

SUBJEKTY REGULUJÚCE ŠÍRENIE DEZINFORMÁCIÍ V PODMIENKACH SLOVENSKEJ REPUBLIKY A MIMO NEJ

ENTITIES REGULATING THE SPREAD OF DISINFORMATION IN SLOVAK REPUBLIC AND BEYOND

JUDr. Branislav BELICA

Ministerstvo obrany Slovenskej republiky

Kutuzovova 8, 832 47 Bratislava, Slovenská republika

belica1996@gmail.com

Abstrakt: Šírenie dezinformácií a ich dopady predstavujú kritickú hrozbu pre demokratickú spoločnosť. Táto hrozba sa znásobuje každým technologickým pokrokom v oblasti digitálnych služieb a online platforiem. Spolu so zvyšujúcim sa potenciálom umelej inteligencie sa zvyšujú aj riziká jej ďalšieho zneužitia na polarizáciu spoločnosti a ovplyvňovanie verejnej mienky. Snaha eliminovať negatívne dopady dezinformácií je reflektovaná vytváraním regulačných mechanizmov, ktoré majú najmä vzdelávací, legislatívny a inštitucionálny charakter. Tieto mechanizmy sú vnímané v rovine národnej, nadnárodnej, medzinárodnej a mimovládnej. Pôsobiť môžu preventívne, ale aj represívne. Spoločným pôsobením subjektov vo všetkých rovinách a oblastiach sú vytvárané podmienky na efektívnu a účinnú reguláciu šírenia dezinformácií. Autor sa preto vo svojom príspevku, s využitím relevantných metód kvalitatívneho teoretického vedeckého výskumu, zaoberá analýzou subjektov regulujúcich šírenie dezinformácií v podmienkach Slovenskej republiky a mimo nej.

Kľúčové slová: Dezinformácie, bezpečnosť, hybridné hrozby, regulácia, subjekty.

Abstract: The spread of disinformation and its impacts represent a critical threat to democratic society. This threat is doubled with each technological advancement in the field of digital services and online platforms. Alongside the increasing potential of artificial intelligence, the risks of its further misuse for societal polarization and influencing public opinion also escalate. Efforts to eliminate the negative impacts of disinformation are reflected in the creation of regulatory mechanisms, primarily of an educational, legislative, and institutional nature. These mechanisms are perceived at national, supranational, international, and non-governmental levels. They can act preventively as well as repressively. Through the collective action of entities across all levels and areas, conditions are being created for effective and efficient regulation of the spread of disinformation. Therefore, the author in his contribution, utilizing

relevant methods of qualitative theoretical scientific research, addresses the analysis of entities regulating the spread of disinformation within the Slovak Republic and beyond.

Keywords: Security, hybrid threats, disinformation, regulation, entities.

ÚVOD

Vyhľadávanie, prijímanie a prenos informácií sa stali v posledných rokoch, vyznačujúcich sa globálne postupujúcou informatizáciou a digitalizáciou, výrazne rýchlejšími a intenzívnejšími. Z dôvodu širokej dostupnosti moderných technológií, komunikačných zariadení a nových médií sme však v posledných rokoch svedkami nielen ich mohutného využívania na rozličné prospešné účely, ale aj masívneho zneužívania týchto nástrojov na šírenie rozmanitých falošných správ, hoaxov, dezinformácií a propagandy.¹ Najmä sociálne siete a rôzne internetové portály sa stali účinnými a účelnými prostriedkami na šírenie falošných, zavádzajúcich, klamlivých, skreslených alebo úplne vymyslených informácií.² Sociálna a politická polarizácia spoločnosti, spolu s anonymitou a nedostatočnou reguláciou na internete a sociálnych sieťach, nanešťastie vytvárajú prostredie, kde sa takéto informácie ľahko šíria a majú veľký dosah na jednotlivcov i spoločnosť bez výrazných rizík pre ich šíriteľov.³

Slovenská republika (ďalej len „SR“) nie je v tomto ohľade výnimkou. Podobne ako iné krajiny, aj slovenská spoločnosť čelí škodlivým následkom dezinformačných kampaní, ktoré vyvolávajú nedôveru a zmätok medzi občanmi. Uvedeným spôsobom sa podkopávajú základné princípy demokracie a zneužívajú sa základné práva, ako je sloboda prejavu, na úkor systému,

¹ IVANČÍK, R. – MÜLLEROVÁ, J. 2022. Dezinformácie ako hybridná hrozba šírená prostredníctvom sociálnych sietí. In *Policajná teória a prax*, 2022, roč. 30, č. 3, s. 22; KUCHTOVÁ, J. 2018. Aktuálne trendy súvisiace s využívaním moderných technológií. In *Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava: Akadémia Policajného zboru v Bratislave, 2018, s. 90-98; IVANČÍK, R. 2023. On Disinformation and Propaganda in the Context of the Spread of Hybrid Threats. In *Vojenské reflexie*, 2023, roč. 18, č. 3, s. 38-58; HAJDÚKOVÁ, T. – ŠIŠULÁK, S. 2022. Abuse of modern means of communication to manipulate public opinion. In *INTED 2022 – Proceedings from 16th International Technology, Education and Development Conference*. IATED Spain, 2022, s. 1992-2000.

² ZACHAR KUCHTOVÁ, J. 2022. Bezpečnosť na sociálnych sieťach. In *Bezpečnosť elektronickej komunikácie : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2022, s. 237-247; HAJDÚKOVÁ, T. – KURILOVSKÁ, L. – MARR, S. 2023. Riziká komunikácie na sociálnych sieťach. In *Zborník z konferencie RELIK 2023: Reprodukcia ľudského kapitálu – vzájomné väzby a súvislosti*, 2023, s. 58-69; IVANČÍK, R. 2022. Kybernetická (ne)bezpečnosť a sociálne siete. In *Aktuálne výzvy kybernetickej bezpečnosti: zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2022; LISOŇ, M. – FIDLER, Ľ. 2022. Potreba a možnosti identifikácie rizík z realizácie hybridných hrozieb. In *Policajná teória a prax*, 2022.

³ ŠIŠULÁK, S. – ČÍCHOVÁ, M. 2019. Fake news a propaganda v kybernetickom priestore In *Aktuálne výzvy kybernetickej bezpečnosti v podmienkach bezpečnostných zložiek – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2019, s. 156-167; IVANČÍK, R. 2023. Aktuálne východiská skúmania problematiky hybridných hrozieb. In *Policajná teória a prax*, 2023; ZACHAR, Š. 2022. Úvod do anonymných sietí – história ich vzniku a základné prvky. In *Aktuálne výzvy kybernetickej bezpečnosti : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2022, s. 73-83.

ktorý ich garantuje, s cieľom ho narušiť, poškodiť alebo úplne zničiť. Okrem ovplyvňovania verejnej mienky môžu byť dôsledky šírenia nepravdivých, klamlivých a zavádzajúcich informácií, t. j. dezinformácií aj iné, napríklad ekonomické škody, poškodenie zdravia či ohrozenie života. Aj preto sa problematika regulácie šírenia dezinformácií stala široko diskutovanou témou na viacerých úrovniach spoločnosti a stala sa aj námetom vedeckej a publikačnej činnosti autora. Ten sa v článku, s využitím relevantných metód kvalitatívneho teoretického vedeckého výskumu, zaoberá analýzou subjektov regulujúcich šírenie dezinformácií v podmienkach SR s cieľom poukázať najmä na inštitucionálny rámec regulácie šírenia dezinformácií.

1 REGULÁCIA ŠÍRENIA DEZINFORMÁCIÍ ŠTÁTNYMI SUBJEKTMÍ

Subjekty, ktoré sa priamo alebo nepriamo zaoberajú otázkami šírenia dezinformácií a ktoré pôsobia na území SR, majú národný, nadnárodný, medzinárodný, ale aj mimovládny charakter. Metódy, ktoré používajú môžu byť preventívne alebo represívne. Využívané nástroje sa líšia najmä z hľadiska ich účelu a tiež podľa kompetencií jednotlivých organizácií. Môže ísť o strategickú komunikáciu, vzdelávanie, finančnú podporu rôznych projektov, ale aj ukladanie sankcií a reštriktívnych opatrení. Nie je možné presne určiť, ktorý z uvedených faktorov má najvýraznejší vplyv na reguláciu šírenia dezinformácií. Je však dôležité si uvedomiť, že každý z využívaných nástrojov má svoje nezastupiteľné miesto v systéme kontroly a regulácie šírenia dezinformácií, pretože pomáhajú zamedzovať negatívnym dôsledkom šírenia dezinformácií.

Základnou myšlienkou predloženého článku je vytvoriť logickú hierarchiu subjektov v podobe úradov, orgánov, inštitúcií, organizácií alebo občianskych združení (ďalej v texte len „subjekt“) v zmysle ich jednotlivých kompetencií a rozsahu ich pôsobnosti. Uvedená hierarchia vychádza z miery zásahu do základných práv a slobôd, a taktiež z miery intenzity pôsobenia na území SR. V prvom rade budú analyzované štátne, ďalej nadnárodné a medzinárodné, a napokon mimovládne subjekty. Represívne orgány budú mať prednosť pred preventívnymi, pričom niektoré zo subjektov môžu vykonávať súčasne viac druhov činností.

