

[571] NORDEMANN, J. Website Blocking under EU Copyright Law. In ROSATI, E. (ed.). *The Routledge Handbook of EU Copyright Law* (Routledge 2021), s. 359-361.

[572] COGO, A. - RICOLFI, M. Administrative Enforcement of Copyright Infringement in Europe. In FROSIO, G. (ed), *The Oxford Handbook of Online Intermediary Liability*, OUP, 2020, s. 586-602.

[573] Pozri rozhodnutia Európskeho súdu pre ľudské práva vo veci Kharitonov proti Rusku, sťažnosť č. 10795/14; Bulgakov proti Rusku, sťažnosť č. 20159/15; Engels proti Rusku, sťažnosť č. 61919/16; OOO Flavus a ostatní proti Rusku, sťažnosť č. 12468/15.

Prvým je spôsob využívania samotnej blokovanej stránky. Druhým kritériom je vplyv na legitímnu komunikáciu spôsobený zablokovaním stránky. Zároveň by mali súdy zohľadňovať, verejný záujem na prístupe k informáciám, a či sú informácie dostupné v inej forme ako na blokovanom webe. V neposlednom rade je potrebné zohľadniť aj vplyv na používateľov internetu a sprostredkovateľov.[574] Právo na slobodu prejavu a informácie však nie sú jedinými základnými právami a slobodami, ktoré môžu byť blokovaním ovplyvnené. Je nutné spomenúť ešte minimálne právo na podnikanie resp. právo vlastniť majetok. Pri zablokovaní webového sídla, cez ktoré jednotlivec podniká je nevyhnutne zasiahnuté aj do týchto práv a slobôd. Zároveň, ak blokovaný subjekt nedisponuje dostatočnými prostriedkami obrany voči takémuto konaniu zo strany súdu resp. štátu, dochádzka k výraznému ovplyvneniu práva na spravodlivý súdny proces.

Ako bolo uvedené vyššie, slovenská právna úprava upravuje inštitút blokovania webových stránok v zmysle § 27b a § 27c zákona č. 69/2018 o kybernetickej bezpečnosti v znení neskorších predpisov (ďalej len „ZoKB"). V zmysle danej právnej úpravy môže Národný bezpečnostný úrad SR (ďalej len „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."*[575] Pri procesnom postupe viaceré ustanovenia odkazujú na tzv. Pravidlá blokovania, ktoré ani na záver júna 2022 neboli publikované v právnej forme. NBÚ môže z vlastnej iniciatívy rozhodnúť o blokovaní iba s platnosťou do 30. júna 2022. Na blokovania po podnete od iného orgánu sa daný limit nevzťahuje.[576] 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.

[574] GEIGER, CH. - IZYUMENKO, E. The Role of Human Rights in Copyright Enforcement Online: Elaborating a Legal Framework for Website Blocking. In (2016) 32(1) *AUILR* 43.
[575] ZoKB, § 27b ods. 3.
[576] Pozri ZoKB, § 27c ods. 9.

Samotný mechanizmus blokovania webstránok bol podrobený odbornej kritike.[577] Aj judikatúra Európskeho súdu pre ľudské práva a Súdneho dvora EÚ[578] formuluje jasné požiadavky na mechanizmus blokovania webstránok. Základnou požiadavkou je, aby mechanizmus blokovania bol komplexne upravený v zákone. Nestačí, že časť mechanizmu bude súčasťou podzákonného právneho aktu alebo štát 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 zneužitú. Menovať možno predovšetkým nasledujúce:

1) **Posúdenie vplyvu v legislatívnom procese** – akýkoľvek invazívnejší zásah do práv a slobôd musí prejsť prísnym posúdením vplyvu ešte pred prijatím právnej úpravy. V slovenskej právnej realite je ale posúdenie vplyvu častokrát iba formálne naplnenie tabuľky bez tvrdších dát;

2) **Nezávislý dohľad** – blokovanie musí byť predmetom prieskumu *ex-ante*, nie len *ex-post*. To znamená, že na mechanizmus musí dohliadať na to určený orgán (vo veľkej väčšine prípadov súd), ktorý musí mať zároveň právomoci rozhodnutie o blokovaní zvrátiť. Vo vyššie uvedenom nastavení rozhodnutia vydával NBÚ a tieto neboli zo zákona preskúmavané.

3) **Transparentnosť** – rozhodnutia o blokovaní by mali byť transparentne dostupné verejnosti. Zároveň, ak užívateľ príde na webstránku, ktorá je blokovaná, mal by mať nárok vedieť, prečo sa nemôže dostať k informáciám, ktoré vyhľadáva.

4) **Spravodlivý proces** – mechanizmus blokovania musí spĺňať atribúty spravodlivého procesu. To znamená, že iba v najviac ojedinelých prípadoch by malo dochádzať k blokovaniu bez predošlého upozornenie prevádzkovateľa webu a lehoty na odstránenie nezákonného obsahu. Zároveň by mal prevádzkovateľ disponovať možnosťou sa voči rozhodnutiu brániť a to nielen súdnou cestou. Proces blokovania musí rešpektovať „rovnosť zbraní."[579]

[577] Pozri napríklad HUSOVEC, M. *Súčasné blokovanie dezinformačných stránok je ústavne problematické. Čo s tým?* Denník N. Dostupné na: https://dennikn.sk/2818631/sucasne-blokovanie-dezinformacnych-stranok-je-ustavne-problematicke-co-s-tym/?ref=list.

[578] Pozri rozhodnutia Európskeho súdu pre ľudské práva vo veci Kharitonov proti Rusku, sťažnosť č. 10795/14; Bulgakov proti Rusku, sťažnosť č. 20159/15; Engels proti Rusku, sťažnosť č. 61919/16; OOO Flavus a ostatní proti Rusku, sťažnosť č. 12468/15.

[579] K hlbšej analýze jednotlivých záruk blokovania pozri 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.

Viaceré z vyššie uvedených požiadaviek mechanizmus blokovania nespĺňa. Azda najvýraznejšie chýbajú záruky obrany proti rozhodnutiu (okrem napadnutia na súde) a transparentnosti. Nezávislý dohľad nad rozhodnutiami NBÚ zabezpečený nie je a privítali by sme rolu nezávislých súdov pri takomto procese.

Vyššie uvedené nedostatky mala odstrániť navrhovaná vládna novela ZoKB, ktorou sa štát snažil zaviesť systémové opatrenie pre blokovanie škodlivého obsahu.[580] 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.

3.2.4 Nástroje ochrany osobných údajov

Na úrovní Európskej únie bola viac ako 20 rokov v platnosti smernica Európskeho parlamentu a Rady 95/46/EHS z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov. Nakoľko však išlo o smernicu, členské štáty si povinnosti uvedené v nej implementovali do svojich národných právnych poriadkov odlišným spôsobom a vytvorili tak neželanú fragmentáciu. Od roku 2012 prebiehali odborné diskusie a debaty v rámci európskych štruktúr týkajúcich sa modernizácie daného právneho rámca. Výsledkom spoločnej snahy viacerých aktérov bolo prijatie nového legislatívneho rámca regulujúceho ochranu osobných údajov v podobe nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov alebo GDPR). Tento právny predpis zároveň dopĺňajú osobitné právne úpravy regulujúce spracúvanie osobných údajov orgánmi presadzovania práva,[581] inštitúciami EÚ[582] či ochrany súkromia v elektronických komunikáciách.[583] Zároveň je potrebné dodať, že GDPR v

[580] *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.

[581] Smernica Európskeho parlamentu a Rady (EÚ) 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV. Ú. v. EÚ L 119, 4.5.2016, s. 89 – 131.

[582] Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1725 z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES. Ú. v. EÚ L 295, 21.11.2018, s. 39 – 98.

[583] Smernica Európskeho parlamentu a Rady2002/58/ES z 12. júla 2002, týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách).

určitých otázkach ponechalo voľnosť pre členské štáty a tie a tak v národných právnych poriadkoch mohli upraviť určité otázky.[584]

3.2.4.1 Pôsobnosť právneho predpisu

Predtým, než sa pustíme do analýzy a diskusia požiadaviek GDPR relevantných pre boj s dezinformáciami online, považujeme za nevyhnutné načrtnúť pôsobnosť predmetného právneho predpisu.

Vecná pôsobnosť GDPR je upravená v článku 2 ods. 1 GDPR. Dané ustanovenie upravuje pozitívnu vecnú pôsobnosť GDPR. V zmysle dikcie predmetného článku sa GDPR aplikuje na spracúvanie osobných údajov, ktoré je vykonávané (i) automatizovanými prostriedkami, (ii) čiastočne automatizovanými prostriedkami alebo (iii) manuálne, ak osobné údaje tvoria súčasť informačného systému.

Samotné spracúvanie osobných údajov je definované v článku 4 bode 2 GDPR, a to demonštratívnymi výpočtom spracovateľských operácií, ktoré možno subsumovať pod definíciu spracúvania osobných údajov. V zmysle daného článku sa pod spracúvaním osobných údajov rozumie: *„operácia alebo súbor operácií s osobnými údajmi alebo súbormi osobných údajov, napríklad získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo poskytovanie iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie alebo likvidácia, bez ohľadu na to, či sa vykonávajú automatizovanými alebo neautomatizovanými prostriedkami.*" Automatizované šírenie dezinformácií, ktoré obsahujú osobné údaje bude spadať pod dikciu predmetného ustanovenia. Zároveň je potrebné poznamenať, že aj činnosť odporúčacích systémov, prostredníctvom ktorých sa dezinformácie šíria je založené na automatizovanom spracúvaní osobných údajov užívateľov a určitej miere profilovania.

Ústredným pojmom GDPR je však definícia osobného údaju. Osobným údajom *„je akékoľvek informácia týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby.*" [585] Identifikovateľná fyzická osoba je taká osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä prostredníctvom odkazu na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú

[584] K tomu pozri MESARČÍK, M. Potrebujeme nový zákon o ochrane osobných údajov? (1. časť). In *Justičná revue*. - Roč. 73, č. 1 (2021), s. 17-29; MESARČÍK, M. Potrebujeme nový zákon o ochrane osobných údajov? (2. časť). In *Justičná revue*. - Roč. 73, č. 2 (2021), s. 184-193.
[585] GDPR, článok 4 bod 1.

špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby. Pre otázku dezinformácií je vysoko relevantný faktor, že osobný údaj predstavuje „akúkoľvek informáciu." Z pohľadu povahy resp. kvality osobného údaju môže ísť o akékoľvek tvrdenia o konkrétnej osobe na akomkoľvek nosiči. Môže ísť o informácie objektívne alebo subjektívne. Z nášho pohľadu je kľúčové, že na to, aby informácie boli osobnými údajmi, nie je potrebné, aby boli pravdivé alebo preukázané. Legislatíva na ochranu osobných údajov takúto situáciu predpokladá a ustanovuje právo dotknutej osoby na prístup k týmto informáciám a na ich spochybnenie prostredníctvom vhodných opravných prostriedkov.[586]

Pojem identifikovateľnosti ďalej vykladá recitál 26 GDPR.[587] Tento recitál reprezentuje tzv. test primeranej pravdepodobnosti, ktorý odpovedá na to, či konkrétna dotknutá osoba je skutočne identifikovateľná. Predmetným testom sa zaoberal aj Súdny dvor Európskej únie v prípade *Patrick Breyer v Spolková republika Nemecko*. Skutkovo sa prípad týkal otázky, či dynamická IP adresa predstavuje osobný údaje v zmysle staršej legislatívy na ochranu osobných údajov. Prevádzkovateľ webového sídla mal k dispozícií IP adresa užívateľa, avšak nemal priamo informáciu, na koho je táto IP adresa registrovaná. Tieto informácie má zvyčajne k dispozícií poskytovateľ internetového pripojenia. Otázka teda bola, či pre prevádzkovateľa webového sídla predstavuje IP adresa osobný údaj v zmysle legálnej definície. Luxemburský súd judikoval: *„...že dynamická IP adresa, ktorú poskytovateľ online mediálnych služieb uchováva v súvislosti s prehliadaním si určitou osobou internetovej stránky, ktorú tento poskytovateľ sprístupnil verejnosti, predstavuje pre tohto poskytovateľa osobný údaj v zmysle tohto ustanovenia, ak má k dispozícii právne prostriedky, na základe ktorých dokáže identifikovať dotknutú osobu vďaka ďalším informáciám, ktorými disponuje poskytovateľ internetového pripojenia tejto osoby."*[588] Toto rozhodnutie tak znamená, že ak existujú právom dovolené prostriedky na identifikáciu jednotlivca, pôjde o osobné údaje. K pojmu osobný údaj teda možno záverom dodať, že nie každá informácia je automaticky osobným údajom. Vždy bude záležať od konkrétnych okolností a kontextu, či je daná osoba identifikovateľná alebo nie.

[586] ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 4/2007 on the concept of personal data*. Adopted on 20th June, 01248/07/EN.WP 136, s. 6.

[587] *„Na určenie toho, či je fyzická osoba identifikovateľná, by sa mali brať do úvahy všetky prostriedky, pri ktorých existuje primeraná pravdepodobnosť, že ich prevádzkovateľ alebo akákoľvek iná osoba využije, napríklad osobitným výberom, na priamu alebo nepriamu identifikáciu fyzickej osoby. Na zistenie toho, či je primerane pravdepodobné, že sa prostriedky použijú na identifikáciu fyzickej osoby, by sa mali zohľadniť všetky objektívne faktory, ako sú náklady a čas potrebný na identifikáciu so zreteľom na technológiu dostupnú v čase spracúvania, ako aj na technologický vývoj."*

[588] Rozhodnutie Súdneho dvora Európskej únie, C-582/14 Patrick Breyer proti Bundesrepublik Deutschland.

GDPR upravuje v článku 2 ods. 2 negatívnu pôsobnosť nariadenia. Ide predovšetkým o situácie, na ktoré sa neaplikuje právo Európskej únie, otázky národnej bezpečnosti a tajných služieb či otázky patriace do pôsobnosti smernice upravujúcej spracúvanie osobných údajov orgánmi presadzovania práva. Osobitne zaujímavou otázkou je výnimka z pôsobnosti, ktorá sa aplikuje v prípade, že spracúvanie osobných údajov prebieha fyzickou osobou v rámci výlučne osobnej alebo domácej činnosti.[589] GDPR však nedefinuje, o aké situácie konkrétne ide. Judikatúra SDEÚ však naznačuje určitý smer, kedy sa GDPR vzhľadom na negatívnu pôsobnosť nevzťahuje. O spracúvanie v rámci výlučne osobnej alebo domácej činnosti nepôjde vtedy, ak sú osobné údaje zverejnené na internete[590] prípadne monitorovanie ulice kamerovým systémom umiestneným nad dverami domu.[591]

GDPR upravuje územnú pôsobnosť v rámci článku 3. Je faktom, že nariadenie sa aplikuje v rámci spracúvania osobných údajov v prevádzke, ktorá má sídlo v EÚ (tzv. intra-teritoriálny režim), ale zároveň aj na prevádzkovateľov, ktorí majú sídlo mimo EÚ (tzv. extra-teritoriálny režim) za predpokladu, že ponúkajú osobám v EÚ tovary a služby alebo sledujú ich správania napríklad prostredníctvom webovej aktivity.

Z hľadiska osobnej pôsobnosti je potrebné rozlišovať 5 typov entít v zmysle GDPR. Najdôležitejšími pojmami sú dotknutá osoba, prevádzkovateľ a sprostredkovateľ. Pre kompletnosť uvádzame aj definíciu pojmov príjemcov a tretej strany.

Dotknutá osoba znamená identifikovanú alebo identifikovateľnú osobu, ktorej sa osobné údaje týkajú. GDPR nedefinuje termín dotknutá osoba, ale jej vymedzenie možno odvodiť z ustanovení týkajúcich sa pojmu osobný údaj (článok 4 bod 1 GDPR).

Prevádzkovatelia a sprostredkovatelia sú v zmysle GDPR entity zodpovedné za spracúvanie osobných údajov a preto sa na nich vzťahuje niekoľko povinnosti.

Prevádzkovateľ[592] je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý sám alebo spoločne s inými určí účely a prostriedky spracúvania osobných údajov, pričom platí, že ak sa účely a prostriedky tohto spracúvania stanovujú v práve Únie alebo v práve členského štátu, možno prevádzkovateľa alebo konkrétne kritériá na jeho určenie určiť v práve Únie alebo v práve členského štátu. Najdôležitejším aspektom definície prevádzkovateľa je „určenie účelu." Entita, ktorá určí účel spracúvania osobných údajov (dôvod,

[589] GDPR, článok 2 ods. 2 písm. c).
[590] Rozhodnutie Súdneho dvora Európskej únie, C-101/01- Lindqvist.
[591] Rozhodnutie Súdneho dvora Európskej únie, C-212/13-Ryneš.
[592] GDPR, článok 4 bod 7.

prečo sú osobné údaje spracúvané) je prevádzkovateľom. Prevádzkovateľom tak môže byť napríklad orgán verejnej moci, ktorý monitoruje výskyt dezinformácií na sociálnych médiách v krajine alebo aj súkromná spoločnosť, ktorá vyvíja nástroje na detekciu dezinformačných aktivít. Ak dvaja alebo viacerí prevádzkovatelia spoločne určia účely a prostriedky spracúvania, sú spoločnými prevádzkovateľmi. Sprostredkovateľ[593] je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý spracúva osobné údaje v mene prevádzkovateľa. To znamená, že v tomto prípade je nevyhnutné mať poverenie a pokyny od prevádzkovateľa ako spracúvať osobné údaje v jeho mene. Nie je vylúčené, že jedná entita môže figurovať aj ako prevádzkovateľ a aj ako sprostredkovateľ. GDPR okrem týchto pojmov ešte pracuje so subjektami ako príjemca, tretia strana a dotknutá osoba. Kľúčové povinnosti však na seba viažu prevádzkovatelia a sprostredkovatelia.

Za najvšeobecnejšiu formuláciu povinností možno považovať článok 24 ods. 1 GDPR: *„S ohľadom na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb prevádzkovateľ prijme vhodné technické a organizačné opatrenia, aby zabezpečil a bol schopný preukázať, že spracúvanie sa vykonáva v súlade s týmto nariadením.*" Táto povinnosť sa v praxi zabezpečuje prijatím interných dokumentov (napríklad interná politika ochrany osobných údajov alebo bezpečnostná politika) a implementovaním organizačných a technických opatrení pri práci s osobnými údajmi v organizácií. Táto povinnosť je dynamická a znamená, že v prípade prijatia vyššie uvedených opatrení je ich potrebné pravidelne posudzovať a aktualizovať. Z hľadiska zodpovednosti môžu byť za porušenie pravidiel na ochranu osobných údajov v zmysle GDPR braní na zodpovednosť aj prevádzkovateľ aj sprostredkovateľ. Nariadenie umožňuje, aby bol za porušenie GDPR zodpovedný aj sprostredkovateľ a to buď priamym porušením jemu ustanovených povinností alebo v prípade, ak spracúva osobné údaje v priamom rozpore s pokynmi prevádzkovateľa.

GDPR je právny akt, ktorý je koncipovaný z pohľadu ochranu jednotlivca – dotknutej osoby. V praktickej rovine sa to prejavuje aj tým spôsobom, že samotné nariadenie upravuje niekoľko práv dotknutej osoby, ktoré pri pochybnostiach o legálnosti alebo legitímnosti spracovateľských operácií si dotknutá osoba môže uplatniť. GDPR špecificky upravuje minimálne:

- Právo na informácie o spracúvaní osobných údajov podľa článkov 12 až 14 GDPR;

[593] GDPR, článok 4 bod 8.

- Právo na prístup k osobným údajom podľa článku 15 GDPR;
- Právo na opravu podľa článku 16 GDPR;
- Právo na vymazanie a zabudnutie podľa článku 17 GDPR;
- Právo na obmedzenie spracúvania podľa článku 18 GDPR;
- Právo na prenosnosť podľa článku 20 GDPR;
- Právo namietať podľa článku 21 GDPR;
- Právo nebyť predmetom automatizovaného individuálneho rozhodovania podľa článku 22 GDPR;
- Právo odvolať súhlas so spracúvaním osobných údajov podľa článku 7 GDPR;
- Právo na informácie o porušení osobných údajov podľa článku 34 GDPR;
- Právo podať sťažnosť dozornému orgánu podľa článku 77 GDPR;
- Právo na účinný súdny prostriedok nápravy voči rozhodnutiu dozorného orgánu podľa článku 78 GDPR;
- Právo na účinný súdny prostriedok nápravy voči prevádzkovateľovi alebo sprostredkovateľovi podľa článku 79 GDPR.

Predmetné práva však nie sú absolútne. Na ich uplatnenie je potrebné splniť taxatívne dané požiadavky a zároveň nesmie byť aplikovateľná žiadna z výnimiek, ktoré GDPR pri konkrétnom práve obsahuje.

3.2.4.2 Inštitúty relevantné pre šírenie dezinformácií

Dezinformácie môžu obsahovať aj osobné údaje. Ide spravidla o situácie, ak sa šíria konkrétne nepravdivé informácie o konkrétnom jednotlivcovi. Praktickým príkladom je šírenie dezinformácií o zdravotníckych pracovníkoch počas pandémie COVID-19.[594] Zároveň, odporúčacie systémy na sociálnych sieťach fungujú na kreovaní profilov na základe osobných údajov. Aké nástroje a inštitúty poskytuje GDPR či už z hľadiska systémových nástrojov alebo individuálnych práv? Za systémov nástroje budeme považovať také, ktoré predstavujú horizontálne požiadavky na prevádzkovateľov prípadne sprostredkovateľov. Podľa nášho

[594] ROZHLAS A TELEVÍZIA SLOVENSKA. *Verdikt v spore lekára Sabaku s hnutím Republika by mohol padnúť o necelý mesiac*. Dostupné na: https://spravy.rtvs.sk/2023/06/sudny-spor-lekara-p-sabaku-s-hnutim-republika-vrcholi-verdikt-by-mohol-padnut-o-necely-mesiac/.

názoru z týchto systémových nástrojov je nutné diskutovať požiadavky na automatizované individuálne rozhodovanie, vykonanie posúdenia vplyvu na ochranu údajov, inštitút špecificky navrhnutej a štandardnej ochrany osobných údajov. Za individuálne možnosti nápravy pri šírení dezinformácií, ktoré obsahujú osobné údaje považujeme využitie niektorých práv dotknutej osoby a to konkrétne právo na opravu, právo na vymazanie (zabudnutie) a ďalšie práva týkajúce sa podania sťažnosti na dozorný orgán a obrany na súde.

Automatizované individuálne rozhodovanie

Automatizované individuálne rozhodovanie je pojem, s ktorým operuje GDPR na viacerých miestach. Pred tým, než sa pustíme do analýzy požiadaviek pri jeho vykonávaní, považujeme za nevyhnutné predmetný pojem charakterizovať. Za automatizované spracúvanie možno v zmysle GDPR považovať spracúvanie osobných údajov bez ľudského zásahu výlučne prostredníctvom informačných technológií.[595]

Predmetom analýzy tejto časti je článok 22 všeobecného nariadenia o ochrane údajov, ktorý upravuje automatizované individuálne rozhodovanie (ďalej aj ako „AIR"). V zmysle článku 22 ods. 1 GDPR: *„Dotknutá osoba má právo na to, aby sa na ňu nevzťahovalo rozhodnutie, ktoré je založené výlučne na automatizovanom spracúvaní, vrátane profilovania, a ktoré má právne účinky, ktoré sa jej týkajú alebo ju podobne významne ovplyvňujú."* Pri automatizovanom individuálnom rozhodovaní je potrebné odlišovať všeobecne rozhodnutia na základe profilovania a rozhodnutia urobené výlučne automatizovaným spracúvaním s právnymi účinkami na dotknutú osobu. O rozhodnutie na základe profilovania pôjde napríklad v prípade, ak údaje dotknutej osobe spracuje algoritmus, ktorý na základe týchto dát vydá odporúčanie ohľadom rozhodnutia; predmetné rozhodnutia už ale urobí ľudská bytosť. Rozhodnutie urobené výlučne automatizovaným spracúvaním osobných údajov vrátane profilovania, ktoré má právne účinky na dotknutú osobu, ktoré sa dotknutej osoby týkajú alebo dotknutú osobu podobne významne ovplyvňujú ilustruje situácia, ak by občanovi došlo rozhodnutie o priamo od algoritmu, ktorý o ňom spracúval dáta a sám rozhodol o výsledku jeho žiadosti.[596] Článok 22 GDPR sa aplikuje iba na poslednú z ilustrovaných situácií. Usmernenie Výboru na ochranu osobných údajov,[597] zároveň potvrdzuje, že rutinná ľudská intervencia môže stále znamenať, že

[595] KUNER, CH. – BYGRAVE, L. – DOCKSEY, CH. *The EU General Data Protection Regulation (GDPR). A commentary*. Oxford: Oxford University Press, 2020, s. 121.
[596] ARTICLE 29 DATA PROTECTION WORKING PARTY. *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.* Adopted on 3 October 2017. As last Revised and Adopted on 6 February, s. 9.
[597] V zmysle GDPR nahradená Výborom na ochranu údajov, pričom jeho/jej stanoviská sú relevantné pre adresátov noriem a taktiež orgány aplikujúce právo.

rozhodnutie je urobené výlučne automatizovanými prostriedkami.[598] Dôležitou časťou definície AIR v zmysle GPDR je, že rozhodnutia musí mať právny alebo podobný efekt na dotknutú osobu. Ide o pomerne komplikovanú požiadavku, ktorú je v aplikačnej praxi náročné naplniť. Právny účinok vyžaduje, aby rozhodnutie, ktoré je založené výlučne na automatizovanom spracovaní, ovplyvnilo práva, ako je sloboda združovať sa s inými, hlasovať vo voľbách alebo prijímať právne kroky. Právnym účinkom môže byť aj niečo, čo ovplyvňuje právne postavenie osoby alebo jej práva podľa zmluvy.[599] Zaujímavejším pojmom je však práve „podobne významný vplyv" ako právny efekt. Aby spracovanie údajov niekoho významne ovplyvnilo, musia byť účinky spracovania dostatočne veľké alebo dôležité. Ako príklady Výbor na ochranu osobných údajov uvádza zásadnú zmenu okolností, správania alebo volieb dotknutej osoby s dlhotrvajúcim vplyvom, v extrémnych prípadoch vedúcich k diskriminácií.[600] K totožnému výkladu dospel aj generálny advokát Súdneho dvora EÚ vo svojom názore v prípade *OQ proti Land Hessen,* ktorý je prvým prejedávaným prípadom týkajúcim sa výkladu článku 22 GDPR.[601]

Osobitne usmernenie Výboru na ochranu údajov analyzuje zobrazovanie reklamy (v širšom kontexte obsahu) užívateľom, ktoré je taktiež založené na automatickej analýze osobných údajov. Práve tento kontext je veľmi dôležitý pre šírenie dezinformácií online. Výbor uvádza, že zobrazovanie reklamy štandardne nebude spôsobovať právny alebo podobne závažný vplyv na dotknutú osobu.[602] Avšak nie je vylúčené, že pri zohľadnení určitých skutočností takýto vplyv môže zobrazovanie online reklamy mať. Pre naše účely je vhodné upriamiť pozornosť na dva faktory a to konkrétne invazívnosť procesu profilovania vrátane sledovania jednotlivcov v rôznych webových stránkach, zariadeniach a službách a využitie znalostí o zraniteľnosti dotknutých osôb.[603] Zobrazovanie dezinformácií môže využívať zraniteľnosť dotknutých osôb, či už z pohľadu geografickej lokalizácie alebo veku. V určitých prípadoch by sa článok 22 GDPR mohol podľa nášho názoru vzťahovať aj na zobrazovanie obsahu na základe zozbieraných osobných údajov zo strany napríklad sociálnych médií.

Po výklade pojmu AIR prejdeme ku konkrétnym požiadavkám naň kladenými. Zahraničná doktrína akcentuje dva názory na výklad daného inštitútu – ide o všeobecný zákaz

[598] Tamže, s. 21.
[599] ARTICLE 29 DATA PROTECTION WORKING PARTY. *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.* Adopted on 3 October 2017. As last Revised and Adopted on 6 February, s. 21.
[600] Tamže.
[601] *Stanovisko Generálneho Advokáta Priit Pikamäe predneseného dňa 16.3.2023 vo veci C-634/21 OQ proti Land Hessen za účasti: SCHUFA Holding AG*, body 34 – 35.
[602] Tamže, s. 22.
[603] Tamže.

alebo právo namietať? Prvá skupina autorov (a Výbor na ochranu údajov)[604] tvrdí, že článok 22 GDPR reprezentuje všeobecný zákaz vykonávania individuálnych rozhodnutí automatizovaným spôsobom a takýto proces je možné vykonávať iba na základe výnimiek uvedených v článku 22 ods. 2 GDPR. Tieto výnimky predstavujú (i) plnenie zmluvy s dotknutou osobou; (ii) legislatívne povolenie v národnom právnom poriadku alebo poriadku EÚ so zakotvením vhodných opatrení zaručujúcich ochranu práv a slobôd a oprávnených záujmov dotknutej osoby alebo (iii) ak dotknutá osoba vyjadrila výslovný súhlas s takýmto spracúvaním. Literatúra v prospech danej argumentácie predovšetkým argumentuje koherentnosťou právneho rámca na ochranu osobných údajov v prospech dotknutej osoby a existenciou záruk a derogácií ustanovených v článku 22 GDPR.[605] K takémuto výkladu sa prihlásil aj generálny advokát Súdneho dvora EÚ vo svojom názore v prípade *OQ proti Land Hessen*.[606] Budúcnosť ukáže, či totožný postoj zaujme aj samotná súdna inštancia.

Druha skupina autorov argumentuje v prospech výkladu, že článok 22 GDPR je koncipovaný ako právo dotknutej osoby namietať voči daným rozhodnutiam. Svoje tvrdenia opierajú o juxtapozíciu predmetného inštitútu v kapitole právneho predpisu týkajúcich sa práv dotknutých osôb a absencie úmyslu zákonodarcu koncipovať článok 22 ako všeobecný zákaz vzhľadom na historický vývoj diskutovaného inštitútu. Ďalšími argumentmi v prospech výkladu článku 22 GDPR ako práva namietať sú ustanovenia týkajúce sa informačnej povinnosti, ktoré v sebe obsahujú aj povinnosť informovať o AIR či povinnosť vykonať posúdenie vplyvu na ochranu údajov podľa článku 35 GDPR v prípade systematického a extenzívneho monitorovania osobných aspektov dotknutých osôb vrátane AIR. V prípade všeobecného zákazu by predmetná povinnosť nemala zmysel, nakoľko jej poslaním je posúdiť spracúvanie osobných údajov pred jeho začatím vrátane rizík.[607] Výnimky uvedené v článku 22 ods. 2 GDPR by v takomto prípade predstavovali výnimky z práva namietať a reprezentovali by situácie, v ktorých dotknutá osoba nemôže takémuto spracúvaniu osobných údajov namietať.[608]

[604] ARTICLE 29 DATA PROTECTION WORKING PARTY. *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.* Adopted on 3 October 2017. As last Revised and Adopted on 6 February, s. 19.

[605] BYGRAVE, L. Automated individual decision-making, including profiling. In KUNER, CH. – BYGRAVE, L. – DOCKSEY, CH.: *The EU General Data Protection Regulation (GDPR). A commentary.* Oxford: Oxford University Press, 2020, s. 530 - 531.

[606] *Stanovisko Generálneho Advokáta Priit Pikamäe predneseného dňa 16.3.2023 vo veci C-634/21 OQ proti Land Hessen za účasti: SCHUFA Holding AG*, body 31 – 32.

[607] Tamže, s. 531 – 532.

[608] Aj v prípade nemožnosti namietania však má prevádzkovateľ v zmysle článku 22 ods. 3 GDPR vykonať vhodné opatrenia na ochranu práv a slobôd a oprávnených záujmov dotknutej osoby, a to aspoň práva na ľudský zásah zo strany prevádzkovateľa, práva vyjadriť svoje stanovisko a práva napadnúť rozhodnutie.

Prikláňame sa k názoru, že článok 22 GDPR je koncipovaný ako právo dotknutej osoby nebyť predmetom AIR. Zároveň je však potrebné poznamenať, že predmetný inštitút má komplikované vyjadrenie a zvádza k viacerým výkladom. V prospech výkladu ako práva jednoznačne hovorí jeho pozícia v právnom predpise a nedostatok úmyslu zákonodarcu koncipovať daný inštitút ako všeobecný zákaz. Navyše, samotné znenie GDPR na viacerých miestach pracuje s AIR ako „bežnou" spracovateľskou operáciou, ktorá podlieha viacerým špecifickým povinnostiam. V prípade všeobecného zákazu by tieto povinnosti stratili na účinku a boli by nadbytočné. Jediný všeobecný zákaz v súvislosti s AIR sa nachádza v ustanovení článku 22 ods. 4 GDPR, podľa ktorého je zakázané vykonávať AIR na základe citlivých osobných údajov. Prirodzene, aj z tohto zákazu existujú dve výnimky a to v prípade výslovného súhlasu dotknutej osoby a nevyhnutného verejného záujmu na základe právneho poriadku EÚ alebo národného právneho poriadku. Spoločnou podmienkou využitia vyššie uvedených výnimiek je zavedenie vhodných opatrení na zaručenie práv a slobôd a oprávnených záujmov dotknutej osoby zo strany prevádzkovateľa. Práve tu GDPR uvádza opatrenia ako právo na ľudský zásah zo strany prevádzkovateľa, právo vyjadriť svoje stanovisko a právo napadnúť rozhodnutie. Ide tak o špecifický koncept práv voči rozhodnutiam stroja, ktorý sa častokrát používa ako príklad pre budúcu reguláciu.

Posúdenie vplyvu na ochranu údajov

Posúdenie vplyvu na ochranu údajov (*Data protection impact assessment – DPIA*) je novým inštitútom pri spracúvaní osobných údajov, ktorý substituuje viaceré notifikačné povinnosti. DPIA je pevnou súčasťou zásady zodpovednosti (*accountability*), ktorá reflektuje preventívne povinnosti pre prevádzkovateľov predchádzať a zmierňovať neželané riziká pri spracúvaní osobných údajov. Podstatou daného inštitútu je analýza právnych rizík pri spracúvaní osobných údajov a vypracovanie dokumentu, ktorý danú povinnosť dokumentuje. Toto posúdenie sa musí vykonať pred[609] samotným začatím spracúvania osobných údajov. Tento inštitút je obzvlášť dôležitý v kontexte využívania nových technológií pri spracúvaní osobných údajov. Výbor vydal usmernenie k posúdeniu vplyvu na ochranu údajov, ktoré daný proces vysvetľuje a precizuje.[610]

Povinnosť vykonať posúdenie vplyvu na ochranu údajov je viazaná na špecifické podmienky, ktoré sú upravené v článkoch 35 ods. 3 (špecifické prípady) a 35 ods. 1 (všeobecná

[609] Pozri článok 35 ods. 1 GDPR.
[610] ARTICLE 29 DATA PROTECTION WORKING PARTY. *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk" for the purposes of Regulation, 2016/679*.

klauzula) GDPR. Prevádzkovateľ by mal v praxi najprv posúdiť, či sa naňho nevzťahuje jeden zo špecifických prípadov uvedených v článku 35 ods. 3 GDPR a ak nie, analyzovať podmienky všeobecnej klauzuly v článku 35 ods. 1 GDPR. Na tomto mieste je taktiež nutné doplniť, že v zmysle článku 35 ods. 4 GDPR bol každý dozorný orgán členského štátu povinný vypracovať a zverejniť zoznam tých spracovateľských operácií, ktoré podliehajú požiadavke na posúdenie vplyvu na ochranu údajov. Úrad na ochranu osobných údajov Slovenskej republiky takýto zoznam taktiež publikoval.[611]

Článok 35 ods. 3 GDPR ustanovuje, že posúdenie vplyvu sa vykoná najmä v prípadoch:

- systematického a rozsiahleho hodnotenia osobných aspektov týkajúcich sa fyzických osôb, ktoré je založené na automatizovanom spracúvaní vrátane profilovania a z ktorého vychádzajú rozhodnutia s právnymi účinkami týkajúcimi sa fyzickej osoby alebo s podobne závažným vplyvom na ňu;
- spracúvania vo veľkom rozsahu osobitných kategórií údajov podľa článku 9 ods. 1 alebo osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky podľa článku 10, alebo;
- systematického monitorovania verejne prístupných miest vo veľkom rozsahu.

