A U S P I C I A

Recenzovaný vědecký časopis pro oblast společenských a humanitních věd

Reviewed Scholarly Journal Dealing with Social Sciences

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ
ČESKÉ BUDĚJOVICE
VYSOKÁ ŠKOLA TECHNICKÁ A EKONOMICKÁ – ÚSTAV PODNIKOVÉ STRATEGIE
ČESKÉ BUDĚJOVICE
Ročník XXI, číslo 1

2024

AUSPICIA
Recenzovaný vědecký časopis pro otázky společenských a humanitních věd.
Založen v roce 2004. Vydáván Vysokou školou evropských a regionálních studií, České Budějovice, Česká republika a Vysokou školou technickou a ekonomickou, České Budějovice, Česká republika.

Rada pro výzkum, vývoj a inovace jako odborný a poradní orgán vlády ČR zařadila recenzovaný vědecký časopis Auspicia pro rok 2015 mezi recenzované neimpaktované časopisy, které uvedla v oborech Národního referenčního rámce excelence (NRRE).

V roce 2016 byl recenzovaný vědecký časopis Auspicia zařazen do mezinárodní databáze ERIH PLUS a od roku 2024 do online knihovny pro střední a východní Evropu – CEEOL.

AUSPICIA
A peer-reviewed scholarly journal for questions of the social sciences and humanities.
Founded in 2004. Published by The College of European and Regional Studies, České Budějovice, Czech Republic and The Institute of Technology and Business, České Budějovice, Czech Republic.

The Research, Development and Innovation Council, as a professional and consultative body of the Government of the Czech Republic, indexed Auspicia – a peer-reviewed scholarly journal on a list of peer-reviewed non-impacted journals in 2015, being published in the fields of the National Reference Framework of Excellence.

In 2016 Auspicia – a peer-reviewed scholarly journal was indexed in the international database ERIH PLUS and since 2024, it has been indexed in the Central and Eastern Europe Online Library – CEEOL.

Adresa redakce: Vysoká škola evropských a regionálních studií, z. ú., Žižkova tř. 1632/5b, 370 01 České Budějovice, tel.: 00420 386 116 839, https://auspicia.cz. Vychází dvakrát ročně v elektronické verzi (od roku 2019). **Únor 2024**. Časopis je financován VŠERS a VŠTE. **ISSN 2464-7217 (Online)**. **DOI: 10.36682/a_2024_1**.

Editorial Office Address: Vysoká škola evropských a regionálních studií, z. ú., Žižkova tř. 1632/5b, 370 01 České Budějovice, tel.: 00420 386 116 839, https://auspicia.cz. It has been published twice a year electronically (since 2019). **February2024**. This journal is financed by The College of European and Regional Studies and The Institute of Technology and Business. **ISSN 2464-7217 (Online)**. **DOI: 10.36682/a_2024_1.**

EDIČNÍ RADA VŠERS · EDITORIAL BOARD OF VŠERS

Předseda ediční rady · Chairman of the Editorial Board

doc. Ing. Jiří **DUŠEK**, Ph.D.

Interní členové · Internal Members

doc. JUDr. PhDr. Jiří **BÍLÝ**, CSc.; RNDr. Růžena **FEREBAUEROVÁ**; PhDr. Jan **GREGOR**, Ph.D.; doc. Ing. Marie **HESKOVÁ**, CSc.; PhDr. Štěpán **KAVAN**, Ph.D.; Mgr. Josef **KŘÍHA**, PhD.; doc. PhDr. Miroslav **SAPÍK**, Ph.D.; doc. Ing. Ladislav **SKOŘEPA**, Ph.D.; doc. Ing. Jaroslav **SLEPECKÝ**, PhD, MBA.; doc. JUDr. Roman **SVATOŠ**, Ph.D.

Externí členové · External Members

Ing. Jiří **ALINA**, Ph.D. *(Jihočeská univerzita, České Budějovice,* **ČR)**; doc. PhDr. PaedDr. Silvia **BARNOVÁ**, PhD., MBA (Vysoká škola *DTI*, **Slovensko**); prof. Berislav **BOLFEK**, Ph.D. (*Zadarská univerzita, Zadar*, **Chorvatsko**); doc. Ing. Jozefína **DROTÁROVÁ**, PhD., MBA (*Vysoká škola bezpečnostného manažérstva v Košiciach*, **Slovensko**); doc. MUDr. Lenka **HODAČOVÁ**, Ph.D. *(Univerzita Karlova, Hradec Králové,* **ČR)**; doc. Ing. Petra **PÁRTLOVÁ**, Ph.D. (*Vysoká škola technická a ekonomická v Českých Budějovicích*, **ČR**); prof. PhDr. Miroslava **SZARKOVÁ**, CSc. *(Ekonomická univerzita, Bratislava*, **Slovensko***)*; doc. Ing. Jarmila **STRAKOVÁ**, Ph.D. *(Vysoká škola technická a ekonomická v Českých Budějovicích,* **ČR***)*

REDAKCE ČASOPISU AUSPICIA · EDITORIAL OFFICE OF JOURNAL AUSPICIA

Předseda redakční rady · Chairman of the Editorial Board

doc. Ing. Jiří **DUŠEK**, Ph.D. *(Vysoká škola evropských a regionálních studií, České Budějovice,* ***ČR)***

Místopředseda redakční rady · Vice-chairman of the Editorial Board

doc. et doc. PaedDr. Mgr. Zdeněk **CAHA**, Ph.D., MBA, MSc. *(Vysoká škola technická a ekonomická v Českých Budějovicích,* ***ČR)***

Šéfredaktor · Editor-in-Chief

doc. PhDr. Miroslav **SAPÍK**, Ph.D.