Z hľadiska vytvorenia určitej hierarchie subjektov podľa miery ich zasahovania do práv a slobôd pri regulácii dezinformácií uvádzame ako prvý Policajný zbor (ďalej len „PZ“), ktorého kompetencie v rámci boja s dezinformáciami vnímame v troch rovinách.

V prvom rade ide o nerepresívnu činnosť vykonávanú oddelením komunikácie a prevencie na úrovni prezídia PZ a krajských riaditeľstiev PZ. Tieto oddelenia majú značný potenciál využívať nástroje strategickej komunikácie, vyvracať dezinformácie, vzdelávať

občanov a vytvárať a realizovať rôzne preventívne kampane.⁴ V tomto smere je dôležité najmä vzdelávať mladých ľudí a seniorov (ako dve najzraniteľnejšie skupiny obyvateľstva), upozorňovať ich na nebezpečenstvá a nástrahy internetu a sociálnych sietí, na ktorých sa okrem obrovského množstva relevantných a pravdivých informácií šíri aj značné množstvo dezinformácií.⁵ Zvyšovanie odolnosti obyvateľstva voči dezinformáciám sa ukazuje ako kľúčový faktor pri zamedzovaní ich ďalšieho šírenia.⁶

Z ďalších činností PZ má svoje nezastupiteľné miesto postupovanie informácií na ďalšie konanie. Môže ísť o trestné alebo správne konanie podľa miery závažnosti skutku. V tomto zmysle ide v trestnom konaní hlavne o operatívno-pátraciu činnosť a kriminálne spravodajstvo, ktorých výsledkom môže byť „realizačný návrh“, ako náhrada trestného oznámenia.⁷ V prípade, že nejde o trestný čin, môže vyšetrovateľ alebo poverený príslušník PZ rozhodnúť o postúpení veci, ak ide o skutok, ktorý by mohol byť priestupkom alebo iným správnym deliktom alebo by mohol byť prejednaný v disciplinárnom konaní.⁸

Ako najzásadnejšia sa zo širokého súboru činností realizovaných PZ pri regulácii šírenia dezinformácií javí samotná represívna činnosť PZ. Pri naplnení skutkovej podstaty trestného činu PZ koná ako orgán činný v trestnom konaní a vedie trestné stíhanie. V zmysle správneho konania PZ plní úlohy v rámci odhaľovania priestupkov, pričom v prípadoch ustanovených zákonom priestupky objasňuje a prejednáva.⁹ Z hľadiska vytvorenej hierarchie má PZ najširšie kompetencie zásahu do práv a slobôd osôb. Pri najzávažnejších formách konania môže zasahovať až do osobnej slobody.¹⁰

Okrem PZ sa v SR problematike dezinformácií venujú a detailne monitorujú situáciu aj spravodajské služby – Slovenská informačná služba (ďalej len „SIS“) a Vojenské spravodajstvo (ďalej len „VS“). SIS podľa zákona plní úlohy vo veciach „ochrany ústavného zriadenia, vnútorného poriadku, bezpečnosti štátu a ochrany zahraničnopolitických a hospodárskych záujmov štátu v rozsahu vymedzenom týmto zákonom. Vo svojej činnosti sa spravuje ústavou, ústavnými zákonmi, zákonmi a ostatnými všeobecne záväznými právnymi predpismi“.¹¹

⁴ §2 ods. 3 Zákona č. 171/1993 Z. z. o Policajnom zbore.

⁵ HAJDÚKOVÁ, T. 2024. Zdroje informácií alebo dezinformácií. In *Auspicia*, 2024; ZACHAR KUČTOVÁ, J. 2024. Bezpečnostné riziká šírenia dezinformácií na internete prostredníctvom nástrojov umelej inteligencie. In *Auspicia*, 2024; IVANČÍK, R. 2024. Dezinformácie ako bezpečnostná hrozba šírená na internete. In *Auspicia*, 2024; DUŠEK, J. – KAVAN, Š. 2024. Dezinformácie ako súčasť hybridných hrozieb – česko-slovenský pohľad. In *Auspicia*, 2024.

⁶ GLOBSEC. 2023. Globsec Trends. In *Globsec.org*, 2023.

⁷ §39 a 39a Zákona č. 171/1993 Z. z. o Policajnom zbore.

⁸ §1 ods. 2 Zákona č. 46/1996 Z. z. o Slovenskej informačnej službe.

⁹ §2 ods. 1 písm. b), d), k) Zákona č. 171/1993 Z. z. o Policajnom zbore.

¹⁰ Napríklad predvedenie podľa §17 a 17b, zaistenie osoby v zmysle §19 Zákona č. 171/1993 Z. z. o Policajnom zbore; zadržanie osoby v zmysle §85-88 Zákona č. 301/2005 Z. z. Trestný poriadok; alebo väzba a s ňou spojené úkony na základe rozhodnutia súdu podľa §71-73 Zákona č. 301/2005 Z. z. Trestný poriadok.

¹¹ §1 ods. 2 Zákona č. 46/1996 Z. z. o Slovenskej informačnej službe.

Hlavným poslaním VS je plnenie úloh spravodajského zabezpečenia obrany, obranyschopnosti a bezpečnosti SR v pôsobnosti Ministerstva obrany SR.¹²

Spravodajské služby primárne vykonávajú analýzu bezpečnostného prostredia, vyhodnocujú získané informácie a v prípade potreby ich postupujú zákonným prijímateľom. V rámci predmetnej problematiky ide najmä o informácie súvisiace s hybridnými hrozbami, informačnými operáciami a šírením dezinformácií.¹³ Napriek tomu, že sa na prvý pohľad môže javiť činnosť spravodajských služieb ako latentná, neznamena to, že spravodajské služby svojou činnosťou nezasahujú do práv a slobôd osôb. Spravodajské služby svojou činnosťou pri získavaní informácií v zmysle zákona vo vybraných situáciách zasahujú do práva na súkromie, ktoré je v Ústave SR garantované spolu s nedotknuteľnosťou osoby.¹⁴

Ako ďalší subjekt uvádzame Národný bezpečnostný úrad (ďalej len „NBÚ“). Do 30. septembra 2022 NBÚ disponoval oprávneniami z vlastnej iniciatívy rozhodovať o blokovaní, spôsobe blokovania a vykonávať blokovanie škodlivého obsahu alebo škodlivej aktivity, ktorá smeruje dovnútra alebo von z kybernetického priestoru SR. NBÚ tým v zmysle zákona obmedzoval slobodu prejavu a právo na informácie.¹⁵ Od ukončenia platnosti tohto ustanovenia nebolo vydané ďalšie rozhodnutie a taktiež neboli implementované zmeny do zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti (ďalej len „ZoKB“), ktoré by ďalej umožňovali v predmetnej agende blokovania škodlivého obsahu pokračovať. Časovo obmedzené zákonné splnomocnenie bolo schválené pre NBÚ v skrátanom legislatívnom konaní ako reakcia na vojenskú agresiu Ruskej federácie voči Ukrajine.¹⁶

Predmetné zákonné ustanovenia boli v minulosti kritizované verejnosťou aj mimovládnyimi organizáciami. Ako reakcia na kritiku verejnosti sa pripravila novela zákona, ktorá reagovala na pripomienky, že voči rozhodnutiu o zablokovaní webstránok sa nedalo odvolať, bolo ihneď vykonateľné a jeho preskúmanie súdom by trvalo roky. Taktiež sa objavila kritika vydaných rozhodnutí pre nedostatočné odôvodnenie.¹⁷

¹² § 1 ods. 1 Zákona č. 198/1994 Z. z. o Vojenskom spravodajstve.

¹³ LISOŇ, M. – FIDLER, E. 2022, Potreba a možnosti identifikácie rizík z realizácie hybridných hrozieb. In *Policajná teória a prax*, 2022; LUKÁČOVÁ, V. 2020. Hybridné hrozby v kybernetickom priestore. In *Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2020; IVANČÍK, R. 2023. On Disinformation and Propaganda in the Context of the Spread of Hybrid Threats. In *Vojenské reflexie*, 2023; TOMÁŠEK. 2023. Hybridná vojna a hybridné hrozby. In *Bezpečnosť elektronickej komunikácie 2023 – zborník z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2023.

¹⁴ Čl. 16 ods. 1 Zákona č. 460/1992 Z. z. Ústava Slovenskej republiky.

¹⁵ Čl. 26 ods. 1 až 4 Zákona č. 460/1992 Z. z. Ústava Slovenskej republiky.

¹⁶ DUGOVIČ, T. 2022. Štát bude mať možnosť blokovat škodlivé weby. Parlament zmenu schválil pre vojnu na Ukrajinu. In *Standard.sk*, 2022.

¹⁷ KRAJČOVIČ, M. 2022. Kritika zabrala. Štát bude musieť zverejniť, prečo blokuje Hlavné správy a Infovojnu. In *Fontech*, 2022.