Diskutovaný článok obsahuje demonštratívny výpočet prípadov, keď prevádzkovateľ bude mať povinnosť posúdenie vplyvu vykonať. Ako je evidentné z tohto výpočtu, dané prípady obsahujú veľké množstvo právne neurčitých pojmov ako systematické a rozsiahle hodnotenie, veľký rozsah alebo verejne prístupné miesto. Tieto termíny bližšie charakterizuje usmernenie Výboru.

Ak prevádzkovateľ nenašiel posudzovanú spracovateľskú operáciu v špecifickej klauzule článku 35 ods. 3 GDPR, automaticky to neznamená že DPIA nemá vykonať. Povinnosť vykonať DPIA totiž môže vyplynúť aj po analýze kritérií v kontexte všeobecnej klauzuly podľa článku 35 ods. 1 GDPR. Článok 35 ods. 1 GDPR ustanovuje, že *„...ak typ spracúvania, najmä s využitím nových technológií a s ohľadom na povahu, rozsah, kontext a účely spracúvania pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, prevádzkovateľ pred spracúvaním vykoná posúdenie vplyvu plánovaných spracovateľských operácií na ochranu osobných údajov.*

[611] Pozri Úrad na ochranu osobných údajov SR. *Zoznam spracovateľských operácií podliehajúcich posúdeniu vplyvu na ochranu osobných údajov Slovenskej republiky*. Dostupné na https://dataprotection.gov.sk/uoou/sites/default/files/zoznam_spracovatelskych_operacii_ktore_podliehaju_posudeniu_vplyvu.pdf.

Pre súbor podobných spracovateľských operácií, ktoré predstavujú podobné vysoké riziká, môže byť dostatočné jedno posúdenie."[612] Rozhodujúcim faktorom pre vykonanie posúdenia vplyvu je tak miera rizika pre práva a slobody fyzických osôb (vyžaduje sa vysoké riziko).

Na účely posúdenia vplyvu definoval Výbor niekoľko kritérií, ktoré by mal prevádzkovateľ vziať do úvahy pri posúdení miery rizika spracúvania osobných údajov. Na aktiváciu všeobecnej klauzuly posúdenia vplyvu stačí, ak sú splnené dve nižšie uvedené kritériá, ktoré uvádzame v tabuľke s krátkou charakteristikou:

Kritérium	Charakteristika
Vyhodnocovanie určitých aspektov týkajúcich sa dotknutej osoby	Výbor vo svojom usmernení výslovne zahŕňa medzi príklady vyhodnocovania určitých aspektov dotknutých osôb profilovanie a vytváranie predpovedí o dotknutej osobe. Medzi relevantnými aspektmi demonštratívne uvádza hodnotenie činnosti dotknutej osoby v rámci výkonu práce, jej majetkových pomerov, zdravia, osobných preferencií alebo záujmov, spoľahlivosti alebo správania, polohy alebo pohybu.
Automatizované rozhodovanie s právnym alebo podobne závažným účinkom	Druhým indikátorom je, že spracúvanie osobných údajov je vykonané automatizovane s automatizovaným rozhodnutím, ktoré má právny alebo podobne závažný účinok na dotknutú osobu. Zjednodušene povedané, automatizované rozhodovanie je taký proces, v ktorom nie je prítomný ľudský zásah.
Systematické monitorovanie osobných údajov	Systematické monitorovanie údajov je potrebné interpretovať v intenciách takých situácií, keď sú dotknuté osoby pozorované, kontrolované a monitorované vrátane sledovania prostredníctvom internetovej siete. Je prakticky nemožné nebyť predmetom takéhoto monitorovania. Monitorovanie verejne dostupných miest zahŕňa napríklad verejné priestranstvá, knižnice, úrady alebo obchodné domy.
Spracúvanie citlivých osobných údajov	Ďalším indikátorom je spracúvanie citlivých osobných údajov a údajov týkajúcich sa páchania priestupkov a trestných činov. Navyše Výbor uvádza, že medzi citlivé osobné údaje možno zahrnúť aj osobné dokumenty, elektronické správy, denníky, poznámky a údaje spracúvané v rámci mobilných aplikácií, ktoré odhaľujú osobnostné aspekty o dotknutých osobách.

[612] GDPR, článok 35 ods. 1.

Spracúvanie údajov vo veľkom rozsahu	Posúdenie vplyvu na ochranu údajov je potrebné vykonať aj v prípadoch, ak sa spracúvanie vykonáva vo veľkom rozsahu. Výbor menuje faktory, ktoré indikujú, či ide o spracúvanie osobných údajov vo veľkom rozsahu alebo nie – (i) počet dotknutých osôb, (ii) kvantita údajov a ich rozsah, (iii) doba spracovateľskej operácie a (iv) geografický rozsah spracúvania osobných údajov.
Spájanie alebo kombinovanie súborov a údajov pochádzajúcich z rôznych spracovateľských operácií	Ďalším indikátorom je spájanie a kombinovanie údajov z rôznych zdrojov alebo od rôznych prevádzkovateľov.
Spracúvanie údajov týkajúcich sa *„zraniteľných"* dotknutých osôb	Zraniteľné osoby sú v diskutovanom usmernení Výbor vymedzené ako také osoby, ktoré nie sú v rovnoprávnom postavení voči prevádzkovateľovi. Ako príklad možno opätovne uviesť občanov voči orgánom verejnej moci alebo zamestnanca voči zamestnávateľovi.
Využitie nových technológií, technologických alebo organizačných riešení a postupov	Ako nové technológie Výbor uvádza ako príklad *blockchain*, algoritmy na báze umelej inteligencie alebo internet vecí.
Spracúvanie bráni dotknutým osobám uplatniť svoje právo alebo využiť službu alebo zmluvu	Ku spracúvaniu údajov, ktoré bráni dotknutým osobám uplatniť svoje právo alebo využiť službu alebo zmluvu, dochádza napr. vtedy, keď banka preverí klienta v referenčnej databáze úverov a na základe toho s ním neuzavrie zmluvu.

Tabuľka: Faktory, ktoré sa zohľadňujú pri posúdení potreby vypracovania posúdenia vplyvu. Zdroj: Európsky výbor na ochranu údajov.

Ak vezmeme do úvahy technické fungovanie odporúčacích systémov na sociálnych médiách, prostredníctvom ktorých sa dezinformácie efektívne šíria, musíme konštatovať že, že pre takúto činnosť ja naplnených viacero kritérií. Určite pôjde o vyhodnocovanie určitých aspektov týkajúcich sa dotknutej osoby na základe ich správania na sociálnych médiách. Zároveň nechávame otvorené vzhľadom na diskusiu vyššie, či pôjde o AIR s právnym alebo podobným účinkom. Každopádne, činnosť odporúčacích systémov je založená na spracúvaná veľkého množstva údajov, v ktorých môžu figurovať aj citlivé osobné údaje (ako údaje o zdravotnom stave či národnosti) a štandardne je tvorené kombináciou údajov z rôznych zdrojov na základe webovej aktivity konkrétneho užívateľa. Prevádzkovatelia takýchto systémov podliehajú povinnosti vykonať posúdenie vplyvu.

Metodologický základ, ako posúdenie vplyvu efektívne urobiť, poskytuje samotné GDPR a vyhláška Úradu na ochranu osobných údajov Slovenskej republiky z 29. mája 2018 o postupe pri posudzovaní vplyvu na ochranu osobných údajov. GDPR v článku 35 ods. 7 upravuje, že posúdenie vplyvu by malo najmä obsahovať tieto všeobecné body:

- systematický opis plánovaných spracovateľských operácií a účely spracúvania, vrátane prípadného oprávneného záujmu, ktorý sleduje prevádzkovateľ
- posúdenie nutnosti a primeranosti spracovateľských operácií vo vzťahu k účelu
- posúdenie rizika pre práva a slobody dotknutých osôb uvedeného v odseku 1 a
- opatrenia na riešenie rizík vrátane záruk, bezpečnostných opatrení a mechanizmov na zabezpečenie ochrany osobných údajov a na preukázanie súladu s týmto nariadením, pričom sa zohľadnia práva a oprávnené záujmy dotknutých osôb a ďalších osôb, ktorých sa to týka.

Z pohľadu šírenia dezinformácií na základe spracúvaných osobných údajov kľúčovú časť DPIA predstavuje posúdenie rizík pre práva a slobody dotknutých osôb. Posúdenie rizika pre práva a slobody dotknutých osôb by malo predstavovať právne cvičenie, ktoré spočíva v kreovaní modelových situácií, ktoré predstavujú riziko pre práva a slobody dotknutých osôb[613] (napr. únik údajov alebo kompromitovanie údajov) a následnú analýzu ohrozenia špecifických práv a slobôd dotknutých osôb.[614] Ak prevádzkovateľ zobrazuje obsah na základe zozbieraných osobných údajov užívateľov a v rámci neho sa šíria dezinformácie, malo by to byť riziko, ktoré by prevádzkovateľ mal identifikovať, zohľadniť a zmierniť v procese DPIA.

Špecificky navrhnutá a štandardná ochrana osobných údajov

GDPR v článku 25 ustanovuje v európskej právnej kultúre pomerne nový inštitút špecificky navrhnutej a štandardnej ochrany osobných údajov. Predmetný článok však vychádza z filozofie špecificky navrhnutej ochrany súkromia, ktorý má svoje dlhoročné uplatnenie a miesto v anglo-americkej právnej tradícii. Možno teda konštatovať, že článok 25 GDPR vychádza a nadväzuje na koncepciu špecificky navrhnutej ochrany súkromia (*Privacy by Design*). Tento koncept rozvinula bývala kanadská dozorná úradníčka pre ochranu údajov Ann Cavoukian, ktorá určila sedem nosných zásad[615], na ktorých musí stáť každé poňatie vyššie

[613] Napr. Úrad na ochranu osobných údajov SR vydal zoznam 156 práv a slobôd v zmysle právnej úpravy v Charte. Dostupné na: https://dataprotection.gov.sk/uoou/sites/default/files/otazka_uoou.pdf, s. 3.

[614] Vyhláška v danom prípade vyžaduje zohľadniť *„najmä riziko súvisiace s náhodným alebo nezákonným poškodením, zničením, stratou, zmenou, neoprávneným prístupom a poskytnutím alebo zverejnením osobných údajov, ako aj s akýmkoľvek iným neprípustným spôsobom spracúvania, pričom identifikuje*
a) hrozby a pravdepodobnosť ich výskytu,
b) zraniteľnosti zneužiteľné hrozbami,
c) riziká a pravdepodobnosť ich výskytu a závažnosť,
d) a zhodnotí mieru dopadu na práva fyzickej osoby v dôsledku straty integrity, dôvernosti a dostupnosti údajov,
e) vysoké riziko pre práva fyzickej osoby, ak neprijme opatrenia na zmiernenie rizika." (§ 5 ods. 2 Vyhlášky).

[615] *CAVOUKIAN, A. Privacy by Design – The Seven Foundational Principles*. Dostupné na https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.

diskutovaného inštitútu. Z filozofie *Privacy by Design* vychádza aj článok 25 GDPR. Diskutovaný článok je tvorený tromi veľmi komplikovanými vetnými štruktúrami, ktoré je potrebné analyzovať podrobnejšie.

Článok 25 ods. 1 GDPR reflektuje požiadavky špecificky navrhnutej ochrany osobných údajov: *„So zreteľom na najnovšie poznatky, náklady na vykonanie opatrení a na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou, ktoré spracúvanie predstavuje pre práva a slobody fyzických osôb, prevádzkovateľ v čase určenia prostriedkov spracúvania aj v čase samotného spracúvania prijme primerané technické a organizačné opatrenia, ako je napríklad pseudonymizácia, ktoré sú určené na účinné zavedenie zásad ochrany údajov, ako je minimalizácia údajov, a začlení do spracúvania nevyhnutné záruky s cieľom splniť požiadavky tohto nariadenia a chrániť práva dotknutých osôb.*"[616] Napriek komplexnej štruktúre daného ustanovenia možno jeho myšlienku zhrnúť do idey, pri ktorej už pri koncipovaní informačných systémov, aplikácií alebo posúdenia spracúvania osobných údajov v organizácii je potrebné brať do úvahy právny poriadok s osobitným zreteľom na právo na ochranu osobných údajov v zmysle článku 8 Charty. Inými slovami, pri diskusii o technickom a organizačnom prevedení spracúvania osobných údajov by mal byť od začiatku okrem bezpečnostných analytikov a informatikov prítomný vždy človek zdatný v právnej oblasti, ktorý dokáže relevantne posúdiť právne riziká plynúce zo zavádzania nových procesov alebo programovania novej aplikácie v danej organizácii. Tento prístup reflektuje aj požiadavku *tailor-made data governance*, čo znamená, že každá organizácia si môže už v úvodných fázach nových procesov v zákonných mantineloch špecificky prispôsobiť spracúvanie osobných údajov.

Jednotlivé požiadavky článku 25 ods. 1 GDPR možno dešifrovať v nasledujúcej tabuľke s previazaním na konkrétnu povinnosť, prípadne požiadavky v technických štandardoch.

Požiadavka článku 25 GDPR	Povinnosť/Úloha/Súlad
Pozitívny záväzok prevádzkovateľa konať – *„prijať primerané technické a organizačné opatrenia*"	Článok 32 GDPR Recitál 78 GDPR ENISA Report *„Privacy and Data Protection by Design*"
... a navrhnúť a implementovať *„zásady ochrany údajov... a začlení do spracúvania nevyhnutné záruky s cieľom splniť požiadavky tohto nariadenia a chrániť práva dotknutých osôb.*"	Článok 5 GDPR Práva dotknutých osôb Požiadavky GDPR vo všeobecnosti (vizualizácia spracúvania osobných údajov)

[616] GDPR, článok 25 ods. 1.

… efektívnym spôsobom	Proporcionalita Odborný prístup
… prístupom založeným na posudzovaní rizika berúc do úvahy →	Povaha, rozsah a kontext spracúvania Najnovšie poznatky (*state-of-the-art*) Náklady na vykonanie opatrení Účel spracúvania Riziká s rôznou pravdepodobnosťou a závažnosťou, ktoré spracúvanie predstavuje pre práva a slobody fyzických osôb
„v čase určenia prostriedkov spracúvania aj v čase samotného spracúvania"	Pred a počas spracúvania osobných údajov

Tabuľka: Konkrétne požiadavky článku 25 GDPR a ich dešifrovanie.
Zdroj: V poznámke pod čiarou.[617]

Diskutovaný inštitút vysvetľuje aj usmernenie Výboru.[618] Povinnosť zohľadniť tieto aspekty dopadá na všetkých prevádzkovateľov, vrátane prevádzkovateľov odporúčacích systémov. Podľa nášho názoru ide o jeden z kľúčových nástrojov pri zmierňovaní šírenia dezinformácií na základe spracúvaných osobných údajov, ktoré GDPR ponúka, nakoľko prevádzkovateľ by mal potenciálne riziká odhaliť už vo fáze dizajnu spracovateľských operácií. Tomuto konštatovaniu nasvedčuje aj výklad článku 25 optikou zásady spravodlivosti (*fairness*) v usmernení Výboru. Výbor akcentuje využívanie spravodlivých algoritmov. Prevádzkovateľ by mal pravidelne vyhodnocovať, či algoritmy fungujú v súlade s vytýčenými účelmi a modifikovať ich tak, aby sa zmiernili odhalené predsudky a zabezpečila sa spravodlivosť pri spracovaní.[619] Šírenie dezinformácií alebo nenávistného obsahu na základe nesprávne zvolených parametrov odporúčacích systémov nepredstavuje spravodlivé spracúvanie osobných údajov a nastavenie algoritmov. Práve článok 25 by už vo fáze dizajnu a nastavenia mal napomôcť prevádzkovateľov identifikovať toto riziko.

[617] Vypracované podľa JASMONTAITE, L., KAMARA, I., ZANFIR-FORTUNA, G., LEUCII, S. Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR. In. *EDPL*, Vol. 2, 2018, s. 168 – 189.
[618] EUROEPAN DATA PROTECTION BOARD. *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default.* Version 2.0 Adopted on 20 October 2020. Dostupné na: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.
[619] Tamže, s. 18.

Práva dotknutých osôb

Okrem systémovejších nástrojov obsahuje GDPR aj individuálne práva dotknutej osoby, ktoré si môže akákoľvek dotknutá osoba u prevádzkovateľa uplatniť. V kontexte šírenia dezinformácií o konkrétnej osobe považujeme za nevyhnutné diskutovať právo na opravu, právo na vymazanie (zabudnutie), právo namietať a ďalšie práva týkajúce sa podania sťažnosti na dozorný orgán a obrany na súde. Dotknuté osoby majú aj **právo na opravu**, v zmysle ktorého má dotknutá osoba *„právo na to, aby prevádzkovateľ bez zbytočného odkladu opravil nesprávne osobné údaje, ktoré sa jej týkajú. So zreteľom na účely spracúvania má dotknutá osoba právo na doplnenie neúplných osobných údajov, a to aj prostredníctvom poskytnutia doplnkového vyhlásenia."*[620] Toto právo obsahuje v skutočnosti dva dielčie práva a to právo na opravu nesprávnych osobných údajov a právo na doplnenie neúplných osobných údajov. Ako jedno z mála práv v zmysle GDPR, neobsahuje konkrétnejšie podmienky na jeho uplatnenie a ani výnimky, kedy sa právo na opravu neuplatňuje. Pri šírení dezinformácií o svojej osobe by sa tak podľa nášho názoru vzťahovalo diskutované právo, nakoľko postačuje, že dotknutá osoba žiada o opravu údajov, ktoré sa *jej týkajú*. Potenciálnym problémom môže byť, že na opravu má dotknutá osoba nárok iba v prípade, ak sú osobné údaje nesprávne. GDPR neustanovuje žiadny test správnosti údajov a bude iba na dotknutej osobe, aby preukázala ich nesprávnosť. Tento aspekt môže pri šírení sofistikovanejších foriem dezinformácií predstavovať výzvu a problém, nakoľko v konečnom dôsledku to bude rozhodnutie prevádzkovateľa, či opravu vykoná alebo nie.

Článok 17 GDPR upravuje **právo na vymazanie**. V zmysle daného ustanovenia má dotknutá osoba právo dosiahnuť u prevádzkovateľa bez zbytočného odkladu vymazanie osobných údajov, ktoré sa jej týkajú, pričom prevádzkovateľ je povinný bez zbytočného odkladu vymazať osobné údaje, ak je splnený niektorý z dôvodov ustanovených v článku 17 ods. 1 GDPR. Prevádzkovateľ tak v prvom rade skúma, či existuje legitímny dôvod na vymazanie. Tieto dôvody sú nasledujúce: nepotrebnosť osobných údajov na účel, na ktorý sa získavali; odvolanie súhlasu a neexistencia iného právneho základu; ak prevádzkovateľ nevie preukázať prevahu oprávneného záujmu a namieta spracúvanie osobných údajov; nezákonnosť spracúvania osobných údajov; splnenie povinnosti kladenej právnym poriadkom SR alebo EÚ a ak sa osobné údaje získavali v súvislosti s ponukou služieb informačnej spoločnosti dieťaťu na základe jeho súhlasu podľa článku 8 ods. 1 GDPR.[621] Z vyššie uvedených dôvodov pri šírení

[620] GDPR. článok 16.
[621] GDPR, článok 17 ods. 1.

dezinformácií a uplatnení daného práva je použiteľným dôvodom nezákonnosť spracúvania. Nezákonnosť spracúvanie je však potrebné pri uplatnení práva na vymazanie odôvodniť rozhodnutím správneho alebo súdneho orgánu. Pre dotknutú osobu tak môže byť častokrát neskoro. Zároveň upozorňujeme, že právo na vymazanie obsahuje aj niekoľko výnimiek, kedy prevádzkovateľ nemusí právu na vymazanie vyhovieť. Jednou z nich je, ak prevádzkovateľ osobných údajov tieto údaje dotknutej osoby potrebuje na uplatnenie práva na slobodu prejavu a na informácie. Možno predpokladať, že právo na vymazanie a právo na slobodu prejavu sa pomerne často dostanú do konfliktu, pričom určitý návod na riešenie a vyváženie daných práv v konflikte predstavuje rozhodnutie SDEÚ vo veci *Google v. CNIL.*[622] Predmetná výnimka môže predstavovať výraznú prekážku pre úspešné uplatnenie práva na vymazanie o konkrétnej osobe v kontexte šírenia dezinformácií.

V prípade, ak prevádzkovateľ zverejnil osobné údaje a dotknutá osoba si úspešne uplatnila právo na vymazanie, so zreteľom na dostupnú technológiu a náklady na vykonanie opatrení je povinný podniknúť primerané opatrenia vrátane technických opatrení, aby informoval prevádzkovateľov, ktorí vykonávajú spracúvanie osobných údajov, že dotknutá osoba ich žiada, aby vymazali všetky odkazy na tieto osobné údaje, ich kópiu alebo repliky.[623]

Dotknutá osoba má taktiež **právo namietať** podľa článku 21 GDPR. Toto právo má v prípade, ak sú osobné údaje spracúvané na právnom základe verejného záujmu alebo oprávneného záujmu a v taktom prípade prevádzkovateľ musí vedieť preukázať prevahu takéhoto záujmu nad právami, slobodami a záujmami dotknutej osoby. Ak toto bremeno neunesie, spracúvanie osobných údajov musí prestať. Ak by spracúvanie osobných údajov napríklad v rámci odporúčacích systémov prebiehali na právnom základe verejného záujmu alebo oprávneného záujmu, dotknutá osoba môže na svoju obranu pri šírení dezinformácií o nej využiť aj právo namietať.

Okrem vyššie uvedených práv majú dotknuté osoby možnosť obrátiť sa na dozorný orgán alebo súd. Na dozorný orgán zriadený podľa GDPR (v slovenských podmienkach Úrad na ochranu osobných údajov SR) sa dotknuté osoby môžu obrátiť či už pre porušenie hmotnoprávnych ustanovení GDPR alebo pri neúspešnom uplatnení práv dotknutej osoby. Sťažnosť dozornému orgánu tak nie je limitovaná iba na využitie konkrétnych práv dotknutej osoby, ale dotknutá osoba prípadne osoby, ktoré tvrdia, že je priamo dotknutá na svojich

[622] Rozhodnutie SDEÚ z 24. septembra 2019 *GC a i. v. Commission nationale de l'informatique et des libertés (CNIL)*. Vec č. C-136/17.
[623] GDPR, článok 17 ods. 2.

právach[624] môžu podať podnet na preskúmanie súladu prevádzkovateľa s požiadavkami na automatizované individuálne rozhodovanie, špecificky navrhnutú ochranu osobných údajov či posúdenie vplyvu. Môže ísť teda o prínosný nástroj, ktorým disponuje dotknutá osoba pri šírení dezinformácií u konkrétneho prevádzkovateľa. Dozorné orgány môžu prevádzkovateľov kontrolovať a konať voči ním aj z úradnej povinnosti.

Na inštitút podania sťažnosti nadväzuje možnosť podať súdny prostriedok nápravy voči týmto rozhodnutiam[625] či konkrétnemu prevádzkovateľovi alebo sprostredkovateľovi.[626]

3.2.5 Priestupky

Ďalším nástrojom verejného práva pre boj s dezinformáciami online môže byť priestupkové právo. Priestupky ako druh správnych deliktov máme v právnom poriadku upravené v zákone č. 372/1990 Zb. o priestupkoch (ďalej len „Zákon o priestupkoch"), prípadne v osobitných predpisoch. Ide o čiastočnú kodifikáciu, nakoľko časť právnej úpravy priestupkov sa nachádza v osobitných zákonoch.

Z hľadiska teritoriálnej pôsobnosti Zákona o priestupkoch považujeme za vhodné zvýrazniť, že tento zákon sa vzťahuje na všetky priestupky spáchané na území Slovenskej republiky.[627] Toto obmedzenie by mohlo predstavovať prekážku pri šírení dezinformácií v online priestore prostredníctvom osôb z územia iného štátu.

V zmysle uvedeného zákona je *„priestupkom zavinené konanie, ktoré porušuje alebo ohrozuje záujem spoločnosti a je za priestupok výslovne označené v tomto alebo v inom zákone, ak nejde o iný správny delikt postihnuteľný podľa osobitných právnych predpisov, alebo o trestný čin."*[628] Legálna definícia je založená na kombinácií materiálneho znaku, formálnych znakov, pozitívneho a negatívneho vymedzenia.[629] V kontexte naplnenia materiálneho znaku sa skúma miera nebezpečenstva resp. škodlivosti špecifického konania. Inými slovami, naplnenie formálnych všeobecných a typových znakov niektorej zo skutkových podstát priestupku

[624] Zákon o ochrane osobných údajov, § 100 ods. 1.
[625] GDPR, článok 78.
[626] GDPR, článok 79.
[627] Zákon o priestupkoch, § 8 ods. 1.
[628] Zákon o priestupkoch, § 2 ods. 1.
[629] HAMUĽÁKOVÁ, Z., HORVAT, M. *Základy správneho práva trestného*. Bratislava : Wolters Kluwer, 2019, s. 84 – 85.

nemusí postačovať na klasifikovanie konania ako priestupku.[630] Samotný záujem spoločnosti je právne neurčitý pojem, ktorý správne orgány interpretujú podľa svojej úvahy.[631]

Na vyvodenie zodpovednosti za spáchanie priestupku postačuje zavinenie z nedbanlivosti, ak právna úprava explicitne nevyžaduje úmyselné zavinenie.[632] Je nutné zvýrazniť, že páchateľom priestupku môže byť jedine fyzická osoba. Zákon o priestupkoch diferencuje štyri sankcie za priestupky a to konkrétne pokarhanie, pokuta, zákaz činnosti a prepadnutie veci. Pri ukladaní sankcie sa prihliada na *„závažnosť priestupku, najmä na spôsob jeho spáchania a na jeho následky, na okolnosti, za ktorých bol spáchaný, na mieru zavinenia, na pohnútky a na osobu páchateľa, ako aj na to, či a akým spôsobom bol za ten istý skutok postihnutý v kárnom alebo disciplinárnom konaní."*[633] Najčastejšie ukladanou sankciou je pokuta, ktorej výšku limituje samotný Zákon o priestupkoch. Konanie o priestupkoch je možné začať na podnet v taxatívne vymedzených prípadoch, ale aj *ex offo*.[634]

Na nasledujúcich riadkoch budeme diskutovať konkrétne skutkové podstaty priestupkov, v rámci ktorých je podľa nášho názoru možné subsumovať aj vytvárania alebo šírenie dezinformácií v online priestore. Identifikovali sme nasledujúce skutkové podstaty:

- Priestupky vyskytujúce sa na viacerých miestach správy (neoprávnené vydávania sa za verejného činiteľa)
- Priestupky na úseku zdravotníctva (falšovanie informácií o zdravotnom stave)
- Priestupky proti verejného poriadku (vzbudenie verejného pohoršenia)
- Priestupky proti občianskemu spolunažívaniu (ublíženie na cti a vyhrážanie).

§ 21 ods. 1 písm. g) Zákona o priestupkoch ustanovuje, že *„priestupku sa dopustí ten, kto úmyselne neoprávnene sa vydáva za verejného činiteľa."* Ide o špecifické protiprávne konanie, pri ktorom sa subjekt priestupku vydáva za verejného činiteľa, pričom ním nie je. Pojem verejný činiteľ máme legálne definovaný v § 128 Trestného zákona.[635] Inými slovami, môže ísť o formu

[630] Tamže, s. 85.
[631] SREBALOVÁ, M. a kolektív. *Zákon o priestupkoch. Komentár*. 2. vydanie. Bratislava: C. H. Beck, 2020, komentár k § 2, dostupné na beck-online.sk.
[632] Zákon o priestupkoch, § 3.
[633] Zákon o priestupkoch, § 12 ods. 1.
[634] Pozri Zákon o priestupkoch, § 67 a 68.
[635] § 128 Trestného zákona: *„Verejným činiteľom sa na účely tohto zákona rozumie prezident Slovenskej republiky, poslanec Národnej rady Slovenskej republiky, poslanec Európskeho parlamentu, člen vlády, sudca Ústavného súdu Slovenskej republiky, sudca, prokurátor alebo iná osoba zastávajúca funkciu v orgáne verejnej moci, príslušník ozbrojených síl, osoba v služobnom pomere, starosta, predseda vyššieho územného celku, poslanec orgánu územnej samosprávy, štátny zamestnanec alebo zamestnanec orgánu štátnej správy, územnej samosprávy alebo iného štátneho orgánu, osoba, ktorá vykonáva pôsobnosť v rámci právnickej osoby, ktorej zákon zveruje právomoc rozhodovať v oblasti*

personifikácie dezinformácie, ktorá je však veľmi špecifická a týka sa skutkovo obmedzeného rozsahu situácií. V tomto prípade sa nevyžaduje úmyselné zavinenie a v prípade spáchania priestupku z nedbanlivosti, by neboli naplnené požiadavky na úmyselné zavádzanie takým spôsobom, akým to vyžadujú definícia dezinformácií.

§ 29 ods. 1 písm. c) Zákona o priestupkoch upravuje jeden z priestupkov na úseku zdravotnej starostlivosti. V zmysle tohto ustanovenia *„priestupku sa dopustí ten, kto sfalšuje alebo zámerne vyhotoví nepravdivý výpis zo zdravotnej dokumentácie, potvrdenie týkajúce sa zdravotného stavu osoby alebo potvrdenie týkajúce sa poskytnutej zdravotnej starostlivosti, alebo kto si nechá vyhotoviť alebo použije nepravdivý výpis zo zdravotnej dokumentácie, nepravdivé potvrdenie týkajúce sa zdravotného stavu osoby alebo nepravdivé potvrdenie týkajúce sa poskytnutej zdravotnej starostlivosti, alebo kto zneužije zdravotnú dokumentáciu."*[636] Predmetná skutková podstata bola novelizovaná a značne rozšírená v roku 2021, počas krízovej situácie v dôsledku pandémie COVID-19. V zmysle dôvodovej správy *„cieľom je osobitne postihovať falšovanie a nepravdivý výpis zo zdravotnej dokumentácie, potvrdenia týkajúceho sa zdravotného stavu osoby alebo potvrdenia týkajúce sa poskytnutej zdravotnej starostlivosti. Najmä v čase pandémie COVID-19 je používanie, falšovanie a vyhotovovanie nepravdivých uvedených dokumentov, ktoré môžu mať formu potvrdenia o absolvovaní očkovania proti ochoreniu COVID-19, potvrdenia o prekonaní ochorenia COVID-19 alebo potvrdenia o negatívnom výsledku testu na ochorenie COVID-19, či už v listinnej, alebo elektronickej podobe, významne negatívnym faktorom z hľadiska kontroly dodržiavania protiepidemických opatrení a následného dopadu na šírenie ochorenia COVID-19."*[637] Predmetná skutková podstata tak postihuje úmyselné šírenie nepravdivých informácií o subjekte spáchania priestupku. Podľa nášho názoru nemôžeme takéto konanie považovať za šírenie dezinformácií vždy, nakoľko na zavinenie postačuje zavinenie z nedbanlivosti. Ak by však páchateľ tohto priestupku konal úmyselne, boli by naplnené znaky šírenia nepravdivej informácie (o sebe) s úmyslom získať určitý benefit ako napríklad lepšie pracovné miesto, vstup do prevádzky alebo výnimku z pravidiel. Zároveň je potrebné zvýrazniť, že ide opäť iba o veľmi špecificky prípad dezinformácií v podobe informácií týkajúcich sa zdravotného stavu.

verejnej správy, notár, súdny exekútor, člen lesnej stráže, vodnej stráže, rybárskej stráže, poľovníckej stráže, stráže prírody alebo osoba, ktorá má oprávnenie člena stráže prírody, ak sa podieľa na plnení úloh spoločnosti a štátu a používa pritom právomoc, ktorá mu bola v rámci zodpovednosti za plnenie týchto úloh zverená."

[636] Zákon o priestupkoch , § 29 ods. 1 písm. c).

[637] *Dôvodová správa k Vládnemu návrhu zákona, ktorým sa menia a dopĺňajú niektoré zákony v súvislosti s treťou vlnou pandémie ochorenia COVID-19*.

V rámci priestupkov proti verejnému poriadku sa ako hodný diskusie javí § 47 ods. 1 písm. c) Zákona o priestupkoch, v zmysle ktorého *„priestupku sa dopustí ten, kto vzbudí verejné pohoršenie."* Kľúčový pre diskutovaný skutkovú podstatu je pojem „verejné pohoršenie," ktorý je právne neurčitým pojmom. Za znaky verejného pohoršenia možno označiť to, že konanie je verejné, subjektívne pohoršuje viac ako dve osoby a konanie je v rozpore s dobrými mravmi.[638] Na spáchanie daného priestupku postačuje zavinenie z nedbanlivosti. Z tohto dôvodu ak by sme chceli v rámci diskutovanej skutkovej podstaty subsumovať pod dané konanie aj šírenie alebo vytváranie dezinformácií, muselo by ísť o úmyselné konanie. Otvorenou otázkou je, či vytváranie alebo šírenie dezinformácií vzbudzuje verejné pohoršenie. Podľa nášho názoru môže byť odpoveď kladná. Vo všeobecnosti, úmyselné šírenie nepravdivých informácií alebo ich manipulatívne podanie môže v časti slušnej spoločnosti spôsobiť pohoršenie. Takéto konanie by jednoznačne mohlo byť klasifikované ako verejné a odporujúce dobrým mravom. Zároveň, konkrétne dezinformácie môžu mať aj pohoršujúcu podobu ako napríklad šírenie falošných obrázkov alebo videí verejne známych osôb v situáciách, v intímnych situáciách.

Priestupky proti občianskemu spolunažívaniu obsahujú dve skutkové podstaty, ktoré považujeme za vhodné diskutovať. Spoločným menovateľom týchto skutkových podstát je ich objekt, ktorým je občianske spolunažívanie. Ide znova o právne neurčitý pojem. Všeobecne sa občianske spolunažívanie považuje súhrn pravidiel správania nad rámec právnych noriem, ktorých dodržanie je podľa všeobecného názoru a presvedčenia nevyhnutnou podmienkou pokojného, usporiadaného a riadneho spolunažívania osôb v danom mieste, čase a situácii.[639]

Prvou je skutková podstata priestupku ustanoveného v § 49 ods. 1 písm. a), v zmysle ktorej *„priestupku sa dopustí ten, kto inému ublíži na cti tým, že ho urazí alebo vydá na posmech."* Tento priestupok možno spáchať ústne, písomne alebo neverbálnym prejavom. Ako uvádza Srebalovová *„urážka a zosmiešnenie môžu spočívať aj v* ***oznámení nepravdivého, ale aj pravdivého údaja o inej osobe, ktorý je hanlivý****. Výrok alebo iný skutok teda musí byť urážlivý alebo zosmiešňujúci a zároveň musel páchateľ o tejto skutočnosti vedieť (platí pravidlo, podľa ktorého sa nikto nemôže dopustiť urážky, ak sám nevie, že uráža)."*[640] Máme za to, že pri úmyselnom konaní páchateľa by špecifické situácie vytvárania a šírenia dezinformácií o určitej osobe mohli byť subsumované pod diskutovanú skutkovú podstatu. Išlo by o situácie, ak by sa

[638] SREBALOVÁ, M. a kolektív. *Zákon o priestupkoch. Komentár*. 2. vydanie. Bratislava: C. H. Beck, 2020, komentár k § 47, dostupné na beck-online.sk.
[639] MACHAJOVÁ, J. *Základy priestupkového práva. Komentár*. Šamorín: Heuréka, 1998, s. 73. Porovnaj SREBALOVÁ, M. a kolektív. *Zákon o priestupkoch. Komentár*. 2. vydanie. Bratislava: C. H. Beck, 2020, komentár k § 49, dostupné na beck-online.sk.
[640] SREBALOVÁ, M. a kolektív. *Zákon o priestupkoch. Komentár*. 2. vydanie. Bratislava: C. H. Beck, 2020, komentár k § 49, dostupné na beck-online.sk.

dezinformácia týkala konkrétnej osoby, bola by hanlivá alebo urážlivá a zároveň by páchateľ priestupku mal benefit z vytvorenia alebo šírenia takýchto dezinformácií.