Výkonný redaktor · Managing Editor

doc. PhDr. Miroslav **SAPÍK**, Ph.D.

Technická redaktorka · Technical Editor

RNDr. Růžena **FEREBAUEROVÁ**

Redaktoři anglických textů · English Language Editors

Centrum jazykových služeb Vysoké školy technické a ekonomické

ČLENOVÉ MEZINÁRODNÍ REDAKČNÍ RADY (25) · MEMBERS OF THE INTERNATIONAL EDITORIAL BOARD (25)

OBSAH

BEZPEČNOST

CONTENTS

SAFETY

BEZPEČNOST • SAFETY

DOI: 10.36682/a_2024_1_1

DEZINFORMACE JAKO SOUČÁST HYBRIDNÍCH HROZEB – ČESKO-SLOVENSKÝ POHLED

Disinformation as Part of Hybrid Threats – Czech-Slovak View

Jiří DUŠEK – Štěpán KAVAN

České Budějovice, Czech Republic

ABSTRACT:
The paper presents a comparative analysis of research on the issue of disinformation among students of two educational institutions in České Budějovice and Bratislava, namely the College of European and Regional Studies (CZ) and the Academy of the Police Force in Bratislava (SK). The research focuses on the comparison of attitudes, abilities, and awareness of disinformation among students from both institutions within their respective educational environments. The data were collected through questionnaire surveys and analysis of specific situations related to disinformation are relevant to security study programmes. Based on the partial results obtained through the questionnaire survey, three key findings emerged. The first finding indicates that almost all respondents confirm having experienced encounters with disinformation. The second finding points to the relatively low ability of the respondents to competently identify disinformation, with only 7.42 % of VŠERS students and 7.91 % of APZ students demonstrating this skill. The third crucial finding suggests that the training of security experts in both institutions needs to be changed and improved, as only 23.44 % of VŠERS students and 25.32 % of APZ students declare being sufficiently informed about the disinformation issue. These findings emphasize the need to upgrade the educational programs and highlight the challenge of increasing students´ awareness and skills related to combating disinformation. This research provides valuable insights for the educational programmes of both institutions and may serve as support for further development of teaching methodologies aimed at enhancing students' abilities to identify and handle the issues concerning spreading disinformation in society.

Key words: Czech Republic – disinformation – hybrid war – Slovakia – student.

ABSTRAKT:
Tento článek představuje komparativní analýzu výzkumu zaměřeného na problematiku dezinformací mezi studenty dvou vzdělávacích institucí v Českých Budějovicích a Bratislavě, konkrétně Vysoké školy evropských a regionálních studií (CZ) a Akademie policejního sboru v Bratislavě (SK). Výzkum klade důraz na srovnání postojů, schopností a povědomí o dezinformacích u studentů obou institucí v rámci jejich vzdělávacích prostředí. Data byla získána prostřednictvím dotazníkového šetření a analýzy konkrétních situací souvisejících s dezinformacemi, které jsou relevantní pro bezpečnostní studijní programy. Z dílčích výsledků získaných prostřednictvím dotazníkového šetření vyplynula tři klíčová zjištění. První zjištění naznačuje, že téměř všichni respondenti potvrzují zkušenost se setkáním s dezinformacemi. Druhé zjištění poukazuje na poměrně nízkou schopnost respondentů kvalifikovaně rozpoznat dezinformace, přičemž tuto dovednost prokázalo pouze 7,42 % studentů VŠERS a 7,91 %

studentů APZ. Třetí zásadní poznatek naznačuje, že je třeba změnit a zlepšit přípravu bezpečnostních pracovníků v obou institucích, neboť pouze 23,44 % studentů VŠERS a 25,32 % studentů APZ deklaruje, že jsou dostatečně informováni o problematice dezinformací. Tato zjištění podtrhují potřebu aktualizace vzdělávacích programů a zdůrazňují náročnost informovanosti a dovedností studentů v boji proti dezinformacím. Tento výzkum poskytuje cenné poznatky pro vzdělávací programy obou institucí a může sloužit jako podpora pro další rozvoj metodik výuky zaměřených na zvýšení schopností studentů identifikovat a řešit problémy spojené s dezinformacemi ve společnosti.

Klíčová slova: Česká republika - dezinformace - hybridní válka - Slovensko - student.