Argumentovalo sa napríklad aj rozhodnutím Európskeho súdu pre ľudské práva, kde sa uvádzalo, že: „celkové zablokovanie prístupu k webovým stránkam je extrémne opatrenie, porovnateľné so zákazom novín alebo televíznych staníc. Takéto opatrenie zámerne ignoruje rozdiel medzi zákonnými a nezákonnými informáciami, ktoré môže webová stránka obsahovať a robí neprístupným veľké množstvo obsahu, ktorý nebol identifikovaný ako nezákonný. Zablokovanie prístupu k celej webovej stránke má praktický dopad, pretože rozširuje pôsobnosť blokačného príkazu ďaleko za rámec pôvodne cieleného nezákonného obsahu.“¹⁸

Predkladané znenie novely predmetného zákona upravovalo postup blokovania úradom iba so súhlasom súdu. Novela však nebola prijatá zákonodarným zborom. Momentálne sa v novom parlamentnom zložení nediskutuje o ďalšej úprave postupu NBÚ a obnovení jeho kompetencií ktoré uplynutím lehoty uvedenej v zákone nemôžu byť ďalej aplikovateľné.¹⁹ V tomto smere je potrebné vykonať zmeny, aby bol postup NBÚ v súlade s európskou judikatúrou. Možnosť blokovania škodlivého obsahu je rovnako dôležitým nástrojom boja proti dezinformáciám ako represia štátu, a to najmä preto, že v kybernetickom priestore nie je vždy možné odhaliť konkrétneho páchatel'a (najmä kvôli využívaniu zahraničných domén) a nie všetky druhy šírenia dezinformácií majú také škodlivé následky, aby nástrojom ich kontroly musela byť trestnoprávna alebo správnoprávna represia. Aj preto uvádzame NBÚ ako subjekt s vysokým potenciálom v oblasti opatrení proti šíreniu dezinformácií. NBÚ má potenciál ďalej plniť dôležitú funkciu v systéme štátnych orgánov, pričom by vedel reagovať na škodlivý obsah aj v prípadoch, kedy by vyššie spomínané mechanizmy represie boli ťažko aplikovateľné.

Momentálne je možné v zmysle ZoKB vykonávať blokovanie iba na základe žiadosti subjektu podľa osobitného predpisu. Ide napríklad o žiadosť v zmysle Zákona č. 30/2019 Z. z. o hazardných hrách. Okrem toho sú náklady spojené s výkonom blokovaní na základe žiadosti žiadateľa a zodpovednosť za škodu spôsobenú blokovaním znášané žiadateľom.²⁰ Efektívitu momentálnej právnej úpravy odzrkadľuje verejne dostupný zoznam blokovaných subjektov, ktorý je od 1.7.2022 prázdny.²¹

Ako ďalší subjekt uvádzame Radu pre mediálne služby (ďalej len „RPMS“), ktorá je oprávnená ukladať sankcie v zmysle Zákona č. 264/2022 Z. z. o mediálnych službách (ďalej len „ZoMS“). RPMS vykonáva dohľad nad dodržiavaním právnych predpisov v oblasti vysielania, retransmisie, poskytovania audiovizuálnych mediálnych služieb na požiadanie

¹⁸ ŠAMKO, P. 2022. Blokovanie webových stránok a jeho možný rozpor s judikatúrou Európskeho súdu pre ľudské práva. In *Právne listy*, 2022.

¹⁹ HNONLINE. 2022. Nbú by mohol škodlivý online obsah blokovat' aj v budúcnosti, so súhlasom súdu. In *Stratégia*, 2023.

²⁰ §27c ods. 1 a 7 Zákona č. 69/2018 Z. z. o Kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.

²¹ NBÚ. 2024. Zoznam blokovaných subjektov. In *nbu.gov.sk*, 2024.

a poskytovania platforiem na zdieľanie obsahu. V kontexte regulácie šírenia dezinformácií dohliada na pluralitu informácií, ochranu spotrebiteľa a transparentnosť majetkových a personálnych vzťahov.²²

Jej činnosť, v kontexte regulácie šírenia dezinformácií, nie je zásadná, najmä preto že okruh regulovaných subjektov je limitovaný na: rozhlasové a televízne vysielanie, vysielanie prostredníctvom internetu, poskytovanie audiovizuálnych mediálnych služieb, prevádzkovanie retransmisie a platformy na zdieľanie videí. Zoznam regulovaných subjektov, ktorých činnosť je vykonávaná prostredníctvom internetu je ku dnešnému dňu limitovaný iba na tri subjekty. V dvoch prípadoch ide o online rádio a v jednom o platformu na zdieľanie videí *nikefondsportu.sk*.²³ Okrem toho však zákon pozná aj platformu na zdieľanie obsahu a obsahovú službu, ktorá nevyžaduje oprávnenie. Ide napríklad o elektronickú periodickú publikáciu, spravodajský portál alebo agentúrny servis.

Limity ZoMS nie sú však iba v jeho pôsobnosti, ale v kontexte regulácie šírenia dezinformácií najmä v definícii nelegálneho obsahu. Ten je definovaný ako obsah, ktorý:

- napĺňa znaky detskej pornografie alebo extrémistického materiálu,
- podnecuje ku konaniu, ktoré napĺňa znaky niektorého z trestných činov terorizmu,
- schvaľuje konanie, ktoré napĺňa znaky niektorého z trestných činov terorizmu,
- 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.²⁴

Napriek tomu, že v niektorých prípadoch môžu dezinformačné naratívy šírené prostredníctvom regulovaných subjektov napĺňať uvedené znaky, ide najmä o konania, ktoré majú znaky trestného činu. Sankcie, ktoré je možné v tomto ohľade uložiť sú:

- upozornenie na porušenie zákona,
- uverejnenie oznamu o porušení zákona,
- pozastavenie vysielania alebo poskytovania programu alebo jeho časti,
- pokuta,
- zrušenie autorizácie za závažné porušenie povinnosti.²⁵

²² RADA PRE MEDIÁLNE SLUŽBY. 2024. Postavenie a poslanie Rady pre mediálne služby. In *rpms.sk*, 2024.

²³ RADA PRE MEDIÁLNE SLUŽBY. 2024. Zoznamy regulovaných subjektov. In *rpms.sk*, 2024.

²⁴ RADA PRE MEDIÁLNE SLUŽBY. 2024. Čo je podnet týkajúci sa nelegálneho obsahu. In *rpms.sk*, 2024.

²⁵ §134 Zákona č. 264/2022 Z. z. o mediálnych službách.

V zmysle vytvorenej hierarchie uvádzame RPMS ako posledný subjekt, nakoľko sankcie a miera zásahu do práv a slobôd subjektov v pomere s predmetnými porušeniami sú najmiernejšie. Dôležitosť postihovania šíritel'ov nelegálneho obsahu nástrojmi správneho práva vidíme ako zásadnú najmä preto, že pri vyvodzovaní zodpovednosti z priestupkov alebo iných správnych deliktov platí zásada, že pokiaľ nie je vyslovene uvedené, že musí ísť o úmyselné zavinenie, stačí zavinenie z nedbanlivosti. Ide teda o posilnenie regulácie v prípadoch, kedy nie je možné využiť nástroje trestného práva najmä z dôvodu chýbajúceho alebo nepreukázaného úmyslu.

Vyššie uvedené subjekty označujeme ako represívne. V rámci SR však pôsobia aj dôležité štátne subjekty, ktoré napriek tomu že nemajú represívne pôsobenie, tvoria neoddeliteľnú súčasť systému regulácie šírenia dezinformácií. Ide najmä o tie subjekty, ktoré vykonávajú analytickú činnosť, podieľajú sa na vytváraní strategickej komunikácie alebo na vzdelávacích aktivitách zameraných na zvyšovanie odolnosti proti dezinformáciám.

Na úrovni Úradu vlády SR bol v roku 2022 vytvorený odbor strategickej komunikácie, ktorý má v kompetencii riešenie problematiky strategickej komunikácie na celoštátnej úrovni.²⁶ 14. februára 2024 bol uznesením vlády SR č. 88 prijatý štatút Situačného centra SR (ďalej len „SITCEN“). Ide o vládne informačné analytické pracovisko s celoštátnou pôsobnosťou pre oblasť vyhodnocovania zmien v bezpečnostnom prostredí aj s využívaním zahraničnej spolupráce začlenené do Kancelárie Bezpečostnej rady SR. Pôsobnosť a úlohy SITCEN spočívajú najmä v sústred'ovaní, spracovávaní a vyhodnocovaní informácií, z ktorých sú následne vytvárané analytické produkty a informačné výstupy pre vrcholných predstaviteľ'ov štátu, relevantné štátne orgány, spolupracujúce zložky a ostatné subjekty podľa dohody.²⁷

SITCEN, v zmysle platného štatútu, úzko spolupracuje s Národným bezpečnostným analytickým centrom (ďalej len NBAC), ktoré je súčasťou SIS. NBAC združuje, vyhodnocuje, analyzuje a vydáva ucelené výstupy bezpečnostných zložiek štátu. V rámci NBAC spolupracujú vyslaní zástupcovia SIS, VS, PZ, Kriminálneho úradu finančnej správy (ďalej len „KÚ FS“, Ministerstva zahraničných vecí a európskych záležitostí SR (ďalej len „MZVEZ SR“), NBÚ, Generálneho štábu Ozbrojených síl SR (ďalej len „OS SR“) a Úradu vlády SR. Ústredné analytické pracovisko umožňuje priamy kontakt a pružnú komunikáciu medzi NBAC a jednotlivými subjektmi prostredníctvom ich vyslaných zástupcov a zároveň včasné poskytnutie spravodajského produktu relevantným externým príjemcom. Zároveň naviazalo bilaterálnu spoluprácu s partnerskými centrami z členských krajín EÚ a NATO.²⁸

²⁶ CBHH. 2024. Úrad vlády SR. In *Hybridnehrozby.sk*, 2024.