Druhou zaujímavou skutkovou podstatou je § 49 ods. 1 písm. d), podľa ktorého *„priestupku sa dopustí ten, kto úmyselne naruší občianske spolunažívanie vyhrážaním ujmou na zdraví, drobným ublížením na zdraví, nepravdivým obvinením z priestupku, schválnosťami alebo iným hrubým správaním."* Na účely diskusie je potrebné vymedziť, čo môžu predstavovať pojmy nepravdivé obvinenie, schválnosti a iné hrubé správanie. Nepravdivé obvinenie z priestupku je konanie, ktoré smeruje proti konkrétnej osobe s cieľom iniciovať správne konanie.[641] Schválnosťami možno označiť *„také skutky, ktoré narušujú, resp. zasahujú do pokojného, usporiadaného a riadneho spolunažívania hrubým spôsobom."*[642] V zmysle judikatúry sa schválnosť definuje ako *„zámerná a cielená činnosť subjektu, ktorý zo zlomyseľnosti, pomsty a lebo iných racionálne nevysvetliteľných príčin a pohnútok vedome strpčuje a sťažuje život inému subjektu drobnými priekmi a prekážkami."*[643] Na účely vyvodenia administratívnoprávnej zodpovednosti musí schválnosť zodpovedať konaniu, ktoré hrubo porušuje občianske spolunažívanie.[644] Iným hrubým správaním možno rozumieť *„hrubé správanie sa, ktoré narušuje občianske spolunažívanie aj iným spôsobom než výslovne uvedenými prípadmi."*[645] Ide teda o také správanie, ktoré prekračuje rámec iným spôsobom nevhodného, napríklad nezdvorilého správania.[646] Je potrebné odlišovať konanie, ktoré je hrubé a konanie, ktoré je inak nevhodné.[647] Zároveň, pojem hrubé správanie je správnym orgánom potrebné interpretovať objektívne.[648]

Tento priestupok možno spáchať iba úmyselne, s cieľom narušiť občianske spolunažívanie.[649] V zmysle judikatúry pod neho možno subsumovať aj posielanie správ a listov s urážlivým a hanlivým obsahom[650] alebo oznámenie nepravdivých údajov.[651] V kontexte dezinformácií možno uviesť, že nakoľko sa vyžaduje úmyselné zavinenie, možno v zmysle tohto priestupku postihovať vytváranie a šírenie dezinformácií. Šírenia nepravdivých informácií o konkrétnej osobe môže objektívne narušiť občianske spolunažívanie a taktiež môže byť spáchane prostredníctvom schválnosti alebo hrubého správania. Kľúčovou sa ale javí posúdenie

[641] Tamže.
[642] Tamže.
[643] Rozsudok Krajského súdu Trenčín, sp. zn. 5C0/8/2016.
[644] KOŠIČIAROVÁ, S. *Zákon o priestupkoch - Podrobný komentár s judikatúrou*. Leges. 2021, s. 406.
[645] Tamže. Zhodne Rozsudok Krajského súdu Žilina, sp. zn. 25Sa/3/2021.
[646] SREBALOVÁ, M. a kolektív. *Zákon o priestupkoch. Komentár*. 2. vydanie. Bratislava: C. H. Beck, 2020, komentár k § 49, dostupné na beck-online.sk.
[647] Rozsudok Krajského súdu Žilina, sp. zn. 25Sa/3/2021.
[648] Tamže.
[649] KOŠIČIAROVÁ, S. *Zákon o priestupkoch - Podrobný komentár s judikatúrou*. Leges. 2021, s. 407.
[650] Rozsudok Krajského súdu Trenčín, sp. zn. 5C0/8/2016.
[651] Rozsudok Krajského súdu Prešov, sp. zn. 6Sa/19/2020.

intenzity zásahu, nakoľko pri šírení závažných dezinformácií o konkrétnej osobe nemožno hovoriť o drobných priekoch. Zároveň je otázne, či šírenie dezinformácii nie o konkrétnej osobe, ale o javoch by spadalo pod danú skutkovú podstatu.

3.2.6 Trestné činy

Ako ukazujú právne poriadky iných krajín, vytváranie alebo šírenie dezinformácií môže mať aj trestnoprávnu povahu. Z tohto dôvodu považujeme za nevyhnutné načrtnúť aj potenciálne postihovania vytvárania alebo šírenia dezinformácii prostredníctvom noriem trestného práva.

Základy trestnej zodpovednosti, druhy trestov, druhy ochranných opatrení, ich ukladanie a skutkové podstaty trestných činov[652] upravuje zákon č. 300/2005 Z. z. Trestný zákon (ďalej len „Trestný zákon"). Trestné právo chráni základné hodnoty a vzťahy upravené v iných právnych predpisoch.[653] Avšak, trestné právo je prostriedok *ultima ratio*, čo prakticky znamená, že jeho aplikácia by mala prísť až vtedy, ak prostriedky iných právnych odvetví nestačia.[654] S tým úzko súvisí aj zásada subsidiarity trestnej represie. *„Zásada subsidiarity trestnej represie pomáha spod pôsobnosti trestného práva eliminovať porušenia práva s nižšou spoločenskou závažnosťou, čiže drobné delikty v zmysle právnej zásady minima non curat praetor (o drobné záležitosti sa prétor nestará).* "[655]

Podobne ako pri Zákone o priestupkoch považujeme za vhodné zvýrazniť teritoriálnu pôsobnosť Trestného zákona. Na rozdiel od Zákona o priestupkoch, Trestný zákon nelimituje svoju pôsobnosť na trestné činy spáchané na územie Slovenskej republiky,[656] ale pracuje aj s kategóriami tzv. dištančných deliktov. Tieto môžu nastať, ak sa páchateľ dopustil konania aspoň z časti na území Slovenskej republiky a zároveň porušenie alebo ohrozenie záujmu chráneného Trestným zákonom nastalo alebo malo nastať celkom alebo sčasti mimo územia Slovenskej republiky[657] alebo sa páchateľ dopustil konania mimo územia Slovenskej republiky, ak tu malo nastať porušenie alebo ohrozenie záujmu chráneného Trestným zákonom alebo ak mal na území Slovenskej republiky nastať aspoň sčasti taký následok.[658] Ak sme konštatovali

[652] Trestný zákon, § 1.
[653] BURDA, E. a kol. *Trestný zákon. Všeobecná časť*. Komentár. I. diel. 1. vydanie. Praha: C. H. Beck, 2010, komentár k § 1, dostupné na beck-online.sk.
[654] Tamže.
[655] BURDA, E. - BELEŠ, A. - ĽORKO, A. - MIHÁLIK, S. *Trestná zodpovednosť*. 1. vyd. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2022, s. 21.
[656] Trestný zákon, § 3 ods. 1.
[657] Trestný zákon, § 3 ods. 2 písm. a).
[658] Trestný zákon, § 3 ods. 2 písm. b).

určité potenciálne obmedzenie v kontexte Zákona o priestupkoch vyplývajúce z teritoriálnej pôsobnosti, pri Trestnom zákone predmetné obmedzenie neplatí.

Podobne ako pri Zákone o priestupkoch, aj pri Trestnom zákone budeme diskutovať konkrétne skutkové podstaty trestných činov, v rámci ktorých je podľa nášho názoru možné subsumovať aj vytváranie alebo šírenie dezinformácií v online priestore. Konkrétne budeme analyzovať:

- Trestný čin ohovárania
- Trestný čin šírenia poplašnej správy
- Trestný čin ohrozenia bezpečnosti vzdušného dopravného prostriedku a lode
- Trestný čin falšovania a vyhotovenia nepravdivej zdravotnej dokumentácie
- Trestný čin teroristického útoku.

Niektoré z vyššie uvedených skutkových podstát sú prirodzene relevantnejšie a použiteľnejšie vo všeobecnom kontexte, avšak nebudeme opomínať ani špecifickejšie skutkové podstaty viazané na špecifický objekt.

Prvou vhodnou skutkovou podstatou na riešenie šírenia a vytvárania dezinformácií v online priestore je trestný čin ohovárania podľa § 373 Trestného zákona: *„Kto o inom oznámi nepravdivý údaj, ktorý je spôsobilý značnou mierou ohroziť jeho vážnosť u spoluobčanov, poškodiť ho v zamestnaní, v podnikaní, narušiť jeho rodinné vzťahy alebo spôsobiť mu inú vážnu ujmu, potrestá sa odňatím slobody až na dva roky.*" Kľúčové pojmy pre interpretáciu v kontexte objektívnej stránky sa týkajú oznámenia, nepravdivého údaju a následkov oznámenia nepravdivého údaju. Nepravdivý údaj je informácia, ktorá nezodpovedá skutočnosti, pričom nepravdivosť je vždy potrebné dokázať v trestnom konaní.[659] Oznámenie môže páchateľ vykonať rôznou formou, nevylučuje sa teda ani šírenie nepravdivého údaju v online priestore. Postačuje, ak je oznámenie urobené čo i len jednej osobe.[660] Za závažnejší spôsobom konania sa považuje spáchania tohto trestného činu verejne.[661] Zásah značnej miery je potrebné vždy posudzovať od prípadu k prípadu a je nutné prihliadať na spoločenské postavenie dotknutej osoby, charakter, charakter nepravdivého údaju, spôsob a kontext šírenia a ďalšie faktory.[662]

[659] BURDA, E. a kol. *Trestný zákon. Všeobecná časť. Komentár. I. diel*. 1. vydanie. Praha: C. H. Beck, 2010, komentár k § 373, dostupné na beck-online.sk.
[660] Tamže.
[661] Trestný zákon, § 373 ods. 2 písm. c).
[662] BURDA, E. a kol. *Trestný zákon. Všeobecná časť. Komentár. I. diel*. 1. vydanie. Praha: C. H. Beck, 2010, komentár k § 373, dostupné na beck-online.sk.

Vážnosť osoby môže predstavovať poškodenie v zamestnaní, narušenie rodinných vzťahov alebo inú vážnu ujmu.[663] Predmetný trestný čin slúži na stíhanie iba v prípade najzávažnejších zásahov do osobnostných práv a pri šírení informácií, ktoré zreteľne presahujú mieru bežných lží a neprávd, ktoré o sebe šíria ľudia v bežnom živote.[664] Zároveň je potrebné zvýrazniť, že tento trestný čin je využiteľný iba v prípade porušenia individuálnych práv[665] a nie je ho možné subsumovať pod konania, pri šírení iných dezinformácií ako o konkrétnej osobe.

Ďalšou skutkovou podstatou v kontexte šírenia dezinformácií je trestný šírenia poplašnej správy podľa § 361 a § 362 Trestného zákona. Trestného činu šírenia poplašnej správy sa dopustí ten, *„kto úmyselne spôsobí nebezpečenstvo vážneho znepokojenia aspoň časti obyvateľstva nejakého miesta tým, že rozširuje poplašnú správu, ktorá je nepravdivá, alebo sa dopustí iného obdobného konania spôsobilého vyvolať také nebezpečenstvo, potrestá sa odňatím slobody až na dva roky.*"[666] Druhá možnosť realizácie konanie šírenia poplašnej správy je uvedená v § 361 ods. 1 Trestného zákona: *„Kto správu alebo iné obdobné konanie uvedené v odseku 1, hoci vie, že sú nepravdivé a môžu vyvolať opatrenie vedúce k nebezpečenstvu vážneho znepokojenia aspoň časti obyvateľstva nejakého miesta, oznámi právnickej osobe alebo Policajnému zboru alebo inému štátnemu orgánu alebo hromadnému informačnému prostriedku, potrestá sa odňatím slobody na jeden rok až päť rokov.*" Opätovne považujeme za vhodné bližšie analyzovať kľúčové pojmy v kontext objektívnej stránky tohto trestného činu. Na naplnenie objektívnej stránky musia byť kumulatívne splnené dve požiadavky. Prvou je, že konanie páchateľa spôsobí nebezpečenstvo vážneho znepokojenia aspoň časti obyvateľstva nejakého miesta prostredníctvom rozširovania poplašnej správy, ktorá je nepravdivá alebo alternatívny iným obdobným konaním. Časťou obyvateľstva sa rozumie bližšie neurčitý, väčší počet osôb, ktorých sa správa môže dotknúť citeľnejším spôsobom.[667] Miestom môže byť *„obec, mesto, resp. jeho časť, určitá štvrť, alebo nejaká organizácia, ako napríklad škola, budova súdu, budova nemocnice, resp. zdravotníckeho zariadenia, budova divadla, športového štadiónu a pod.*"[668] Pod pojem rozširovanie môžeme rozumieť také konanie, ktoré znamená sprístupňovanie poplašnej správy väčšiemu okruhu osôb. Rozširovať poplašnú správu možno prostredníctvom rôznych

[663] ČENTÉŠ, J. a kol. *Trestný zákon - Veľký komentár*. 5. aktualizované vydanie. Žilina: Eurokódex, 2022, s. 798.
[664] Uznesení Nejvyššíhou soudu České republiky, sp. zn. 3 Tdo 288/2021 zo dňa 19.05.2021.
[665] Analogicky pri právnických osobách je použiteľná skutková podstata trestného činu poškodzovania cudzích práv podľa § 375 Trestného zákona.
[666] Trestný zákon, § 361 ods. 2.
[667] BURDA, E. a kol. *Trestný zákon. Všeobecná časť. Komentár. I. diel.* 1. vydanie. Praha: C. H. Beck, 2010, komentár k § 361, dostupné na beck-online.sk.
[668] NESVADBA, A. – MARKOVÁ, V. Šírenie dezinformácií a možné trestnoprávne následky v zmysle Trestného zákona. In MEDELSKÝ, J., LACA, N. 2022. *Dezinformácie a právo (úlohy a postavenie bezpečnostných zložiek).* Zborník príspevkov. Bratislava. Akadémia Policajného zboru v Bratislave, s. 167.

zariadení vrátane masovokomunikačných prostriedkov či počítača.[669] Máme za to, že aj šírenie prostredníctvom internetovej siete naplní podmienku rozširovania. *„Poplašná správa je taká, ktorá je svojim obsahom spôsobilá vyvolať vážne znepokojenie vo forme strachu, úzkosti, paniky, atď.*"[670] Môže ísť napríklad o správy týkajúce sa vojenského ohrozenia krajiny, spochybňovania vedecky preverených zdravotníckych postupov alebo prírodných katastrof. Nepravdivá poplašná správa nezodpovedá skutočnosti, alternatívne je skreslená.[671] Iné obdobné konanie môže spočívať v rozširovaní falošných predmetov, ktoré môžu spôsobiť značné znepokojenie obyvateľstva.[672] Druhý odsek § 361 ustanovuje špecifický prípad skutkovej podstaty šírenia poplašnej správy, pričom na jeho dokonanie postačuje oznámenie poplašnej správy špecifickému subjektu, ktorým je právnická osoba, Policajný zbor, iný štátny orgán alebo hromadný informačný prostriedok.

§ 362 ustanovuje skutkovú podstatu trestného činu šírenia poplašnej správy za krízovej situácie: *„Kto za krízovej situácie štátu spôsobí, čo aj z nedbanlivosti, nebezpečenstvo vážneho znepokojenia, malomyseľnosti alebo porazeneckej nálady aspoň u časti obyvateľstva nejakého miesta tým, že rozširuje poplašnú správu, potrestá sa odňatím slobody na šesť mesiacov až tri roky.*" Oproti § 361 sa vyžaduje, aby šírenie poplašnej správy prebiehalo počas krízovej situácie a okrem vážneho znepokojenia môže spôsobovať malomyseľnosť alebo porazeneckú náladu časti obyvateľstva nejakého miesta. Za krízovú situáciu sa považuje núdzový stav, výnimočný stav, vojnový stav alebo vojna.[673] Spôsobenie malomyseľnosti je možné vykladať ako vyvolanie pesimistických nálad a názorov, ktoré oslabujú schopnosť alebo motiváciu vyvíjať odpor proti nepriateľov.[674] *„Porazeneckou náladou sa rozumie pocit zbytočnosti, bezvýznamnosti alebo neschopnosti vyvíjať odpor proti nepriateľovi.*"[675] Trestnosť konania páchateľa nespočíva v rozširovaní nepravdivých informácií, ale v jej oznámení určitému subjektu.[676] Pri tomto trestnom čine postačuje, ak ide o poplašnú správ, pravdivosť je irelevantná. Za trestné činy podľa § 361 a 362 nemožno stíhať právnickú osobu.

Ďalšie trestné činy, pod ktoré možno subsumovať šírenie dezinformácií sú naviazané na špecifický kontext. Možno hovoriť o trestnom čine oznámenia nepravdivej informácie, ktorá

[669] BURDA, E. a kol. *Trestný zákon. Všeobecná časť. Komentár. I. diel.* 1. vydanie. Praha: C. H. Beck, 2010, komentár k § 361, dostupné na beck-online.sk.
[670] Tamže.
[671] Tamže.
[672] Tamže.
[673] Trestný zákon, § 134.
[674] BURDA, E. a kol. *Trestný zákon. Všeobecná časť. Komentár. I. diel*. 1. vydanie. Praha: C. H. Beck, 2010, komentár k § 362, dostupné na beck-online.sk.
[675] Tamže.
[676] ČENTÉŠ, J. a kol. *Trestný zákon - Veľký komentár*. 5. aktualizované vydanie. Žilina: Eurokódex, 2022, s. 781.

môže ohroziť bezpečnosť alebo prevádzku určitého objektu. V zmysle § 292 Trestného zákona: *„Kto oznámi nepravdivú informáciu, ktorá môže ohroziť bezpečnosť alebo prevádzku vzdušného dopravného prostriedku za letu alebo lode za plavby, potrestá sa odňatím slobody až na tri roky.*" Ide teda o šírenie nepravdivej informácie v úzko vymedzenom časovom rozsahu – účinok nepravdivej informácie sa musí prejaviť počas letu vzdušného dopravného prostriedku alebo plavby lode.[677]

Iným relevantným trestným činom je podobne ako pri Zákone o priestupkoch falšovanie zdravotnej dokumentácie: *„Kto falšuje zdravotnú dokumentáciu alebo zámerne vyhotoví nepravdivú zdravotnú dokumentáciu v úmysle použiť ju ako pravú v konaní pred orgánom verejnej moci, alebo ju použije ako pravú v konaní pred orgánom verejnej moci, alebo kto si nechá takúto zdravotnú dokumentáciu vyhotoviť v úmysle použiť ju ako pravú v konaní pred orgánom verejnej moci, alebo použije takúto zdravotnú dokumentáciu ako pravú v konaní pred orgánom verejnej moci, potrestá sa odňatím slobody až na dva roky.*"[678] Zakotvenie tohto trestného činu v roku 2019 bolo reakciou na absenciu trestnoprávnej zodpovednosti za manipuláciu s údajmi v zdravotnej dokumentácií konkrétnej osoby.[679]

Šírenie nepravdivej informácie figuruje aj v trestnom čine teroristického útoku podľa § 419 Trestného zákona: *„Kto v úmysle poškodiť ústavné zriadenie alebo obranyschopnosť štátu, narušiť alebo zničiť základnú politickú, hospodársku alebo spoločenskú štruktúru štátu alebo medzinárodnej organizácie, závažným spôsobom zastrašiť obyvateľstvo alebo donútiť vládu štátu alebo iný orgán verejnej moci alebo medzinárodnej organizácie, aby niečo konala, opomenula alebo strpela…zmocní sa lietadla, lode, iného prostriedku osobnej dopravy alebo nákladnej dopravy alebo pevnej plošiny na podmorskej plytčine, alebo nad takým dopravným prostriedkom alebo pevnou plošinou vykonáva kontrolu, alebo zničí alebo vážne poškodí navigačné zariadenie alebo zasahuje do jeho prevádzky,* ***alebo oznámi nepravdivú informáciu, čím ohrozí život alebo zdravie ľudí, bezpečnosť takého dopravného prostriedku****, alebo vydá cudzí majetok do nebezpečenstva škody veľkého rozsahu, alebo takým konaním hrozí.*"[680] V zmysle predmetného ustanovenia ide skutkovú podstatu, ktorá chráni vnútropolitické usporiadanie štátov a ich vzájomné vzťahy.[681] Objekt diskutovaného trestného činu možno rozlíšiť na primárny a sekundárny. Primárnym objektom je spoločnosť a jej demokratické fungovanie.

[677] BURDA, E. a kol. *Trestný zákon. Všeobecná časť. Komentár. I. diel*. 1. vydanie. Praha: C. H. Beck, 2010, komentár k § 292, dostupné na beck-online.sk.
[678] Trestný zákon, § 352a.
[679] *Dôvodová správa k vládnemu návrhu zákona, ktorým sa mení a dopĺňa zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony.*
[680] Trestný zákon, § 419 ods. 1 písm. d).
[681] STRÉMY, T. – KURILOVSKÁ, L. *Trestný zákon. Komentár. Zväzok II*. Wolters Kluwer, 2022, s. 1304.

Sekundárnym objektom je ochrana života, zdravia, majetku a iné hodnoty.[682] Objektívna stránka spočíva v naplnení jedného z alternatívnych konaní. V kontexte šírenia dezinformácii by mohlo ísť o poškodenie ústavného poriadku[683] či obranyschopnosti štátu, zastrašovanie obyvateľstva závažným spôsobom alebo manipulácia správania vlády alebo štátneho orgánu. Objektívna stránka vyššie uvedeného trestného činu v kontexte šírenia dezinformácií spočíva v ohrození dopravného prostriedku prostredníctvom oznámenia nepravdivej informácie. Ide tak o veľmi limitovanú množinu situácií, keď by mohlo byť predmetné ustanovenie aplikované v súvislosti so šírením dezinformácií.

3.2.6.1 Návrh osobitnej skutkovej podstaty trestného činu šírenia dezinformácií

Aj vzhľadom na vyššie uvedené skutočnosti sa slovenský zákonodarca pokúsil ustanoviť špecifické skutkové podstaty namierené proti šíreniu dezinformácií v roku 2022.[684] Aj samotný zákonodarca v dôvodovej správe priznáva potrebu reakcie na *„aktuálne nepriaznivé následky šírenia dezinformácií a nebezpečenstvo hybridných hrozieb."*[685]

Oproti súčasnej právnej úprave novela Trestného zákona odčlenila skutkovú podstatu v zmysle § 361 a upravila nové trestné činy v navrhovaných § 361a a 362.

Navrhovaný trestný čin šírenia poplašnej správy v zmysle navrhovaného § 361 obsahuje porovnateľné znenie skutkovej podstaty, aké dnes upravuje Trestný zákon v § 361 ods. 2. [686] Novinkou je iba pridanie kvalifikačného znaku za krízovej situácie, čo reflektuje šírenie dezinformácií v súvislosti so šírením nebezpečne nákazlivej choroby COVID-19.[687] Ako uvádza

---

[682] Tamže, s. 1305.

[683] Pojem ústavný poriadok je priamo definovaný v Trestnom zákone ako *„demokratický systém základných práv a slobôd garantovaný náležitým usporiadaním a fungovaním orgánov štátnej moci, územnej samosprávy a politických strán a hnutí upravený Ústavou Slovenskej republiky."* Trestný zákon, § 134 ods. 1.

[684] *LP/2021/744*. Zákon, ktorým sa mení a dopĺňa zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov a o zmene a doplnení niektorých zákonov.

[685] *Dôvodová správa k zákonu, ktorým sa mení a dopĺňa zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov a o zmene a doplnení niektorých zákonov*. Dostupné na: https://www.slov-lex.sk/legislativne-procesy/-/SK/dokumenty/LP-2021-744.

[686] Navrhované znenie:
„(1) Kto oznámi Policajnému zboru alebo inému orgánu verejnej moci, právnickej osobe alebo hromadnému informačnému prostriedku poplašnú správu, ktorá nie je pravdivá a
ktorá môže vyvolať opatrenia na zabezpečenie bezpečnosti, ochranu zdravia, života alebo majetku, potrestá sa odňatím slobody na jeden rok až päť rokov.
(2) Odňatím slobody na tri roky až osem rokov sa páchateľ potrestá, ak spácha čin
uvedený v odseku 1
a) a už bol za taký čin odsúdený, alebo
b) a spôsobí ním vážnu poruchu v hospodárskej prevádzke alebo hospodárskej činnosti
právnickej osobe alebo v činnosti štátneho orgánu alebo iný obzvlášť závažný následok
c) za krízovej situácie."

[687] *Dôvodová správa k zákonu, ktorým sa mení a dopĺňa zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov a o zmene a doplnení niektorých zákonov*. Dostupné na: https://www.slov-lex.sk/legislativne-procesy/-/SK/dokumenty/LP-2021-744.

Nesvadba a Marková, prakticky totožné znenie tejto skutkovej podstaty dáva za pravdu názorom ohľadom aplikovateľnosti § 361 ods. 2 súčasného Trestného zákona.[688]

Novela Trestného zákona však zakotvila aj ďalšie skutkové podstaty trestných činov namierených proti šíreniu dezinformácií a to „šírenie nepravdivej informácie." V zmysle navrhovaného § 361a ods. 1: *„Kto vyrobí alebo rozširuje nepravdivú informáciu, ktorá je spôsobilá vyvolať nebezpečenstvo vážneho znepokojenia aspoň časti obyvateľstva nejakého miesta, ohroziť životy alebo zdravie ľudí alebo ovplyvniť obyvateľstvo pri jeho rozhodovaní o závažných otázkach celospoločenského významu alebo sa dopustí iného obdobného konania slovne alebo písomne, prostredníctvom elektronickej komunikačnej služby, zvukového záznamu, zvukovo -obrazového záznamu alebo iného záznamu, potrestá sa odňatím slobody na jeden rok až päť rokov."*[689] V zmysle navrhovanej skutkovej podstaty je objektom trestného činu ochrana obyvateľstva pred šírením nepravdivých informácií. Objektívna stránka je definovaná alternatívne a to prostredníctvom troch typov konania:

- Vyrobením nepravdivej správy, ktorá je spôsobilá vyvolať nebezpečenstvo vážneho znepokojenia aspoň časti obyvateľstva nejakého miesta, ohroziť životy alebo zdravie ľudí alebo ovplyvniť obyvateľstvo pri jeho rozhodovaní o závažných otázkach celospoločenského významu,
- Rozširovaním nepravdivej správy, ktorá je spôsobilá vyvolať nebezpečenstvo vážneho znepokojenia aspoň časti obyvateľstva nejakého miesta, ohroziť životy alebo zdravie ľudí alebo ovplyvniť obyvateľstvo pri jeho rozhodovaní o závažných otázkach celospoločenského významu,
- Dopustením sa iného obdobného konania slovne alebo písomne, prostredníctvom elektronickej komunikačnej služby, zvukového záznamu, audiovizuálneho záznamu alebo iného záznamu.

Subjekt navrhovaného trestného činu je všeobecný a z hľadiska subjektívnej stránky sa vyžaduje úmysel.

[688] NESVADBA, A. – MARKOVÁ, V. Šírenie dezinformácií a možné trestnoprávne následky v zmysle Trestného zákona. In MEDELSKÝ, J., LACA, N. 2022. *Dezinformácie a právo (úlohy a postavenie bezpečnostných zložiek).* Zborník príspevkov. Bratislava. Akadémia Policajného zboru v Bratislave, s. 169.

[689] *Návrh zákona, ktorým sa mení a dopĺňa zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony*. Dostupné na: https://www.slov-lex.sk/legislativne-procesy/-/SK/dokumenty/LP-2021-744.

Odborná literatúra podrobila navrhovanú právnu úpravu kritike z hľadiska použitia vágnych pojmov,[690] ktoré sme namietali už v úvodných častiach tejto práce.

Podľa navrhovaného § 362: *„Kto z nedbanlivosti opakovane rozširuje nepravdivú informáciu, ktorá je spôsobilá vyvolať nebezpečenstvo vážneho znepokojenia aspoň časti obyvateľstva nejakého miesta, ohroziť životy alebo zdravie ľudí alebo ovplyvniť obyvateľstvo pri jeho rozhodovaní o závažných otázkach celospoločenského významu, potrestá sa až na jeden rok.*"[691] Navrhovaná skutková podstata upravuje nedbanlivostnú modalitu. Z hľadiska objektívnej stránky je limitovaná na rozširovanie. Je však potrebné upozorniť, že v zmysle analýzy definícií dezinformácie sa vyžaduje úmysel nepravdivé informácie šíriť alebo rozširovať pravdivé informácie manipulatívnych spôsobom. Z tohto dôvodu a aj vzhľadom na úlohu trestného práva ako prostriedku *ultima ratio* nerozumieme nevyhnutnosti zakotvovať nedbanlivostnú formu zavinenia takéhoto trestného činu.

3.2.7 Činnosť a úlohy spravodajských orgánov

Šírenie dezinformácií je súčasťou vedenia hybridnej vojny prostredníctvom informačných operácií a na tento fakt reagovala aj slovenská legislatíva v roku 2022 v podobe prijatia nového zákona č. 500/2022 Z. z. o Vojenskom spravodajstve (ďalej len ako „Zákon o vojenskom spravodajstve"). Samotné Vojenské spravodajstvo je v zmysle daného zákona definované ako *„spravodajská služba, ktorá plní úlohy na úseku obrany, obranyschopnosti a bezpečnosti Slovenskej republiky v pôsobnosti Ministerstva obrany Slovenskej republiky*"[692] pričom tieto úlohy plní predovšetkým prostredníctvom spravodajskej činnosti a prijímania bezpečnostných opatrení na predmetnom úseku.[693] Spravodajskou činnosťou sa v zmysle diskutovaného zákona rozumie *„súhrn spravodajských, analytických a iných úkonov vykonávaných Vojenským spravodajstvom spravidla utajeným spôsobom vrátane zabezpečenia realizácie týchto úkonov a jej podpora, zameraných na získavanie informácií a vecí, a to aj používaním osobitných prostriedkov a využívaním osobitných oprávnení, sústreďovanie a vyhodnocovanie získaných informácií.*"[694] Právna úprava neobsahuje ani demonštratívny výpočet primeraných bezpečnostných opatrení.

[690] Napríklad NESVADBA, A. – MARKOVÁ, V. Šírenie dezinformácií a možné trestnoprávne následky v zmysle Trestného zákona. In MEDELSKÝ, J., LACA, N. 2022. *Dezinformácie a právo (úlohy a postavenie bezpečnostných zložiek)*. Zborník príspevkov. Bratislava. Akadémia Policajného zboru v Bratislave.

[691] *Návrh zákona, ktorým sa mení a dopĺňa zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony*. Dostupné na: https://www.slov-lex.sk/legislativne-procesy/-/SK/dokumenty/LP-2021-744.

[692] Zákon o vojenskom spravodajstve, § 4 ods. 1.

[693] Zákon o vojenskom spravodajstve, § 4 ods. 2.

[694] Zákon o vojenskom spravodajstve, § 3 ods. 1.

Z hľadiska dezinformácií je kľúčové, že v novej právnej úprave má Vojenské spravodajstvo explicitne ustanovenú povinnosť získavania, sústreďovania vyhodnocovania informácií na *„hybridné hrozby a dezinformácie, ak ohrozujú obranu alebo obranyschopnosť Slovenskej republiky."*[695] Dôvodová správa k novej povinnosti uvádza, že hybridné hrozby vrátane šírenia dezinformácií vznikajú pred deklarovanými vojenskými operáciami, pričom *„polarizujú spoločnosť, vnášajú neistotu, a tým podkopávajú legitimitu, dôveryhodnosť, akcieschopnosť štátnych inštitúcií a demokratický ústavný poriadok a majú negatívny vplyv na realizáciu bezpečnostných záujmov štátu."*[696] Dôvodová správa ďalej uvádza, že dezinformácie môžu mať rôznu podobu nepravdivého alebo zmanipulovaného textu, obrázku, videa alebo zvuku, ale aj pravdivej informácie, ktorá je podaná manipulatívnym spôsobom.[697] Vojenské spravodajstvo tak získalo nové úlohy s cieľom výraznejšie zabezpečiť obranu a obranyschopnosť Slovenskej republiky. Je nutné dodať, že činnosť Vojenského spravodajstva je v utajenom režime[698] a z tohto dôvodu nemáme údaje o plnení jeho úloh.

Zákon č. 46/1993 Z. z. o Slovenskej informačnej službe („Zákon o SIS") neupravuje úlohy v oblasti hybridných hrozieb prípadne dezinformácií ako právna úprava Vojenského spravodajstva. To však automaticky neznamená, že dezinformácie nie sú predmetom spravodajského záujmu Slovenskej informačnej služby (ďalej len „SIS"). Medzi úlohy SIS patrí získavanie, sústreďovanie a vyhodnocovanie informácií o zákonom stanovených predmetoch spravodajského záujmu, medzi ktoré patrí aj činnosť ohrozujúca ústavné zriadenie, územnú celistvosť a zvrchovanosť SR, činnosť smerujúca proti bezpečnosti SR, aktivity a ohrozenia v kybernetickom priestore, ak ohrozujú bezpečnosť štát či skutočnosti spôsobilé vážne ohroziť alebo poškodiť hospodárske záujmy SR.[699]

Či už v kontexte činnosti SIS alebo vojenského spravodajstva, dezinformácie sa môžu dostať pod drobnohľad spravodajských služieb. Môže ísť o situácie, ak je dezinformácie využívaná ako nástroj primárneho objektu spravodajského záujmu (cudzia spravodajská služba alebo teroristická organizácia) alebo má potenciál ohroziť záujem, ktorý ja zabezpečený spravodajskou činnosťou štátu ako napríklad obrana alebo bezpečnosti.[700]

[695] Zákon o vojenskom spravodajstve, § 5 ods. 1 písm. k).
[696] *Dôvodová správa k Zákonu o vojenskom spravodajstve*.
[697] Tamže.
[698] Zákon o vojenskom spravodajstve, § 2 ods. 3.
[699] Zákon o SIS, § 2 ods. 1.
[700] KUKLÍK, J. (Dez)informácie ako nástroj hybridnej hrozby optikou spravodajských služieb. In MEDELSKÝ, J., LACA, N. 2022. *Dezinformácie a právo (úlohy a postavenie bezpečnostných zložiek)*. Zborník príspevkov. Bratislava. Akadémia Policajného zboru v Bratislave, s. 106.

Osobitnou otázkou je autorizované šírenie dezinformácií prostredníctvom štátnych služieb proporcionálnym spôsobom ako jedno z bezpečnostných opatrení.[701]

[701] Tamže, s. 107 – 108.