ÚVOD

Problematika dezinformací úzce souvisí se změnami, kterými prošla média v posledních 30 letech. V minulosti byla odpovědnost za pravdivost informací a jejich ověření kladeno na vydavatele konkrétního média (novin, časopisů), který musel posuzovat v souladu s etickými kodexy zpravodajství a publicistiky. Většina populace pak byla především příjemci informací, nikoli jejich tvůrci. Navíc produkce informací (časopisů, novin) vyžadovala finance (kapitál). S příchodem informační společnosti, otevřením světa internetu a sociálních sítí odpadly veškeré bariéry – produkovat obsah může kdokoli, kdykoli, bez nutnosti disponovat financemi, bez požadavku na ověřování informací. Jen část informací je přebírána z ověřených zdrojů – tiskových agentur a kanceláří (Kopecký, K. – Szotkowski, R., 2019, s. 2). Masivní šíření dezinformací, misinformací a dalšího manipulativního obsahu prostřednictvím sociálních sítí představuje dlouhodobý celospolečenský problém (Ivančík, 2023), jeho aktuálnost a palčivost byla v roce 2020 zásadně zvýrazněna pandemií způsobenou celosvětovou krizí. Vynucená izolace odkázala miliony lidí do domácí sféry, čímž ještě více posílila roli, kterou hrají sociální sítě a média v získávání informací. Zároveň také společně se vznikem krizové situace došlo k nárůstu škodlivého obsahu, který se prostřednictvím sítí šířil, jako i celkovému zahlcení informačního prostoru zprávami o pandemii a jejích dopadech. WHO v této souvislosti hovoří o tzv. infodemii – cirkulaci nadměrného množství mnohdy ne zcela důvěryhodných informací, v jejímž důsledku je obtížné identifikovat spolehlivé zdroje a zorientovat se ve složitém a neznámém tématu (Ministerstvo vnitra ČR, 2020).

Pandemie COVID-19 totiž odstartovala u lidí všech věkových skupin a s různým typem vzdělání vysokou poptávku po informacích o tomto onemocnění. Nejčastější dotazy byly o původu samotného viru, možné cesty jeho přenosu, prevenci, závažnosti onemocnění a léčbě. Právě toto je situace, kdy jsou lidé extrémně zranitelní dezinformacemi, které mohou mít nemalý dopad na jejich zdraví (Saling, L. L., et al, 2021).

POJMY, KONCEPTY, DEFINICE

Téma dezinformací je téma poměrně komplikované a ani odborníci se neshodnou na jednoznačné definici, popř. se používané pojmosloví kontinuálně vyvíjí. Níže je uvedena charakteristika základních pojmů, se kterými odborníci v současné době pracují nejčastěji při popisu a analýze daného problému.

- Dezinformace – Dezinformace představují komplexní jev, jehož podstata spočívá v úmyslném a cíleném šíření nepravdivých nebo zavádějících informací s cílem ovlivnit veřejné mínění. Tento fenomén se v digitálním věku stává stále prominentnějším a nabývá různorodých forem. Klíčovým prvkem je úmyslnost a záměr, kdy vytváření a šíření dezinformací nespočívá ve shodě, ale v organizovaném a systematickém postupu. Sociální média se stala klíčovým prostředkem pro šíření dezinformací. Virální kampaně, falešné profily a sdílení obsahu mezi uživateli umožňují rychlé šíření klamavých informací a zvyšují jejich dosah. To je patrné z výzkumu, například práce Allcotta, H. a Gentzkowa, M., 2017, o vlivu sociálních médií na americké volby v roce 2016. Dezinformace často slouží k dosažení politických, sociálních nebo ekonomických cílů. Jejich motivace je komplexní a může zahrnovat manipulaci veřejného mínění, ovlivňování volebních výsledků nebo podkopávání důvěry v instituce. V tomto ohledu se dezinformace stávají nástrojem politického boje a mohou způsobit významné společenské a politické dopady. Dezinformace mohou oslabit důvěru v tradiční informační zdroje, polarizovat společnost posilováním již existujících názorových bariér, a v extrémních případech vyvolávat politické nebo společenské nepokoje. V této souvislosti je „*nezbytné zkoumat postupy a taktiky, které využívají aktéři šířící dezinformace*“, jak naznačuje výzkum Diresty, R. a Shaffera, K. et al, 2018. Více lidí dle Millera, C. a Wildeho, G., 2022, ví, že „*informační prostor je různými způsoby napadán, a vynakládá se více prostředků na to, aby se těmto pokusům zabránilo*“.
- Misinformace – „*Misinformace představuje v digitálním věku rozsáhlý fenomén, jehož podstata spočívá ve šíření nepravdivých informací bez explicitního záměru klamání. Je to komplexní jev, který se stal výrazným problémem v informačním prostoru, zejména na sociálních médiích. Chápat misinformaci vyžaduje zhodnocení, jak vzniká, jaké jsou její dopady a jak lze předcházet neúmyslnému šíření chybných informací. Misinformace se často rodí z nedorozumění, chybné interpretace nebo špatného porozumění faktu. Přestože šiřitelé nemají záměr klamání, nesprávné informace mohou rychle získat virální charakter, zejména díky sociálním sítím. Virální kampaně, sdílení obsahu mezi uživateli a existující algoritmy mohou urychlit šíření klamavých informací*“