²⁷ VLÁDA SR. 2024. Štatút Situačného centra Slovenskej republiky. In *vlada.gov.sk*, 2024.

²⁸ SLOVENSKÁ INFORMAČNÁ SLUŽBA. 2024. Poslanie a úlohy NBAC. In *sis.gov.sk*, 2024.

V rámci organizačnej štruktúry Ministerstva vnútra SR (ďalej len „MV SR“) plní dôležitú úlohu Centrum boja proti hybridným hrozbám (ďalej len „CBHH“). Medzi hlavné úlohy CBHH patrí:

- vytváranie pravidelných analytických výstupov, ktoré prispievajú k lepšiemu nastaveniu politik a situačnému povedomiu smerujúcemu k prijatiu adekvátnych opatrení na zvyšovanie odolnosti voči hybridným hrozbám;
- vytvorenie metodiky a systému na zber informácií o incidentoch a udalostiach vykazujúcich prvky hybridných hrozieb v rámci rezortu MV SR, ich vyhodnocovanie a spracovanie;
- zvyšovanie povedomia subjektov verejnej správy v rámci MV SR o problematike hybridných hrozieb formou vzdelávaní, prednášok a tvorby informačných materiálov;
- komunikácia so zahraničnými partnermi v oblasti hybridných hrozieb;
- audit strategickej komunikácie a spolupodieľanie sa na vytvorení komunikačných stratégií pre MV SR;
- analytická podpora pre MV SR v oblasti strategickej komunikácie;
- audit odolnosti vybraných subjektov štátnej správy voči hybridným hrozbám, mapovanie zraniteľností a návrhy opatrení;
- vypracovanie komplexných scenárov simulácie hybridných útokov zapájajúcich široké spektrum aktérov verejnej správy a ostatných zložiek bezpečnostného systému SR a ich priama realizácia.²⁹

CBHH taktiež vytvorilo E-learningový kurz, ktorý poskytuje základný prehľad o problematike hybridných hrozieb, ich formách a spôsoboch ochrany pred nimi. Tento kurz je dostupný pre všetkých zamestnancov relevantných subjektov verejnej správy a regionálnej samosprávy.³⁰

Ďalšími relevantnými štátnymi subjektmi sú Odbor pre hybridné hrozby a strategickú komunikáciu v rámci štruktúry Ministerstva obrany SR (ďalej len „MO SR“), ktorého činnosť je zameraná najmä na zber, analýzu a vyhodnocovanie informácií, vypracovávanie výstupov (grafických, video, statusy) a ich následnú prezentáciu na sociálnych sieťach,³¹ a Analytický útvar MO SR, ktorý sa podieľa na vypracovávaní analýz, strategických hodnotení a výstupov

²⁹ CBHH. 2024. Vzdelávanie zamestnancov verejnej správy v oblasti hybridných hrozieb. In *Hybridnehrozby.sk*, 2024.

³⁰ CBHH. 2024. Hlavné úlohy CBHH MV SR. In *Hybridnehrozby.sk*, 2024.

³¹ SLIZ, M. 2022. Štát sa pokúsi predbehnúť dezinformátorov. In *Aktuality.sk*, 2022.

v prospech MO SR. V minulosti sa útvár vo svojej publikačnej činnosti venoval aj problematike dezinformácií a nakoľko ide o veľmi aktuálnu tému, je vysoká pravdepodobnosť, že v tomto trende bude pokračovať.³²

Svoje opodstatnené miesto v hierarchii štátnych subjektov, ktoré sa podieľajú na regulácii šírenia dezinformácií sú aj novovytvorené štruktúry OS SR, konkrétne Veliteľstva síl pre špeciálne operácie – 57. samostatný oddiel, ktorý vznikol transformáciou a rozšírením strediska CIMIC a PSYOPS v auguste 2021. Jednotky CIMIC, PSYOPS a INFOOPS majú v prostredí OS SR za úlohu riadiť civilno-vojenskú spoluprácu, psychologické a informačné operácie. V rámci týchto činností prebieha strategická komunikácia na zvyšovanie dôveryhodnosti OS SR, v súvislosti s ktorou sa najmä príslušníci INFOOPS sústreďujú aj na analýzu, vyhodnocovanie a tiež reakciu na šírené dezinformácie najmä z prostredia OS SR, alebo na informácie, ktoré by mohli mať dopad na ich fungovanie a dôveryhodnosť.³³

MZVEZ SR sa venuje viacerým oblastiam, ktoré priamo súvisia s bojom proti hybridným hrozbám a budovaním odolnosti štátu voči nim, a to predovšetkým v doméne zahraničnej politiky SR. MZVEZ je dlhodobo aktívne v boji proti dezinformáciám týkajúcich sa zahraničnej politiky, v problematike zahranično-politických aspektov kybernetickej a energetickej bezpečnosti a zabezpečuje tiež informovanie o hybridnom pôsobení v zahraničí prostredníctvom siete zastupiteľských úradov. Rezort je tiež komunikačným kanálom pre bilaterálne a multilaterálne konzultácie so spojencami v rámci NATO a EÚ o témach spojených s bojom proti hybridným hrozbám a posilňovaním odolnosti štátu. MZVEZ SR taktiež zastupuje SR pri tvorbe politík v tejto oblasti na príslušných medzinárodných fórach a v pracovných skupinách medzinárodných organizácií.³⁴

Okrem MV SR, MO SR a MZVEZ SR sa do boja proti dezinformáciám aktívne zapája aj Ministerstvo investícií, regionálneho rozvoja a informatizácie SR (ďalej len „MIRRI SR“). To napríklad vyhlásilo výzvu na finančnú podporu projektov zameraných na vzdelávacie aktivity, rozvoj digitálnych nástrojov a techník v boji proti šíreniu dezinformácií či vytváranie a distribúciu vzdelávacích materiálov. Okrem toho sa MIRRI SR podieľa na technických riešeniach pre novovzniknuté CBHH.³⁵

³² ANALYTICKÝ ÚTVAR MOSR. Analytický útvár MO SR, 2022.

³³ PAŽICKÝ, M. 2019. TASR: "Veliteľstvo Síl pre špeciálne operácie posilnili ďalšie útvary". In *vesso.mil.sk*, 2019.

³⁴ CBHH. 2024. Ministerstvo zahraničných vecí a európskych záležitostí SR. In *Hybridnehrozby.sk*, 2024.

³⁵ ITAPA. 2021. Štát má niekoľko konkrétnych plánov, ako bojovať proti dezinformáciám. MIRRI už začalo. In *Itapa.sk*, 2021.

2 NADNÁRODNÉ A MEDZINÁRODNÉ SUBJEKTY REGULUJÚCE ŠÍRENIE DEZINFORMÁCIÍ

Z pomedzi nadnárodných a medzinárodných subjektov, ktoré majú priamy dosah na kontrolu šírenia dezinformácií na území SR vyberáme inštitúcie Európskej únie (ďalej len „EÚ“) a Severoatlantickej aliancie (ďalej len „NATO“).

Prvým subjektom je Rada EÚ, ktorá má v kompetencii zakázať vysielacie činnosti médií. V súvislosti s vojnou na Ukrajine išlo o reštriktívne opatrenia voči vysielacej činnosti médií Sputnik a Russia Today do ukončenia agresie voči Ukrajine a dotedy, kým Ruská federácia a jej pridružené média neprestanú vykonávať dezinformačné aktivity a akcie zamerané na ovplyvňovanie verejnej mienky a manipuláciu informácií namierenými proti EÚ a jej členským štátom.³⁶ Napriek snahám ruskej televízie RT o napadnutie rozhodnutia na Súdnom dvore EÚ, tribunál Súdneho dvora potvrdil marcový zákaz vysielania pre systematické dezinformácie.³⁷ Zoznam blokovaných subjektov na základe rozhodnutia Rady EÚ je dostupný online na webovom sídle NBÚ.³⁸

Ďalším subjektom je Európska komisia (ďalej len „EK“), ktorá sa podieľa na:

- implementácií zákona o digitálnych službách (Digital Services Act – ďalej len „DSA“);
- podpore projektov na overovanie pravdivosti informácií;
- vytváraní vlastných projektov v predmetnej oblasti.