4. KAPITOLA
TAXONÓMIA NÁSTROJOV VEREJNÉHO PRÁVA PRE BOJ S DEZINFORMÁCIAMI V ONLINE PRIESTORE A POSÚDENIE VHODNOSTI ICH VYUŽITIA

V predchádzajúcej kapitole sme sa obšírne venovali identifikácií konkrétnych nástrojov verejného práva pre boj s dezinformáciami v online priestore. Je na mieste konštatovať, že či už právo EÚ alebo Slovenskej republike poskytuje dostatočné množstvo týchto nástrojov. Pri niektorých z nich je na mieste otázka aplikačnej praxe. Zároveň, máme za to, že pri ich korektnej aplikácií by mali zohľadnené súvislosti s rešpektovaním slobody prejavu a práva na informácie, princíp proporcionality a poznatky z iných vedných odvetví, ktoré sme zhrnuli v prvej kapitole.

Z tohto dôvodu si dovolíme na tomto mieste navrhnúť tri nosné princípy, ktoré by mali byť pri aplikovaní nástrojov verejného práva pre boj s dezinformáciami aplikované. Následne prezentujeme taxonómiu nástrojov verejného práva pre boj s dezinformáciami a dáme ju do kontextu faktorov pôsobiacich na dôveru v dezinformácie a šírenie dezinformácií.

Princípy pri aplikovaní nástrojov verejného práva by mali byť nasledujúce:

- Rešpektovanie slobody prejavu a práva na informácie,
- Proporcionalita pri posudzovaní dezinformácií,
- Zohľadnenie faktorov pôsobiacich na dôveru v dezinformácie a šírenie dezinformácií.

V tejto kapitole taktiež pri konkrétnych nástrojov verejného práva pre boj s dezinformáciami v online priestore uvedieme niektoré naše návrhy a úvahy pre efektívnejšiu právnu úpravu.

4.1 Princípy pri využití nástrojov verejného práva pre boj s dezinformáciami v online priestore

4.1.1 Rešpektovanie slobody prejavu a práva na informácie

Pri diskusiách o rôznych nástrojoch pre boj s dezinformáciami vo všeobecnej rovine častokrát zaznieva argument potreby rešpektovania slobody prejavu a práva na informácie. Tieto práva sú pevnou súčasťou právneho rámca základných ľudských práv a slobôd tak v EÚ, ako aj v Slovenskej republike.

V zmysle článku 11 Charty základných práv a slobôd EÚ: *„Každý má právo na slobody prejavu. Toto právo zahŕňa slobodu zastávať názory a prijímať a rozširovať informácie a myšlienky bez zasahovania orgánov verejnej moci a bez ohľadu na hranice.*"[702] Druhý odsek predmetného článku zaručuje slobodu a pluralitu médií.[703] SDEÚ pri výklade článku 11 častokrát podporuje výklad Európskeho súdu pre ľudské práva pri otázkach slobody prejavu a práva na informácie. Jedným z cieľov daného práva je podpora verejných diskusií a participácia občanov na správe veci verejných.[704] Tento model demokratickej verejnej sféry je založený na myšlienke, že najlepšou zárukou pre kontrolu správy veci verejných je rovnováha medzi silami pôsobiacimi v štáte, čo si vyžaduje neustálu vzájomnú kontrolu, diskusiu a kritiku. Legislatíva „stráži" vedenie tohto sporu prostredníctvom možnosti argumentácie a kritiky. Ekonomický tlak, vyhrážky a dezinformácie teda nie sú zlučiteľné so slobodným utváraním názoru.[705]

Diskutovaná sloboda je koncipovaná ako pozitívna a negatívna sloboda. V negatívnom zmysle to znamená, že chráni pred zásahom zo strany štátu. V takomto kontexte je evidentné, že sloboda prejavu a právo na informáciu musia byť rešpektované aj pri právnych nástrojoch boja proti dezinformáciám v online priestore.[706] Z pohľadu pozitívneho záväzku chrániť slobodu prejavu a právo na informácie štát môže zaviesť mechanizmy na podporu predmetnej slobody. Zároveň ale pozitívna obligácia môže znamenať dohľad nad reguláciou pri moderovaní obsahu vrátane dezinformácií napríklad na sociálnych médiách.[707] SDEÚ vo veci Connolly proti Spojenému kráľovstvu[708] týkajúcej sa práva na slobodu prejavu zamestnanca inštitúcií EÚ, v súlade s judikatúrou ESĽP uviedol, že akékoľvek obmedzenia tohto práva sa musia vykladať reštriktívne a opatrenia predbežného obmedzenia resp. povahy si vyžadujú osobitnú pozornosť. Vyššie uvedené nazeranie na slobodu prejavu naznačuje, že SDEÚ by pravdepodobne nepodporil mechanizmy proti dezinformáciám, ktoré by mohli mať ochromujúci účinok (*chilling effect*), ako je cenzúra alebo kontinuálny online dohľad. V inom kontexte, SDEÚ naznačil, že opatrenia, ktorých cieľom je obmedziť šírenie dezinformácií, a nie ich úplné odstránenie, s väčšou pravdepodobnosťou spĺňajú kritérium proporcionality.[709]

[702] Charta, článok 11 ods. 1.
[703] Tamže, článok 11 ods. 2.
[704] BARENDT, E. *Freedom of Speech*. Oxford University Press, 2005, s. 19-20
[705] EUROPEAN PARLIAMENT, DIRECTORATE-GENERAL FOR INTERNAL POLICIES OF THE UNION, BATURA, O., HOLZNAGEL, B., LUBIANIE, K. The fight against disinformation and the right to freedom of expression, European Parliament. 2021. Dostupné na: https://data.europa.eu/doi/10.2861/305, s. 18.
[706] Tamže, s. 20.
[707] Tamže, s. 23.
[708] Rozhodnutie Súdneho dvora Európskej únie, sp. zn. C-274/99, Connolly v. Commission, bod. 39.
[709] Rozhodnutie Súdneho dvora Európskej únie , sp. zn. C-622/17, Baltic Media Alliance v. Lietuvos radijo.

Z pohľadu rozhodovacej praxe ESĽP sa ako kľúčové v kontexte dezinformácií javí rozhodnutie vo veci Salov proti Ukrajine.[710] V kontexte výkladu článku Dohovoru, ktorý ustanovuje slobodu prejavu uviedol, že tento článok je konštruovaný takým spôsobom, ktorý nezakazuje diskusiu alebo šírenie informácií aj keď existuje vážne podozrenie, že tieto informácie nie sú pravdivé. Opačný výklad by zbavil jednotlivca práva vyjadrovať svoje názory a stanoviská k tvrdeniam vyjadrených v masmédiách, a tým by sa neprimerane obmedzila sloboda prejavu.[711] Tento prípad sa však týkal šírenia nepravdivých informácií prostredníctvom tlačovín a nebral tak do úvahy potenciálne šírenie dezinformácií prostredníctvom virálneho online prostredia s nasadením techník umelej inteligencie.

Jediný doteraz rozhodovaný prípad, keď ESĽP ukázal nulovú toleranciu voči šíreniu nepravdivých informácií je popieranie holokaustu.[712] Je však nutné poukázať na fakt, že ESĽP svoje rozhodnutie nezaložil na porušení slobody prejavu, ale na článku Dohovoru ustanovujúceho zákaz zneužitia práv.[713] Výsledným efektom rozhodnutia pre sťažovateľov však je, že dezinformácie o holokauste nepožívajú ochranu slobody prejavu.

Ďalšie relevantné rozhodnutia v kontexte potenciálnych mechanizmov zamedzujúcich šírenie dezinformácií v online priestore sa týkali politického mikrocielenia (*microtargeting*) a komerčnej komunikácie. Analyzovaná judikatúra ESĽP[714] naznačuje, že obmedzenie mikrocielenej politickej reklamy by mohlo byť súladné s rešpektovaním slobody prejavu. Toto obmedzenie by napĺňalo ciele na zachovanie spoločného a zdravého informačného prostredia, pluralitu názorov a v konečnom dôsledku demokraciu. Legitímny cieľ takéhoto obmedzenia by mohol predstavovať ochranu pasívnej stránky slobody prejavu, t. j. prístupu k verejným informáciám pre všetkých členov spoločnosti.[715] Ako uvádzame v prvej kapitole, ekonomika pozornosti a kapitalizmus dohľadu slúžia na získanie primárne finančného profitu pre poskytovateľov digitálnych služieb. Z tohto dôvodu je aj komerčná komunikácia napríklad vo forme reklám alebo plateného obsahu predmetom diskusie cez prizmu slobody prejavu. V tejto súvislosti je nevyhnutné diskutovať rozhodnutia vo veci *Hertel* a *Raëlien Suisse.* Rozhodnutie ESĽP vo veci Hertel sa týka diskusia ohľadom škodlivých efektov mikrovlniek na ohrievané

[710] Rozhodnutie Európskeho súdu pre ľudské práva vo veci Salov v. Ukraine. Sťažnosť č. 65518/01, 6 September 2005.
[711] Tamže, bod 113.
[712] Rozhodnutie Európskeho súdu pre ľudské práva vo veci Garaudy v. France. Sťažnosť č. 65831/01, 24 June 2003.
[713] Dohovor, článok 17: *„Nič v tomto dohovore sa nesmie vykladať ako oprávnenie pre štát, skupinu alebo osobu vykonávať činnosť alebo uskutočniť skutok s cieľom narušiť práva alebo slobody v dohovore zakotvené, alebo na obmedzovanie týchto práv a slobôd vo väčšom rozsahu, než je stanovené v dohovore.*"
[714] Hlavne Rozhodnutie Európskeho súdu pre ľudské práva vo veci Animal Defenders International v. the United Kingdom, App. No. 48876/08, 22 April 2013, body 115 a nasledujúce.
[715] K tomu pozri napríklad Rozhodnutie Európskeho súdu pre ľudské práva vo veci Kenedi v. Hungary. Sťažnosť č. 31475/05, 26 May 2009, alebo Rozhodnutie Európskeho súdu pre ľudské práva vo veci Sdružení Jihočeské Matky v. Czech Republic. Sťažnosť č. 19101/03.

jedlo.[716] Štrasburský súd v tejto veci opakovane potvrdil, že takéto informácie môžu byť komunikované, avšak nemôžu byť prezentované ako vedecké fakty. Prípad *Raëlien Suisse* sa týkal štátneho zákazu propagácie podujatia organizáciou, ktorá okrem iného verila v mimozemský pôvod života na zemi.[717] Tieto prípady naznačujú, že ESĽP by mohol byť pripravený priznať širší priestor na posúdenie a klasifikovať ako kvázi-komerčné nepravdivé tvrdenia, ktoré neprispievajú k verejnej diskusii vo verejnom záujme a predstavujú riziko poškodenia práv iných osôb.[718]

Sloboda prejavu a právo na informácie sa zaručuje aj Ústavou Slovenskej republiky.[719] Článok 26 koncipuje slobodu prejavu a právo na informácie ako politické právo, v zmysle ktorého má každý slobodu prejavu a právo na informácie. *„ Každý má právo vyjadrovať svoje názory slovom, písmom, tlačou, obrazom alebo iným spôsobom, ako aj slobodne vyhľadávať, prijímať a rozširovať idey a informácie bez ohľadu na hranice štátu.*"[720] Diskutovaný článok zakazuje cenzúru[721] a umožňuje obmedziť slobodu prejavu a právo vyhľadávať informácie iba zákonom, *„ak ide o opatrenia v demokratickej spoločnosti nevyhnutné na ochranu práv a slobôd iných, bezpečnosť štátu, verejného poriadku, ochranu verejného zdravia a mravnosti.*"[722]

Ústavný súd Slovenskej republiky vo svojej rozhodovacej praxi nespája ochranu objektívnosti a nestrannosti foriem prejavu v masmédiách, aj keď Drgonec uvádza, že o tomto vzťahu je možné uvažovať.[723] Ústavný súd Slovenskej republiky v tomto kontexte dodáva: *„keďže právo prijímať informácie zahŕňa právo prijímať informácie tak pravdivé, overiteľné a neutrálne, ako aj fiktívne, neoveriteľné, nepravdivé alebo pravdu skresľujúce či prezentujúce určitý svetonázor. Aj informácie, ktoré sú fiktívne, nepresné a nezakladajú sa na pravde, podnecujú recipienta pri konfrontácii s informáciou prijímanou z iných početných zdrojov informácií k tej istej téme ku kritickému mysleniu a potencujú vôľu po vyhľadávaní a osvojení si iných názorov na tému. Uvedené smeruje k sebarealizácii človeka a podporuje nekončiaci spoločenský diskurz k téme. Ústavný súd hodnotí túto skutočnosť ako demokratický prvok slobodnej spoločnosti.*"[724] Ústavný

[716] Rozhodnutie Európskeho súdu pre ľudské práva vo veci Hertel v. Switzerland. Sťažnosť č. 25181/94, 25 August 1998.
[717] Tamže.
[718] EUROPEAN PARLIAMENT, DIRECTORATE-GENERAL FOR INTERNAL POLICIES OF THE UNION, BATURA, O., HOLZNAGEL, B., LUBIANIE, K. The fight against disinformation and the right to freedom of expression, European Parliament. 2021. Dostupné na: https://data.europa.eu/doi/10.2861/305, s. 30.
[719] 460/1992 Zb. Ústava Slovenskej republiky.
[720] Ústava Slovenskej republiky, článok 26 ods. 1.
[721] Tamže, článok 26 ods. 3.
[722] Tamže, článok 26 ods. 4.
[723] DRGONEC, J. *Ústava Slovenskej republiky – Komentár*. 2. vydanie. 2019. Praha: C.H. Beck. Dostupné na beck-online.sk.
[724] Nález Ústavného súdu SR, sp. zn. II. ÚS 307/2014 z 18. decembra 2014 . ZNUÚS 2014, s. 726 – 727.

súd Slovenskej republiky v súvislosti s rozhodovaním o dĺžke volebného moratória vyjadril niekoľko úvah aj v kontexte dezinformácií nakoľko autori zákona predlžujúceho moratórium na volebné prieskumy argumentovali práve šírením dezinformácií pri predĺžení moratória. Ústavný súd k tomu uviedol: *„Zo strany ústavného súdu by bolo nesprávne ponechať bez adekvátnej odozvy (prípadne ju mlčky akceptovať) argumentáciu zákonodarcu týkajúcu sa ochrany občanov pred dezinformáciami a účelovými informáciami. Žiadne takéto právo ústava ani dohovor neobsahujú. Občan na základe ústavy a ani dohovoru nemá právo na ochranu pred dezinformáciami a účelovými informáciami z dôvodu, že to neumožňuje sloboda prejavu a sloboda prijímať informácie. Už vôbec neexistuje pozitívna povinnosť štátu chrániť občanov či voličov pred dezinformáciami a účelovými informáciami.*"[725]

Z vyššie uvedených výrokov Ústavného súdu SR sa môže javiť, že ochrana obyvateľstva pred dezinformáciami môže naraziť na reštriktívny a limitujúci výklad tohto orgánu pri potenciálnych konaniach o súlade právnych predpisov s Ústavou SR. Posledná veta vyššie citovaného výroku dokonca vyjadruje neexistenciu ochrany občanov pred dezinformáciami, čo nemusí byť v súlade s politikami EÚ, ale aj rozhodovacou praxou SDEÚ a ESĽP.[726] Môžeme len hádať, akým spôsobom by sa Ústavný súd SR vysporiadal s konfliktom právnej úpravy limitujúcej šírenie dezinformácií v dnešnej situácií, keď virálne príspevky v online priestore môžu v konečnom dôsledku viesť k ujme na zdraví, bezpečnosti až živote.

Vo všeobecnosti možno konštatovať, že regulovať priamo dezinformačný obsah môže naraziť na limity rešpektovania slobody prejavu a práva na informácie. Z tohto dôvodu považujeme za vhodnejšie nastavenie regulácie na kontext šírenia dezinformácií a zároveň oporu v inom základnom ľudskom práve ako to vyvážil ESĽP v prípade popierania holokaustu.[727] Inou ilustráciou je zákaz vysielania ruských televízií Russia Today a Sputnik na území EÚ, ktoré v zmysle rozhodnutia Rady EÚ[728] ohrozovali národnú bezpečnosť, volebné procesy a občiansku spoločnosť. Práve z týchto dôvodov predmetný zákaz „prežil" aj hodnotenie kompatibility zo strany SDEÚ.[729]

---

[725] Nález Ústavného súdu Slovenskej republikym sp. zn. PL. ÚS 26/2019, bod 108.

[726] K tomu pozri aj SHATTOCK, E. Fake News in Strasbourg: Electoral Disinformation and Freedom of Expression in the European Court of Human Rights (ECtHR). In *European Journal of Law and Technology*, Vol 13 No.1 (2022).

[727] Zhodne BAYER, J. et al. *Disinformation and propaganda: impact on the functioning of the rule of law and democratic processes in the EU and its Member States - 2021 update*. Dostupné na: https://www.europarl.europa.eu/thinktank/en/document/EXPO_STU(2021)653633.

[728] *Rozhodnutie Rady (SZBP) 2022/351 z 1. marca 2022, ktorým sa mení rozhodnutie 2014/512/SZBP o reštriktívnych opatreniach s ohľadom na konanie Ruska, ktorým destabilizuje situáciu na Ukrajine*, Ú. v. EÚ L 65, 2.3.2022, s. 5 – 7

[729] Rozhodnutie Súdneho dvora Európskej únie vo veci *RT France v. Council of the European Union*, vec č. T-125/22.. Bližšie k tomu pozri KUDRNA, J. The possibilities of combating so-called disinformation in the context of the european union legal framework and of constitutional guarantees of freedom of expression in the european union

Z hľadiska vhodnosti regulačných zásahov v kontext dezinformácií možno rozlišovať reguláciu obsahu (samotný dezinformačný obsah), osobných údajov nevyhnutných pre potreby dezinformácií a pravidlá pre digitálne platformy.[730] Využitie konkrétneho nástroja však môže mať odlišné konotácie v súvislosti so slobodou prejavu a právom na informácie.

V prípade nástrojov smerujúcich na obsah možno hovoriť o trestnoprávnom alebo administratívnoprávnom postihu konkrétneho konania. Ide o dezinformácie, ktoré napĺňajú literu nelegálneho obsahu ako popierania holokaustu či extrémistických prejavov. Regulačné nástroje nemusia nevyhnutne smerovať iba k postihu jednotlivcov, ale aj napríklad digitálnych platforiem, ktoré môžu byť nútené na základe príkazov a požiadaviek zo strany štátu určitý obsah v časovom limite stiahnuť. Pri takýchto regulačných zásahov vždy musí existovať autorita, ktorá posudzuje pravdivosť informácií,[731] čo však z hľadiska sociologického efektu na spoločnosť nemusí byť vhodná alternatíva. Práve nástroje smerované na obsah a posudzovania pravdivosti môžu byť najväčším ohrozením z hľadiska slobody prejavu.[732] Avšak, posudzovanie obsahu a jeho kontrola na platformách by nemalo absentovať zo strany občianskej spoločnosti.

Regulácia prostredníctvom práva na ochranu osobných údajov smeruje predovšetkým k limitom z pohľadu mikro-sledovania jednotlivcov a následnému zobrazovaniu konkrétneho obsahu. Osobitne sa mikrocielenie presadzuje vo volebnej kampani. Údaje sú buď prostredníctvom všeobecnej alebo špecifickej regulácie relevantným subjektom legislatívy, pretože zohrávajú významnú úlohu v dynamike šírenia informácií na digitálnych platformách.[733] Takáto regulácia, nakoľko stojí na rešpektovaní práva na ochranu osobných údajov respektíve práva na súkromie, môže byť najmenej invazívna voči slobode prejavu.[734]

Tretím typom regulačnej aktivity je právna úprava digitálnych platforiem, ktorá týmto subjektom predpisuje rôzne požiadavky z hľadiska transparentnosti a zodpovednosti. Ohrozenie slobody závisí od konkrétnej požiadavky. Prirodzene, požiadavky na moderovanie obsahu môžu predstavovať väčší zásah ako požiadavky na transparentnosť. Podobne ako pri regulácií ochrany osobných údajov však platí, že nástroje prostredníctvom regulácie digitálnych

member states. In *International Comparative Jurisprudence*, 2022 Volume 8 Issue 2. Dostupné na: http://dx.doi.org/10.13165/j.icj.2022.12.002.

[730] IGLESIAS KELLER, C. Don't Shoot the Message: Regulating Disinformation Beyond Content. In *Direito Público*, Instituto Brasiliense de Direito Público – IDP, Brasília DF, Vol. 18, Iss. 99, s. 486-515. Dostupné na: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/6057.

[731] Tamže, s. 507 – 511.

[732] Tamže, s. 517.

[733] Tamže, s. 514.

[734] Tamže, s. 518.

platforiem nemusia nevyhnutne zasahovať do slobody prejavu v takej miere, ako pri regulácií obsahu.[735]

4.1.2 Proporcionalita pri posudzovaní dezinformácií

Druhým princípom, ktorý by mal byť rešpektovaný v kontexte zavádzania a aplikácia nástrojov na boj s dezinformáciami v online priestore je posúdenie ich proporcionality v kontexte daného nástroja a typu dezinformácie. Pre ilustráciu uvádzame niekoľko výrokov:

- *Zem je plochá doska* (Výrok 1),
- *Vakcíny proti nebezpečne nákazlivej chorobe spôsobujú výrazné negatívne vedľajšie účinky až smrť* (Výrok 2),
- *Najvyšší ústavní činitelia sú pod priamym vplyvom cudzej moci alebo elít* (Výrok 3).

Napriek tomu, že každý z vyššie uvedených výrokov predstavuje nebezpečenstvo pre zdravý informačný ekosystém, pri aplikácií konkrétnych právnych nástrojov je potrebné zohľadňovať ich negatívny potenciál, úmysel šírenia a vplyv na spoločnosť. Kým Výrok 1 predstavuje dezinformáciu s nízkym alebo minimálnym rizikom, ktorá je jednoducho vyvrátiteľná, Výrok 2 predstavuje či už v čase pandémie nebezpečne nákazlivých chorôb, ale aj dlhodobého zdravia spoločnosti výraznejšie riziko ako Výrok 1. Je to z toho dôvodu, že dôvera jednotlivcov k Výroku 2 môže mať za následok ohrozenie seba a iných na zdraví alebo živote. Najvážnejšie riziko predstavuj Výrok 3, ktorý priamo spochybňuje lojalitu najvyšších ústavných činiteľov alebo ich konanie vo verejnom záujme. Pri úspechu dezinformačných kampaní, ktoré by takýto naratív šírili je rizikom strata dôvery v inštitúcie, občianske nepokojne, veľká polarizácia spoločnosti či zvrhnutie demokracia a rozvrat právneho štátu. Nakoľko ide o základné piliere vládnutia, podobné aktivity by mali byť posudzované cez prizmu invazívnejších zásahov z pohľadu právnych nástrojov ako pri Výroku 1 alebo Výroku 2.

Z tohto dôvodu máme za to, že by mala existovať metodika posudzovania závažnosti vplyvu dezinformácií. Jednu z metodík posudzovania škodlivosti informačných operácií (vrátane dezinformácií) sme diskutovali v prvej kapitole. Diskutovaná metodika je súčasťou Koordinovaného mechanizmu odolnosti Slovenskej republiky voči informačným operáciám,[736] obsahuje 14 kritérií a po ich analýze je determinovaný vplyv na škále od nepatrného, znepokojujúceho až po vysoký a kritický. Predmetná metodika je zameraná na analýzu

[735] Tamže, s. 318 – 320.
[736] ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY. *Koordinovaný mechanizmus odolnosti Slovenskej republiky voči informačným operáciám*, s. 11 – 12.

škodlivosti informačných operácií vo všeobecnosti a preto nemusí nevyhnutne odzrkadľovať dezinformačné kampane, za ktorými nie je významný vplyv tretích strán alebo tretích krajín. Potrebu hodnotenia negatívnych vplyvov dezinformácií na základe definovaných kritérií vyjadruje aj odborná literatúra.[737]

Vhodnejšiu metodiku podľa nášho názoru predstavuje metodika od DisinfoLab, ktorá reflektuje riziko vplyvu (dopadu) dezinformácií z hľadiska ich virálnosti a angažovanosti subjektov.[738] Táto metodika upravuje 8 faktorov s bodovacím hodnotením, pričom výsledná hodnota ukazuje vplyv dezinformácie v podobe alarmujúcej, vysokej, strednej alebo nízkej. Predmetnú metodiku považujeme za vhodnú využitia aj na namapovanie taxonómie nástrojov verejného práva pre boj s dezinformáciami v online priestore s tým, že na niektorých miestach si dovolíme kritéria mierne upraviť a pridať komentár s ich relevanciou v Slovenskej republike v kontexte vyvíjajúcej sa judikatúry slovenských súdov v prípadoch týkajúcich sa dezinformácií.

Samotné kritéria predmetnej metodiky sú nasledujúce:

- Angažovanosť (*engagement*) na sociálnych sieťach: meranie zdieľaní a reakcií,
- Vystavenie (*exposure*) na sociálnych sieťach: meranie zobrazení,
- Cirkulácia obsahu: počet platforiem,
- Difúzia medzi komunitami: jazyk ako zástupný ukazovateľ,
- Dosah na mainstreamové média,
- Typ aktéra: verejne činné a trvalé osoby dezinformačné vysielače,
- Odlišné formáty dezinformácie,
- Výzva na konanie (*call to action*) a nebezpečenstvo príbehu: násobiteľ efektu dezinformácie.[739]

Vzhľad na širší kontext šírenia dezinformácií si dovoľujeme pridať niekoľko kritérií, ktoré podľa nášho názoru prispejú k vhodnejšej a efektívnejšej analýze šírenia dezinformácii:

[737] Napríklad KOZYREVA, A. et al. Incorporating Psychological Science Into Policy Making. The Case of Misinformation. In *European Psychologist*, 28(3), 2023, s. 206–224. Dostupné na: https://doi.org/10.1027/1016-9040/a000493.
[738] EU DISINFOLAB. *Towards an impact-risk index of disinformation: Measuring the virality and engagement of single hoaxes*. Dostupné na: https://www.disinfo.eu/publications/towards-an-impact-risk-index-of-disinformation-measuring-the-virality-and-engagement-of-single-hoaxes/.
[739] Tamže.

- Cieľ dezinformácie,
- Otázka verejného záujmu

Prvé kritérium v podobe angažovanosti reflektuje počet interakcií s konkrétnym príspevkom na online platforme. Väčší počet zdieľaní a reakcií vedie k vyššej virálnosti príspevku a šíreniu dezinformácie.[740] Toto kritérium spolu s ďalším kritériom v podobe vystavenie zohľadňujú aj slovenské súdy pri dezinformačných prejavoch. Ilustrovať to možno na rozhodovaní v spore medzi prezidentkou Zuzanou Čaputovou a poslancom Národnej rady SR Ľubošom Blahom, v ktorom okresný a krajský súd rovnako vyhodnotili virálnosť príspevkov označujúcich prezidentku ako agentku cudzích mocností, ktorá spáchala vlastizradu za dôležité kritérium.[741]

Druhým kritériom je vystavenie dezinformácie počtu užívateľov alebo jednotlivcov. Meria sa počet zobrazení konkrétneho príspevku.[742]

Tretím kritériom je počet online platforiem, na ktorých sa dezinformácia šíri.[743]

Štvrtým kritériom je počet jazykov, v ktorých sa dezinformácia v online priestore šíri. Vyšší počet jazykových mutácií ako jedna naznačuje vyššiu rizikovosť negatívneho vplyvu dezinformácií.[744]

Piatym kritériom je, či dezinformácia bola rozoberaná aj v mainstreamových médiách. Môže ísť o jej autentické šírenie alebo analýzu s cieľom dezinformáciu vyvrátiť.[745]

Šiestym kritériom je typ osoby, ktorý dezinformácie šíri. Vyššie riziko platí pri verene činných osobách, kde by sme nemali tieto osoby zužovať iba na predstaviteľov štátu alebo politikov, ale taktiež umelcov alebo influencerov s veľkým zásahom v online priestore. Kritérium zohľadňuje, aj či ide o opakované šírenie dezinformácií u konkrétneho subjektu.[746]

Siedme kritérium reflektuje, či sa dezinformácia šíri prostredníctvom viacerých formátov ako texty, videá, zvukové záznamy a iné.[747]

[740] Tamže.
[741] Uznesenie Okresného súdu Bratislava I. sp. zn. 21C/12/2022 zo dňa 22. 03. 2022 a Uznesenie Krajského súdu v Bratislave sp. zn. 5Co/95/2022 zo dňa 21. 07. 2022.
[742] Tamže.
[743] Tamže.
[744] Tamže.
[745] Tamže.
[746] Tamže.
[747] Tamže.

Ôsme kritérium reflektuje, či šírenie dezinformácie vyzýva ku konkrétnej aktivite ako napríklad verejné zhromaždenie, protest, nahlasovanie obsahu alebo obťažovanie konkrétnych jednotlivcov. Tento ukazovateľ je vzhľadom na svoju dôležitosť násobiteľom angažovanosti (prvé kritérium) na sociálnych sieťach.[748]

Zároveň máme za to, že navrhovaná metodika by mala odzrkadľovať ďalšie faktory. Deviatym kritériom by mala byť analýza toho, čo je cieľom dezinformácie. Cieľom dezinformácie totiž môže byť jednotlivec, skupina osôb až štátne zriadenie. Intenzita pri odlišných cieľoch je iného rizika. Vyššie riziko pri šírení dezinformácií o skupine obyvateľov alebo komunite hodnotia aj slovenské súdy, čo možno ilustrovať na odsúdení šéfredaktora časopisu Zem a Vek za článok s antisemitským obsahom.[749]

Desiatym kritériom by malo byť reflektované, či obsahom dezinformácie je vec verejného záujmu. V prípade sporu medzi lekárom Petrom Sabakom a poslancom Národnej rady Slovenskej republiky Milanom Mazurekom okresný súd a aj krajský súd potvrdil, že ak ide o vec verejného záujmu ako napríklad verejné zdravie, nemožno aplikovať širší výklad slobody prejavu.[750]

Kritérium	Meranie	Body
Angažovanosť	0 - 1 000 zdieľaní a reakcií = 0 bodov 1 001 - 10 000 zdieľaní a reakcií = 1 bod 10 001 - 100 000 zdieľaní a reakcií = 2 body Viac ako 100 001 zdieľaní a reakcií = 3 body	0-3
Vystavenie	0 – 1.000 zobrazení = 0 bodov 1.001 – 10.000 zobrazení = 1 bod 10.001 – 100.000 zobrazení = 2 body	0-2
Počet platforiem	Obsah zdieľaný na jednej alebo dvoch platformách = 0 bodov Obsah zdieľaný na viac ako dvoch platformách = 1 bod	0-1
Počet jazykov	Obsah šírený v jednom jazyku = 0 bodov Obsah šírený vo viac ako jednom jazyku = 1 bod	0-1
Dosah na mainstreamové médiá	Obsah sa nedostal do hlavných médií = 0 bodov Obsah sa dostal aspoň do jedného mainstreamového média = 1 bod	0-1

[748] Tamže.
[749] Rozsudok Špecializovaného trestného súdu sp. zn. 2T/31/2019 zo dňa 16. 12. 2019 a Uznesenie Najvyššieho súdu sp. zn. 2To/4/2020 zo dňa 26. 10. 2021.
[750] Uznesenie Okresného súdu Kežmarok sp. zn. 8C/71/2021 zo dňa 06. 12. 2021 a Uznesenie Krajského súdu v Prešove sp. zn. 9Co/14/2022 zo dňa 29. 03. 2022.

Typ aktéra	Šíriteľ/zosilňovač nie je verejnou osobou žiadneho druhu = 0 bodov Šíriteľ/zosilňovač je verejne známa osoba a/alebo sa opakovane vyskytuje ako dezinformátor, ktorý bol už predtým preverený = 1 bod	0-1
Formát	Obsah šírený výlučne v jednom formáte = 0 bodov Obsah šírený vo viac ako jednom formáte = 1 bod	0-1
Výzva na konanie	Obsah neobsahuje žiadne nabádanie = 0 bodov Angažovanosť je 0. Potom angažovanosť x nabádanie je 0 x 0 = 0 výzva na konanie: 0 bodov Angažovanosť je 1. Potom 1 x 0 = 0 -> výzva na konanie: 0 bodov Angažovanosť je 2. Potom 2 x 0 = 0 -> výzva na konanie: 0 bodov Angažovanosť je 3. Potom 3 x 0 = 0 -> výzva na konanie: 0 bodov Obsah obsahuje nabádanie = 1 bod s násobiteľom: Potom angažovanosť x nabádanie je 0 x 1 = 0 výzva na konanie: 0 bodov Angažovanosť je 1. Potom 1 x 1 = 1 -> výzva na konanie: 1 bod Angažovanosť je 2. Potom 2 x 1 = 1 -> výzva na konanie: 2 body Angažovanosť je 3. Potom 3 x 1 = 3 -> výzva na konanie: 3 body	0-3 a ich násobky
Cieľ dezinformácie	Cieľom dezinformácie je: Jednotlivec = 1 bod Skupina ľudí alebo komunita = 2 body Štát alebo demokratické zriadenie = 3 body	1-3
Vec verejného záujmu	Obsah nesúvisí s vecami verejného záujmu = 0 bodov Obsah súvisí s vecami verejného záujmu = 1 bod	0-1

Tabuľka: Atribúty posudzovania škodlivosti dezinformácií.
Zdroj: Disinfo.eu, vlastný výskum autora.

Konkrétna dezinformácia môže získať hodnotu od 0 do 17 bodov aplikovaním vyššie uvedenej metodiky. Podľa získaných bodov možno následne dezinformácie diferencovať ohľadom ich vplyvu na:

Bodové ohodnotenie	Vplyv
17-14	Alarmujúci
13 – 9	Vysoký
8 – 4	Stredný
0 - 3	Nízky

Tabuľka: Hodnotenie vplyvu škodlivosti dezinformácií.
Zdroj: Disinfo.eu, vlastný výskum autora.

4.1.3 Zohľadnenie faktorov pôsobiacich na dôveru v dezinformácie a šírenie dezinformácií

Tretím princípom pri aplikovaní nástrojov verejného práva by malo byť zohľadnenie faktorov vplývajúcich na ich šírenie a dôveru v takéto informácie. Nie je účelné riešiť dizajn online platforiem alebo nedostatky v kritickom myslení trestnoprávnou rovinou. Z tohto dôvodu máme za to, že nástroje verejného práva pri boji s dezinformáciami v online priestore by mali zohľadňovať poznatky z mimo-právnych vied. Základné faktory sme uviedli v prvej kapitole. Pre pripomenutie ich uvádzame aj v prehľadnej tabuľke:

Oblasť	Faktory
Psychológia	Kognitívne faktory ako intuitívne premýšľanie, kognitívne zlyhania a iluzórna pravda
	Sociálne afektívne faktory ako zdroj informácie, emócie a názory a viera adresáta informácie
Sociológia	Úbytok sociálneho kapitálu
	Nárast nerovnosti
	Zvyšujúcu sa polarizáciu spoločnosti
	Nedôvera vo vedu
	Evolúciu mediálneho prostredia
Ekonómia	Ekonomika pozornosti
	Dohľad kapitalizmu
Technické faktory	Personalizácia obsahu odporúčacími systémami (umelá inteligencia)
	Filtračné bubliny

Tabuľka: Faktory ovplyvňujúce dôveru a šírenie dezinformácií.
Zdroj: Výskum autora.