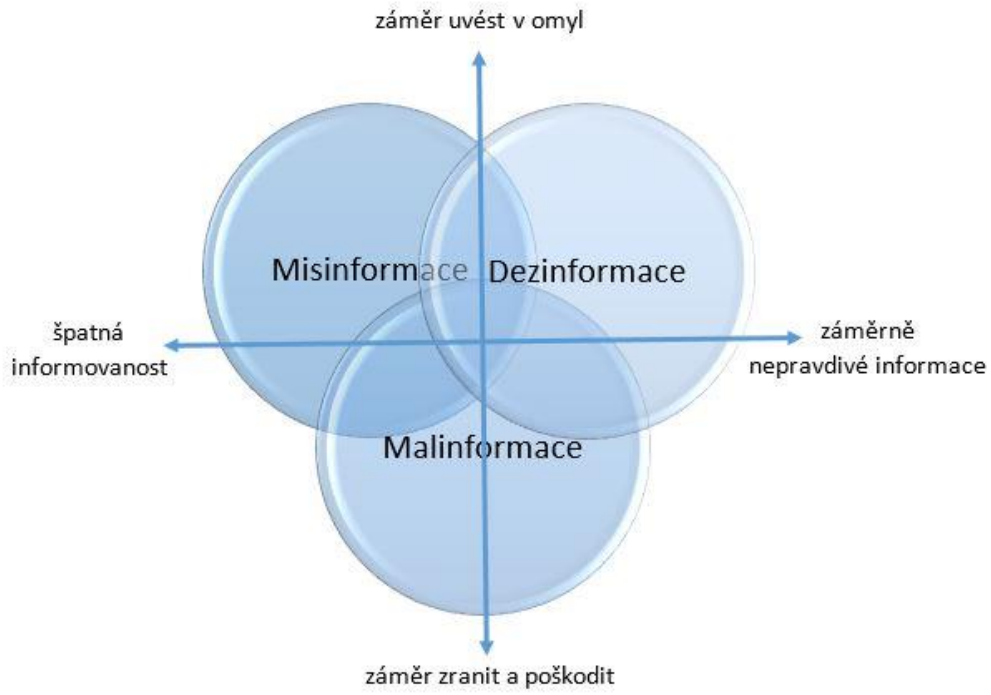
(Pennycook, G. – Bear, A. – Collins, E. T. – Rand, D. G., 2018). Svým obsahem misinformace často útočí na emoce, ať pozitivní (kupříkladu vyvoláváním pocitů nostalgie po dětství a minulých, lepších časech, načež typicky navazuje kritika současné státní garnitury), či negativní, většinou ve formě hrozby či morálního pohoršení (Žabka, J., 2021). Misinformace má široké dopady na společnost. „*Když jsou nesprávné informace vnímány jako pravdivé, může to snížit důvěru veřejnosti v tradiční informační zdroje a podkopat důvěryhodnost médií"* (Pennycook, G. – Bear, A. – Collins, E. T. – Rand, D. G., 2018). Dále může přispět k polarizaci společnosti, když posiluje existující názorové bariéry a vytváří tzv. „informační bubliny". Prevence misinformací vyžaduje komplexní přístup. Zvýšená mediální gramotnost veřejnosti (posílení kritického myšlení a hodnocení informací), transparentnost informačních zdrojů a spolupráce mezi vládou, médii a občanskou společností jsou klíčovými nástroji proti jejich šíření.

- Malinformace – Malinformace lze dle Havlíka, M., 2022, „*popsat jako skupinu informací, které jsou většinou založeny na realitě, ale jsou určeny k ublížení osobě, organizaci, skupině obyvatel nebo zemi (např. někdo použije obrázek mrtvého dětského uprchlíka bez kontextu ve snaze podnítit nenávist ke konkrétní etnické skupině, proti které jsou apod.)*". Tato forma dezinformace se liší od misinformace, kde klamání není primárním cílem, ačkoliv malinformace může zahrnovat různé taktiky, jako jsou přehánění, záměrné vynechávání kontextu a prezentace nejednoznačných informací. Malinformace se vyznačuje záměrným úsilím o šíření dezinformací s cílem klamání. Může vycházet z různých motivací, včetně politických, ekonomických nebo sociálních. Tato forma manipulace informací může být aktivně využívána k ovlivňování veřejného mínění, deformaci faktů a vytváření zkresleného obrazu skutečnosti. Malinformace má potenciál vytvářet hluboké narušení ve společnosti. Když je úmyslně šířena, může posílit polarizaci a vytvářet napětí mezi různými skupinami. V kombinaci s rychlostí šíření informací na sociálních médiích může mít malinformace okamžité a rozsáhlé dopady na veřejné mínění a stabilitu společnosti. Boj proti malinformacím vyžaduje integrovaný přístup, např. zvýšení mediální gramotnosti veřejnosti, ověřování faktů, sledování a identifikace zdrojů malinformací atd. Transparentnost informačních zdrojů, označování potenciálně klamavého obsahu a spolupráce digitálních platforem jsou základem prevence.