17. februára 2024 sa začal uplatňovať DSA na všetky online platformy v rámci EÚ. Tento právne záväzný dokument upravuje práva používateľov online platforiem a povinnosti ich prevádzkovateľov. V rámci výkonu kontroly ustanovuje EK ako subjekt, ktorý má právo vo veciach porušenia DSA viesť vyšetrovanie a ukladať sankcie. V prípade porušenia určených povinností je možné uložiť pokutu až do výšky 6 % ročného obratu prevádzkovateľa. Okrem toho môže EK pristúpiť k periodickým pokutám až do výšky 5 % priemerného denného celosvetového obratu za každý deň, ktorý platforma nedodríava určené povinnosti. Ako posledný nástroj môže EK pristúpiť k dočasnému pozastaveniu služby na základe návrhu EK a následného rozhodnutia súdu dotknutého členského štátu. Regulácia online platforiem prostredníctvom EK spočíva najmä v dohľade nad dodržiavaním uložených povinností, v dôsledku porušenia ktorých môže prísť k uloženiu sankcie alebo návrhu na dočasné

³⁶ RADA EÚ. 2022. EÚ uložila sankcie štátnym médiám RT/Russia Today a Sputnik s vysielaním v EÚ. In *European Council*, 2022.

³⁷ RTVS. 2022. Tribunál Súdneho dvora EÚ potvrdil zákaz vysielania ruskej televízie RT. In *Správy RTVS*, 2022.

³⁸ NBÚ. 2024. Zoznam subjektov blokovaných EÚ. In *nbu.gov.sk*, 2024.

obmedzujúce opatrenie.³⁹ Dôležitosť implementácie DSA spočíva najmä v spoločnom postupe národných štátov, ktorých individuálne snahy o reguláciu technologických gigantov s celosvetovým presahom sú oveľa efektívnejšie presadzované v rámci silného geopolitického celku, akým EÚ nepochybne je.

EK vyčleňuje značné zdroje na overovanie pravdivosti informácií v tradičných médiách a na sociálnych médiách. Z týchto zdrojov financuje rôzne projekty, ktoré sú zamerané proti šíreniu dezinformácií a analýzu sociálnych sietí.⁴⁰ Ako príklad uvádzame projekt European Digital Media Observatory (ďalej len „EDMO“), ktorý spája overovateľov faktov, mediálnych expertov a akademických výskumníkov v práci zameranej na pochopenie a analyzovanie dezinformácií. Ide teda o multidisciplinárnu platformu, ktorá prispieva k hlbšiemu pochopeniu dezinformácií, ich šíriteľov, techník, cieľov a dopadov na spoločnosť. EDMO sa zameriava na poskytovanie školení a publikačnú činnosť v rámci tejto problematiky.⁴¹

EK taktiež vytvorila Účinnejší (posilnený) Kódex postupov EÚ proti šíreniu dezinformácií, ktorý je kódexom pre súkromné spoločnosti. Tie sa môžu dobrovoľne prihlásiť k jeho dodržiavaniu. Ide o v poradí druhý kódex postupov a teda aktualizácia kódexu z roku 2018. V porovnaní s dokumentom z roku 2018 je tento kódex rozsiahlejší, má viac signatárov (34 oproti 16) a obsahuje viac opatrení, ktoré by mali byť implementované na účinný boj proti dezinformáciám. Signatári sa svojim podpisom zaväzujú k dodržiavaniu kódexu. Medzi opatrenia patria:

- prísnejšie opatrenia na demonetizáciu dezinformácií,
- zvýšenie transparentnosti politickej reklamy,
- zabezpečenie komplexného pokrytia prebiehajúceho a vznikajúceho manipulatívneho správania,
- rozšírenie a posilnenie účinnosti nástrojov, ktoré používateľom umožňujú odhaľovať a poukazovať na nepravdivý obsah,
- rozširovanie overovania faktov v krajinách EÚ,
- poskytovanie lepšieho prístupu k údajom vedcov, akademikov a výskumníkov.⁴²

Dôležitým projektom EÚ, konkrétne Európskej služby pre vonkajšiu činnosť, je stránka *EU vs DISINFO*, ktorá bola založená v roku 2015 a jej úlohou je zvyšovanie povedomia

³⁹ EUROPEAN COMMISSION. 2024. Digital Services Act starts applying to all online platforms in the EU. In *European Commission*. 2024.; EUROPEAN COMMISSION. 2024. The enforcement framework under the Digital Services Act. In *European Commission*, 2024.

⁴⁰ EURÓPSKA KOMISIA. 2024. Existujúce projekty. In *European Commission*, 2024.

⁴¹ EDMO. 2024. About us. In *Edmo.eu*, 2024.

⁴² EURÓPSKA KOMISIA. 2022. Účinnejší Kódex postupov EÚ proti šíreniu dezinformácií. In *European Commission*, 2022.

verejnosti o dezinformačných operáciách, najmä analýzou médií v 15 jazykoch a odhaľovaním dezinformácií spolu s ich šíriteľmi. Okrem toho stránka publikuje články a analýzy o vývoji techník a metód a spolupracuje na medzinárodnom výskume tejto problematiky.⁴³

Ďalším subjektom je Európske centrum excelentnosti pre boj proti hybridným hrozbám (ďalej len „Hybrid CoE“). Ide o spoločný projekt EÚ a NATO, ktorý vznikol v roku 2017 a k dnešnému dňu sa na jeho činnosti podieľa 35 participujúcich štátov. Úlohou Hybrid CoE je posilniť odolnosť členských štátov poskytovaním informácií, vedomostí a školení na boj proti hybridným hrozbám. Hlavným cieľom je posilniť kapacity zúčastnených štátov na predchádzanie a boj proti hybridným hrozbám. Tento cieľ sa Hybrid CoE snaží dosiahnuť zdieľaním overených metód, odporúčaní a testovaním nových nápadov a prístupov v tejto oblasti. Centrum má tiež kapacity na školenia a praktické workshopy. Okrem iného vytvára strategické koncepty a pomáha pri ich implementácii. Taktiež sa venuje publikačnej činnosti za účelom propagácie problematiky a poskytovania informácií verejnosti.⁴⁴

Ako ďalší medzinárodný subjekt uvádzame NATO Strategic Communications Centre of Excellence (ďalej len „Stratcom CoE“). Ide o medzinárodnú vojenskú organizáciu pod záštitou NATO, ktorá však nie je súčasťou veliacej štruktúry NATO. Cieľom Stratcom CoE je prispievať k zlepšovaniu možností strategickkej komunikácie v rámci Aliancie a spojeneckých štátov. Strategická komunikácia je základom pre dosiahnutie politických a vojenských cieľov, nakoľko je dôležité o nich komunikovať vhodne, včasne a aktívne v súvislosti s vývojom situácie. Centrum sa skladá z medzinárodného zoskupenia subjektov z rôznych sektorov (civilného, verejného, vojenského, akademického), pričom využíva moderné technológie a metódy na vytváranie analýz a výskumov ako podklad pre rozhodovanie. Strategická komunikácia je kľúčovým nástrojom boja proti dezinformáciám. Je preto dôležité budovať kapacity, získavať informácie a praktické zručnosti najmä prostredníctvom členstva v medzinárodných organizáciách, vďaka ktorým je získanie skúseností a informácií oveľa efektívnejšie ako pomocou vlastných kapacít. Členstvo SR v Stratcom CoE a jeho činnosť preto zásadným spôsobom pomáha k zefektívneniu boja proti šíreniu dezinformácií.⁴⁵

Posledným subjektom je Európske spravodajské a situačné centrum. Toto centrum bolo vytvorené v roku 2012. Jeho úlohou je zber a analýza rôznych druhov informácií v rôznych oblastiach bezpečnosti od členských štátov EÚ prostredníctvom ich spravodajských a bezpečnostných zložiek. Z takto zozbieraných informácií sa ďalej vytvárajú rôzne analytické a spravodajské výstupy. Centrum je zložené z civilnej a vojenskej časti a jeho hlavnou úlohou

⁴³ EUVSDISINFO. 2024. About. In *euvsdisinfo.eu*, 2024.

⁴⁴ HYBRID COE. 2024. What is Hybrid CoE? In *hybridcoe.fi*, 2024.

⁴⁵ NATO STRATCOM COE. 2024. About NATO StratCom COE. In *Stratcomcoe.org*, 2024.

je poskytovať informačné výstupy pre relevantné orgány Európskej únie ako podporu pri ich rozhodovacom procese.⁴⁶

3 PÔSOBENIE MIMOVLÁDNYCH SUBJEKTOV V BOJI PROTI DEZINFORMÁCIÁM

Na boji proti šíreniu dezinformácií a hybridným hrozbám sa okrem štátnych, nadnárodných a medzinárodných subjektov podieľajú aj subjekty tretieho sektora.