Kozyreva a kolektív zákonodarcom pri regulovaní fenoménu dezinformácií odporúčajú sústredenie na konanie tvorcu alebo šíriteľa na základe merateľných faktorov ako neautentické správania (falošné účty) alebo opakované zdieľanie dezinformácií.[751]

4.2 Taxonómia nástrojov verejného práva pre boj s dezinformáciami v online priestore

V tretej kapitole predkladanej práce sme identifikovali niekoľko kľúčových právnych aktov a konkrétnych nástrojov verejného práva pre boj s dezinformáciami online. Na tomto mieste si dovolíme tieto nástroje zhrnúť ako podklad pre nasledujúcu stať, v ktorej ich budeme hodnotiť z hľadiska vhodného legislatívneho uchopenia, princípu proporcionality a faktorov ovplyvňujúcich šírenie a dôveru v dezinformácie v online priestore. Pri analýze konkrétnych nástrojov sme zohľadňovali reguláciu digitálnych služieb na úrovni EÚ, návrhu aktu o umelej inteligencií na úrovni EÚ, legislatívu na ochranu osobných údajov EÚ, špecifické nástroje správneho práva ako priestupkové právo, mediálne právo a osobitné právne úpravy zvyšujúce transparentnosť a zodpovednosť digitálnych platforiem. Pozornosť sme venovali aj vyvodzovaniu trestnoprávnej zodpovednosti za šírenie nepravdivých správ a činnosti spravodajských zložiek štátu. Nižšie uvádzame konkrétne nástroje, či ide o systematický alebo individuálny nástroj a jeho adresáta:

Právna úprava	Nástroj	Systémový / Individuálny	Adresát
Akt o digitálnych službách (DSA)	Posudzovanie a zmierňovanie rizík	Systémový	Digitálna platforma
	Auditovanie	Systémový	Digitálna platforma
	Požiadavky na odporúčacie systémy	Systémový	Digitálna platforma
	Požiadavky na transparentnosť	Systémový	Digitálna platforma
	Požiadavky na dizajn platforiem	Systémový	Digitálna platforma
	Požiadavky na zobrazovanie reklamy	Systémový	Digitálna platforma
	Dôveryhodní nahlasovatelia, prístup k údajom	Systémový	Občianska spoločnosť

[751] KOZYREVA, A. et al. Incorporating Psychological Science Into Policy Making. The Case of Misinformation. In *European Psychologist*, 28(3), 2023, s. 206–224. Dostupné na: https://doi.org/10.1027/1016-9040/a000493.

	Zodpovednosť za obsah tretí strán	Systémový	Digitálna platforma
Návrh aktu o umelej inteligencií (AIA)	Požiadavky na kvalitu a správu údajov	Systémový	Poskytovateľ AI systému vysokého rizika
	Požiadavky na ľudský dohľad	Systémový	Poskytovateľ AI systému vysokého rizika
	Požiadavky na presnosť, spoľahlivosť a kybernetickú bezpečnosť	Systémový	Poskytovateľ AI systému vysokého rizika
	Vykonanie posúdenia vplyvu na základné ľudské práva a slobody	Systémový	Poskytovateľ AI systému vysokého rizika
	Požiadavky na generatívne systémy AI	Systémový	Poskytovateľ AI systému vysokého rizika
	Požiadavky transparentnosti vrátane deepfakes	Systémový	Poskytovateľ AI systému vysokého rizika
Zákon o mediálnych službách	Konanie vo veci zamedzenia šírenia nelegálneho obsahu	Hybridný	Orgán verejnej moci / Jednotlivec
Návrh zákona o opatreniach na zvýšenie bezpečnosti a dôveryhodnosti platforiem v on-line prostredí	Požiadavky na transparentnosť a zodpovednosť digitálnych služieb	Systémový	Digitálna platforma
Zákon o kybernetickej bezpečnosti	Blokovanie webových stránok	Systémový	Orgán verejnej moci / Jednotlivec
Všeobecné nariadenie o ochrane osobných údajov (GDPR)	Požiadavky na automatizované individuálne rozhodovanie	Hybridný	Prevádzkovateľ osobných údajov
	Posúdenie vplyvu na ochranu údajov	Systémový	Prevádzkovateľ osobných údajov
	Špecificky navrhnutá a štandardná ochrana osobných údajov	Systémový	Prevádzkovateľ osobných údajov
	Právo na opravu	Individuálny	Dotknutá osoba
	Právo na vymazanie	Individuálny	Dotknutá osoba
	Právo namietať	Individuálny	Dotknutá osoba
	Právo domáhať sa ochrany na dozornom orgáne alebo súde	Individuálny	Dotknutá osoba

Zákon o priestupkoch	Priestupky vyskytujúce sa na viacerých miestach správy	Hybridný	Orgán verejnej moci / Jednotlivec
	Priestupky na úseku zdravotníctva	Hybridný	Orgán verejnej moci / Jednotlivec
	Priestupky proti verejného poriadku	Hybridný	Orgán verejnej moci / Jednotlivec
	Priestupky proti občianskemu spolunažívaniu	Hybridný	Orgán verejnej moci / Jednotlivec
Trestný zákon	Trestný čin ohovárania	Hybridný	Orgán verejnej moci / Jednotlivec
	Trestný čin šírenia poplašnej správy	Hybridný	Orgán verejnej moci / Jednotlivec
	Trestný čin ohrozenia bezpečnosti vzdušného dopravného prostriedku a lode	Hybridný	Orgán verejnej moci / Jednotlivec
	Trestný čin falšovania a vyhotovenia nepravdivej zdravotnej dokumentácie	Hybridný	Orgán verejnej moci / Jednotlivec
	Trestný čin teroristického útoku	Hybridný	Orgán verejnej moci / Jednotlivec
	Návrh osobitnej skutkovej podstaty trestného činu šírenia dezinformácií	Hybridný	Orgán verejnej moci / Jednotlivec
Zákon o slovenskej informačnej službe **Zákon o vojenskom spravodajstve**	Činnosť a úlohy spravodajských orgánov	Systémový	Orgán verejnej moci

Tabuľka: Nástroje verejného práva v boji proti dezinformáciám v online priestore.
Zdroj: Výskum autora.

Je zjavné, že šírenie dezinformácií neodstráni jeden právny nástroj[752] a zároveň platí, že štát nie je jediným zainteresovaným subjektom, ktorý môže pri zamedzení šírenia dezinformácií pomôcť. Malo by ísť o úzku symbiózu spolupráce medzi štátom, digitálnymi platformami a občianskou spoločnosťou. Rola digitálnych platforiem je primárne pri monitorovaní obsahu na svojej službe a moderovaní obsahu, spolupráci s ostatnými

[752] K diskusií ohľadom ďalších nástrojov pozri napríklad KOBERNJUK, A. - KASPER, A. Normativity in the EU's Approach towards Disinformation. In *TalTech Journal of European Studies*,11(1), s. 170-202. Dostupné na: https://doi.org/10.2478/bjes-2021-0011 alebo GARCÍA BOUZA, L. – OLEART, A. Regulating Disinformation and Big Tech in the EU: A Research Agenda on the Institutional Strategies, Public Spheres and Analytical Challenges. In *JCMS* 2023 s. 1–13.

zainteresovanými subjektami a definovaní a vymáhaním svojich pravidiel a príslušnej legislatívy. Občianska spoločnosť by mala byť ostražitá, upozorňovať na potenciálne zlyhania digitálnych platforiem a ich riziká, aktívne sa podieľať na formovaní zdravého informačného ekosystému a zároveň sledovať štát, či prijímané právne akty sú v súlade s princípom proporcionality a slobodou prejavu. Štát by mal vyžadovať prostredníctvom legislatívy transparentnosť a zodpovednosť digitálnych platforiem, chrániť demokratické hodnoty, pluralitu médií a poskytnúť jednotlivcom nástroje a prostriedky na ochranu pred dezinformáciami.[753]

Zároveň, ako uvádza Harrison, ak fenomén dezinformácií budeme regulačne ignorovať, dezinformácie zamoria informačný priestor a stanú sa mainstreamom. Naopak, ak ich pre-regulujeme, zvýši to nedôveru v štát a média a môže to spôsobiť ochladzujúci efekt na slobodu prejavu.[754]

4.3 Posúdenie vhodnosti nástrojov verejného práva pre boj s dezinformáciami v online priestore

V tejto časti syntetizujeme poznatky uvedené v predchádzajúcich kapitolách a predstavíme nástroje verejného práva pre boj s dezinformáciami online, ktoré sú vhodné podľa miery rizika a negatívne vplyvu v zmysle metodiky uvedenej v časti 4.1.2. Zároveň si uvedomujeme, že niektoré nástroje je potrebné vnímať na meta-úrovni. To znamená, že by mali byť využívané bez ohľadu na mieru rizika s cieľom minimalizovať škody na kvalitnom informačnom ekosystéme.

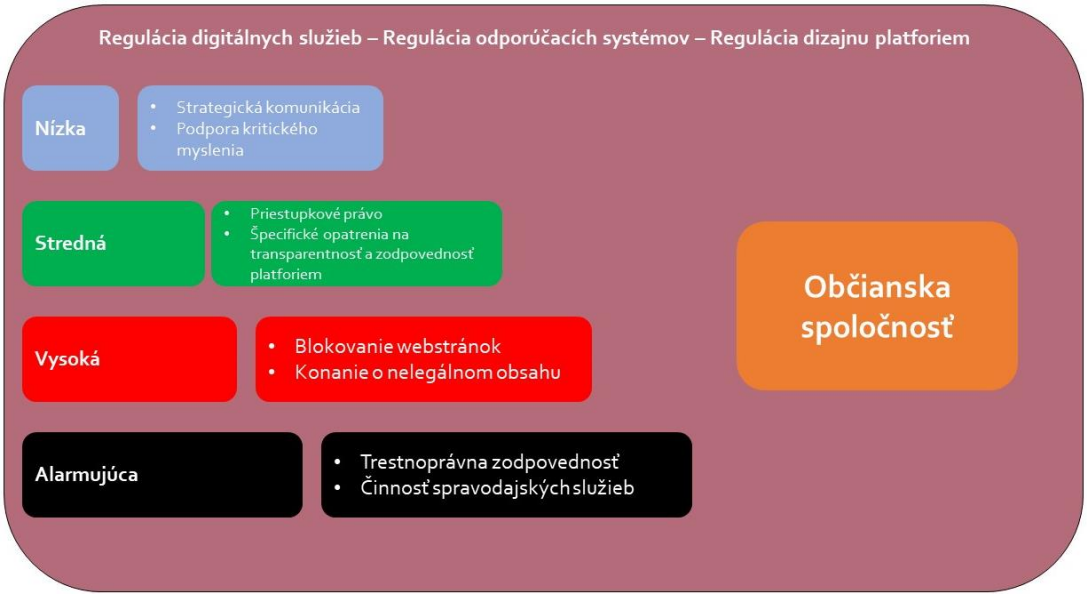
Zároveň je potrebné zvýrazniť, že individuálne nástroje je možné využiť v zásade pri akomkoľvek ohrození práv a záujmov jednotlivca. Nie je preto účelné ich subsumovať pod konkrétnu intenzitu rizika.

Taktiež platí, že každý nástroj o úroveň nižšie je prirodzene možné využiť aj pri boji s dezinformáciami vyššieho rizika. To znamená, že nástroje pre nízku alebo strednú úroveň rizika je možné využiť aj pre vysokú alebo alarmujúcu úroveň. Naopak to ale neplatí.

---

753 GOLDZWEIG, R. *Disrupted Democracies: A multistakeholder approach to fight disinformation*. 2021. Dostupné na: https://www.ippi.org.il/disrupted-democracies-a-multistakeholder-approach-to-fight-disinformation/.

754 HARRISON, R. *Tackling Disinformation in Times of Crisis: The European Commission's Response to the Covid-19 Infodemic and the Feasibility of a Consumer-centric Solution.* 17(3) Utrecht Law Review, 2021 s. 18–33. DOI: https://doi.org/10.36633/ulr.675.



Obrázok: Nástroje verejného práva pre boj s dezinformáciami online v kontexte škodlivosti dezinformácií.
Zdroj: Vlastná tvorba autora.

4.3.1 Nástroje verejného práva pre boj s dezinformáciami v online priestore pôsobiace na všetkých úrovniach vplyvu

Na začiatku tretej kapitoly sme spomínali delenie právnych nástrojov pre boj s dezinformáciami v online priestore na systémové a individuálne, priame a nepriame. Medzi nepriame nástroje zaraďujeme také, ktoré regulujú hlavné amplifikátory dezinformácií a to konkrétne digitálne služby a odporúčacie systémy (AI systémy) na digitálnych službách. Práve reguláciu týchto nástrojov považujeme za esenciálnu pre vytvorenie zdravého informačného priestoru. Z tohto dôvodu by mali pôsobiť na všetkých úrovniach rizík.

Z pohľadu škodlivého obsahu, vrátane dezinformácií za kľúčové považujeme inštitúty posudzovania a zmierňovania rizík a auditovania. Korektná a efektívna aplikácia týchto inštitútov môže viesť k výraznej zmene v dizajne platforiem, ktorá nebude umožňovať zvýraznenie škodlivého obsahu alebo umožní označovanie takéhoto obsahu či zákaz reklamy obsahujúcej dezinformácie. Analýza rizík z hľadiska spracúvania osobných údajov vyplýva aj z povinnosti vykonať posúdenie vplyvu na ochranu údajov podľa GDPR. Zároveň, skutočne nezávislý audit môže predmetné riziká odhaliť alebo poukázať na ich nedostatočné zmierňovanie. Dôsledná analýza rizík môže odhaliť uzatváranie užívateľov do filtračných bublín alebo komôr s ozvenou (*echo chambers*)

Za výrazné mínus DSA považujeme, že od účinnosti daného nariadenia nebola legislatívne zakotvená možnosť vypnutia odporúčacích systémov. To znamená, že všetkým užívateľom by digitálne platforma štandardne odo dňa účinnosti DSA vypla odporúčanie a užívatelia by si ho museli zapnúť sami, ak by o takýto krok mali záujem. Osobitne zdôrazňuje požiadavky transparentnosti na zobrazovaný obsah a reklamy. Zverejňovanie a možná zmena nastavenia odporúčacích systémov je krokom vpred, ktorý môže ovplyvniť informačný obsah ponúkaný konkrétnemu užívateľovi.

Za kľúčové považujeme, aby sa regulácia umelej inteligencie zamerala na odporúčacie systémy ako systémy AI vysokého rizika, čo by prinieslo viac požiadaviek z hľadiska kvality údajov, ľudského dohľadu alebo presnosti. Osobitne potreba ľudského dohľadu býva zvýrazňovaná aj odbornou literatúrou pri využití automatizovaných nástrojov.[755] Zároveň je osobitne potrebne zvýrazniť potrebu transparentnosti pri generovanom obsahu systémami AI a požiadavkami na takéto systémy. Máme za to, že jednotlivec by mal jednoznačne vedieť okamžite identifikovať, že interaguje s generovaným obsahom systémom AI prostredníctvom viditeľného oznámenia alebo označenia. Taktiež platí, že tieto modely by pri ich nasadení mali spĺňať špecifické požiadavky na transparentnosť zdrojov, na základe ktorých boli natrénované, aby sa zamedzilo negatívnym vplyvom na ľudské práva, demokraciu a právny štát.

Za výrazné meta-nástroje považujeme aj dizajn platforiem a požiadavky na automatizované individuálne rozhodovanie v zmysle GDPR. Dizajn platforiem by nemal zvádzať k manipulácií užívateľov a ich správania.[756] Totožné konštatovanie platí aj pre nastavenie odporúčacích systémov z pohľadu spracúvania osobných údajov.[757] Vyššie uvedené ustanovenia by mali nabádať poskytovateľov online platforiem a prevádzkovateľov osobných údajov zohľadňovať riziká vplyvu dezinformácií pri kreovaní svojich produktov a služieb. Problémom je aplikačná prax. Porušenie článku 25 GDPR posudzujú dozorné orgány spravidla ako „prívesok" pri porušení iných noriem. Jedinou výnimkou je prípad Mety pri uložení sankcie 265 miliónov eur výlučne za porušenie požiadaviek článku 25 GDPR.[758] Je teda možné, že v budúcnosti bude tento nástroj efektívnejší. Dizajn platforiem výrazne ovplyvňujú ekonomické faktory spôsobujúce monetizáciu informácií a osobitne dezinformačného obsahu. Piliere, na ktorých je založená ekonomika pozornosti a kapitalizmus dohľadu sú práve tie, na ktoré

[755] MARSDEN, CH. – MEYER, T. – BROWN, I. Platform values and democratic elections: How can the law regulate digital disinformation? In *Computer Law & Security Review,* Volume 36, April 2020, 105373.
[756] DSA, článok 25.
[757] GDPR, článok 25.
[758] DATA PROTECTION COMMISSION. *Data Protection Commission announces decision in Facebook "Data Scraping" Inquiry*. Dostupné na: https://dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-in-facebook-data-scraping-inquiry.

regulácia digitálnych služieb prostredníctvom požiadaviek na dizajn, transparentnosť a zodpovednosť cieli.

Automatizované individuálne rozhodovanie môže za istých okolností predstavovať ďalší nástroj na pozadí boja s dezinformáciami v online priestore. Ide o systémovú požiadavku, ktorá ale rezultuje v konkrétne individuálne práva dotknutej osoby. V prípade aplikácie na odporúčacie systémy by znamenala viac informovanosti a hmatateľných práv pre dotknuté osoby.

Vo všeobecnej súvislosti sú pre tvorbu zdravého informačného ekosystému dôležité nástroje občianskej spoločnosti, ktorá by mala byť ostražitá voči digitálnym platformám a zároveň strážiť dodržiavanie slobody prejavu pri prijímaní regulácií zo strany štátu. Inštitúty preverených výskumníkov a ich prístupu k údajom alebo dôveryhodných nahlasovateľov by mali podľa nášho názoru pôsobiť aj v rámci preventívnej funkcie na všetkých úrovniach rizika. Práve inštitút dôveryhodných nahlasovateľov môže pomôcť pri obnove dôvery vo vedecké poznanie.

4.3.2 Nástroje verejného práva pre boj s dezinformáciami v online priestore pri nízkom vplyve

Pri nízkom vplyve dezinformácií máme za to, že nie sú potrebné invazívne nástroje verejného práva. V tomto smere si dovoľujeme zvýrazniť aj mimoprávne nástroje, ktoré by mali byť schopné posilniť kritické myslenie a reflektovať potrebu odlíšenia pravdivých informácií od nepravdivých. Jedným z nástrojov pre tento účel sa javí strategická komunikácia štátu, v Slovenskej republike prijatá vládou SR v lete 2023 spolu s Koncepciou boja proti hybridným hrozbám a Akčným plánom koordinácie boja proti hybridným hrozbám diskutovaným v druhej kapitole.

4.3.3 Nástroje verejného práva pre boj s dezinformáciami v online priestore pri strednom vplyve

Pri strednom vplyve dezinformácií by mali orgány verejne moci konať a pôsobiť reaktívne a zároveň aj preventívne. Máme za to, že v tejto sfére sú vhodné predovšetkým dva nástroje verejného práva a to konkrétne (i) špecifické právne úpravy vyžadujúce transparentnosť a zodpovednosť digitálnych platforiem a (ii) priestupkové právo.

Momentálne, Slovenská republika nemá prijaté špecifické ustanovenia vyžadujúce transparentnosť a zodpovednosť digitálnych platforiem. Napriek tomu, že v roku 2023 bol do medzirezortného pripomienkového konania predložený návrh zákona o opatreniach na

zvýšenie bezpečnosti a dôveryhodnosti platforiem v on-line prostredí, vzhľadom na vysoký počet odborných pripomienok je veľmi pravdepodobné, že sa nikdy nestane realitou. Podobná právna úprava totiž musí rešpektovať primát práva EÚ v podobe Aktu o digitálnych službách a postavenie nezávislých orgánov, ktorým by boli zverené podobné úlohy. Nemecký NetzDG bude po nadobudnutí plnej účinnosti DGA zrušený a nahradený transpozičnou normou, ktorá ale nerieši dezinformácie.[759] Napriek tomu je nutné poznamenať, že manévrovací priestor pre členské štáty EÚ v boji proti dezinformáciám existuje a to minimálne v podobe regulácie platforiem, na ktoré sa DSA nevzťahuje (ako napríklad Telegram a iné). Otázne je, nakoľko jednotlivé členské štáty EÚ môžu takúto právnu úpravu prijať, pretože rozhodovacia prax SDEÚ konštantne potvrdzuje, že digitálne platformy majú plniť požiadavky krajiny usadenia.[760] Priestor sa ponúka iba pri prevádzkovateľoch, ktorí nemajú na území EÚ svojho zástupcu. Zároveň ostávajú v platnosti tzv. mäkké opatrenia, ktorými disponuje napríklad Rada pre mediálne služby pri komunikácií s digitálnymi platformami a ktoré sa osvedčili po teroristickom útoku na Zámockej ulici v Bratislave.[761]

Druhým vhodným nástrojom pri strednom vplyve dezinformácií je priestupkové právo. Bolo by to však možné iba za podmienky úmyselného zavinenia, nakoľko jedným z definičných znakov dezinformácie je práve úmysel šíriť alebo tvoriť informácie manipulatívnym spôsobom. Vo všeobecnej rovine, je podľa nášho názoru možné šírenie dezinformácií subsumovať pod skutkové podstaty priestupkov proti verejnému poriadku v podobe vzbudenia verejného pohoršenia a v prípade dezinformácií o jednotlivcoch aj priestupky proti občianskemu spolunažívaniu v podobe ublíženia na cti a vyhrážanie.

4.3.4 Nástroje verejného práva pre boj s dezinformáciami v online priestore pri vysokom vplyve

Pri vysokom vplyve dezinformácií by mali orgány verejne moci konať prostredníctvom minimálne dvoch už pomerne invazívnych prostriedkov, ktoré verejné právo ponúka. Konkrétne máme na mysli blokovanie webstránok a konanie o zamedzení šírenia nelegálneho obsahu.

[759] LOVELLS, H. *Online Regulation: Germany's plans to tackle "digital violence" (and likely other issues, too)*. Dostupné na: https://www.lexology.com/library/detail.aspx?g=67cc1c39-dc71-4a05-9843-54207bc331c2.
[760] Rozhodnutie Súdneho dvora EÚ z 9. novembra 2023 vo veci C-376/22, Google Ireland Limited, Meta Platforms Ireland Limited, Tik Tok Technology Limited proti Kommunikationsbehörde Austria (KommAustria).
[761] RADA PRE MEDIÁLNE SLUŽBY. *Teroristický útok na Zámockej ulici v Bratislave: bezprostredné a preventívne aktivity Rady pre mediálne služby na zamedzenie šírenia nelegálneho a škodlivého obsahu. Správa o reakciách digitálnych platforiem na útok a o ich podiele na radikalizácii páchateľa*. Dostupné na webovom sídle Rady pre mediálne služby.

Blokovanie webstránok na základe šírenia škodlivých dezinformácií v našom právnom poriadku existuje, ale momentálne je daný mechanizmus neúčinný. Ako sme uviedli v tretej kapitole, ide o mimoriadne invazívny prostriedok nielen z pohľadu práva na informácie a slobody prejavu, ale aj práva na podnikanie či súkromie. Preto je veľmi dôležité, aby právna úprava blokovanie webstránok spĺňala kritéria, ktoré na ňu kladie konštantná judikatúra SDEÚ a ESĽP. Technická realizácia blokovania a jej vhodnosť by mala byť taktiež zohľadnená.

Súčasná právna úprava blokovania je nedostatočná a nespĺňa tieto štandardy. V prvom rade by mal zákonodarca pri prijímaní takéhoto mechanizmu vykonať komplexné posúdenie vplyvu v legislatívnom procese, čo sa nestalo. Zákonodarca by mal analyzovať všetky potenciálne pozitívne a negatívny vplyvy na základné ľudské práva a slobody a vyhodnocovať, či legislatívne nastavený proces blokovania webstránok je nastavený správne, proporcionálne a naozaj v nevyhnutnej miere.

V druhom 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 užívateľ mal mať hneď informáciu, že stránka bola zablokovaný zo špecifických dôvodov a s odkazom na rozhodnutie. Zároveň, proces vyhodnocovania dezinformácií by mal byť tiež 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.

V treťom rade by celý mechanizmus mal mať nezávislý dohľad. Nemôže ísť o blokovanie po rozhodnutí orgánu výkonnej 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. Ako vhodný kandidát sa javí Najvyšší správny súd Slovenskej republiky, ktorý by v určenej lehote posudzoval splnenie kritérií na blokovanie po návrhu orgánu výkonnej moci. Ten by blokovanie vykonal až po schválení súdom.

V neposlednom rade, musí existovať „rovnosť zbraní" medzi blokujúcim a blokovaným subjektom. To znamená viacero rovín. V prvom rade by sa k blokovaniu nemalo pristupovať arbitrárne a takým spôsobom, že blokovaný subjekt nedostane lehotu na vyjadrenie a možnosť sám potenciálne nebezpečný obsah odstrániť. Ak by ho v lehote neodstránil, až následne by sa malo pristúpiť k blokovaniu. Prirodzene, ak by išlo o veľmi škodlivý obsah, vieme si z tohto

pravidla predstaviť výnimky. Zároveň, proti rozhodnutiu o blokovaniu by malo byť možné podať opravný prostriedok a nielen mať možnosť preskúmať napadnuté rozhodnutie na súde.

Takto koncipovaná právna úprava blokovania by mala spĺňať prísne štandardy proporcionality a nevyhnutnosti takéhoto zásahu.

Druhým nástrojom verejného práva pri silnom negatívnom vplyve dezinformácií by malo byť konanie o nelegálnom obsahu. Ako z našej analýzy predmetného konania vyplýva, toto konanie sa týka iba dezinformácií, ktoré napĺňajú literu nelegálnosti. Inými slovami ide o dezinformačné materiály týkajúce sa neznášanlivosti k určitej skupine ľudí, popierania holokaustu, detskej pornografie alebo terorizmu. Aj z rozhodovacej praxe Rady pre mediálne služby je zjavné, že takto koncipované právomoci sa môžu javiť ako príliš úzke. Je na mieste uvažovať, či by medzi definíciu nelegálneho obsahu nebolo vhodné zakotviť aj obsah, ktorý napĺňa znaky trestného činu šírenia poplašnej správy podľa § 361 Trestného zákona, prípadne jeho modifikáciu. Druhým prídavkom by mohla byť skutková podstata nelegálneho obsahu, ktorá by umožňovala začatie správneho konania v prípadoch systematického šírenia nepravdivých správ s cieľom podkopať dôveru v inštitúcie, demokraciu alebo vládu práva. Takýmto spôsobom by sa dosiahlo preklenutie medzery medzi Zákonom o priestupkom a Trestným zákonom a pridala by sa možnosť vyvodenia administratívnoprávnej zodpovednosti prostredníctvom konania vo veci zamedzenia šírenia nelegálneho obsahu.

4.3.5 Nástroje verejného práva pre boj s dezinformáciami v online priestore pri alarmujúcom vplyve

Alarmujúci vplyv dezinformácií znamená, že situácia smeruje k obrovskej polarizácií spoločnosti, ujme na základných právach a slobodách až občianskym nepokojom. Z tohto pohľadu máme za to, že v tomto prípade by mali byť použité najinvazívnejšie nástroje verejného práva pre boj s dezinformáciami online a to najmä v podobe trestnoprávnej zodpovednosti a prijatí opatrení zo strany spravodajských služieb.

Z hľadiska trestnoprávnej roviny sú relevantné pre šírenie dezinformácií primárne trestné činy ohovárania a šírenia poplašnej správy. Trestný čin ohovárania je však využiteľný iba v prípadoch naozaj intenzívnych zásahov do osobnostných práv konkrétneho jednotlivca. Nemožno prostredníctvom neho stíhať šírenie nepravdivých informácií týkajúcich sa javov alebo iných subjektov ako je človek.

Iným prípadom je trestný čin šírenia poplašnej správy, prípadne navrhované skutkové podstaty trestných činov šírenia nepravdivej informácie. Kľúčové pre potenciál vyvodzovanie

trestnoprávnej zodpovednosti za spáchania tohto trestného činu je interpretácia pojmu poplašná správa. Ak sa pozrieme na doktrinálny výklad pojmu „poplašná správa," ide o správu, ktorá je spôsobilá vyvolať vážne znepokojenie vo forme strachu, úzkosti, paniky prípadne podobný emocionálny stav. So zohľadnením toho, že diskutovaná skutková podstata vyžaduje aj naplnenie atribútu „nepravdivosti" poplašnej správy a z príkladov uvedených v komentárovej literatúre[762] sa predmetná skutková podstata javí ako využiteľná aj pri stíhaní najzávažnejších foriem dezinformácií. Problematickým bodom je vyžadovanie nepravdivosti informácie, nakoľko za dezinformáciu možno označiť aj pravdivú informáciu šírenú manipulatívnym spôsobom. Z tohto dôvodu ani navrhovaná právna úprava trestného činu šírenia nepravdivej informácie by nereflektovala tento problém.

Prostriedky trestného práva by mali byť využívanie *ultima ratio* t.j. ako posledná inštancia. Súhlasíme so súčasným nastavením trestného činu šírenia poplašnej správy podľa § 361 a 362 Trestného zákona, ktorý reflektuje trestnoprávny postih nepravdivých informácií veľkej intenzity. Zásadne sa nestotožňujeme so zakotvením nedbanlivostnej formy trestných činov, ktoré by postihovali šírenie nepravdivých informácií z dôvodu vyžadovania konkrétneho úmyslu a cieľa v zmysle definičných znakov dezinformácií.

V rámci uplatnenia nástrojov verejného práva pri dezinformáciách s alarmujúcim vplyvom považujeme za nevyhnutné, aby opatrenia prijímali aj spravodajské služby. Nakoľko právna úprava nedefinuje presný rozsah právomoci spravodajských orgánov v zmysle konkrétnych opatrení, nemôžeme diskutovať vhodnosť ich aplikácie.

[762] BURDA, E. a kol. *Trestný zákon. Všeobecná časť. Komentár. I. diel*. 1. vydanie. Praha: C. H. Beck, 2010, komentár k § 361, dostupné na beck-online.sk.

ZÁVER

V rámci predkladanej práce sme sa zaoberali fenoménom dezinformácií z hľadiska nástrojov verejného práva, ktoré by mohli výrazne pomôcť pri zamedzení ich šírenia v online priestore. V úvode práce sme si vytýčili výskumnú otázku a tri hypotézy, ktoré sme postupne verifikovali našim výskumom.

Prvá kapitola tejto práce sa venovala pojmu dezinformácie, jeho legálneho definovania a taktiež kontextu, v ktorom sa dezinformácie šíria. Doktrína k pojmu dezinformácie pristupuje rôznym spôsobom, avšak za najčastejšie sa vyskytujúce pojmové znaky dezinformácie patrí úmyselné šírenie overiteľne nepravdivých informácií so špecifickým cieľom, či už v podobe ekonomického zisku alebo ohrozenia demokratických hodnôt ako dôvera v štátne zriadenie, základné ľudské práva a slobody či volebné procesy. Od pojmu dezinformácie je potrebné odlišovať iné pojmy, hlavne misinformácie, ktoré nie sú šírené úmyselným spôsobom. Rôzne k definícií dezinformácie pristupujú aj strategické dokumenty na úrovni EÚ a Slovenskej republiky. Z hľadiska legálnej definície, právny poriadok Slovenskej republiky ani EÚ definíciu dezinformácie neobsahuje. K pojmu sa iba veľmi striedmo vyjadruje judikatúra Ústavného súdu SR, Najvyššieho súdu SR, Najvyššieho správneho súdu SR a krajských súdov. Tieto súdne orgány iba v minimálne miere poskytli analytickejším spôsobom rozdiel medzi pojmami dezinformácia a nepravda.

Prvá hypotéza tejto práce bola formulovaná nasledovným spôsobom: *„Právny poriadok Slovenskej republiky alebo Európskej únie definuje pojem dezinformácia.*" Túto hypotézu sa nepodarilo overiť, vyššie uvedené právne poriadky pojem dezinformácie legálne nedefinujú. Navrhovaná právna úprava v podobe návrhu zákona o opatreniach na zvýšenie bezpečnosti a dôveryhodnosti platforiem v on-line prostredí dezinformáciu nedefinovala spôsobom, akým k tomuto pojmu pristupuje doktrína.

V rámci prvej kapitoly sme sa venovali životnému cyklu dezinformácií, motívoch ich zdieľania a hlavne faktorom, ktoré šírenie a dôveru v dezinformácie ovplyvňujú. Na základe prehľadových štúdií z mimo-právnych vied sme identifikovali nasledujúce faktory ovplyvňujúce šírenie a dôveru v dezinformácie:

Oblasť	Faktory
Psychológia	Kognitívne faktory ako intuitívne premýšľanie, kognitívne zlyhania a iluzórna pravda
	Sociálne afektívne faktory ako zdroj informácie, emócie a názory a viera adresáta informácie
Sociológia	Úbytok sociálneho kapitálu

	Nárast nerovnosti
	Zvyšujúcu sa polarizáciu spoločnosti
	Nedôvera vo vedu
	Evolúciu mediálneho prostredia
Ekonómia	Ekonomika pozornosti
	Dohľad kapitalizmu
Technické faktory	Personalizácia obsahu odporúčacími systémami (umelá inteligencia)
	Filtračné bubliny

Tabuľka: Faktory ovplyvňujúce dôveru a šírenie dezinformácií.
Zdroj: Výskum autora.

Tieto faktory sme následne zohľadnili v štvrtej kapitole pri posúdení vhodnosti nástrojov verejného práva pre boj s dezinformáciami v online priestore.

Predmetom skúmania druhej kapitoly boli politické dokumenty na úrovni EÚ a Slovenskej republiky, ktoré poskytujú nevyhnutný kontext pre prijatie regulačných opatrení pre boj s dezinformáciami online.

Na úrovni EÚ možno spomenúť aktivity od založenia expertnej skupiny na vysokej úrovni pre falošné správy a online dezinformácie zloženej z odborníkov v oblasti médií, akadémie, overovateľov faktov, občianskej spoločnosti a platforiem, ktorá vypracovala záverečnú správu s odporúčaniami v boji proti dezinformáciám. Zároveň, táto skupina predstavila aj vhodnú definíciu pojmu dezinformácia. Ďalšími strategickými dokumentami na úrovni EÚ v boji proti dezinformáciám online boli Oznámenie komisie európskemu parlamentu, rade, európskemu hospodárskemu a sociálnemu výboru a výboru regiónov Boj proti dezinformáciám na internete: európsky prístup z roku 2018, Spoločné Oznámenie Európskemu Parlamentu, Európskej Rade, Rade, Európskemu Hospodárskemu A Sociálnemu Výboru A Výboru Regiónov Akčný plán proti dezinformáciám z roku 2018 a Oznámenie Komisie Európskemu Parlamentu, Rade, Európskemu Hospodárskemu a Sociálnemu Výboru a Výboru Regiónov o akčnom pláne pre európsku demokraciu z roku 2020. Tieto dokumenty postupne vyzývajú na investície do vzdelávania, transparentnosť a zodpovednosť digitálnych platforiem či reguláciu.

V rámci Slovenskej republiky bolo prezentovaných taktiež viacero strategických dokumentov, ktoré vnímajú dezinformácie ako hybridnú hrozbu alebo negatívny fenomén s potrebou prijatia ďalších krokov. Menovite možno spomenúť Koncepciu pre boj Slovenskej republiky proti hybridným hrozbám z roku 2018, Bezpečnostnú stratégiu Slovenskej republiky z roku 2021, Obrannú stratégiu Slovenskej republiky z roku 2021, Koordinovaný mechanizmus odolnosti Slovenskej republiky voči informačným operáciám z roku, Akčný plán koordinácie

boja proti hybridným hrozbám 2022 – 2024 a v neposlednom rade Koncepciu strategickej komunikácie Slovenskej republiky z roku 2023. Najpodrobnejšie záväzky pre konkrétne orgány verejnej moci predstavuje Akčný plán koordinácie boja proti hybridným hrozbám. Za osobitne dôležité považujeme prijatie Koncepcie strategickej komunikácie Slovenskej republiky z roku 2023, ktorá opakovane zdôrazňuje rolu štátu a jeho komunikácií pri šírení dezinformácií.