Dezinformace, misinformace a malinformace představují různé aspekty šíření nepravdivých informací, ačkoliv se liší v úmyslu a povaze. Dezinformace zahrnuje úmyslné šíření klamavých informací s cílem ovlivnit veřejnost. Na druhou stranu misinformace a

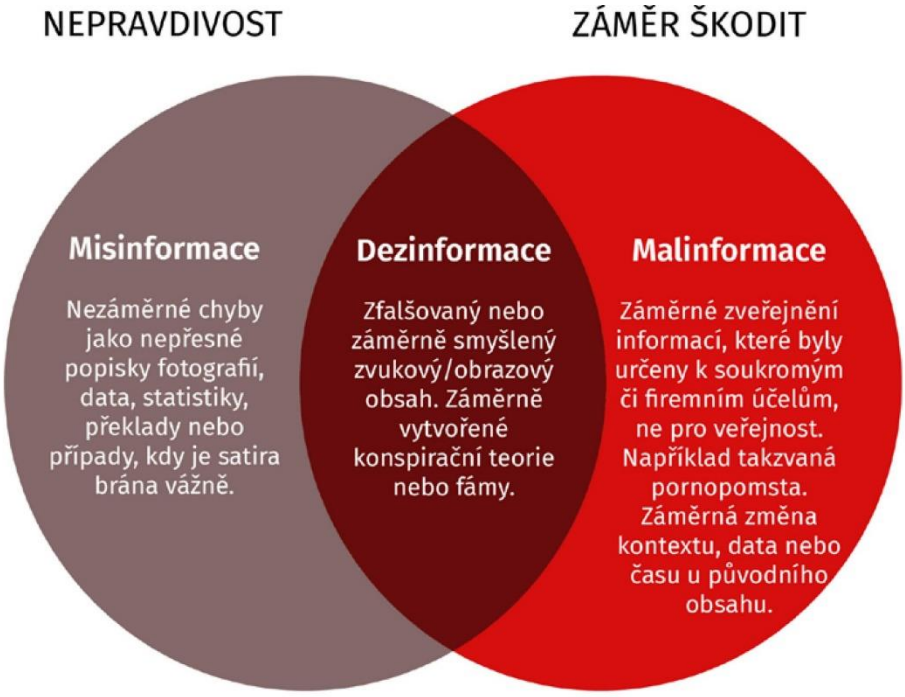
malinformace mohou být neúmyslné, přičemž první představuje poskytování chybných informací, zatímco druhá označuje neúmyslné šíření zavádějících nebo neúplných faktů. Blíže viz také Vosoughi, S. – Roy, D. – Aral, S., 2018. V kontextu těchto třech pojmů je dle Bahenského, V., 2023, důležité vést v patrnosti dva důležité aspekty jejich používání. První je, že hranice mezi dezinformací a misinformací může být velmi tenká, zvláště pokud někdo uvěří dezinformaci a následně ji šíří v dobré víře. Druhý důležitý aspekt terminologie dis-, mis – a malinformace je, že jejich rozlišení do značné míry závisí na identifikaci motivace šiřitele, která je empiricky velmi obtížně zkoumatelná a často ji nelze jednoznačně prokázat. Je na místě uvést ještě jeden pojem obtížně přeložitelný do českého jazyka – „bullshit“. Pojem, který lze volně chápat jako „kecy“, se užívá pro informace, jež jsou produkovány s cílem vyvolat určitý dojem nebo reakci (např. interakce přinášející výnos z reklamy), přičemž původce informace nutně vědomě nelže, pouze je mu pravdivostní hodnota informace lhostejná (Benkler, Y. – Faris, R. – Roberts, H., 2018, Pennycook, G. – Rand, D. G., 2020). V každém případě je klíčové rozlišovat mezi těmito pojmy, abychom lépe porozuměli příčinám a důsledkům šíření nepravdivých informací v moderní společnosti. Ochrana před těmito fenomény vyžaduje nejen snahu jednotlivců ověřovat a kriticky hodnotit informace, ale také zdokonalení médií, platforem a vzdělávacích institucí v boji proti nepravdivým obsahům a zachování důvěry v informační ekosystém.

Obrázek 1: Tři základní typy informačních mutací



Zdroj: Havlík, M., 2022, dle Helvoorta, J. van a Hermanse, M., 2020.

Obrázek 2: Typy informačního nepořádku



Zdroj: Allea, 2021, dle Wardle, C. a Derakhshana, H., 2017.

DRUHY DEZINFORMACÍ

Dezinformace mohou být klasifikovány podle různých kritérií, včetně záměru, média, formy a obsahu. Zde je několik způsobů kategorizace druhů dezinformací:

- Podle záměru:
  - Desinformace: Informace, která je nesprávná, ale šířena neúmyslně bez záměru klamat.
  - Misinformace: Nenapravitelné nesprávné informace, které jsou šířeny s dobrou vírou.
  - Dezinformace: Úmyslně šířené nepravdivé informace za účelem klamání a manipulace.
- Podle média:
  - Online dezinformace: Šíření dezinformací prostřednictvím sociálních sítí, webových stránek, blogů a dalších online platforem.
  - Dezinformace v tradičních médiích: Manipulace informací ve zpravodajství tradičních médií, jako jsou televize, rozhlas a noviny.
- Podle formy:
  - Textová dezinformace: Šíření nepravdivých informací prostřednictvím psaného textu.
  - Vizuální dezinformace: Využívání zkreslených nebo upravených obrázků, videí nebo grafiky.
  - Zvuková dezinformace: Manipulace s audio záznamy a šíření zkreslených zvukových informací.
- Podle obsahu:
  - Politická dezinformace: Šíření lží nebo zkreslení informací v politickém kontextu za účelem ovlivňování veřejného mínění, voličů nebo politických rozhodnutí.
  - Zdravotní dezinformace: Falešné informace o zdraví, léčbě nemocí nebo očkování.
  - Společenská dezinformace: Dezinformace, která ovlivňuje sociální skupiny, náboženství nebo etnické komunity.Podle úrovně organizovanosti:
  - Státní dezinformace: Organizovaná a koordinovaná dezinformační kampaň prováděná státem nebo jeho aktéry.
  - Nestátní dezinformace: Dezinformace šířená nevládními skupinami, jednotlivci nebo neorganizovanými subjekty.