Ako prvý subjekt uvádzame Slovenský inštitút pre bezpečnostnú politiku (ďalej len „SSPI“). Ide o mimovládnu organizáciu, ktorá spája expertov v oblasti bezpečnostnej a obrannej politiky z vládnej, súkromnej a akademickej oblasti. Sústreďuje sa najmä na výskum a analýzu aktuálnych bezpečnostných výziev s cieľom zvyšovať verejné povedomie o týchto otázkach. SSPI je zakladateľom slovenského portálu, ktorý sa zaoberá kybernetickou bezpečnosťou – *CyberSec.sk* a prevádzkuje webovú stránku *Antipropaganda.sk*, ktorá sa zameriava na odhaľovanie dezinformácií a propagandy. Táto stránka, napriek tomu, že je stále aktívna a obsahuje značné množstvo užitočných článkov, sa v roku 2022 presunula pod projekt *infosecurity.sk*.⁴⁷ Ako príklad činnosti inštitútu tiež uvádzame projekt *Nenalet.im*, ktorého úlohou je zvyšovať povedomie o témach dezinformácií a extrémizmu za účelom budovania odolnosti obyvateľstva voči týmto hrozbám. Ide o voľne online dostupný kurz pre učiteľov, prostredníctvom ktorého môžu pomôcť študentom rozvíjať kritické myslenie a objasniť zložité témy ohľadom šírenia dezinformácií, radikalizmu a extrémizmu.⁴⁸

Ďalším mimovládnym subjektom v oblasti medzinárodných vzťahov a bezpečnosti, ktorý sa tiež venuje problematike hybridných hrozieb a dezinformácií je Adapt Institute, donedávna známy ako Strategic Policy Institute (STRATPOL). Táto mimovládna organizácia sa podobne ako SSPI zameriava na publikačnú činnosť, združuje odborníkov z rôznych oblastí a vytvára či podporuje rôzne projekty z oblasti bezpečnosti a medzinárodných vzťahov.⁴⁹ Ako príklad uvádzame projekt *InfoKompas*, ktorý sa zameriava na vzdelávanie mladých v súvislosti s témou dezinformácií a informačnej gramotnosti. Cieľom je zapojiť študentov stredných škôl, učiteľov dejepisu a náuky o spoločnosti prostredníctvom interaktívnych workshopov a seminárov.⁵⁰

⁴⁶ EUINTCEN. 2015. Main functions and tasks. In *Statewatch.org*, 2015.

⁴⁷ SSPI. 2024. Kto sme? In *Slovaksecurity.org*, 2024.

⁴⁸ NENALET. 2024. O projekte. In *Nenalet.im*, 2024.

⁴⁹ ADAPT INSTITUTE. 2024. About us. In *adaptinstitute.org*, 2024.

⁵⁰ INFOKOMPAS. 2024. O projekte. In *infokompas.stratpol.sk*, 2024.

Ako spoločný projekt SSPI a Adapt Institute vznikol portál *infosecurity.sk*, ktorý je zameraný na kontrolu informačného priestoru vo vzťahu k dezinformáciám a bezpečnosti na sociálnych sieťach. Cieľom tohto projektu je odhaľovanie a vyvracanie nebezpečného a nepravdivého obsahu, ozdravovanie informačného priestoru a budovanie spoločenského povedomia a dôležitých témach.⁵¹

Mimovládny subjektom je aj GLOBSEC – organizácia, ktorá združuje odborníkov z oblasti bezpečnosti za účelom výskumu a analýz bezpečnostných hrozieb a rizík ohrozujúcich našu spoločnosť. GLOBSEC organizuje rôzne fóra a diskusie na dôležité témy z oblasti bezpečnosti. Táto organizácia má tiež rozsiahlu publikačnú činnosť a kvalitné analytické výstupy, ktoré pomáhajú pri ďalšom riešení problematiky bezpečnosti a boja proti dezinformáciám.⁵²

Ako príklad uvádzame prieskumy organizácie GLOBSEC, ktoré mapujú a porovnávajú názory obyvateľov v rámci EÚ a NATO na otázky dezinformácií a propagandy či podpory členstva v EÚ a NATO. V rámci tohto prieskumu sa Slovenská republika umiestnila spolu s Bulharskom na najnižších priečkach najmä v oblasti dezinformácií a podpory Ruska v kontexte vojny na Ukrajine. Napríklad pri otázke, kto môže za vojnu na Ukrajine, až 34 % Slovákov odpovedalo, že vojna bola vyprovokovaná západom, čo predstavuje najväčší podiel spomedzi Poľska, Česka, Litvy, Rumunska, Lotyšska, Bulharska a Maďarska. Tieto prieskumy dokážu vo vysokej miere dopomôcť k prijatiu adekvátnych opatrení a strategických rozhodnutí pri tvorbe politiky na vnútroštátnej ale aj medzinárodnej úrovni. GLOBSEC sa tiež venuje analýze, hodnoteniu a vytváraniu odporúčaní ako efektívne bojovať s dezinformáciami.⁵³

K subjektom podieľajúcim sa na regulácii šírenia dezinformácií môžeme zaradiť aj projekt „*konspiratori.sk*“, ktorý vznikol spojením nadšencov z digitálnych a komunikačných agentúr. Cieľom projektu je vytvorenie a aktualizácia zoznamu stránok s dezinformačným, konšpiračným a škodlivým obsahom, za účelom zabránenia financovania týchto webov objednávateľmi reklám. V rámci tohto projektu bol preto vytvorený kód, ktorého používaním sa objednávateľia vyhnú inzerovaniu svojej reklamy na stránkach so škodlivým obsahom. Takýmto spôsobom môže byť stránkam so škodlivým obsahom znížený príjem z reklám a zároveň sa objednávateľia reklám na internete vyhnú spájaniu svojej značky s týmito stránkami. Na zoznam stránky sa pritom škodlivé weby dostávajú na základe odôvodneného rozhodnutia odbornej komisie, ktorá poskytuje argumenty a dôkazy verejne dostupné na stránke *konspiratori.sk*.⁵⁴

⁵¹ INFOSECURITY. 2024. Portál infosecurity.sk. In *Infosecurity.sk*, 2024.

⁵² GLOBSEC. 2024. About us. In *Globsec.org*, 2024.

⁵³ GLOBSEC. 2023. Globsec Trends. In *Globsec.org*, 2023.

⁵⁴ KONSPIRATORI.SK. 2024. Prečo vznikla táto iniciatíva. In *konspiratori.sk*, 2024.

Ako veľmi užitočný vnímame aj projekt „*Bezpečne na nete*“ spoločnosti ESET, ktorý je zameraný na informovanie verejnosti o problematike nástrah na internete. Informácie z tejto stránky sú jednoduché, prehľadné a užitočné a môžu pomôcť užívateľom eliminovať negatívne dôsledky rôznych podvodných a dezinformačných kampaní.⁵⁵

ZÁVER

Záverom možno konštatovať, že dopady šírenia dezinformácií na jednotlivcov i celú spoločnosť sú tak závažné, že je potrebné neustále prijímať efektívne a účinné opatrenia a vynakladať ďalšie úsilie na vytváranie, transformáciu a posilňovanie subjektov, ktorých úlohou je regulovať alebo ktoré sa svojou činnosťou podieľajú na regulácii tohto nebezpečného fenoménu. Aj preto sa tento článok zaoberal analýzou subjektov podieľajúcich sa na regulácii šírenia dezinformácií v podmienkach SR i mimo SR. Pozornosť bola zameraná na relevantné štátne subjekty, ich kompetencie a vzájomné vzťahy v kontexte regulácie šírenia dezinformácií. Okrem štátnych subjektov sa na regulácii šírenia dezinformácií podieľajú aj nadnárodné a medzinárodné organizácie, ktorých je SR členom. Preto boli analyzované aj kompetencie uvedených subjektov a ich činnosť v tejto oblasti. Nezastupiteľné miesto pri znižovaní škodlivých účinkov dezinformácií majú aj mimovládne subjekty. Tie okrem svojej publikačnej a edukačnej činnosti spracovávajú aj odporúčania pre jednotlivé štáty a medzinárodné spoločenstvá.

Problematika dezinformácií je komplexným problémom, na ktorý je potrebné hľadať komplexné riešenia. Veľmi dôležitá je najmä edukácia v rámci práce s informáciami a rozvíjanie kritického myslenia. Okrem vzdelávania občanov je taktiež dôležitý prístup štátu v rámci strategickej komunikácie ako efektívneho spôsobu reakcie na dezinformácie. V rámci tejto oblasti boli prijaté viaceré koncepčné dokumenty. Napriek tomu však stále chýba určitá centralizácia a metodická koordinácia jednotlivých subjektov z jedného centra. Návrh na vytvorenie centralizovaného subjektu zodpovedného za oblasť regulácie šírenia dezinformácií už bol v minulosti diskutovanou témou. V roku 2023 bol predložený do pripomienkového konania návrh zákona o opatreniach na zvýšenie bezpečnosti a dôveryhodnosti platforiem v online prostredí. V súvislosti s týmto návrhom bol zámer zriadiť na Úrade vlády SR zložku, ktorou budú opatrenia proti dezinformačným kpaniam koordinovane prijímané, so zapojením príslušných subjektov a pod koordináciou a rozhodovaním úradu vlády. Podobne ako ďalšie spomínané návrhy, aj tento bol kritizovaný odbornou verejnosťou, najmä kvôli nerovnováhe moci a nezabezpečenia účinného a včasného prostriedku súdneho prieskumu a súdnej

⁵⁵ ESET. 2022. Nepodľahnite klamstvám o vojne. In *bezpecnenanete.eset.com*, 2022.

ingerencie.⁵⁶ Napriek tomu bol na Úrade vlády SR vytvorený odbor strategickej komunikácie, ktorý síce nepokrýva celoštátne problematiku hybridných hrozieb, avšak je dôležitým prvkom v systéme koordinácie strategickej komunikácie na celoštátnej úrovni.