Tretia kapitola s názvom Nástroje verejného práva pre boj s dezinformáciami v online prostredí analyzuje identifikované právne úpravy a derivuje konkrétne inštitúty využiteľné pri boji s dezinformáciami online. Z hľadiska regulácie sa zameriavane nie len na nástroje priamo reagujúce na dezinformačný obsah, ale aj na prostredie, v ktorom sa dezinformácie šíria a nástroje, ktoré dezinformácie napomáhajú šíriť.

Z hľadiska prostredia sme skúmali reguláciu digitálnych služieb a sociálnych sietí, na ktorých sa dezinformácie šíria exponenciálnym spôsobom. Pozornosť sme zamerali na najnovšiu legislatívu na úrovní EÚ v podobe Aktu o digitálnych službách (DSA). DSA upravuje niekoľko nástrojov, ktoré môžu v boji s dezinformáciami pomôcť, avšak samotné nariadenie sa primárne zameriava na nelegálny obsah, pričom dezinformácie predstavujú „iba" obsah škodlivý. Škodlivému obsahu sa venujú predovšetkým inštitúty posudzovania a zmierňovania rizík a auditovania. Za dôležité považujeme aj nástroje zvyšujúce transparentnosť (hlavne odporúčacích systémov), zobrazovania reklamy a dizajnu platforiem. Osobitnú pozornosť si zasluhujú aj inštitúty občianskej spoločnosti v podobe dôveryhodných nahlasovateľov a prístupu k údajom zo strany preverených výskumníkov. Úprava zodpovednosti za obsah tretích strán sa týka iba nelegálneho obsahu.

Z hľadiska nástrojov podporujúcich šírenie dezinformácií sme skúmali právnu úpravu umelej inteligencie (AI) v podobe návrhu Aktu o umelej inteligencií (AIA) na úrovni EÚ. Ak by finálne znenie AIA za vysokorizikové systémy AI považovalo aj odporúčacie systémy na sociálnych sieťach, bol by to výrazný krok k lepším požiadavkám na odporúčacie systémy. Uplatňovali by sa totiž na nich požiadavky správy údajov, ľudského dohľadu alebo presnosti a vhodnosti využitých údajov. Za osobitne dôležité považujeme aj požiadavky na transparentnosť systémov AI a špecifické pravidlá pre veľké jazykové modely a generatívnu AI.

Ďalej sme v tretej kapitole analyzovali špecifické nástroje verejného práva. Zákon o mediálnych službách upravuje špecifické správne konanie vo veci zamedzenia šírenia nelegálneho obsahu, ktorý môže slovenská Rada pre mediálne služby uložiť povinnosť určitý obsah vymazať. Problematickou časťou danej právnej úpravy je však jej úzka pôsobnosť na veľmi vymedzený okruh skutkových podstát. Tento fakt je evidentný aj z hlbšej analýzy rozhodnutí Rady pre mediálne služby ohľadom podaných podnetov, ktoré sú verejné dostupné.

Štáty môžu prijať aj špecifické právne úpravy obsahujúce opatrenia na zvýšenie transparentnosti a zodpovednosti v online priestore. Takýmto pokusom bol aj návrh o opatreniach na zvýšenie bezpečnosti a dôveryhodnosti platforiem v on-line prostredí, ktorý rozširoval definíciu nezákonného obsahu, zakotvoval opatrenia na zásahy štátu voči dezinformáciám a obmedzoval anonymitu v online diskusiách. Návrh zákona však narážal na limity unifikácie týchto právnych vzťahov na úrovni EÚ v podobe DSA a limity rešpektovania základných ľudských práv a slobôd. Osobitne problematické otázky sa týkali aj navrhovaného dohľadu, ktorý nenapĺňal kritéria nestrannosti a nezávislosti.

Ďalším nástrojom je blokovanie webových stránok. Ide o legitímny nástroj v demokratickej spoločnosti, ktorý však podlieha určitým limitom a pravidlám. Tieto limity ustanovuje konštantná judikatúra Európskeho súdu pre ľudské práva. Predovšetkým ide o požiadavky na vykonanie posúdenia vplyvu v legislatívnom procese, nezávislý dohľad, transparentnosť a spravodlivý proces (rovnosť zbraní). Blokovanie webstránok na základe škodlivého obsahu vrátane závažných dezinformácií ustanovuje aj Zákon o kybernetickej bezpečnosti. Právna úprava, ktorá je v tejto chvíli neúčinná však nenapĺňa kritériá uvedené vyššie.

Legislatíva ochrany osobných údajov taktiež poskytuje niekoľko nástrojov ktoré môžu napomôcť pri zamedzení šírenia dezinformácií vo len priestore. Je to hlavne z toho dôvodu, že odporúčacie systémy na digitálnych platformách fungujú na základe získaných osobných údajov a zároveň niektoré dezinformačné prejavy sa môžu týkať identifikovanej dotknutej osoby. Na jednej strane sme diskutovali individuálne práva dotknutých osôb ako právo na informácie, právo na prístup, právo na opravu, právo na vymazanie, právo na obmedzenie spracúvania, právo na prenosnosť a právo namietať. Oveľa zaujímavejšie sa však javia systematické nástroje ktoré regulácia ochrany osobných údajov ponúk. V tomto smere sme analyzovali právnu úpravu automatizovaného individuálneho rozhodovania podľa článku 22 GDPR ktorá sa za určitých okolností môže týkať aj šírenia dezinformácií. Zároveň za veľmi významné inštitúty, ktoré by mohli riziko šírenia dezinformácií znížiť považujeme posúdenie vplyvu na ochranu údajov a špecificky navrhnutú a štandardnú ochranu osobných údajov.

Diskutovali sme aj právnu úpravu priestupkového práva. Zákon o priestupkoch sa však vzťahuje iba na fyzické osoby a štandardne postačuje iba zavinenie z nedbanlivosti. Práve subjektívna stránka spáchania priestupku môže byť problematická, nakoľko pri šírení dezinformácií sa vyžaduje úmysel. Analyzovali sme konkrétne skutkové podstaty priestupkov ako neoprávnené vydávanie sa za verejného činiteľa, falšovanie informácií o zdravotnom stave a priestupky proti verejnému poriadku a proti občianskemu spolunažívaniu. Prvé dva menované priestupky sa však uplatňujú iba vo veľmi špecifickom kontexte a za veľmi špecifických okolností. zároveň na

ich spáchanie postačuje iba zavinenie z nedbanlivosti. Podľa nášho názoru je pri šírení dezinformácií použiteľný priestupok proti verejnému poriadku, ktorý spočíva vzbudení verejného pohoršenia za predpokladu že by išlo o úmyselné konanie páchateľa. Totožné konštatovanie možno uviesť v kontexte priestupkov proti občianskemu spolunažívaniu.
Trestné právo ako prostriedok *ultima racio*, taktiež ponúka niekoľko zaujímavých skutkových podstát, ktoré by mohli byť uplatniteľné v dezinformačnom kontexte. Analýze sme podrobili päť trestných činov a to konkrétne trestný čin ohovárania, trestný čin šírenia poplašnej správy, trestný čin ohrozenia bezpečnosti vzdušného dopravného prostriedku a lode, trestný čin falšovania a vyhotovenia nepravdivej zdravotnej dokumentácie, a trestný čin teroristického útoku. Posledné tri menované trestné činy však opäť platia iba vo veľmi špecifickom kontexte a za splnenia veľmi špecifických okolností. Pri trestnom čine ohovárania máme za to že táto skutková podstata by bola aplikovateľná v prípade, ak dezinformácia smeruje voči konkrétnemu jednotlivcovi. Oveľa zaujímavejšie sa však javí trestný čin šírenia poplašnej správy podľa § 361 a Trestného zákona. Máme za to že pri naozaj najzávažnejšom type nepravdivých informácií v podobe poplašných správ je táto skutková podstata použiteľná aj na šírenie dezinformácií. Analyzovali sme aj návrhy osobitnej skutkovej podstaty trestného činu šírenia dezinformácií, ktoré boli do medzirezortného pripomienkového konania predložené v roku 2022. Podľa nášho názoru však táto navrhovaná právna úprava nereflektovala, že dezinformácie sa musia šíriť úmyselným spôsobom a zároveň nebol dodržaný princíp proporcionality.

Poslednými nástrojmi verejného práva ktorými sme sa zaoberali boli nástroje ktorými disponujú spravodajské orgány konkrétne Slovenská informačná služba a Vojenské spravodajstvo. Z hľadiska dezinformácií, je kľúčové že v novej právnej úprave má Vojenské spravodajstvo explicitne ustanovenú povinnosť získavania, sústreďovania a vyhodnocovania informácií ktoré sa týkajú hybridných hrozieb a dezinformácií. Vzhľadom na utajený režim Vojenského spravodajstva nemáme ucelené informácie ktoré by nám umožňovali hlbšie analyzovať napĺňanie tejto úlohy a prípadne prijaté opatrenia. Podobné konštatovanie možno uviesť aj voči právnej úprave Slovenskej informačnej služby ktorá však explicitné zmocnenie na analýzu dezinformačných aktivít alebo hybridných hrozieb v zákone nemá. To ale neznamená, že dezinformačné aktivity nemôžu byť pod drobnohľadom tejto spravodajskej služby.

Druhú hypotézu sme formulovali nasledovným spôsobom: *„Právny poriadok Slovenskej republiky alebo Európskej únie poskytuje nástroje na minimalizáciu šírenia dezinformácií v online priestore z pohľadu všeobecnej regulácie verejného práva.*" Máme za to, že druhá hypotéza sa potvrdila.

V štvrtej kapitole sme predstavili taxonómiu nástrojov verejného práva pre boj s dezinformáciami v online priestore a zároveň sme posúdili vhodnosť ich využitia. Identifikovali sme konkrétne princípy ktoré by mali byť aplikované na nástroje verejného práva pri boji s dezinformáciami v online priestore. Tieto princípy sú nasledujúce: rešpektovanie slobody prejavu a práva na informácie, proporcionalita pri posudzovaní dezinformácií, zohľadnenie faktorov pôsobiacich na dôveru v dezinformácie a šírenie dezinformácií. Z hľadiska slobody prejavu a práva na informácie sme analyzovali priestor, ktorý zákonodarca na právnu úpravu pri limitovaní určitého obsahu má. V kontexte judikatúry Európskeho súdu pre ľudské práva, Súdneho dvora Európskej únie a Ústavného súdu slovenskej republiky vyplýva, že tento priestor tu existuje, avšak je oveľa legitímnejšie a vhodnejšie regulovať digitálne platformy a prostriedky prostredníctvom ktorých sa dezinformácie šíria v porovnaní s priamou reguláciou obsahu. Druhým princípom je proporcionalita pri posudzovaní dezinformácií. Analyzovali sme viaceré metodiky, na základe ktorých možno identifikovať riziko vplyvu alebo dopadu dezinformácií z hľadiska angažovanosti subjektov. Tieto metodiky sme upravili podľa potrieb zákonodarcu na základe rozhodnutí slovenských súdov identifikovali sme 9 kritérií, ktoré by mali byť pri analýze vplyvu dezinformácií zohľadnené. Konkrétne ide o angažovanosť na sociálnych sieťach, vystavenie na sociálnych sieťach, cirkulácia obsahu, difúzia medzi komunitami, dosah na mainstreamové médiá, typ aktéra, odlišné formáty dezinformácie, výzva na konanie a nebezpečenstvo príbehu, cieľ dezinformácie či ide o otázku verejného záujmu. Tieto kritériá majú identifikované konkrétne merateľné ukazovatele, na základe ktorých sú im prideľované body. Konkrétna dezinformácia môže získať hodnotu od 0 do 17 bodov podľa získaných bodov a následne možno dezinformácie diferencovať v kontexte ich vplyvu na alarmujúce, vysoké, stredné, nízke. Tretím princípom, ktorý by mal byť aplikovaný pri nástrojoch verejného práva by malo byť zohľadnenie faktorov pôsobiacich na dôveru dezinformácie a ich šírenie. Tieto faktory sme uviedli vyššie.

Na základe identifikovaných nástrojov verejného práva a po zohľadnení metodiky pre posúdenie vplyvu dezinformácií, sme následne tieto poznatky syntetizovali. Máme za to, že pri nízkom vplyve dezinformácií je potrebné využívať predovšetkým možnosti, ktoré ponúka strategická komunikácia zo strany štátu a činnosti pre podporu vývoja kritického myslenia. Pri strednej intenzite dezinformácií by mali byť využité prostriedky, ktoré ponúka priestupkové právo a priestor, ktorý umožňuje právna úprava Európskej únii pri prijímaní špecifických opatrení vyžadujúcich transparentnosť a zodpovednosť platforiem. Pri vysokom vplyve dezinformácií, za vhodné nástroje považujeme blokovanie webstránok a konanie o nelegálnom obsahu. Z hľadiska ich legislatívneho uchopenia však zvýrazňujeme zásadnú úpravu inštitútu

blokovanie webstránok takým spôsobom, aby reflektovala judikatúru Európskeho súdu pre ľudské práva. Zároveň úzku pôsobnosť konania o nelegálnom obsahu odporúčame rozšíriť minimálne o možnosť konania pri šírení poplašných správ v zmysle Trestného zákona. Pri alarmujúcom vplyve dezinformácií vidíme priestor na uplatnenie trestnoprávnej zodpovednosti a prijímanie opatrení spravodajských služieb. Z hľadiska šírenia dezinformácií o javoch máme za to, že právna úprava trestného činu šírenia poplašnej správy je dostatočná, nakoľko reflektuje princíp *ultima ratio* trestného práva. Mimo konkrétnych nástrojov namapovaných na konkrétnu intenzitu zásahu dezinformácie stoja nástroje, ktoré ponúka regulácia digitálnych služieb, regulácia odporúčacích systémov (umelej inteligencie) a regulácia dizajnu platforiem. Z pohľadu škodlivého obsahu vrátane dezinformácií za kľúčové považujeme inštitúty posudzovania a zmierňovania rizík a auditovania vrátane posúdenia vplyvu na ochranu údajov. Dôsledná analýza rizík môže odhaliť uzatváranie užívateľov do filtračných bublín. Za výrazné mínus regulácie odporúčacích systémov však považujeme to, že nedošlo k vypnutiu týchto systémov na základe regulačného príkazu od účinnosti právne úpravy digitálnych služieb. Osobitne zdôrazňujeme reguláciu odporúčacích systémov v kontexte navrhovanej právnej úpravy umelej inteligencie, ktorá by na nich zamerala svoju pozornosť v súvislosti s požiadavkami na kvalitu údajov, ľudský dohľad alebo presnosť. Podceňovať nemožno ani požiadavky na transparentnosť systémov AI. Taktiež považujeme za nevyhnutné zdôrazniť požiadavky na dizajn platforiem, ktorý nemôže byť manipulatívny a mal by reflektovať najvyššie požiadavky z pohľadu ochrany osobných údajov pre užívateľa. Osobitne stoja nástroje občianskej spoločnosti, ktorá by mala dohliadať na to či digitálne platformy vo veľkej miere nešíria škodlivý obsah a zároveň by mala byť strážcom toho aby štát neprijímal príliš invazívne regulácie s cieľom obmedzovania slobody prejavu a práva na informácie.

Tretia hypotéza sa zameriava na skúmanie proporcionality a efektívnosti vybraných nástrojov ktoré môžu byť použité na minimalizáciu šírenia dezinformácií v online prostredí prostredníctvom noriem verejného práva a formulovaná nasledovným spôsobom: „*Právny poriadok Slovenskej republiky alebo Európskej únie poskytuje proporcionálne a efektívne nástroje na minimalizáciu šírenia dezinformácií v online priestore z pohľadu všeobecnej regulácie verejného práva.*" Táto hypotéza sa nepotvrdila. Je to z toho dôvodu že sme identifikovali viacero legislatívnych medzier pri právnych úpravách nástrojov verejného práva prepojené s informáciami online priestor. Zároveň máme za to že princíp proporcionality by mal byť lepšie zohľadnený práve pri aplikácii jednotlivých nástrojov čo sa v aplikačnej praxi nie vždy deje.

Pri skúmaní fenoménu dezinformácií z pohľadu nástrojov verejného práva sme si stanovili nasledujúcu výskumnú otázku: „*Verejné právo poskytuje dostatok efektívnych nástrojov*

pre minimalizovanie šírenia a vplyvu dezinformácií v online priestore." na výskumnú otázku teda možné odpovedať nasledovne. Verejné právo síce poskytuje dostatok nástrojov pre minimalizovanie šírenia vplyvu dezinformácií v online priestore predovšetkým z pohľadu regulácie prostredia a nástrojov ich šírenia, avšak tieto právne úpravy nie sú bez chýb a nie vždy reflektujú princíp proporcionality. Prílišné sústredenie sa na nástroje, ktoré smerujú k odstraňovaniu konkrétneho obsahu alebo vyvodzovaniu zodpovednosti konkrétnych aktérov môžu naraziť na nevyhnutné limity slobody prejavu a práva na informácie. Z tohto dôvodu si myslíme, že väčšia pozornosť z hľadiska zákonodarcu by mala byť smerovaná na nástroje verejného práva, ktoré sú systémovejšie a môžu liečiť dôvody šírenia dezinformácií namiesto dôsledkov. V rámci tejto práce sme sa snažili načrtnúť aj naše odporúčania a naše úvahy práve v súlade s vyššie uvedenými závermi.

Veríme, že sme prispeli k diskusii o fenoméne dezinformácií a možnostiach jeho regulácie z pohľadu nástrojov verejného práva.

ZOZNAM POUŽITEJ LITERATÚRY

- ABELOVSKÝ, T. Virtualizácia ako metóda riešenia spoločenských problémov. In *Právny obzor*, 98, 2015, č.2, s. 164 – 177.
- ACERBI, A. Cognitive attraction and online misinformation. In *Palgrave Commun*. 5, 15, 2019.
- *Ako sa máte Slovensko? Dôvera v inštitúcie*. Dostupné na: https://www.akosamateslovensko.sk/tema/dovera-v-institucie/.
- ALDRICH, D. P. - MEYER, M. A. Social capital and community resilience. In *American Behavioral Scientist*, 59, 2015, s. 254–269. Dostupné na: http://dx.doi.org/10.1177/0002764214550299.
- *Algorithms and Amplification: How Social Media Platforms' Design Choices Shape Our Discourse and Our Minds, Subcommittee on Privacy, Technology, and the Law* (April 27, 2021) (statement by Joan Donovan, Research Director, Shorenstein Center on Media, Politics and Public Policy, Harvard Kennedy School). Dostupné na: https://www.judiciary.senate.gov/imo/media/doc/Donovan%20Testimony%20(updated).pdf.
- ANDRES, R. - SLIVKO, O: *Content Regulation on Social Media: Evidence from NetzDG*. ZEW - Centre for European Economic Research Discussion Paper No. 21-103. 2021. Dostupné na: https://ssrn.com/abstract=4013662 or http://dx.doi.org/10.2139/ssrn.4013662.
- ARTICLE 29 DATA PROTECTION WORKING PARTY. *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.* Adopted on 3 October 2017. As last Revised and Adopted on 6 February.
- ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 4/2007 on the concept of personal data*. Adopted on 20th June, 01248/07/EN.WP 136.
- *Attention*. Britannica. Dostupné na: https://www.britannica.com/science/attention.
- BARENDT, E. *Freedom of Speech*. Oxford University Press, 2005.
- BARGH, J.A. – CHARTRAND, T.L. Studying the Mind in the Middle: A Practical Guide to Priming and Automaticity Research". In REIS H., JUDD C. (EDS.). *Handbook of Research Methods in Social Psychology*. New York, NY: Cambridge University Press, 2000, s. 1–39.
- BAYER, J. et al. *Disinformation and propaganda: impact on the functioning of the rule of law and democratic processes in the EU and its Member States - 2021 update*. Dostupné na: https://www.europarl.europa.eu/thinktank/en/document/EXPO_STU(2021)653633.
- BENDIEK, A. – STÜRZER, I. *Advancing European Internal and External Digital Sovereignty: The Brussels Effect and the EU-US Trade and Technology Council.* IDEAS Working Paper Series from RePEc, (2022).

- *Bezpečnostná stratégia Slovenskej republiky*. 2021. Dostupné na: https://www.mosr.sk/data/files/4263_210128-bezpecnostna-strategia-sr-2021.pdf.
- *Bezpečnostná stratégia Slovenskej republiky*. Dostupné na: https://www.nbu.gov.sk/wp-content/uploads/urad/Bezpecnostna-strategia-SR-2021.pdf.
- BOMMASANI, R. et al. *On the opportunities and risks of foundation models*. arXiv preprint arXiv:2108.07258 (2021).
- BONTRIDDER, N. - POULLET, Y. The role of artificial intelligence in disinformation. In *Data & Policy*, 2021 3, E32. Dostupné na: 10.1017/dap.2021.20.
- BOUZA GARCÍA, L. – ALVAR, O. Regulating Disinformation and Big Tech in the EU: A Research Agenda on the Institutional Strategies, Public Spheres and Analytical Challenges. In *Journal of Common Market Studies*, 2023.
- BRADY, W. et al. Emotion Shapes the Diffusion of Moralized Content in Social Networks. In *Proceedings of the National Academy of Sciences* 114, no. 28 (2017): 7313–8.
- BRASHIER, N. M. - MARSH, E. J. Judging truth. Annu. In *Rev. Psychol*. 71, 499–515 (2020).
- BRAŽINOVÁ, A. a kol. Očkovanie v kontexte ochrany zdravia nielen v boji s pandémiou COVID-19 - Právne, etické a medicínske aspekty. In *Justičná revue*, 6-7/2022.
- BROWN, S. - DAVIDOVIC, J. - HASAN, A. The algorithm audit: Scoring the algorithms that score us. In *Big Data & Society*, 8(1), 2021.
- BRULLE, R. J. - CARMICHAEL, J. - JENKINS, J. C. Shifting public opinion on climate change: an empirical assessment of factors influencing concern over climate change in the U.S. 2002–2010. In *Clim. Change* 114, 169–188 (2012).
- BUITEN, M. *Combating Disinformation and Ensuring Diversity on Online Platforms: Goals and Limits of EU Platform*. 2022. Dostupné na: https://ssrn.com/abstract=4009079.
- BUITEN, M. *The Digital Services Act: From Intermediary Liability to Platform Regulation*. Working Paper. Dostupné na https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3876328.
- BURDA, E. a kol. *Trestný zákon. Všeobecná časť*. Komentár. I. diel. 1. vydanie. Praha: C. H. Beck, 2010, dostupné na beck-online.sk.
- BURDA, E. - BELEŠ, A. - ĽORKO, A. - MIHÁLIK, S. *Trestná zodpovednosť*. 1. vyd. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2022.
- BUSCHMAN, T.J. – MILLER, E.K. Top-down versus bottom-up control of attention in the prefrontal and posterior parietal cortices. In *Science.* 2007 Mar 30;315(5820):1860-2.

- BUSTAMENTE, C. et al. *Technology Primer: Social Media Recommendation Algorithms*. Edited by Ariel Higuchi. Belfer Center for Science and International Affairs, Harvard Kennedy School, August 25, 2022.

- BYGRAVE, L. Information Concepts in Law: Generic Dreams and Definitional Daylight. In *Oxford Journal of Legal Studies,* Vol. 35, No. 1 (2015).

- CASERO-RIPOLLÉS, A. - JORGE T. - BOUZA-GARCÍA, L. The European Approach to Online Disinformation: Geopolitical and Regulatory Dissonance. In *Humanities & Social Sciences Communications*, vol. 10/no. 1, (2023), s. 657-10.

- *CAVOUKIAN, A. Privacy by Design – The Seven Foundational Principles*. Dostupné na https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.

- CENTRUM BOJA PROTI HYBRIDNÝM HROZBÁM. INŠTITÚT SPRÁVNYCH A BEZPEČNOSTNÝCH ANALÝZ MINISTERSTVA VNÚTRA SLOVENSKEJ REPUBLIKY. *Vol'by 2023 a dezinformácie: Analýza šírenia klamlivého a zavádzajúceho obsahu súvisiaceho s vol'bami do Národnej rady Slovenskej republiky 2023*. Dostupné na: https://www.hybridnehrozby.sk/wp-content/uploads/2023/10/Zaverecna-analyza-k-doveryhodnosti-volieb.pdf.

- CIBIK, S. Vývoj konceptu brániacej sa demokracie v slovenskom právnom poriadku. In *Právny obzor*, 106, 2023, č. 3, s. 189 – 201.

- CLEMENT, J. *Facebook's Average Revenue per User (ARPU) from 2012 to 2020*. Statista. Dostupné na: https://www.statista.com/statistics/234056/facebooks-average-advertisingrevenue-per-user/.

- COALITION TO FIGHT DIGITAL DECEPTION. T*rained for Deception: How Artificial Intelligence Fuels Online Disinformation A Report from the Coalition to Fight Digital Deception. Technical Report*. 2022.

- COGO, A. - RICOLFI, M. Administrative Enforcement of Copyright Infringement in Europe. In FROSIO, G. (ed), *The Oxford Handbook of Online Intermediary Liability*, OUP, 2020, s. 586-602.

- COSTANZA-CHOCK, S. - DEBORAH RAJI, I. - BUOLAMWINI, J. Who Audits the Auditors? Recommendations from a Field Scan of the Algorithmic Auditing Ecosystem. In *2022 ACM Conference on Fairness, Accountability, and Transparency* (FAccT '22: 2022 ACM Conference on Fairness, Accountability, and Transparency, Seoul Republic of Korea: ACM, 2022), s. 1571–83. Dostupné na: https://doi.org/10.1145/3531146.3533213.

- *Council of Europe, Declaration on the manipulative capabilities of algorithmic processes*, 13 February 2019, Recommendation CM/Rec(2020).

- ČENTÉŠ, J. a kol. *Trestný zákon - Veľký komentár*. 5. aktualizované vydanie. Žilina: Eurokódex, 2022, s. 798.

- DATA PROTECTION COMMISSION. *Data Protection Commission announces decision in Facebook "Data Scraping" Inquiry*. Dostupné na: https://dataprotection.ie/en/news-

media/press-releases/data-protection-commission-announces-decision-in-facebook-data-scraping-inquiry.

- DEKK. *TRENDY [NE]DÔVERY 2023. Správa o stave [ne]dôvery na Slovensku*. Dostupné na: https://www.dekk.institute/trendy-ne-dovery-2023/.

- DEKK. *TRENDY [NE]DÔVERY 2023. Správa o stave [ne]dôvery na Slovensku*. Dostupné na: https://www.dekk.institute/trendy-ne-dovery-2023/.

- DELFANTI, A. - ARVIDSSON, A. *Introduction to Digital Media*. Wiley, 2019.

- DENNÍK N. *Minúta po minúte zo dňa 7. februára 2023 11:05*. Dostupné na: https://dennikn.sk/minuta/3227529/.

- DEUZE, M. - WITSCHGE, T. Beyond journalism: Theorizing the transformation of journalism. In *Journalism*, 2017. Dostupné na: http://dx.doi.org/10.1177/1464884916688550.

- *Disinformation.* Dostupné na: https://www.etymonline.com/word/disinformation.

- *Dôvodová správa k vládnemu návrhu zákona, ktorým sa mení a dopĺňa zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony.*

- *Dôvodová správa k Vládnemu návrhu zákona, ktorým sa menia a dopĺňajú niektoré zákony v súvislosti s treťou vlnou pandémie ochorenia COVID-19.*

- *Dôvodová správa k zákonu, ktorým sa mení a dopĺňa zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov a o zmene a doplnení niektorých zákonov*. Dostupné na: https://www.slov-lex.sk/legislativne-procesy/-/SK/dokumenty/LP-2021-744.

- DRGONEC, J. *Ústava Slovenskej republiky – Komentár*. 2. vydanie. 2019. Praha: C.H. Beck. Dostupné na beck-online.sk.

- DUBÓCZI, P. – FRIEDL, M. – RUŽIČKOVÁ, M. *DEZINFORMÁCIE A PROPAGANDA AKO BIZNIS. Mapovanie finančného a organizačného pozadia dezinformačných webov na Slovensku*. 2023. Dostupné na: https://infosecurity.sk/dezinfo/dezinformacie-a-propaganda-ako-biznis-mapovanie-financneho-a-organizacneho-pozadia-dezinformacnych-webov-na-slovensku/.

- DUMBRAVA, C. *Key social media risks to democracy. Risks from surveillance, personalisation, disinformation, moderation and microtargeting*. EPRS | European Parliamentary Research Service alebo CHAKRABORTY, T. Dynamics of Fake News Diffusion. In: CHAKRABORTY, T., LONG, C., SANTHOSH, K. G. (ed.). *Data Science for Fake News*. Switzerland: Springer. 2021, s. 101–127.

- ECKER, U.K.H. - LEWANDOWSKY, S. - COOK, J. et al. The psychological drivers of misinformation belief and its resistance to correction. In *Nat Rev Psychol* 1, 13–29 (2022). https://doi.org/10.1038/s44159-021-00006-y.

- EDELSON, L. - GRAEF, I. - LANCIERI, F. *Access to Data and Algorithms: For an Effective DMA and DSA Implementation*. (CERRE, March 2023), Dostupné na:

https://cerre.eu/publications/access-to-data-and-algorithms-for-an-effective-dma-and-dsaimplementation.

- EDRI. *Civil society calls for AI red lines in the European Union's Artificial Intelligence proposal*. Dostupné na: https://edri.org/our-work/civil-society-call-for-ai-red-lines-in-the-european-unions-artificial-intelligence-proposal/.

- ENGLER, A. *Fighting deepfakes when detection fails*, The Brookings Institute. Dostupné na: https://www.brookings.edu/articles/fighting-deepfakes-when-detection-fails/.

- ESPALIÚ-BERDUD, C. Legal and Criminal Prosecution of Disinformation in Spain in the Context of the European Union. In *El Profesional De La Informacion*, vol. 31/no. 3, (2022).

- ESPOSITO, R. et al. *20 Children Died in Newtown, Conn., School Massacre*. ABC News. Associated Press. Dostupné na: https://abcnews.go.com/US/twenty-children-died-newtown-connecticut-school-shooting/story?id=17973836.

- EU DISINFOLAB. *Towards an impact-risk index of disinformation: Measuring the virality and engagement of single hoaxes*. Dostupné na: https://www.disinfo.eu/publications/towards-an-impact-risk-index-of-disinformation-measuring-the-virality-and-engagement-of-single-hoaxes/.

- EUROEPAN DATA PROTECTION BOARD. *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default.* Version 2.0 Adopted on 20 October 2020. Dostupné na: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

- EUROPEAN COMMISSION, DIRECTORATE-GENERAL FOR COMMUNICATIONS NETWORKS, CONTENT AND TECHNOLOGY. *Digital Services Act : application of the risk management framework to Russian disinformation campaigns.* Publications Office of the European Union, 2023. Dostupné na: https://data.europa.eu/doi/10.2759/764631.

- EUROPEAN COMMISSION, JOINT RESEARCH CENTRE, GIANNOPOULOS, G., SMITH, H., THEOCHARIDOU, M. *The landscape of hybrid threats : a conceptual model : public version*. Publications Office of the European Union, 2021. Dostupné na: https://data.europa.eu/doi/10.2760/44985.

- EUROPEAN COMMISSION, JOINT RESEARCH CENTRE, GIANNOPOULOS, G., SMITH, H., THEOCHARIDOU, M., THE LANDSCAPE OF HYBRID THREATS : A CONCEPTUAL MODEL : PUBLIC VERSION, GIANNOPOULOS, G.(EDITOR), SMITH, H.(EDITOR), THEOCHARIDOU, M.(EDITOR). Publications Office of the European Union, 2021. Dostupné na: https://data.europa.eu/doi/10.2760/44985.

- EUROPEAN DATA PROTECTION BOARD. *Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them*. Dostupné na: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en.

- EUROPEAN PARLIAMENT, DIRECTORATE-GENERAL FOR EXTERNAL POLICIES OF THE UNION, COLOMINA, C., SÁNCHEZ MARGALEF, H., YOUNGS, R. *The impact of*

disinformation on democratic processes and human rights in the world. European Parliament, 2021. Dostupné na: https://data.europa.eu/doi/10.2861/59161.

- EUROPEAN PARLIAMENT, DIRECTORATE-GENERAL FOR EXTERNAL POLICIES OF THE UNION, COLOMINA, C., SÁNCHEZ MARGALEF, H., YOUNGS, R. *The impact of disinformation on democratic processes and human rights in the world, European Parliament*. 2021. Dostupné na: https://data.europa.eu/doi/10.2861/59161.

- EUROPEAN PARLIAMENT, DIRECTORATE-GENERAL FOR INTERNAL POLICIES OF THE UNION, GALLI, F., SARTOR, G., LAGIOIA, F. *Regulating targeted and behavioural advertising in digital services : how to ensure users' informed consent*. European Parliament, 2021. Dostupné na: https://data.europa.eu/doi/10.2861/264833.

- EUROPEAN PARLIAMENT, DIRECTORATE-GENERAL FOR INTERNAL POLICIES OF THE UNION, BATURA, O., HOLZNAGEL, B., LUBIANIE, K. *The fight against disinformation and the right to freedom of expression*. European Parliament, 2021. Dostupné na: https://data.europa.eu/doi/10.2861/305.

- EUROPEAN PARLIAMENT, DIRECTORATE-GENERAL FOR INTERNAL POLICIES OF THE UNION, BOTERO ARCILA, B., GRIFFIN, R. *Social media platforms and challenges for democracy, rule of law and fundamental rights : executive summary*. European Parliament, 2023. Dostupné na: https://data.europa.eu/doi/10.2861/304062.

- EUROPEAN PARLIAMENT, DIRECTORATE-GENERAL FOR INTERNAL POLICIES OF THE UNION, BATURA, O., HOLZNAGEL, B., LUBIANIE, K. The fight against disinformation and the right to freedom of expression, European Parliament. 2021. Dostupné na: https://data.europa.eu/doi/10.2861/305.

- EUROPEAN PARLIAMENT, DIRECTORATE-GENERAL FOR INTERNAL POLICIES OF THE UNION, BATURA, O., HOLZNAGEL, B., LUBIANIE, K. The fight against disinformation and the right to freedom of expression, European Parliament. 2021. Dostupné na: https://data.europa.eu/doi/10.2861/305.

- EUROPEAN PARLIAMENT, DIRECTORATE-GENERAL FOR PARLIAMENTARY RESEARCH SERVICES, DUMBRAVA, C. *Key social media risks to democracy – Risks from surveillance, personalisation, disinformation, moderation and microtargeting*. European Parliament, 2021. Dostupné na: https://data.europa.eu/doi/10.2861/135170.

- EUROPEAN PARLIAMENT, DIRECTORATE-GENERAL FOR PARLIAMENTARY RESEARCH SERVICES, BEKE, M., BERENSCHOT, L., DUTTA, S. *The European public health response to the COVID-19 pandemic : lessons for future cross-border health threats*. European Parliament, 2023. Dostupné na: https://data.europa.eu/doi/10.2861/459491.

- EURÓPSKA KOMISIA. Commission staff working document impact assessment accompanying the proposal for a regulation of the european parliament and of the council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts. {COM(2021) 206 final} - {SEC(2021) 167 final} - {SWD(2021) 85 final}.

- EURÓPSKA KOMISIA. Commission staff working document impact assessment accompanying the proposal for a regulation of the european parliament and of the council laying down harmonised rules on artificial intelligence (artificial intelligence act)

and amending certain union legislative acts. {COM(2021) 206 final} - {SEC(2021) 167 final} - {SWD(2021) 85 final}.