- Podle úrovně technické složitosti:
    - Technická dezinformace: Využívání sofistikovaných technologií, jako jsou deepfake videa, generativní modely textu nebo úpravy zvuku, k vytváření klamavého obsahu.
- Podle cílové skupiny:
    - Nacionalistická dezinformace: Zaměřená na posilování národní identity a podkopávání důvěry v mezinárodní spolupráci.
    - Náboženská dezinformace: Zahrnuje klamání ve věcech náboženství a cílení na věřící komunity.
    - Korporátní dezinformace: Směřuje k ovlivňování vnímání firem nebo obchodních značek prostřednictvím nepravdivých informací.
- Podle prostředí šíření:
    - Dezinformace na sociálních sítích: Zaměřená na rychlou šíření pomocí platforem jako Facebook, X, Instagram apod.
    - E-mailová dezinformace: Šíření dezinformací prostřednictvím e-mailů s cílem dosáhnout co největšího dosahu.
    - Webové dezinformace: Vytváření falešných webových stránek s cílem šířit klamavý obsah.
- Podle způsobu manipulace:
    - Cituji nesprávně (quotation out of context): Prezentace citací bez kontextu tak, aby podporovaly falešný narativ.
    - Vyvolávání paniky: Úmyslné šíření dezinformací za účelem vyvolání strachu a paniky.
    - Polarizační dezinformace: Vytváření klamavého obsahu, který záměrně posiluje názorové rozdíly a polarizaci společnosti.

Různé formy dezinformací mohou být kombinovány a mohou se vyvíjet v závislosti na technologických inovacích a společenských trendech. Komplexnost této problematiky vyžaduje integrovaný přístup k vzdělávání, regulaci a technologickým inovacím. Blíže viz například Wardle, C. – Derakhshan, H., 2017, Tandoc, E. C., Jr. – Lim, Z. W. – Ling, R., 2018, Allcott, H. – Gentzkow, M., 2017, Starbird, K. – Palen, L., 2017, Bakir, V. – McStay, A., 2018, atd.

DEZINFORMACE JAKO HYBRIDNÍ HROZBA

Dle Bahenského, V., 2023, dochází k častému označování (zvláště v českém prostředí) nežádoucích informačních intervencí za hybridní hrozbu. Pojmy hybridní vedení války, hybridní válka, hybridní hrozby a hybridní působení pocházejí původně z prostředí amerického obranného establishmentu, kdy byly původně formulovány v reakci na vnímané proměny vedení války a zkušenosti z probíhajících válek na Blízkém východě (např. Fridman, O., 2018, Bahenský, V., 2018, Kurfürst, J. – Paďourek, J., 2022). Postupem času se koncept významně transformoval, zvláště po raketovém růstu jeho popularity po okupaci a anexi Krymu v roce 2014, byť informační dimenze hybridních hrozeb byla obsažen už v původních amerických formulacích konceptu. V současnosti je pojem převážně definován jako otevřené nebo skryté využívání kombinace nástrojů pod hranicí konvenční války za účelem poškození protivníka nebo dosažení jiných cílů (viz např. Giannopoulos, G. – Smith, H. – Theocharidou, M., 2021). Informační působení je pak jedním z možných nástrojů soupeře využívajícího hybridního působení. Zvláště v kontextu ČR jsou hybridní hrozby ztotožňovány s dezinformacemi, vzhledem k tomu, že dezinformace představují nejviditelnější aspekt hybridních hrozeb (Bahenský, V., 2023).

Dezinformace jsou považovány za hybridní hrozbu z důvodu své komplexnosti, různorodosti taktik, různých cílů a motivací. Tato kombinace faktorů přispívá k tomu, že dezinformace jsou mimořádně efektivní při ovlivňování společnosti a někdy i destabilizaci institucí. „*Dezinformace využívají širokou škálu taktik, od vytváření falešných zpráv a manipulace s médii po použití moderních technologií, jako jsou deepfake videa nebo vytváření botů na sociálních sítích. Tato variabilita taktik ztěžuje odhalování a boj proti nim*“ (Allcott, H. – Gentzkow, M., 2017). „*Dezinformace mohou být použity s různými cíli, včetně politické manipulace, destabilizace demokratických procesů, ovlivňování veřejného mínění, nebo dokonce podkopávání důvěry v instituce. Tyto různorodé motivace umožňují aktérům využívat dezinformace k dosažení specifických cílů podle jejich potřeb“* (Wardle, C. – Derakhshan, H., 2017). „*Hybridní hrozby v podobě dezinformací často kombinují online a offline prvky. Například dezinformační kampaně na sociálních médiích mohou být propojeny s konkrétními offline akcemi, jako jsou protesty, demonstrace nebo politické události. Tato kombinace ztěžuje sledování a rozpoznávání celkového dopadu dezinformací“* (Starbird, K. – Palen, L., 2017*)*. „*Díky internetu a sociálním médiím mají dezinformace schopnost rychle se šířit na globální úrovni. To umožňuje šiřitelům dezinformací dosáhnout širokého publika během krátké doby, což může mít vážné důsledky pro společnost*“ (Tandoc, E. C., Jr. – Lim, Z. W. – Ling, R. 2018).