V súčasnej dobe existujú určité koordinačné centrá na úrovni rezortov spolu s analytickým centrom na úrovni štátu. Je však potrebné vytvoriť centralizovaný orgán, ktorý sa bude zaoberať všetkými aspektami hybridných hrozieb – vrátane dezinformácií – na celoštátnej úrovni. Z uvedeného je možné vidieť, že téma centralizovaného koordinačného subjektu vo vzťahu k regulácii šírenia dezinformácií na celoštátnej úrovni, je stále aktuálnou. Preto je dôležité naďalej skúmať predmetnú oblasť a pri kreovaní nových inštitúcií reagovať na pripomienky relevantných subjektov.

Napriek spomínaným nedostatkom boli identifikované aj viaceré pozitívne kroky na národnej i nadnárodnej úrovni najmä prijatím strategických dokumentov a zintenzívneniu činnosti niektorých štátnych a medzinárodných subjektov. Dôležitým krokom v medzinárodnej oblasti je najmä implementácia DSA, ktorý ukladá pomerne široké kompetencie EK v oblasti regulácie digitálnych platforiem. Na národnej úrovni je prínosom pre zamestnancov verejnej správy a regionálnej samosprávy možnosť absolvovania kurzu vzdelávania v oblasti hybridných hrozieb poskytovaným CBHH.

Ako je možné vidieť, v prostredí SR, EÚ a NATO pôsobí spolu veľké množstvo subjektov, ktoré sa svojou činnosťou podieľajú na regulácii negatívnych účinkov dezinformácií. Okrem represívnej činnosti tieto organizácie spájajú odborníkov z rôznych oblastí, ktorí spolupracujú na vytváraní strategických dokumentov, analýz, publikácií, edukačnej činnosti, ale aj iných aktivitách, ktoré majú za následok zvyšovanie povedomia o tejto problematike. Činnosť mimovládnych subjektov v tejto oblasti považujeme tiež za veľmi dôležitú, nakoľko tieto organizácie vedú účinnou formou prezentovať názory verejnosti a zároveň združujú expertov z rôznych oblastí, ktorí vedú kvalifikovane prispieť k fungovaniu národných a medzinárodných subjektov, čím sa vytvára komplexný systém regulácie šírenia dezinformácií.

ZOZNAM POUŽITEJ LITERATÚRY A ZDROJOV:

ADAPT INSTITUTE. 2024. About us. In *adaptinstitute.org*, 2024. [online] [cit. 2024-03-15]. Dostupné na: <<https://lnk.sk/udt9>>.

ANALYTICKÝ ÚTVAR MOSR. 2022. Analytický útvar MO SR. [online] [cit. 2024-03-17]. Dostupné na: <<https://lnk.sk/dagt>>.

⁵⁶ JELINKOVÁ DUDZÍKOVÁ, D. Poznámky k návrhu zákona o boji proti dezinformáciám. In *Právne listy*, 2023.

CBHH. 2024. Hlavné úlohy CBHH MV SR. In *Hybridnehrozby.sk*, 2024. [online] [cit. 2024-03-16]. Dostupné na: <<https://lnk.sk/zbgu>>.

CBHH. 2024. Úrad vlády SR. In *Hybridnehrozby.sk*, 2024. [online] [cit. 2024-03-16]. Dostupné na: <<https://lnk.sk/zbgu>>.

CBHH. 2024. Ministerstvo zahraničných vecí a európskych záležitostí SR. In *Hybridnehrozby.sk*, 2024. [online] [cit. 2024-03-23]. Dostupné na: <<https://lnk.sk/zbgu>>.

CBHH. 2024. Vzdelávanie zamestnancov verejnej správy v oblasti hybridných hrozieb. In *Hybridnehrozby.sk*, 2024. [online] [cit. 2024-03-18]. Dostupné na: <<https://lnk.sk/pau0>>.

DUGOVIČ, T. 2022. Štát bude mať možnosť blokovat' škodlivé weby. Parlament zmenu schválil pre vojnu na Ukrajine. In *Standard.sk*, 2022. [online] [cit. 2024-03-17]. Dostupné na: <<https://lnk.sk/eie9>>.

DUŠEK, J. – KAVAN, Š. 2024. Dezinformace jako součást hybridních hrozeb – česko-slovenský pohled. In *Auspicia*, 2024, roč. 21, č. 1, s. 7-26. ISSN 2464-7217.

EDMO. 2024. About us. In *Edmo.eu*, 2024. [online] [cit. 2024-03-18]. Dostupné na: <<https://lnk.sk/plrz>>.

ESET. 2022. Nepodľahnite klamstvám o vojne. In *bezpecnenanete.eset.com*, 2022. [online] [cit. 2024-03-21]. Dostupné na: <<https://lnk.sk/gdj8>>.

EUINTCEN. 2015. Main functions and tasks. In *Statewatch.org*, 2015. [online] [cit. 2024-03-20]. Dostupné na: <<https://lnk.sk/exil>>.

EUROPEAN COMMISSION. 2024. The enforcement framework under the Digital Services Act. In *European Commission*, 2024. [online] [cit. 2024-03-16]. Dostupné na internete: <<https://lnk.sk/eqp>>.

EURÓPSKA KOMISIA. 2022. Účinnejší Kódex postupov EÚ proti šíreniu dezinformácií. In *European Commission*, 2022. [online] [cit. 2024-03-16]. Dostupné na: <<https://lnk.sk/pit0>>.

EURÓPSKA KOMISIA. 2024. Existujúce projekty. In *European Commission*, 2024. [online] [cit. 2024-03-16]. Dostupné na: <<https://lnk.sk/ocdy>>.

EURÓPSKA KOMISIA. 2024. The Digital Services Act. In *European Commission*, 2024. [online] [cit. 2024-03-16]. Dostupné na: <<https://lnk.sk/inn4>>.

Európska Únia. 2020. Coronavirus: EU Strengthens Action to Tackle Disinformation. In *Európska komisia*, 2020. [online] [cit. 2024-03-18] Dostupné na: <<https://lnk.sk/vm37>>.

Európska Únia. 2020. EEAS Special Report on the Narratives and Disinformation around the COVID-19/Coronavirus Pandemic: questions/answers. Brusel : Európsky parlament, 2020. [online] [cit. 2024-03-19] Dostupné na internete: <<https://lnk.sk/evze>>.

EUVSDISINFO. 2024. About. In *euvsdisinfo.eu*, 2024. [online] [cit. 2024-03-19]. Dostupné na: <<https://lnk.sk/oziu>>.

GLOBSEC. 2023. Globsec Trends. In *Globsec.org*, 2023. [online] [cit. 2024-03-22]. Dostupné na: <<https://lnk.sk/moqn>>.

GLOBSEC. 2024. About us. In *Globsec.org*, 2024. [online] [cit. 2024-03-22]. Dostupné na: <<https://lnk.sk/bmri>>.

HAJDÚKOVÁ, T. – KURILOVSKÁ, L. – MARR, S. 2023. Riziká komunikácie na sociálnych sieťach. In *Zborník z konferencie RELIK 2023: Reprodukcia ľudského kapitálu – vzájomné väzby a súvislosti*, 2023, s. 58-69. ISBN 978-80-245-2499-3.

HAJDÚKOVÁ, T. – ŠIŠULÁK, S. 2022. Abuse of modern means of communication to manipulate public opinion. In *INTED 2022 – Proceedings from 16th International Technology, Education and Development Conference*. IATED Spain, 2022, s. 1992-2000. ISBN 978-84-09-37758-9.

HAJDÚKOVÁ, T. 2024. Zdroje informácií alebo dezinformácií. In *Auspicia*, 2024, roč. 21, č. 1, s. 39-51. ISSN 2464-7217.

HNONLINE. 2022. NBÚ by mohol škodlivý online obsah blokovat' aj v budúcnosti, so súhlasom súdu. In *Stratégie*, 2023. [online] [cit. 2024-03-18]. Dostupné na: <<https://lnk.sk/vwil>>.

HYBRID COE. 2024. What is Hybrid CoE? In *hybridcoe.fi*, 2024. [online] [cit. 2024-03-19]. Dostupné na: <<https://lnk.sk/fubq>>.

INFOKOMPAS. 2024. O projekte. In *infokompas.stratpol.sk*, 2024. [online] [cit. 2024-03-20]. Dostupné na: <<https://lnk.sk/enix>>.

INFOSECURITY. 2024. Portál infosecurity.sk. In *Infosecurity.sk*, 2024. [online] [cit. 2024-03-20]. Dostupné na: <<https://lnk.sk/ivis>>.

ITAPA. 2021. Štát má niekoľko konkrétnych plánov, ako bojovať proti dezinformáciám. MIRRI už začalo. In *Itapa.sk*, 2021. [online] [cit. 2024-03-17] Dostupné na: <<https://lnk.sk/enbn>>.

IVANČÍK, R. – MÜLLEROVÁ, J. 2022. Dezinformácie ako hybridná hrozba šírená prostredníctvom sociálnych sietí. In *Policajná teória a prax*, 2022, roč. 30, č. 3, s. 22-42. ISSN 1335-1370. [online] [cit. 2024-03-20]. Dostupné na: <<https://sdu.sk/MMa>>.

IVANČÍK, R. 2022. Kybernetická (ne)bezpečnosť a sociálne siete. In *Aktuálne výzvy kybernetickej bezpečnosti: zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava: Akadémia Policajného zboru, 2022, s. 35-46. ISBN 978-80-8054-998-5.