- EURÓPSKA KOMISIA. Commission staff working document impact assessment accompanying the proposal for a regulation of the european parliament and of the council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts. {COM(2021) 206 final} - {SEC(2021) 167 final} - {SWD(2021) 85 final}.

- EURÓPSKA KOMISIA. *Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines*. Dostupné na: https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2413.

- EURÓPSKA KOMISIA. *Digital Services Act. Conducting independent audits*. Dostupné na: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13626-Digital-Services-Act-conducting-independent-audits_en.

- EURÓPSKA KOMISIA. *Digital Services Act*. Dostupné na: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en.

- EURÓPSKA KOMISIA. *Impact assessment accompanying the document proposal for a regulation of the european parliament and of the council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC.* SWD(2020) 348 final.

- 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.

- EURÓPSKA KOMISIA. *Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a výboru regiónov. Boj proti dezinformáciám na internete: európsky prístup*. COM/2018/236 final. Dostupné na: https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX%3A52018DC0236.

- EURÓPSKA KOMISIA. *Spoločné oznámenie Európskemu parlamentu, Európskej rade, Rade, Európskemu hospodárskemu a sociálnemu výboru a výboru regiónov. Akčný plán proti dezinformáciám*. JOIN/2018/36 final. Dostupné na: https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX%3A52018JC0036.

- EURÓPSKA KOMISIA. *Tackling online disinformation*. Dostupné na: https://digital-strategy.ec.europa.eu/en/policies/online-disinformation.

- EVANS, S. et al. Explicating Affordances: A Conceptual Framework for Understanding Affordances in Communication Research. In *Journal of Computer-Mediated Communication* 22, no. 1 (2017), s. 35–52. Dostupné na: https://doi.org/10.1111/jcc4.12180.

- EXPERTNÁ SKUPINA NA VYSOKEJ ÚROVNI PRE UMELÚ INTELIGENCIU. Etické Usmernenia Pre Dôveryhodnú Umelú Inteligenciu. Dostupné na: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

- FÁBRY, B. – KASINEC. R. – TURČAN, M. *Teória práva*. 2. vydanie. Bratislava: Wolters Kluwer, 2019.
- FALLIS, D. A Conceptual Analysis of Disinformation. In *iConference 2009 Papers*. Dostupné na: https://www.ideals.illinois.edu/items/15210.
- FALLIS, D. What is Disinformation? In *Library Trends*, Volume 63, Number 3, Winter 2015, s. 404 – 406.
- FETZER, J. Disinformation: The Use of False Information. In *Minds and Machines*, 14(2), 2014.
- FETZER, J. H. Disinformation: The use of false information. In *Minds and Machines*, 2(14), 2014 s. 231–240.
- *Final report of the High Level Expert Group on Fake News and Online Disinformation.* Dostupné na: https://digital-strategy.ec.europa.eu/sk/node/3245.
- FLORIDI, L. Brave.net.world: The internet as a disinformation superhighway? In *Electronic Library*, 14, 1996, 509–514.
- FLORIDI, L. Brave.net.world: The internet as a disinformation superhighway? In *Electronic Library*, 14, 1996, 509.
- FLORIDI, L. Semantic conceptions of information. In *Stanford Encyclopedia of Philosophy*, 2015. Dostupné na: http://plato.stanford.edu/entries/information-semantic.
- FLORIDI, L. The philosophy of information. New York: Oxford University Press, 2021.
- FROSIO, G. - BULAYENKO, O. Website Blocking Injunctions in Flux: Static, Dynamic, and Live. In 16(3) *Journal of Intellectual Property Law and Practice* (2021). Dostupné na: https://ssrn.com/abstract=3848063.
- GALBRAITH, J.K. *The affluent society*. Houghton Mifflin Harcourt, 1998.
- GANGULI, D. Predictability and surprise in large generative models. *ACM Conference on Fairness, Accountability, and Transparency* (2022), 1747-1764.
- GARCÍA BOUZA, L. – OLEART, A. Regulating Disinformation and Big Tech in the EU: A Research Agenda on the Institutional Strategies, Public Spheres and Analytical Challenges. In *JCMS* 2023 s. 1–13.
- GARRETT, R. K. - WEEKS, B. E. - NEO, R. L. Driving a wedge between evidence and beliefs: How online ideological news exposure promotes political misperceptions. In *Journal of Computer-Mediated Communication*, 21, s. 331–348. Dostupné na: http://dx.doi.org/10.1111/jcc4.12164,
- GARRETT, R. K. The echo chamber distraction: disinformation campaigns are the problem not audience fragmentation. In *J. Appl. Res. Mem. Cogn*. 6, 370–376 (2017).

- GEIGER, CH. - IZYUMENKO, E. The Role of Human Rights in Copyright Enforcement Online: Elaborating a Legal Framework for Website Blocking. In (2016) 32(1) *AUILR* 43.

- GELFERT, A. Fake News: A Definition. In *Informal Logic*, Vol.38, No.1, 2018, s. 84–117.

- GLOBSEC. *Nový prieskum GLOBSEC-u: Slovensko zaznamenalo výrazný prepad v prozápadných postojoch*. Dostupné na: https://www.globsec.org/what-we-do/press-releases/novy-prieskum-globsec-u-slovensko-zaznamenalo-vyrazny-prepad-v.

- GOHEL, P. – SINGH, P. – MOHANTY, M. *Explainable AI: current status and future directions*. Dostupné na: https://arxiv.org/abs/2107.07045.

- GOLDZWEIG, R. *Disrupted Democracies: A multistakeholder approach to fight disinformation*. 2021. Dostupné na: https://www.ippi.org.il/disrupted-democracies-a-multistakeholder-approach-to-fight-disinformation/.

- GORWA, R. - GARTON ASH, T. *Democratic transparency in the platform society*. SOC. MEDIA DEMOCR. STATE FIELD PROSPECTS REFORM 286 (2020).

- GRAEF, I. *The EU Regulatory Patchwork for Dark Patterns: An Illustration of an Inframarginal Revolution in European Law?* (April 3, 2023). Forthcoming as a book chapter in Ramsi A. Woodcock, Toward an Inframarginal Revolution: Markets as Wealth Distributors, Cambridge University Press 2023, TILEC Discussion Paper No. 2023-07, Tilburg Law School Research Paper. Dostupné na: http://dx.doi.org/10.2139/ssrn.4411537.

- GRAEUPNER, D. - COMAN, A. The dark side of meaning-making: how social exclusion leads to superstitious thinking. In *J. Exp. Soc. Psychol*. 69, 218–222 (2017).

- GUAGNANO, G. - SANTARELLI, E. - SANTINI, I. Can social capital affect subjective poverty in Europe? An empirical analysis based on a generalized ordered logit model. In *Social Indicators Research*, 2016 128, s. 881–907. Dostupné na: http://dx.doi.org/10.1007/s11205-015-1061-z.

- HAATAJA, M. - BRYSON, J. J. *What costs should we expect from the EU's AI Act?* 2021. Dostupné na: https://doi.org/10.31235/osf.io/8nzb4.

- HACKER, P. et al. *Regulating ChatGPT and other Large Generative AI Models*. FAccT '23, June 12-15, 2023, Chicago, IL, USA.Dostupné na: https://arxiv.org/abs/2302.02337.

- HAGEY, K. - HORWITZ, J. *Facebook Tried to Make Its Platform a Healthier Place. It Got Angrier Instead*. The Wall Street Journal, 2021. Dostupné na: https://www.wsj.com/articles/facebook-algorithm-change-zuckerberg-11631654215.

- HAJDU, D. a kol. *GLOBSEC Trends 2022: Väčšina ľudí na Slovensku stále verí konšpiráciám a cíti sa ohrozene*. Dostupné na: https://www.globsec.org/what-we-do/press-releases/globsec-trends-2022-vacsina-ludi-na-slovensku-stale-veri-konspiraciam.

- HAMUĽÁK, J. – FREEL, L. – NEVICKÁ, D. The comparative analysis of women's status in labor relations in modern Slovakia and the Czech Republic. In *Danube*. Roč. 11, č. 3 (2020), s. 214-227

- HAMUĽÁK, J. – NEVICKÁ, D. Breastfeeding as a (non)exclusive right of women in labor relations - the European approach. In *European studies : the review of European law, economics and politics*. Roč. 7. 1. vyd. Praha : Wolters Kluwer, 2020, s. 273-282.

- HAMUĽÁKOVÁ, Z., HORVAT, M. *Základy správneho práva trestného*. Bratislava : Wolters Kluwer, 2019.

- *Handelsgericht Wien*. Puls 4 TV GmbH & Co. KG v YouTube LLC and Google Austria GmbH, prípad č. 4 R 119/18a.

- HARRISON, R. *Tackling Disinformation in Times of Crisis: The European Commission's Response to the Covid-19 Infodemic and the Feasibility of a Consumer-centric Solution.* 17(3) Utrecht Law Review, 2021 s. 18–33. DOI: https://doi.org/10.36633/ulr.675.

- HARRISON, R. *Tackling Disinformation in Times of Crisis: The European Commission's Response to the Covid-19 Infodemic and the Feasibility of a Consumer-centric Solution.* 17(3) Utrecht Law Review, 2021 s. 18–33. DOI: https://doi.org/10.36633/ulr.675.

- HASELTON M.G. – NETTLE, D. – ANDREWS, P.W. The evolution of cognitive bias. In BUSS, D.M. (ed.). *The Handbook of Evolutionary Psychology*. Hoboken, NJ, US: John Wiley & Sons Inc., 2005, s. 724–746.

- HIGH LEVEL GROUP ON FAKE NEWS AND ONLINE DISINFORMATION. *A multi-dimensional approach to disinformation. Report of the independent High level Group on fake news and online disinformation*. 2018, s. 10. Originálne znenie: "*...false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit.*" Dostupné na: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=50271.

- HOSPODÁRSKE NOVINY. *Ministerstvo spravodlivosti z návrhu Trestného zákona vyškrtlo trestný čin šírenia nepravdivej informácie*. Dostupné na: https://hnonline.sk/slovensko/96040690-ministerstvo-spravodlivosti-z-navrhu-trestneho-zakona-vyskrtlo-trestny-cin-sirenia-nepravdivej-informacie.

- HRČKOVÁ, A. - SRBA, I. - MÓRO, R. - BLAHO, R. - ŠIMKO, J. - NÁVRAT, P. - BIELIKOVÁ, M. Unravelling the basic concepts and intents of misbehavior in post-truth society. In *Bibliotecas. Anales de Investigación*; 15(3), 2019, s. 421-428. Dostupné na: http://revistas.bnjm.cu/index.php/BAI/article/view/109/110.

- https://slovnik.juls.savba.sk/?w=dezinform%C3%A1cia+&s=exact&c=B04a&cs=&d=scs#.

- HUSOVEC, M. Digitálny trh EÚ a zodpovednosť poskytovateľov služieb. In HUSOVEC, M. - MESARČÍK, M. - ANDRAŠKO, J. *Právo informačných a komunikačných technológií I*. TINCT, 2021.

- HUSOVEC, M. – ROCHE LAGUNA, I. *Digital Services Act: A Short Primer* (July 5, 2022). Dostupné na https://ssrn.com/abstract=4153796.

- 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.

- HUSOVEC, M. Injunctions against Innocent Third Parties: The Case of Website Blocking. In 4(2) *JIPITEC* 116, 2013.

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

- HUSOVEC, M. *The DSA's Scope Briefly Explained*. 2023. Dostutpné na: https://ssrn.com/abstract=4365029.

- HUSOVEC, M. *Will the DSA work? On money and effort*. Verfassungsblog. Dostupné na: https://verfassungsblog.de/dsa-money-effort/.

- IGLESIAS KELLER, C. Don't Shoot the Message: Regulating Disinformation Beyond Content. In *Direito Público*, Instituto Brasiliense de Direito Público – IDP, Brasília DF, Vol. 18, Iss. 99, s. 486-515. Dostupné na: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/6057.

- *Income inequality across Europe in 2021*. Eurostat. Dostupné na: https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20230113-1.

- IVANČÍK, R. Dezinformácie ako hybridná hrozba. In MEDELSKÝ, J., LACA, N. 2022. *Dezinformácie a právo (úlohy a postavenie bezpečnostných zložiek).* Zborník príspevkov. Bratislava. Akadémia Policajného zboru v Bratislave.

- JARRAHI, A. - SAFARI, L. Evaluating the effectiveness of publishers' features in fake news detection on social media. In *Multimedia Tools and Applications*. 2022. 82. 10.1007/s11042-022-12668-8.

- JASMONTAITE, L., KAMARA, I., ZANFIR-FORTUNA, G., LEUCII, S. Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR. In. *EDPL*, Vol. 2, 2018, s. 168 – 189.

- JERÓNIMO, P. - ESPARZA, M.S. *Disinformation at a Local Level: An Emerging Discussion*. Publications 2022, 10, 15. Dostupné na: https://doi.org/10.3390/publications10020015.

- JOINT DECLARATION ON FREEDOM OF EXPRESSION AND "FAKE NEWS", DISINFORMATION AND PROPAGANDA. Organization for Security and Co-operation in Europe. 2017. Dostupné na: https://www.osce.org/fom/302796.

- KALIMERIS, D. et al. Preference Amplification in Recommender Systems. In *Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining* (New York: Association for Computing Machinery, 2021): s. 805–15. Dostupné na: https://doi.org/10.1145/3447548.3467298.

- KARLOVA, N. – FISHER, K. A social diffusion model of misinformation and disinformation for understanding human information behaviour. In *Information Research 18.1* (2013).

- KASL, F. Surveillance in digitalized society: the chinese social credit system from a european perspective. In *The Lawyer Quarterly*, Vol 9, No 4 (2019).

- KIM, A. - DENNIS, A. R. Says who? The effects of presentation format and source rating on fake news in social media. In *MIS Quarterly: Management Information Systems*, 43(3), 2019, s. 1025–1039. https://doi.org/10.25300/MISQ/2019/15188.

- KINIT. *Prieskum CEDMO odhalil nízku dôveru Slovákov v demokraciu*. Dostupné na: https://kinit.sk/sk/prieskum-cedmo-odhalil-nizku-doveru-slovakov-v-demokraciu/.

- KOBERNJUK, A. - KASPER, A. Normativity in the EU's Approach towards Disinformation. In *TalTech Journal of European Studies*,11(1), s. 170-202. Dostupné na: https://doi.org/10.2478/bjes-2021-0011.

- *Kódex nakladania s dezinformáciami*. 2018. Dostupné na: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=59125.

- *Kódex nakladania s dezinformáciami*. Dostupné na: https://digital-strategy.ec.europa.eu/en/news/code-practice-disinformation.

- KOLEKTÍV AUTOROV. *Aktuálne otázky teórie práva*. 1. vydanie. Bratislava: Wolters Kluwer, 2018.

- *Koncepcia pre boj Slovenskej republiky proti hybridným hrozbám* schválená uznesením vlády SR č. 345 zo dňa 11. júla 2018.

- *Koncepcia pre boj Slovenskej republiky proti hybridným hrozbám*. Dostupné na: https://www.nbu.gov.sk/wp-content/uploads/PHHD/Koncepcia-boja-SR-proti-hybridnym-hrozbam.pdf.

- *Koordinovaný mechanizmus odolnosti Slovenskej republiky voči informačným operáciám*. Dostupné na slov-lex.sk.

- KOŠIČIAROVÁ, S. *Zákon o priestupkoch - Podrobný komentár s judikatúrou*. Leges. 2021.

- KOUROUTAKIS, A. EU Action Plan Against Disinformation: Public Authorities, Platforms and the People. In *The International Lawyer*, vol. 53/no. 2, (2020), s. 277-290.

- KOZYREVA, A. - LEWANDOWSKY, S. - HERTWIG, R. Citizens versus the internet: confronting digital challenges with cognitive tools. In *Psychol. Sci. Public Interest*. 21, s. 103–156 (2020).

- KOZYREVA, A. et al. Incorporating Psychological Science Into Policy Making. The Case of Misinformation. In *European Psychologist*, 28(3), 2023, s. 206–224. Dostupné na: https://doi.org/10.1027/1016-9040/a000493.

- KOZYREVA, A. et al. Incorporating Psychological Science Into Policy Making. The Case of Misinformation. In *European Psychologist*, 28(3), 2023, s. 206–224. Dostupné na: https://doi.org/10.1027/1016-9040/a000493.

- KUCZERAWY, A. *The Good Samaritan that wasn't: voluntary monitoring under the (draft) Digital Services Act*. Dostupné na: https://verfassungsblog.de/good-samaritan-dsa/.

- KUDRNA, J. The possibilities of combating so-called disinformation in the context of the european union legal framework and of constitutional guarantees of freedom of expression in the european union member states. In *International Comparative Jurisprudence*, 2022 Volume 8 Issue 2. Dostupné na: http://dx.doi.org/10.13165/j.icj.2022.12.002.

- KUKLÍK, J. (Dez)informácie ako nástroj hybridnej hrozby optikou spravodajských služieb. In MEDELSKÝ, J., LACA, N. 2022. *Dezinformácie a právo (úlohy a postavenie bezpečnostných zložiek)*. Zborník príspevkov. Bratislava. Akadémia Policajného zboru v Bratislave.

- KUMAR, S. - SHAH, N. *False information on web and social media: A survey*. arXiv preprint. 2021. Dostupné na: arXiv:1804.08559.

- KUNER, CH. – BYGRAVE, L. – DOCKSEY, CH. *The EU General Data Protection Regulation (GDPR). A commentary*. Oxford: Oxford University Press, 2020.

- L LEISER, M. *Reimagining Digital Governance: The EU's Digital Service Act and the Fight Against Disinformation* 2023. Dostupné na: https://ssrn.com/abstract=4427493.

- LADIVEROVÁ, E. – NEVICKÁ, D. Práca z domu a domácka práva. In *Bratislavské právnické fórum 2021: Realizácia sociálnych práv v období pandémie*. 1. vyd. Bratislava : Právnická fakulta UK, 2021, s. 83-87,.

- LADIVEROVÁ, E. – NEVICKÁ, D. Pružný pracovný čas v home office – súmrak flexibilných foriem zamestnávania. In *Bratislavské právnické fórum 2022: raison ď être pracovného práva a práva sociálneho zabezpečenia na Slovensku - 100 rokov vývoja a vyhliadky do budúcnosti.* 1. vyd. IBratislava : Právnická fakulta UK, 2022, s. 80-86.

- LEISER, M. Dark patterns': The case for regulatory pluralism between the European Union's consumer and data protection regimes. In KOSTA, E. et al. *Research Handbook on EU Data Protection Law*, Eward Elgar 2022.

- LEISER, M. *Reimagining Digital Governance: The EU's Digital Service Act and the Fight Against Disinformation* 2023. Dostupné na: https://ssrn.com/abstract=4427493.

- LEWANDOWSKY, S. - ECKER, U. K. H. - COOK, J. Beyond misinformation: Understanding and coping with the "post-truth" era. In *Journal of Applied Research in Memory and Cognition*, 2017, 6(4), s. 353–369. Dostupné na: https://doi.org/10.1016/j.jarmac.2017.07.008.

- LEWANDOWSKY, S. - ECKER, U. K. H. - COOK, J. Beyond misinformation: Understanding and coping with the "post-truth" era. In *Journal of Applied Research in Memory and Cognition*, 2017, 6(4), s. 353–369. Dostupné na: https://doi.org/10.1016/j.jarmac.2017.07.008.

- LONARDO, L. EU Law Against Hybrid Threats: A First Assessment. In *European Papers* (Online. Periodico), vol. 6/no. 2, (2021), s. 1075-1096.

- LORENZO-DUS, N. - BLITVICH, G.-C. - BOU-FRANCH, P. On-line polylogues and impoliteness: The case of postings sent in response to the Obama Reggaeton YouTube

video. In *Journal of Pragmatics*, 2011, 43, 2578–2593. Dostupné na: http://dx.doi.org/10.1016/j.pragma.2011.03.005.

- LOVELLS, H. *Online Regulation: Germany's plans to tackle "digital violence" (and likely other issues, too)*. Dostupné na: https://www.lexology.com/library/detail.aspx?g=67cc1c39-dc71-4a05-9843-54207bc331c2.

- *LP/2020/507 Koordinovaný mechanizmus odolnosti Slovenskej republiky voči informačným operáciám*. Dostupné na: https://www.slov-lex.sk/legislativne-procesy/-/SK/LP/2020/507.

- *LP/2021/744*. Zákon, ktorým sa mení a dopĺňa zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov a o zmene a doplnení niektorých zákonov.

- *LP/2021/744*. Zákon, ktorým sa mení a dopĺňa zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov a o zmene a doplnení niektorých zákonov.

- MAHONEY, M.J. Publication prejudices: An experimental study of confirmatory bias in the peer review system. In *Cognitive Therapy and Research*, 1997, 1 (2), s. 161–175.

- MACHAJOVÁ, J. *Základy priestupkového práva. Komentár*. Šamorín: Heuréka, 1998, s. 73. Porovnaj SREBALOVÁ, M. a kolektív. *Zákon o priestupkoch. Komentár*. 2. vydanie. Bratislava: C. H. Beck, 2020, komentár k § 49, dostupné na beck-online.sk.

- MARSDEN, CH. – MEYER, T. – BROWN, I. Platform values and democratic elections: How can the law regulate digital disinformation? In *Computer Law & Security Review*, Volume 36, April 2020, 105373.

- MARTEL, C. - PENNYCOOK, G. - RAND, D. G. Reliance on emotion promotes belief in fake news. In *Cognit. Res. Princ. Implic*. 5, 47 (2020).

- MEDELSKÝ, J., LACA, N. *Dezinformácie a právo (úlohy a postavenie bezpečnostných zložiek)*. Zborník príspevkov. Bratislava. Akadémia Policajného zboru v Bratislave. 2022.

- MEEL, P. - VISHWAKARMA, D. K. Fake news, rumor, information pollution in social media and web: A contemporary survey of state-of-the-arts, challenges and opportunities. In *Expert Systems with Applications*. 2020. Vol. 153, s. 112986. DOI 10.1016/j.eswa.2019.112986.

- MERRILL, J. – OREMUS, W. *Facebook prioritized 'angry' emoji reaction posts in news feeds*. The Washington Post. Dostupné na: https://www.washingtonpost.com/technology/2021/10/26/facebook-angry-emoji-algorithm/.

- MESARČÍK, M. Ale prečo? predbežná analýza návrhu zákona o opatreniach na zvýšenie bezpečnosti a dôveryhodnosti platforiem v on-line prostredí. In ŤAŽKÁ, V. (ed). *Míľniky práva v stredoeurópskom priestore 2023*. Bratislava : Právnická fakulta Univerzity Komenského v Bratislave., 2023, s. 122 – 133.

- MESARČÍK, M. a kol. *Analysis of selected regulations proposed by the European Commission and technological solutions in relation to the dissemination of disinformation and the behaviour of online platforms*. 2022. Dostupné na: https://kinit.sk/sk/publikacia/dissemination-of-disinformation-and-the-behaviour-of-online-platforms/.

- MESARČÍK, M. a kol. *Analysis of selected regulations proposed by the European Commission and technological solutions in relation to the dissemination of disinformation and the behaviour of online platforms*. 2022. Dostupné na: https://kinit.sk/sk/publikacia/dissemination-of-disinformation-and-the-behaviour-of-online-platforms/.

- MESARČÍK, M. Potrebujeme nový zákon o ochrane osobných údajov? (1. časť). In *Justičná revue*. - Roč. 73, č. 1 (2021), s. 17-29.

- MESARČÍK, M. Potrebujeme nový zákon o ochrane osobných údajov? (2. časť). In *Justičná revue*. - Roč. 73, č. 2 (2021), s. 184-193.

- MICHIELS, L. What Are Filter Bubbles Really? A Review of the Conceptual and Empirical Work. In *Adjunct Proceedings of the 30th ACM Conference on User Modeling, Adaptation and Personalization* (UMAP '22 Adjunct). Association for Computing Machinery, New York, NY, USA, s. 274–279. Dostupné na: https: //doi.org/10.1145/3511047.3538028.

- MINISTERSTVO OBRANY SR. *Akčný plán koordinácie boja proti hybridným hrozbám 2022 – 2024*. Dostupné na: https://www.nbu.gov.sk/wp-content/uploads/2022/08/AKCNY-PLAN-KOORDINACIE-BOJA-PROTI-HYBRIDNYM-HROZBAM.pdf.

- MOSTERT, F. - LAMBERT, J. *Study on IP Enforcement Measures, Especially Anti-Piracy Measures in the Digital Environment*. WIPO/ACE/14/7 (2019).

- MOTYL, M. - IYER, R. - OISHI, S. - TRAWALTER, S. - NOSEK, B. A. How ideological migration geographically segregates and polarizes groups. In *Journal of Experimental Social Psychology*, 2014, 51, s. 1–14.

- Nález Ústavného súdu Slovenskej republikym sp. zn. PL. ÚS 26/2019,.

- Nález Ústavného súdu SR, sp. zn. II. ÚS 307/2014 z 18. decembra 2014 . ZNUÚS 2014.

- Nález Ústavného súdu SR, sp. zn. III. ÚS 288/ zo dňa 05.12.2017.

- Nález Ústavného súdu SR, sp. zn. PL. ÚS 26/2019 zo dňa 26.05.2021.

- Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti). Ú. v. EÚ L 151, 7.6.2019, s. 15 – 69.

- Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2065 z 19. októbra 2022 o jednotnom trhu s digitálnymi službami a o zmene smernice 2000/31/ES (akt o digitálnych službách). OJ L 277, 27.10.2022, s. 1–102.

- Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2065 z 19. októbra 2022 o jednotnom trhu s digitálnymi službami a o zmene smernice 2000/31/ES (akt o digitálnych službách).

- NÁRODNÝ BEZPEČNOSTNÝ ÚRAD. *Koncepcia pre boj Slovenskej republiky proti hybridným hrozbám*. Dostupné na: https://www.nbu.gov.sk/wp-content/uploads/PHHD/Koncepcia-boja-SR-proti-hybridnym-hrozbam.pdf.

- NÁRODNÝ BEZPEČNOSTNÝ ÚRAD. *Krátky slovník hybridných hrozieb*. Dostupné na: https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/kratky-slovnik-hybridnych-hrozieb/index.html.

- Návrh nariadenia Európskeho parlamentu a Rady, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie (Akt o umelej inteligencií) a menia niektoré legislatívne akty únie. COM/2021/206 final.

- Návrh nariadenia Európskeho parlamentu a Rady, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie (Akt o umelej inteligencii) a menia niektoré legislatívne akty únie

- NESVADBA, A. – MARKOVÁ, V. Šírenie dezinformácií a možné trestnoprávne následky v zmysle Trestného zákona. In MEDELSKÝ, J., LACA, N. 2022. *Dezinformácie a právo (úlohy a postavenie bezpečnostných zložiek).* Zborník príspevkov. Bratislava. Akadémia Policajného zboru v Bratislave, s. 167.

- *Netzwerkdurchsetzungsgesetz*. Dostupné na: https://www.bmj.de/DE/Themen/FokusThemen/NetzDG/NetzDG_EN_node.html;jsessionid=0012EB9BAA0F22E45E36BA0E408CB648.2_cid297.

- NEVICKÁ, D. Rovnaké zaobchádzanie a ochrana práce. In *Legislatívny rámec a prípadové štúdie k Pracovnému právu 2*. 1. vyd. Bratislava : Wolters Kluwer SR, 2020, s. 43-59.

- NIKOLAS GUGGENBERGER. *The Network Enforcement Act*. Dostupné na: https://wilmap.stanford.edu/entries/network-enforcement-act.

- NORDEMANN, J. Website Blocking under EU Copyright Law. In ROSATI, E. (ed.). *The Routledge Handbook of EU Copyright Law* (Routledge 2021), s. 359-361.

- NYHAN, B. - REIFLER, J. When corrections fail: the persistence of political misperceptions. In *Political Behav*. 32, 303–330 (2010).

- Ó FATHAIGH, R. - HELBERGER, N. - APPELMAN, N. The perils of legally defining disinformation. In *Internet Policy Review*, 2021, 10(4). https://doi.org/10.14763/2021.4.1584.

- *Obranná stratégia Slovenskej republiky*. 2021. Dostupné na: https://www.mosr.sk/data/files/4286_obranna-strategia-sr-2021.pdf.

- OECD. *Dark Commercial Patterns*. OECD Digital Economy Papers October 2022 No. 336. Dostupné na:. https://www.oecd.org/digital/dark-commercial-patterns-44f5e846-en.htm.

- OLDENBOURG, A. Digital Freedom and Corporate Power in Social Media'. In *Critical Review of International Social and Political Philosophy*. 2022. Dostupné na: https://doi.org/10.1080/13698230.2022.2113229.

- OLEJÁR, D. Krátky úvod do informačnej a kybernetickej bezpečnosti. In ANDRAŠKO, J. – GÁBRIŠ, T. – HOCHMANN, J. – OLEJÁR, D. *Zákon o kybernetickej bezpečnosti. Komentár*. Bratislava: Wolters Kluwer SR, 2018, s. 14-15.

- *OZNÁMENIE KOMISIE EURÓPSKEMU PARLAMENTU, RADE, EURÓPSKEMU HOSPODÁRSKEMU A SOCIÁLNEMU VÝBORU A VÝBORU REGIÓNOV Boj proti dezinformáciám na internete: európsky prístup*. COM/2018/236 final. Dostupné na: https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX%3A52018DC0236.

- *OZNÁMENIE KOMISIE EURÓPSKEMU PARLAMENTU, RADE, EURÓPSKEMU HOSPODÁRSKEMU A SOCIÁLNEMU VÝBORU A VÝBORU REGIÓNOV o akčnom pláne pre európsku demokraciu*. COM/2020/790 final. Dostupné na: https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=COM%3A2020%3A790%3AFIN&qid=1607079662423.

- PAMMENT, J. *The EU's Role in Fighting Disinformation: Taking Back the Initiative*. Carnegie Endowment for International Peace, 2020, s. 16-17.

- PARISER, E. *The filter bubble: What the internet is hiding from you*. New York: Penguin Press, 2011.

- PENNYCOOK, G. - RAND, D. G. Lazy, not biased: susceptibility to partisan fake news is better explained by lack of reasoning than by motivated reasoning. In *Cognition* 188, 39–50 (2019).

- PENNYCOOK, G. - RAND, D. G. The psychology of fake news. In *Trends Cognit. Sci*. 25, 388–402 (2021).

- *Pracovný materiál Kancelárie Rady na rokovanie Rady dňa 22. 2. 2023, Podnet týkajúci sa nelegálneho obsahu č.: AO-RPMS/2022/00139*.

- *Pracovný materiál Kancelárie Rady na rokovanie Rady dňa 22. 2. 2023, Podnet týkajúci sa nelegálneho obsahu č.: AO-RPMS/2023/01084*.

- *Pracovný materiál Kancelárie Rady na rokovanie Rady dňa 25. 1. 2023, Podnet týkajúci sa nelegálneho obsahu č.: AO-RPMS/2023/00143*.

- *Pracovný materiál Kancelárie Rady na rokovanie Rady dňa 7. 12. 2022, podnet týkajúci sa nelegálneho obsahu č.: AO-RPMS/2022/00254*.

- QUEEN, J. *Alex Jones must pay Sandy Hook families nearly $1 billion for hoax claims, jury says*. Reuters. Dostupné na: https://www.reuters.com/legal/jury-begins-third-day-deliberations-alex-jones-sandy-hook-defamation-trial-2022-10-12/.

- QUINTAIS, J. P. *Generative AI, Copyright and the AI Act*. Kluwer Copyright Blog. Dostupné na: https://copyrightblog.kluweriplaw.com/2023/05/09/generative-ai-copyright-and-the-ai-act/.

- RADA PRE MEDIÁLNE SLUŹBY. *Zasadnutia Rady pre mediálne služby*. Dostupné na: https://rpms.sk/o-nas/zasadnutia/zasadnutia-rady.

- RADA PRE MEDIÁLNE SLUŽBY. *Teroristický útok na Zámockej ulici v Bratislave: bezprostredné a preventívne aktivity Rady pre mediálne služby na zamedzenie šírenia nelegálneho a škodlivého obsahu. Správa o reakciách digitálnych platforiem na útok a o ich podiele na radikalizácii páchateľa*. Dostupné na webovom sídle Rady pre mediálne služby.

- RADA PRE MEDIÁLNE SLUŽBY. *Teroristický útok na Zámockej ulici v Bratislave: bezprostredné a preventívne aktivity Rady pre mediálne služby na zamedzenie šírenia nelegálneho a škodlivého obsahu. Správa o reakciách digitálnych platforiem na útok a o ich podiele na radikalizácii páchateľa*. Dostupné na webovom sídle Rady pre mediálne služby.

- REDAKCIA ČASOPISU ZO SÚDNEJ PRAXE. Ochrana osobných údajov a ochrana súkromia v novej legislatívnej kvalite. In *Zo súdnej praxe* 3/2018.

- REGLITZ, M. Fake News and Democracy. In *Journal of Ethics & Social Philosophy*, vol. 22/no. 2, (2022).

- *Report of the independent High level Group on fake news and online disinformation. A Multi-Dimensional Approach to Disinformation*, s. 22. Dostupné na: https://op.europa.eu/sk/publication-detail/-/publication/6ef4df8b-4cea-11e8-be1d-01aa75ed71a1.

- REUTERS. *Reuters Institute Digital News Report 2023*. 2023. Dostupné na: https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2023-06/Digital_News_Report_2023.pdf.

- RODRÍGUEZ-POSE, A. - VON BERLEPSCH, V. Social capital and individual happiness in Europe. In *Journal of Happiness Studies*, 15, s. 357–386. Dostupné na: http://dx.doi.org/10.1007/s10902-013-9426-y.

- ROZHLAS A TELEVÍZIA SLOVENSKA. *Verdikt v spore lekára Sabaku s hnutím Republika by mohol padnúť o necelý mesiac*. Dostupné na: https://spravy.rtvs.sk/2023/06/sudny-spor-lekara-p-sabaku-s-hnutim-republika-vrcholi-verdikt-by-mohol-padnut-o-necely-mesiac/.

- Rozhodnutie Európskeho súdu pre ľudské práva. Sťažnosť č. 39378/15. STANDARD VERLAGSGESELLSCHAFT MBH v. AUSTRIA (č. 3) zo dňa 7 decembra 2022.

- Rozhodnutie Európskeho súdu pre ľudské práva vo veci Animal Defenders International v. the United Kingdom. Sťažnosť č. 48876/08 zo dňa 22 Apríla 2013.

- Rozhodnutie Európskeho súdu pre ľudské práva vo veci Garaudy v. France. Sťažnosť č. 65831/01 zo dňa 24 Júna 2003.

- Rozhodnutie Európskeho súdu pre ľudské práva vo veci Hertel v. Switzerland. Sťažnosť č. 25181/94 zo dňa 25 Augusta 1998.