Povaha mezinárodní bezpečnosti a konfliktů zůstává stejná. Státy jsou jako obvykle zapleteny do různých vojenských a ekonomických her s nulovým součtem, ozbrojené konflikty se stále zdají nevyhnutelné, bezpečnostní dilemata a balancování probíhají neustále a tak dále… Modus operandi však již není stejný. Konflikty se bojují novými, inovativními a radikálně odlišnými způsoby. S příchodem moderní hybridní války jim jde stále méně o smrtící sílu. Hybridní hrozby představují komplexní strategii, která kombinuje vojenské a nevojenské prostředky za účelem dosažení strategických cílů. Jednou z klíčových složek této strategie je využívání dezinformací, které jsou cíleně šířeny s úmyslem ovlivnit veřejné mínění, oslabit důvěru v instituce a destabilizovat společnost. Jak zdůrazňuje Bilal, A., 2021, „*hybridní hrozby představují vážné bezpečnostní výzvy, které vyžadují komplexní a koordinovanou odpověď*“. Ivančík, R., 2022, „*považuje hybridní a informační operace za největší asymetrické hrozby*“.

Dezinformace v rámci hybridních hrozeb jsou účinným nástrojem, zejména díky využívání moderních technologií a sociálních sítí. Analytické zprávy z Digital Forensic Research Lab (DFRLAB, 2023) ukazují, že dezinformační kampaně jsou často propojeny s kybernetickými útoky a manipulací online diskusí. Příkladem může být rozsáhlá dezinformační kampaň během amerických prezidentských voleb v roce 2016, kde bylo prostřednictvím sociálních médií šířeno množství klamných informací. EU se aktivně angažuje v boji proti dezinformacím prostřednictvím projektu *EU vs Disinfo* (viz EEAS, N.D.). Tento projekt sleduje a odhaluje dezinformace, zejména ty spojené s geopolitickými událostmi. Zároveň zdůrazňuje důležitost osvěty a mediální gramotnosti veřejnosti. V kontextu hybridních hrozeb je nezbytné zdůraznit, že opatření na ochranu společnosti musí být komplexní a globální. Projekty, jako *EU vs Disinfo*, sice přispívají k monitorování a odhalování dezinformací, ale prevence vyžaduje aktivní spolupráci na mezinárodní úrovni. Boj proti dezinformacím vyžaduje neustálý výzkum, inovativní přístupy a spolupráci napříč sektory. Pro udržení integrity informačního prostoru a demokratických hodnot je nezbytné, abychom společně pracovali na posílení rezilience společnosti vůči dezinformacím a jejich negativním dopadům.

CÍL A METODIKA VÝZKUMU

Hlavním cílem příspěvku je analýza názorů studentů studijního programu Bezpečnostně právní činnost Vysoké školy evropských a regionálních studií (VŠERS) a studentů Akadémie Policajného zboru v Bratislave (APZ) na problematiku dezinformací jako součásti hybridních hrozeb šířených především prostřednictvím sociálních sítí. Zaměření na budoucí/současné příslušníky bezpečnostních složek ČR a SR není náhodné, výsledky výzkumu budou využity nejen k diseminaci mezi odbornou veřejností, ale i k úpravě studijních plánů s cílem naučit

studenty dezinformace rozpoznat, monitorovat, analyzovat a komunikovat. Dotazníkové šetření bylo realizováno anonymní elektronickou formou od 30. 10. do 28. 11. 2023 v ČR, zúčastnilo se ho 55 studentů prezenčního studia, 201 studentů kombinovaného studia a 50 účastníků celoživotního vzdělávání (oblast pedagogiky), kteří však v tomto příspěvku nejsou bráni v potaz vzhledem k „nebezpečnostnímu" studijnímu zaměření. Celkově je tak za VŠERS vyhodnocováno 256 dotazovaných, využitou platformou byl Google Forms. Na Akadémii Policajného zboru v Bratislave bylo šetření realizováno od 3. 9. do 6. 12. 2023 přes platformu MS Forms, zúčastnilo se ho 102 studentů prezenčního studia, 172 studentů kombinovaného studia a 42 studentů celoživotního vzdělávání.

Šetření bylo realizováno v rámci vědecko-výzkumné úlohy „*Dezinformácie ako súčasť hybridných hrozieb pre demokratickú spoločnosť a ich vnímanie študentmi vysokých škôl*", reg. číslo APZ-OVVM-14/2023, která je realizována Vysokou školou evropských a regionálních studií a Akadémií Policajného zboru v Bratislavě. Metodika předkládaného příspěvku je založena na využití nejnovějších teoretických poznatků na základě studia odborné literatury, odborných výzkumů a studií, časopisů a materiálů, na hledání a hodnocení vzájemných vztahů a souvislostí, které přispívají k objasnění řešené problematiky a odvození a formulování adekvátních závěrů vyplývajících z této analýzy.