IVANČÍK, R. 2023. Aktuálne východiská skúmania problematiky hybridných hrozieb. In *Policajná teória a prax*, 2023, roč. 31, č. 3, s. 38-52. ISSN 1335-1370. [online] [cit. 2024-03-22]. Dostupné na: <<https://sdu.sk/HVXms>>.

IVANČÍK, R. 2023. On Disinformation and Propaganda in the Context of the Spread of Hybrid Threats. In *Vojenské reflexie*, 2023, roč. 18, č. 3, s. 38-58. ISSN 1336-9202. [online] [cit. 2024-03-21]. Dostupné na: <<https://sdu.sk/OjL>>.

IVANČÍK, R. 2024. Dezinformácie ako bezpečnostná hrozba šírená na internete. In *Auspicia*, 2024, roč. 21, č. 1, s. 27-38. ISSN 2464-7217.

JELINKOVÁ DUDZÍKOVÁ, D. Poznámky k návrhu zákona o boji proti dezinformáciám. In *Právne listy*, 2023. [online] [cit. 2024-03-22]. Dostupné na: <<https://lnk.sk/yqy8>>.

KONSPIRATORI.SK. 2024. Prečo vznikla táto iniciatíva. In *konspiratori.sk*, 2024. [online] [cit. 2024-03-21]. Dostupné na: <<https://lnk.sk/rrvw>>.

KRAJČOVIČ, M. 2022. Kritika zabrala. Štát bude musieť zverejniť, prečo blokuje Hlavné správy a Infovojnu. In *Fontech*, 2022. [online] [cit. 2024-03-17]. Dostupné na: <<https://lnk.sk/xgp6>>.

KUCHTOVÁ, J. 2018. Aktuálne trendy súvisiace s využívaním moderných technológií. In *Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava: Akadémia Policajného zboru v Bratislave, 2018, s. 90-98. ISBN 978-80-8054-773-8.

LISOŇ, M. – FIDLER, L. 2022, Potreba a možnosti identifikácie rizík z realizácie hybridných hrozieb. In *Policajná teória a prax*, 2022, roč. 30, č. 2, s. 38-53. ISSN 1335-1370.

LUKÁČOVÁ, V. 2020. Hybridné hrozby v kybernetickom priestore. In *Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2020, s. 102-105. ISBN 978-80-8040-819-3.

NATO STRATCOM COE. 2024. About NATO StratCom COE. In *Stratcomcoe.org*, 2024. [online] [cit. 2024-03-19]. Dostupné na: <<https://lnk.sk/lyrx>>.

NBÚ. 2024. Zoznam blokovaných subjektov. In *nbu.gov.sk*, 2024. [online] [cit. 2024-03-19]. Dostupné na: <<https://lnk.sk/afi0>>.

NBÚ. 2024. Zoznam subjektov blokovaných EÚ. In *nbu.gov.sk*, 2024. [online] [cit. 2024-03-19]. Dostupné na: <<https://lnk.sk/lpta>>.

NENALET. 2024. O projekte. In *Nenalet.im*, 2024. [online] [cit. 2024-03-18]. Dostupné na: <<https://lnk.sk/hdr4>>.

PAŽICKÝ, M. 2019. TASR: "Veliteľstvo Síľ pre špeciálne operácie posilnili ďalšie útvary". In *vesso.mil.sk*, 2019. [online] [cit. 2024-03-17] Dostupné na: <<https://lnk.sk/sqt7>>.

PLIEŠOVSKÝ, R. 2021. Videli ste už schému nanočipu z vakcíny Pfizer? In *Techbox*, 2021. [online] [cit. 2024-03-15] Dostupné na: <<https://lnk.sk/xcem>>.

POLICAJNÝ ZBOR SR. 2022. Správa Policajného zboru o dezinformáciách na Slovensku v roku 2021. [online] [cit. 2024-03-14] Dostupné na: <<https://lnk.sk/vwa9>>.

POLICAJNÝ ZBOR SR. 2023. Správa Policajného zboru o dezinformáciách na Slovensku v roku 2022. [online] [cit. 2024-03-14] Dostupné na: <<https://lnk.sk/oi25>>.

RADA EÚ. 2022. EÚ uložila sankcie štátnym médiám RT/Russia Today a Sputnik s vysielaním v EÚ. In *European Council*, 2022. [online] [cit. 2024-03-20]. Dostupné na: <<https://lnk.sk/ualv>>.

RADA PRE MEDIÁLNE SLUŽBY. 2024. Čo je podnet týkajúci sa nelegálneho obsahu. In *rpms.sk*, 2024. [online] [cit. 2024-03-18]. Dostupné na: <<https://lnk.sk/djsi>>.

RADA PRE MEDIÁLNE SLUŽBY. 2024. Postavenie a poslanie Rady pre mediálne služby. In *rpms.sk*, 2024. [online] [cit. 2024-03-18]. Dostupné na: <<https://lnk.sk/ikjr>>.

RADA PRE MEDIÁLNE SLUŽBY. 2024. Zoznamy regulovaných subjektov. In *rpms.sk*, 2024. [online] [cit. 2024-03-18]. Dostupné na: <<https://lnk.sk/nugr>>.

REITER, M. 2021. Chcú nás začipovať? A môže za to Pfizer a 5G? In *TouchIT*, 2021. [online] [cit. 2024-03-14] Dostupné na internete: <<https://lnk.sk/woz6>>.

RTVS. 2022. Tribunal Súdneho dvora EÚ potvrdil zákaz vysielania ruskej televízie RT. In *Správy RTVS*, 2022. [online] [cit. 2024-03-15]. Dostupné na: <<https://lnk.sk/xgik>>.

ŠAMKO, P. 2022. Blokovanie webových stránok a jeho možný rozpor s judikatúrou Európskeho súdu pre ľudské práva. In *Právne listy*, 2022. [online] [cit. 2024-03-17]. Dostupné na: <<https://lnk.sk/ily5>>.

ŠIŠULÁK, S. – CÍCHOVÁ, M. 2019. Fake news a propaganda v kybernetickom priestore In *Aktuálne výzvy kybernetickej bezpečnosti v podmienkach bezpečnostných zložiek – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava: Akadémia Policajného zboru, 2019, s. 156-167. ISBN 978-80-8040-819-3.

SLIZ, M. 2022. Štát sa pokúsi predbehnúť dezinformátorov. In *Aktuality.sk*, 2022. [online] [cit. 2024-03-15]. Dostupné na: <<https://lnk.sk/pxaf>>.

SLOVENSKÁ INFORMAČNÁ SLUŽBA. 2022. Správa o činnosti SIS za rok 2021. [online] [cit. 2024-03-18] Dostupné na: <<https://lnk.sk/pack>>.

SLOVENSKÁ INFORMAČNÁ SLUŽBA. 2024. Poslanie a úlohy NBAC. In *sis.gov.sk*, 2024. [online] [cit. 2024-03-18]. Dostupné na: <<https://lnk.sk/iprf>>.

SSPI. 2024. Kto sme? In *Slovaksecurity.org*, 2024. [online] [cit. 2024-03-22]. Dostupné na: <<https://lnk.sk/fw89>>.

TOMÁŠEK. 2023. Hybridná vojna a hybridné hrozby. In *Bezpečnosť elektronickej komunikácie 2023 – zborník z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2023, s. 163-171. ISBN 978-80-8040-631-8.

VLÁDA SR. 2024. Štatút Situačného centra Slovenskej republiky. In *vlada.gov.sk*, 2024. [online] [cit. 2024-03-23] Dostupné na: <<https://lnk.sk/bah3>>.

VOJENSKÉ SPRAVODAJSTVO. 2022. Správa o činnosti VS za rok 2021. [online] [cit. 2024-03-18] Dostupné na: <<https://lnk.sk/wbu1>>.

ZACHAR KUČTOVÁ, J. 2022. Bezpečnosť na sociálnych sieťach. In *Bezpečnosť elektronickej komunikácie : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava: Akadémia Policajného zboru, 2022, s. 237-247. ISBN 978-80-8054-968-8.

ZACHAR KUČTOVÁ, J. 2024. Bezpečnostné riziká šírenia dezinformácií na internete prostredníctvom nástrojov umelej inteligencie. In *Auspicia*, 2024, roč. 21, č. 1, s. 74-85. ISSN 2464-7217.

ZACHAR, Š. 2022. Úvod do anonymných sietí – história ich vzniku a základné prvky. In *Aktuálne výzvy kybernetickej bezpečnosti : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava: Akadémia Policajného zboru, 2022, s. 73-83. ISBN 978-80-8054-998-5.

Zákon č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov.

Zákon č. 198/1994 Z. z. o Vojenskom spravodajstve v znení neskorších predpisov.

Zákon č. 264/2022 Z. z. o mediálnych službách v znení neskorších predpisov.

Zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov.

Zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov.

Zákon č. 46/1996 Z. z. o Slovenskej informačnej službe v znení neskorších predpisov.

Zákon č. 460/1992 Z. z. Ústava Slovenskej republiky.

Zákon č. 69/2018 Z. z. o Kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.