- Rozhodnutie Európskeho súdu pre ľudské práva vo veci Kenedi v. Hungary. Sťažnosť č. 31475/05 zo dňa 26 May 2009.
- Rozhodnutie Európskeho súdu pre ľudské práva vo veci Salov v. Ukraine. Sťažnosť č. 65518/01 zo dňa 6 September 2005.
- Rozhodnutie Európskeho súdu pre ľudské práva vo veci Sdružení Jihočeské Matky v. Czech Republic. Sťažnosť č. 19101/03.
- *Rozhodnutie Rady (SZBP) 2022/351 z 1. marca 2022, ktorým sa mení rozhodnutie 2014/512/SZBP o reštriktívnych opatreniach s ohľadom na konanie Ruska, ktorým destabilizuje situáciu na Ukrajine*, Ú. v. EÚ L 65, 2.3.2022.
- Rozhodnutie Súdneho dvora EÚ C-682/18 zo dňa 22. júna 2021 Frank Peterson proti Google LLC a i. a Elsevier Inc. proti Cyando AG.
- Rozhodnutie Súdneho dvora EÚ C-360/10 zo dňa 16. Februára 2012 vo veci SABAM v Netlog.
- Rozhodnutie Súdneho dvora EÚ č. C-324/09 vo veci z 12. júla 2011 L'Oréal SA a iní proti eBay International AG a iní
- Rozhodnutie Súdneho dvora EÚ spojené veci C-236/08 až C-238/08 z 23. marca 2010 Google.
- Rozhodnutie Súdneho dvora EÚ z 24. septembra 2019 *GC a i. v. Commission nationale de l'informatique et des libertés (CNIL)*. Vec č. C-136/17.
- Rozhodnutie Súdneho dvora EÚ z 9. novembra 2023 vo veci C-376/22, Google Ireland Limited, Meta Platforms Ireland Limited, Tik Tok Technology Limited proti Kommunikationsbehörde Austria (KommAustria).
- Rozhodnutie Súdneho dvora Európskej únie C-622/17, Baltic Media Alliance v. Lietuvos radijo.
- Rozhodnutie Súdneho dvora Európskej únie vo veci *RT France v. Council of the European Union*, vec č. T-125/22.
- Rozhodnutie Súdneho dvora Európskej únie, sp. zn C-101/01- Lindqvist.
- Rozhodnutie Súdneho dvora Európskej únie, sp. zn C-212/13-Ryneš.
- Rozhodnutie Súdneho dvora Európskej únie, sp. zn C-582/14 Patrick Breyer proti Bundesrepublik Deutschland.
- Rozhodnutie Súdneho dvora Európskej únie, sp. zn. C-274/99, Connolly v. Commission.
- Rozsudok Krajského súdu Trenčín, sp. zn. 5Co/8/2016.
- Rozsudok Krajského súdu Žilina, sp. zn. 25Sa/3/2021.
- Rozsudok Špecializovaného trestného súdu sp. zn. 2T/31/2019 zo dňa 16. 12. 2019

- RYSER, R. *Alex Jones back on the hook for damages after bankruptcy judge sends Sandy Hook cases to Texas court*. The News-Times. Dostupné na: https://www.newstimes.com/news/article/Alex-Jones-back-on-the-hook-for-damages-after-17187680.php.

- SAMPLE, I. *What are deepfakes – and how can you spot them?* The Guardian. Dostupné na: https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them.

- SARITHA, R. *In Just 21 Days, Facebook Led New India User to Porn, Fake News*. Bloomberg. Dostupné na: https://www.bloomberg.com/news/articles/2021-10-23/how-facebook-s-algorithm-led-a-new-india-user-to-fake-news-violence?sref=X1c60Hpu.

- SARTER, M. - GEHRING, J.W. - KOZAK, R. More attention must be paid: The neurobiology of attentional effort. In *Brain Research Reviews*, Volume 51, Issue 2, 2006, s. 145-160, ISSN 0165-0173. Dostupné: https://doi.org/10.1016/j.brainresrev.2005.11.002.

- SAURWEIN, F. - SPENCER-SMITH, CH. *Combating Disinformation on Social Media: Multilevel Governance and Distributed Accountability in Europe, Digital Journalism*. 2021. Dostupné na: 10.1080/21670811.2020.1765401.

- SAVIN, A. The EU Digital Services Act: Towards a More Responsible Internet. In *Copenhagen Business School Law Research Paper Series No. 21-04*. Dostupné na: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3786792.

- SCARANTINO, A. - PICCININI, G. Information without truth. In *Metaphilosophy*, 2021, 41(3), s. 313–330.

- SHATTOCK, E. Fake News in Strasbourg: Electoral Disinformation and Freedom of Expression in the European Court of Human Rights (ECtHR). *European Journal of Law and Technology*, vol. 13/no. 1, (2022).

- SHATTOCK, E. Fake News in Strasbourg: Electoral Disinformation and Freedom of Expression in the European Court of Human Rights (ECtHR). In *European Journal of Law and Technology*, vol. 13/no. 1, (2022).

- SHATTOCK, E. Self-Regulation 2:0? A Critical Reflection of the European Fight Against Disinformation. In *Harvard Kennedy School Misinformation Review*., vol. 2/no. 3, (2021).

- SHTULMAN, A. - VALCARCEL, J. Scientific knowledge suppresses but does not supplant earlier intuitions. In *Cognition* 124, 209–215 (2012).

- SCHUETT, J. *Defining the Scope of AI Regulations*. Forthcoming in Law, Innovation and Technology, Legal Priorities Project Working Paper Series No. 9. Dostupné na: https://ssrn.com/abstract=3453632.

- SKITKA, L. J. - MOSIER, K. L. - BURDICK, M. Does automation bias decision-making? In *International Journal of Human-Computer Studies*, 1999, 51, 991-1006.

- SKYRMS, B. *Signals: Evolution, Learning, and Information*. Oxford: Oxford University Press, 2010.

- *Slovník súčasného slovenského jazyka*. Dezinformácia. 2015. Dostupné na: https://slovnik.juls.savba.sk/?w=dezinformacia+&s=exact&c=a31c&cs=&d=sssj#.

- Speech and Privacy. In *UC Irvine Journal of International, Transnational, and Comparative Law*, 2021, 6, s. 9–36.

- *SPOLOČNÉ OZNÁMENIE EURÓPSKEMU PARLAMENTU, EURÓPSKEJ RADE, RADE, EURÓPSKEMU HOSPODÁRSKEMU A SOCIÁLNEMU VÝBORU A VÝBORU REGIÓNOV Akčný plán proti dezinformáciám*. JOIN/2018/36 final. Dostupné na: https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX%3A52018JC0036.

- SRBA, I. et al. Auditing YouTube's Recommendation Algorithm for Misinformation Filter Bubbles. In *ACM Transactions on Recommender Systems*. 1, 1, Article 6 (March 2023), Dostupné na: 10.1145/3568392.

- SREBALOVÁ, M. a kolektív. *Zákon o priestupkoch. Komentár*. 2. vydanie. Bratislava: C. H. Beck, 2020, dostupné na beck-online.sk.

- *Stanovisko Generálneho Advokáta Priit Pikamäe predneseného dňa 16.3.2023 vo veci C-634/21 OQ proti Land Hessen za účasti: SCHUFA Holding AG*.

- STRÉMY, T. – KURILOVSKÁ, L. *Trestný zákon. Komentár Zväzok II*. Wolters Kluwer, 2022.

- STUCKE, E. M. – EZRACHI, A. *The Subtle Ways Your Digital Assistant Might Manipulate You*. The Wired. November 2016. Dostupné na: https://www.wired.com/2016/11/subtle-ways-digital-assistant-might-manipulate/.

- ŠIMKO, J a kol. Towards Continuous Automatic Audits of Social Media Adaptive Behavior and its Role in Misinformation Spreading. In *29th ACM Conference on UMAP'21*.

- TASR. *Tragickú streľbu v Bratislave prekvalifikovali na teroristický útok*. teraz.sk (Bratislava: TASR). Dostupné na: https://www.teraz.sk/slovensko/tragicku-strelbu-v-bratislave-prekvali/667778-clanok.html.

- UNITED NATIONS – HUMAN RIGHTS, OFFICE OF THE HIGH COMMISSIONER. *New and emerging technologies need urgent oversight and robust transparency: UN experts*. Dostupné na: https://www.ohchr.org/en/press-releases/2023/06/new-and-emerging-technologies-need-urgent-oversight-and-robust-transparency.

- Úrad na ochranu osobných údajov SR. *Zoznam spracovateľských operácií podliehajúcich posúdeniu vplyvu na ochranu osobných údajov Slovenskej republiky*. Dostupné na https://dataprotection.gov.sk/uoou/sites/default/files/zoznam_spracovatelskych_operacii_ktore_podliehaju_posudeniu_vplyvu.pdf.

- ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY. *Koordinovaný mechanizmus odolnosti Slovenskej republiky voči informačným operáciám*.

- ÚRAD VLÁDY SR. *Koncepcia strategickej komunikácie Slovenskej republiky*. 2023. Dostupné na: https://www.slov-lex.sk/legislativne-procesy/-/SK/LP/2023/56.
- UUK, R. et al. *Operationalising the Definition of General Purpose AI Systems: Assessing Four Approaches*. 2023. Dostupné na: https://ssrn.com/abstract=4471151.
- Uznesení Nejvyššíhou soudu České republiky, sp. zn. 3 Tdo 288/2021 zo dňa 19.05.2021.
- Uznesenie Krajského súdu v Bratislave sp. zn. 5Co/95/2022 zo dňa 21. 07. 2022.
- Uznesenie Krajského súdu v Prešove sp. zn. 9Co/14/2022 zo dňa 29. 03. 2022.
- Uznesenie Najvyššieho súdu sp. zn. 2To/4/2020 zo dňa 26. 10. 2021.
- Uznesenie Okresného súdu Bratislava I. sp. zn. 21C/12/2022 zo dňa 22. 03. 2022
- Uznesenie Okresného súdu Kežmarok sp. zn. 8C/71/2021 zo dňa 06. 12. 2021
- VAN DER LINDEN, S. - LEISEROWITZ, A. - ROSENTHAL, S. - - MAIBACH, E. Inoculating the public against misinformation about climate change. In *Global Challenges*, 2017, 1, 1600008. Dostupné na: http://dx.doi.org/10.1002/gch2.201600008.
- VAN HOBOKEN, J. - Ó FATHAIGH, R. Regulating Disinformation in Europe: Implications for
- VARIAN, H. Computer Mediated Transactions. In *American Economic Review: Papers and Proceedings*. 100 (2): s. 1–10.
- VEALE, M. - ZUIDERVEEN BORGESIUS, F. Demystifying the Draft EU Arti ficial Intelligence Act — Analysing the good, the bad, and the unclear elements of the proposed approach. In *Computer Law Review International*, vol. 22, no. 4, 2021.
- VEALE, M. - ZUIDERVEEN BORGESIUS, F. Demystifying the Draft EU Arti ficial Intelligence Act — Analysing the good, the bad, and the unclear elements of the proposed approach. In *Computer Law Review International*, vol. 22, no. 4, 2021.
- VERMEULEN, M. Researcher Access to Platform Data: European Developments. In *Journal of Online Trust and Safety*, 1(4), 2022. Dostupné na: https://doi.org/10.54501/jots.v1i4.84.
- VOOSE, P. How AI Detectives Are Cracking Open the Black Box of Deep Learning. In *Science*, July 06, 2017. Dostupné na: https://www.science.org/content/article/how-ai-detectives-arecracking-open-black-box-deep-learning.
- VOSOUGHI, S. - ROY, D. - ARAL, S. The Spread of True and False News Online. In *Science* 359, no. 6380 (2018): 1146–51. Dostupné na: https://www.science.org/doi/full/10.1126/science.aap9559.
- VRABKO, M. a kol. *Správne právo hmotné*. 2. vydanie. Praha: C.H. Beck, 2018.

- WACHTER, S. – MITTLESTADT, B. – FLORIDI, L. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. In *International Data Privacy Law*, Volume 7, Issue 2, May 2017, s. 76–99.

- WARDLE, C. – DERAKSHAN, H. *Information Disorder: Toward an interdisciplinary framework for research and policy making*. Council of Europe, report DGI (2017) 09, 2017.

- WEEKS, B. E. Emotions, partisanship, and misperceptions: how anger and anxiety moderate the effect of partisan bias on susceptibility to political misinformation. In *J. Commun*. 65, 699–719 (2015).

- WIGHT, C. Post-Truth, Postmodernism and Alternative Facts. In *New Perspectives*, vol. 26, no. 3, 2018, s. 17–30. JSTOR, https://www.jstor.org/stable/26675072

- WOLFRAM, S. *Testifying at the Senate about AI-Selected Content on the Internet*. Stephen Wolfram Writings blog, June 25, 2019. Dostupné na: https://writings.stephenwolfram.com/2019/06/testifying-at-the-senate-about-a-i-selected-content-on-the-internet/.

- WORLD HEALTH ORGANIZATION. Infodemic. WHO Website, 2021. Dostupné na: https://www.who.int/health-topics/infodemic#tab=tab_1.

- WSJ SRAFF. *Inside TikTok's Algorithm: A WSJ Video Investigation*. Wall Street Journal, July 21, 2021. Dostupné na: https://www.wsj.com/articles/tiktok-algorithm-video-investigation-11626877477.

- WU, T. *The attention merchants: the epic scramble to get inside our Heads*. Knopf, 2016.

- YONELINAS, A. P. The nature of recollection and familiarity: Aa review of 30 years of research. In *J. Mem. Lang*. 46, 441–517 (2002).

- YOUNG, Z. *French Parliament passes law against 'fake news*.' Politico. Dostupné na: https://www.politico.eu/article/french-parliament-passes-law-against-fake-news/. Text zákona vo francúzštine dostupný na: https://www.assemblee-nationale.fr/dyn/15/textes/l15b0799_proposition-loi.

- ZAKÁCS, J. -BOGNÁR, É. *The impact of disinformation campaigns about migrants and minority groups in the EU*. IN-DEPTH ANALYSIS Requested by the INGE committee.

- Zákon č. 264/2022 Z. z. o mediálnych službách a o zmene a doplnení niektorých zákonov (zákon o mediálnych službách).

- Zákon č. 372/1990 Zb. o priestupkoch.

- Zákon č. 46/1993 Z. z. o Slovenskej informačnej službe.

- Zákon č. 500/2022 Z. z. o Vojenskom spravodajstve.

- Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.

- ZOU, A. et al. *Universal and Transferable Adversarial Attacks on Aligned Language Models*. Dostupné na: https://arxiv.org/abs/2307.15043.

- ZUBOFF, S. Surveillance Capitalism and the Challenge of Collective Action. In *New Labor Forum*. 28 (1): s. 10–29. doi:10.1177/1095796018819461. ISSN 1095-7960.

- ZUBOFF, S. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs, 1. vydanie, 2019.

- ZUIDERVEEN BORGESIUS, F.L. et al. Should We Worry about Filter Bubbles? In *Internet Policy Review* (March 2016).

EXTENDED SUMMARY

In the presented book, we have dealt with the phenomenon of misinformation from the perspective of public law instruments that could significantly help in preventing its spread in the online space. At the beginning of the thesis, we set out a research question and three hypotheses, which we have gradually verified through our research. At the beginning of the book, we have identified three limitations of the research. The first limitation is the concentration of the research on public law due to the potential relevance of systemic tools dealing with disinformation. The second limitation is the emphasis on regulations applicable to online space, where disinformation spreads the most. The third limitation is the focus on general regulations instead of specific or sectoral regulation including political micro-targeting or media freedom.

The first chapter of this thesis dealt with the concept of disinformation, its legal definition, and the context in which disinformation is spread. Doctrine approaches the concept of disinformation in different ways, but the most common conceptual features of disinformation include the deliberate dissemination of verifiably false information with a specific objective, whether in the form of economic gain or a threat to democratic values such as trust in the state system, fundamental human rights, and freedoms, or electoral processes. Other concepts, especially misinformation, which is not disseminated deliberately, should be distinguished from the concept of disinformation. Strategic documents at the EU and Slovak Republic level also take different approaches to the definition of disinformation. In terms of a legal definition, neither Slovak nor EU law contains a definition of disinformation. The concept is only very sparingly addressed in the case law of the Constitutional Court of the Slovak Republic, the Supreme Court of the Slovak Republic, the Supreme Administrative Court of the Slovak Republic, and regional courts. These judicial bodies have only minimally provided a more analytical distinction between the concepts of disinformation and untruth.

The first hypothesis of this thesis was formulated as follows: "The legal order of the Slovak Republic or the European Union defines the concept of disinformation." This hypothesis could not be verified; the above-mentioned legal orders do not legally define the concept of disinformation. The proposed legislation in the form of the Slovak draft law on measures to increase the security and trustworthiness of platforms in the online environment did not define disinformation in the way that the doctrine treats the concept. The proposed definition required disinformation to be quite obviously false information that may trigger various interpretative approaches from judicial or administrative bodies.

In the first chapter, we discussed the life cycle of misinformation, the motives for sharing it, and especially the factors that influence the spread and trust in misinformation. Based on review studies from outside the legal sciences, we identified the following factors affecting the spread and trust in disinformation:

Field	Factors
Psychology	Cognitive factors include thinking by intuition, cognitive failures, and illusory truth
	Socially affective factors include source of information, emotions, and personal faith and beliefs
Sociology	Decrease of social capital
	Increase of inequality
	The increasing polarization of society
	Distrust in science
	Evolution of the media environment
Economy	Attention economy
	Surveillance capitalism
Technical factors	Personalization of content via recommender systems (artificial intelligence)
	Filter bubbles

Psychological factors influence why individuals believe in disinformation. These factors include a combination of preference of thinking by intuition over critical analysis of information, confirmation biases and cognitive biases, and living in illusory truth based on familiarity of disinformation and coherency with personal beliefs. Disinformation is attractive as it offers a simple perception of complex issues.[763] Furthermore, socially effective factors are important as well. These include sources of disinformation where publicly known figures are more believable, emotions in disinformation or emotive perception of them, and locking persons into echo chambers.[764]

[763] For an overview see e.g. ECKER, U.K.H. - LEWANDOWSKY, S. - COOK, J. et al. The psychological drivers of misinformation belief and its resistance to correction. In *Nat Rev Psychol* 1, 13–29 (2022). https://doi.org/10.1038/s44159-021-00006-y.

[764] See e.g. PENNYCOOK, G. - RAND, D. G. The psychology of fake news. In *Trends Cognit. Sci.* 25, 388–402 (2021).

Sociological drivers reflect a decrease in social capital (empathy and trust) and an increase in inequality. These factors are prevalent also in the Slovak Republic based on recent surveys and research. Trust in public bodies and democracy has decreased over the last few years.[765] An increase in inequality contributes to beliefs towards disinformation as social stress is a contributing factor. Further sociological drivers consist of an increase in polarization, distrust in scientific knowledge (evident in the Slovak Republic as well), and the evolution of the media environment with a shift towards digital media.[766]

Economic factors oscillate around concepts of attention economy based on monetizing human attention as a resource. Prediction of relevant content and amplification of potential catching attention content is at the heart of the concept to benefit from advertisements display. Together with the commodification of personal data by digital services (surveillance capitalism) these factors severely influence trust in disinformation.

From the point of technical factors, settings and functioning of recommender systems on digital media are of the essence as this is the crucial tool for content personalization. The specific issue connected to recommender systems is an amplification of disinformation or illegal content. Filter bubbles and locking users into them is a separate issue connected to content personalization from the technical view.

We then took these factors into account in Chapter Four when assessing the suitability of public law tools for combating misinformation in the online space.

We have also analyzed the proposed methodology for classifying the intensity and influence of information operations (including the spread of disinformation) based on Coordinated mechanisms of resilience against information operations. This methodology evaluates several criteria including the potential of causing harm, the potential for the call to action, the size of the audience of information operation, who is subject that creates the information operation, the influence of the subject, the likelihood of influence of addresses, the trustworthiness of information operation, coordination of spread, the channel of spread, geographical origin of information operation, potential crime liability of subject, the existence of neutralization

[765] See e.g. *Ako sa máte Slovensko? Dôvera v inštitúcie*. Dostupné na: https://www.akosamateslovensko.sk/tema/dovera-v-institucie/ or DEKK. *TRENDY [NE]DÔVERY 2023. Správa o stave [ne]dôvery na Slovensku*. Dostupné na: https://www.dekk.institute/trendy-ne-dovery-2023/.

[766] See e.g. LEWANDOWSKY, S. - ECKER, U. K. H. - COOK, J. Beyond misinformation: Understanding and coping with the "post-truth" era. In *Journal of Applied Research in Memory and Cognition*, 2017, 6(4), s. 353–369. Dostupné na: https://doi.org/10.1016/j.jarmac.2017.07.008.

mechanisms and other relevant circumstances.[767] Information operations are after evaluation of the criteria assessed as critical, high, disturbing, or negligible.

The second chapter examined policy documents at the EU and Slovak Republic levels that provide the necessary context for the adoption of regulatory measures to combat online disinformation.

At the EU level, mention can be made of activities since the establishment of the High-Level Expert Group on Fake News and Online Disinformation, composed of media experts, academics, fact-checkers, civil society, and platforms, which produced a final report with recommendations on combating disinformation. At the same time, this group also presented a suitable definition of the term disinformation. Other strategic documents at the EU level in the fight against online disinformation were the 2018 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions Combating Online Disinformation: a European Approach, the 2018 Joint Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on an Action Plan against Disinformation and the 2020 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on an Action Plan for European Democracy. These documents successively call for investment in education, transparency, and accountability of digital platforms or regulation.

Within the Slovak Republic, several strategic documents have also been presented that perceive disinformation as a hybrid threat or negative phenomenon with a need for further action. Namely, we can mention the Concept for the Slovak Republic's fight against hybrid threats from 2018, the Security Strategy of the Slovak Republic from 2021, the Defense Strategy of the Slovak Republic from 2021, the Coordinated Mechanism for the Slovak Republic's Resilience to Information Operations from 2021, the Action Plan for the Coordination of the Fight against Hybrid Threats 2022-2024 and last but not least the Concept for Strategic Communication of the Slovak Republic from 2023. The most detailed commitments for specific public authorities are presented in the Action Plan for the Coordination of Combating Hybrid Threats. We consider particularly important the adoption of the 2023 Concept of Strategic Communication of the

[767] ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY. *Koordinovaný mechanizmus odolnosti Slovenskej republiky voči informačným operáciám*, p. 11 – 12.

Slovak Republic, which repeatedly emphasizes the role of the state and its communications in the dissemination of disinformation.

The third chapter, named Public Law Instruments for Combating Disinformation in the Online Environment, analyses the identified regulations and derives specific institutes potentially relevant in combating online disinformation. From a regulatory perspective, the focus is not only on the instruments directly responding to disinformation content but also on the environment in which disinformation is disseminated and the instruments that facilitate the dissemination of disinformation.

In terms of the environment, we examined the regulation of digital services and social media, where disinformation spreads exponentially. We focused on recent legislation at the EU level in the form of the Digital Services Act (DSA). The DSA contains several tools that can help in the fight against disinformation, but the regulation itself primarily focuses on illegal content, with disinformation representing 'only' harmful content. Harmful content is primarily addressed by the requirements of risk assessment mitigation and auditing. We also consider tools to increase transparency (especially recommendation systems), display advertising, and platform design to be important. Civil society institutes in the form of trusted flaggers and access to data by vetted researchers also deserve special attention. Liability for third-party content provisions only applies to illegal content.

In terms of tools to support the spread of disinformation, we have examined the proposed regulation of Artificial Intelligence (AI) in the form of the draft Artificial Intelligence Act (AIA) at the EU level. If the final version of the AIA also considers recommendation systems on very large online platforms to be high-risk AI systems, this would be a significant step towards better requirements for recommendation systems. This is because they would be subject to requirements on data governance, human oversight, or the accuracy and appropriateness of the data used. We also consider requirements for transparency of AI systems and specific rules for large language models and generative AI to be particularly important as they significantly contribute to the creation and spread of disinformation.

Furthermore, in chapter three we analyzed specific public law tools. The Slovak Media Services Act regulates specific administrative proceedings in the matter of preventing the dissemination of illegal content, which the Slovak Media Services Council may impose an obligation to delete certain content. However, the problematic part of the legislation is its narrow scope of application to a very limited number of circumstances including child pornography, incitement of terrorism, approving terroristic behavior or crimes related to denial

of the holocaust, crimes against humanity or defamation of nation, race, and belief or the offense of incitement to national, racial, and ethnic hatred. This fact is also evident from a deeper analysis of the decisions of the Media Services Council regarding the complaints lodged, which are publicly available. On many occasions, the Media Services Council postponed the complaint related to the spread of disinformation (including e.g. Kremlin propaganda) due to being out of the scope of the proceeding.

EU Member States may also adopt specific legislation containing measures to increase transparency and accountability in the online space. One such attempt in Slovakia was the proposal on measures to increase the safety and trustworthiness of platforms in the online environment, which expanded the definition of illegal content as foreseen by the Slovak Media Services Act mentioned above, enshrined measures for state interventions against disinformation and limited anonymity in online discussions. However, the draft law ran up against the limits of EU unification of these legal relations in the form of the DSA and the limits of respect for fundamental human rights and freedoms. Particularly problematic issues also related to the proposed oversight, which did not meet the criteria of impartiality and independence. The maneuvering space for such laws after the adoption of the DSA is extremely limited, perhaps non-existent.

Another instrument is the blocking of websites. This is a legitimate tool in a democratic society, but it is subject to certain limits and rules. These limits are laid down by the case law of the European Court of Human Rights and the Court of Justice of the EU. There are the requirements to carry out an impact assessment in the legislative process, independent oversight, transparency, and a fair trial (equality of arms). The blocking of websites based on harmful content, including serious disinformation, is also provided for in the Slovak Cybersecurity Act. However, the legislation, which is ineffective now, does not meet the criteria mentioned above and is subject to academic and political criticism.

Data protection legislation also provides several tools that can help to prevent the spread of misinformation in the space. This is mainly because recommendation systems on digital platforms operate based on personal data collected and, at the same time, some disinformation may relate to an identified data subject. On the one hand, we have discussed the individual rights of data subjects such as the right to information, the right to access, the right to rectification, the right to erasure, the right to restriction of processing, the right to portability, and the right to object. However, the systematic tools offered by data protection regulation seem to be much more interesting. In this regard, we have analyzed the regulation of automated

individual decision-making under Article 22 GDPR which, in certain circumstances, may also apply to the dissemination of disinformation. This is due to the problematic scope of the Article 22 GDPR. On the other hand, guidance from the EDPB analyses the display of advertising (in the broader context of content) to users, which is also based on the automated analysis of personal data. This context is crucial for the spread of disinformation online. The EDPB states that the display of advertising shall not, by default, cause a legal or similarly significant impact on the data subject. However, it is not excluded that, taking into account certain facts, online advertising may have such an impact. For our purposes, it is of the essence to draw attention to two factors, namely the invasiveness of the profiling process, including the tracking of individuals across different websites, devices, and services, and the use of knowledge of the vulnerabilities of data subjects. The display of disinformation can exploit the vulnerability of data subjects, whether in terms of geographical location or age. In certain cases, Article 22 of the GDPR could, in our view, also apply to the display of content based on personal data collected by, for example, social media.[768] At the same time, we consider the data protection impact assessment and the specifically designed and standard privacy protection as very important institutes that could reduce the risk of spreading disinformation as risks of spreading disinformation shall be identified and mitigated via these instruments.

We have also discussed the regulation of offense law in Slovakia. However, the law on offenses only applies to natural persons, and, by default, only negligence as a form of culpability is sufficient. It is the subjective aspect of committing an offense that can be problematic, as the intent is required for the dissemination of disinformation. We have analyzed the specific facts of offenses such as unauthorized impersonation of a public official, falsification of health information, and offenses against public order and civil coexistence. However, the first two offenses (unauthorized impersonation and falsification of health information) apply only in a very specific context and under very specific circumstances. On the other hand, offenses against public order and civil coexistence are constructed broadly and may be used in the context of disinformation.

Criminal law, as an *ultima ratio* remedy, also offers some interesting facts that might be applicable in a disinformation context. We have analyzed five offenses, namely the offense of defamation, the offense of spreading and disseminating false news, the offense of endangering the safety of an aircraft or ship, the offense of falsifying and making false medical records, and

[768] ARTICLE 29 DATA PROTECTION WORKING PARTY. *Guidelines on Automated Individual Decision-making and Profiling for Regulation 2016/679.* Adopted on 3 October 2017. As last Revised and Adopted on 6 February, p. 21.

the offense of terrorist attack. Again, however, the latter three offenses apply only in a very specific context and under very specific circumstances. For the offense of defamation, we consider that this offense would be applicable if the disinformation is directed at a specific individual. However, the offense of disseminating false news under section 361 and the Criminal Code appears to be much more interesting. We consider that for the most serious type of false information in the form of alarm messages, this offense is also applicable to the dissemination of disinformation. We have also analyzed the proposals for a specific offense of spreading disinformation that was submitted in 2022, but in our opinion, this proposed legislation did not reflect the fact that disinformation must be spread deliberately, and the principle of proportionality was not respected at the same time.

The last public law instruments that we dealt with were those at the disposal of the intelligence services, namely the Slovak Information Service and the Military Intelligence Service. In terms of disinformation, it is crucial that the new legislation explicitly obliges the Military Intelligence Service to obtain, aggregate, and evaluate information relating to hybrid threats and disinformation. Due to the classified regime of the Military Intelligence, we do not have comprehensive information that would allow us to analyze in more depth the fulfillment of this task and, where appropriate, the measures taken. A similar observation can be made about the legal regulation of the Slovak Information Service, which, however, does not have an explicit mandate to analyze disinformation activities or hybrid threats in the law. This does not mean, however, that disinformation activities cannot be under the scrutiny of this intelligence service.

The second hypothesis was formulated as follows: "The legal order of the Slovak Republic or the European Union provides tools to minimize the dissemination of disinformation in the online space from the perspective of the general regulation of public law." We consider that the second hypothesis has been confirmed.

In Chapter 4, we have presented a taxonomy of public law instruments for combating disinformation in online space and have also assessed the appropriateness of their use. We identified specific principles that should be applied to public law tools to combat misinformation in the online space. These principles are as follows:

- respect for freedom of expression and the right to information,
- proportionality in the assessment of disinformation,
- consideration of factors affecting trust in disinformation and the dissemination of disinformation.

In terms of freedom of expression and the right to information, we have analyzed the scope that the legislator has for regulation in limiting certain content. In the context of the case law of the European Court of Human Rights, the Court of Justice of the European Union, and the Constitutional Court of the Slovak Republic, it is clear that this space exists, but it is much more legitimate and appropriate to regulate digital platforms and the means through which disinformation is disseminated compared to direct regulation of content. The second principle is proportionality in assessing disinformation. We have analyzed several methodologies that can be used to identify the risk of influence or impact of misinformation in terms of the engagement of actors. We have adapted these methodologies to the needs of the legislator based on the decisions of the Slovak courts and have identified 9 criteria that should be taken into account when analyzing the impact of misinformation. Specifically, these are engagement on social media, exposure on social media, circulation of content, diffusion between communities, impact on mainstream media, type of actor, different formats of misinformation, call to action and danger of the story, the target of the misinformation or whether it is a matter of public interest. These criteria have specific measurable indicators identified and points are assigned to them. A particular piece of misinformation can be scored from 0 to 17 points according to the score it receives, and subsequently, misinformation can be differentiated in the context of its impact into alarming, high, medium, and low. A third principle that should be applied to public law tools should be to consider the factors that affect the confidence of misinformation and its dissemination. We have listed these factors above.

Based on the identified public law tools and taking into account the methodology for assessing the impact of disinformation, we then synthesized these findings. We consider that when the impact of disinformation is low, it is necessary to use in particular the opportunities offered by strategic communication by the state and activities to promote the development of critical thinking. At the medium intensity of disinformation, the means offered by the offense law and the space allowed by the European Union legislation in adopting specific measures requiring transparency and accountability of platforms should be used. When the impact of misinformation is high, we consider blocking websites and acting on illegal content to be appropriate tools. However, in terms of their legislative grasp, we highlight the essential modification of the institute of website blocking in such a way as to reflect the case law of the European Court of Human Rights. At the same time, we recommend that the narrow scope of the procedure for illegal content be extended at least to include the possibility of proceedings for the dissemination of false news under the Criminal Code. With the alarming impact of disinformation, we see scope for criminal liability and measures of intelligence services. In terms

of the dissemination of disinformation about phenomena, we consider that the legal regulation of the criminal offense of disinformation of false news is sufficient, as it reflects the ultima ratio principle of criminal law. Beyond the specific tools mapped to the intensity of the disinformation intervention stand the tools offered by the regulation of digital services, the regulation of recommendation systems (artificial intelligence), and the regulation of platform design. From the perspective of harmful content, including disinformation, we consider the institutes of risk assessment and mitigation and auditing, including data protection impact assessments, to be key. Rigorous risk analysis can reveal the locking of users into filter bubbles. However, we see the failure to switch off these systems by default since the digital services legislation came into force as a significant downside of the regulation of recommender systems. We particularly highlight the regulation of recommender systems in the context of the proposed AI legislation, which would focus on them in the context of data quality, human oversight, or accuracy requirements. The requirements for transparency of AI systems cannot be underestimated either. We also consider it essential to emphasize the requirements for the design of platforms, which cannot be manipulative and should reflect the highest requirements in terms of data protection for the user. Civil society tools are worthy of attention, as they should monitor whether digital platforms are not widely disseminating harmful content and should also be the watchdog to ensure that the state does not adopt overly invasive regulations aimed at restricting freedom of expression and the right to information.

The third hypothesis focuses on examining the proportionality and effectiveness of selected tools that can be used to minimize the spread of misinformation in the online environment through public law norms and is formulated as follows: "The legal order of the Slovak Republic or the European Union provides proportionate and effective tools to minimize the spread of misinformation in the online space from the perspective of general public law regulation." This hypothesis has not been confirmed. This is because we have identified several legislative gaps in the regulation of public law instruments linked to the online information space. At the same time, we consider that the principle of proportionality should be better taken into account precisely in the application of individual instruments, which is not always the case in application practice.

In examining the phenomenon of disinformation from the perspective of public law instruments, we set the following research question: "Public law provides sufficient effective tools for minimizing the spread and impact of disinformation in the online space." Thus, the research question can be answered as follows. Although public law provides sufficient tools to minimize the spread and impact of misinformation in the online space, especially in terms of regulating

the environment and tools for its dissemination, these legal regulations are not without flaws and do not always reflect the principle of proportionality. Too much focus on tools that aim to remove specific content or to hold specific actors accountable may run up against the inevitable limits of freedom of expression and the right to information. For this reason, we believe that more attention from the legislator's point of view should be directed towards public law instruments that are more systemic and can treat the reasons for the spread of disinformation rather than the consequences. Within this book, we have also tried to outline our recommendations and our reasoning just in line with the above conclusions.

O AUTOROVI

JUDr. Matúš Mesarčík, PhD., LL.M je absolventom Právnickej fakulty Univerzity Komenského v Bratislave v odbore právo (2016). V roku 2017 ukončil postgraduálne vzdelanie v odbore právo a technológie (Law & Technology) na Tilburg University v Holandskom kráľovstve a získal titul LL.M. Je držiteľom diplomu z anglického práva a práva Európskej únie (British Law Centre Diploma), ktorý udeľuje British Law Centre v spolupráci s University of Cambridge (Veľká Británia). V júli 2020 získal doktorát v odbore správne právo na Právnickej fakulte Univerzity Komenského v Bratislave s témou dizertačnej práce „Dynamika pojmu osobný údaj vo svetle nových technológií". V súčasnosti pôsobí ako odborný asistent na Ústave práva informačných technológií a práva duševného vlastníctva Právnickej fakulty Univerzity Komenského v Bratislave a špecialista na Etiku a právo v Kempelenovom inštitúte inteligentných technológií. Pravidelne publikuje v domácich a zahraničných vedeckých periodikách a zúčastňuje sa na domácich a zahraničných konferenciách. Poskytuje ad hoc konzultačné služby v oblasti ochrany osobných údajov, regulácie umelej inteligencie, právnych aspektov dezinformácií či kybernetickej bezpečnosti primárne pre orgány verejnej moci a je členom a expertom na ochranu súkromia v občianskom združení European Information Society Institute (EISi).

PRÁVNICKÁ FAKULTA
Univerzita Komenského
v Bratislave

ISBN: 978-80-7160-706-9