VÝSLEDKY A DISKUSE

Realizovaný dotazník se skládal z celkem 28 otázek, kdy 5 otázek bylo demograficky orientovaných, 11 otázek zjišťuje uživatelské chování respondentů (způsob zjišťování informací, využívání sociálních sítí, preference respondentů apod.). Jádrem dotazníku je 12 otázek zacílených na dezinformace, zejména se jedná o konkretizaci setkání s nimi, hodnocení jejich nebezpečnosti a schopnost identifikace dezinformací, šetření hodnotí i míru rozsahu dané problematiky ve výuce. V rámci tohoto příspěvku se autoři selektivně zaměřili pouze na otázky konkretizující setkání s dezinformacemi a otázky hodnotící nebezpečnost dezinformací.

Zjištěné výsledky potvrdily předpoklad, že se míra setkání s dezinformacemi v dnešní digitální době zvyšuje, a to zejména v online prostředí. Setkání s dezinformacemi potvrzuje 99,61 % dotazovaných respondentů VŠERS a 98,42 % respondentů APZ. K tak vysoké míře setkání s dezinformacemi přispívá zejména několik faktorů:

- Online média a sociální sítě: Mnoho lidí získává informace z online zdrojů, což může být problematické, pokud nejsou informace ověřené a spolehlivé.

- Filtrovací bubliny: Algoritmy sociálních sítí a vyhledávačů mohou vytvářet filtry, které lidem ukazují obsah, který odpovídá jejich stávajícím názorům, což může vést k izolaci od diverzity informací.
- Cílené kampaně: Některé skupiny nebo státy mohou využívat dezinformace k dosažení svých politických nebo strategických cílů, což může zvyšovat celkový objem dezinformací.
- Nízká mediální gramotnost: Mnoho lidí nemusí být dostatečně gramotných v oblasti mediálního vzdělávání, což znamená, že nejsou schopni efektivně rozlišit mezi spolehlivými a falešnými informacemi.

Nejčastějšími místy setkání jsou logicky internet (80,86 % VŠERS a 85,44 % APZ) a sociální sítě (84,38 % VŠERS a 86,39 % APZ), významným prostorem k setkání s dezinformacemi je i televize (41,8 % VŠERS a 44,62 % APZ) a osobní kontakt (rodinní příslušníci, přátelé, známí a další osoby – 51,95 % VŠERS a 58,23 % APZ). Marginálními odpověďmi byly rádio (6,25 % VŠERS, 10,13 % APZ), tisk (15,23 % VŠERS a 28,48 % APZ) a knihy (1,95 % VŠERS a 4,11 % APZ). Největší rozdíl ČR/SR lze spatřovat zejména v oblasti tisku (Δ 13,25 %).

Míra vysokého přesvědčení respondentů o setkání s dezinformacemi je v částečném rozporu právě s úrovní mediální gramotnosti respondentů, kdy pouze 7,42 % respondentů VŠERS a 7,91 % respondentů APZ deklaruje, že je schopno kvalifikovaně rozpoznat dezinformace. 37,11 % respondentů VŠERS oproti 47,47 % respondentů APZ uvádí, že spíše ano. 54,68 % respondentů VŠERS a 40,82 % respondentů APZ není o své schopnosti rozpoznat dezinformace přesvědčeno (odpověď částečně ne či spíše ne). 0,78 % respondentů VŠERS a 3,8 % respondentů APZ není subjektivně schopno dezinformace rozpoznat. Rozpoznání dezinformací vyžaduje kritické myšlení, schopnost analyzovat informace a důkladnou mediální gramotnost. Mezi klíčové dovednosti a strategie, které mohou pomoci rozpoznat dezinformace patří: ověřování zdrojů, kontrola faktů, rozpoznání emocí, kritické myšlení, analýza původu a obsahu obrázků a videí, zhodnocení titulků a nadpisů, diverzifikace zpravodajství/informačních zdrojů, vzdělávání o dezinformacích apod. Rozpoznání dezinformací je kontinuálním procesem, který vyžaduje aktivní úsilí a vývoj kritického myšlení. Být obezřetný a schopný kriticky posuzovat informace je klíčové pro orientaci v dnešním komplexním informačním prostředí. S ohledem na bezpečnostní zaměření respondentů je nutné též uvést, že dle Ministerstva vnitra ČR, 2023, k identifikaci dezinformací příliš nepřispívá ani česká legislativa, která „*nezná pojem „dezinformace“, ani „propaganda“, tudíž ani v českém trestním právu není definována skutková podstata trestného činu „dezinformace“ či „propagandy“. Tato jednání*

jsou trestná, pouze pokud by k nim došlo v rámci jednání, které by naplnilo např. § 181 Poškození cizích práv, § 184 Pomluva, § 345 Křivé obvinění, § 355 Hanobení národa, rasy, etnické nebo jiné skupiny osob, § 356 Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod, § 357 Šíření poplašné zprávy, § 365 Schvalování trestného činu, § 364 Podněcování k trestnému činu, nebo § 404 projev sympatií k hnutí směřujícímu k potlačení práv a svobod člověka podle zákona č. 40/2009 Sb., trestního zákoníku".

Pokud jde o názor respondentů, zda je dezinformace součástí hybridních hrozeb a hybridní války, tak lze jednoznačně konstatovat, že ano. Tento názor sdílí 77,35 % respondentů VŠERS (46,88 % rozhodně/určitě ano, 30,47 % spíše ano) a 84,07 % respondentů APZ (51,59 % rozhodně/určitě ano, 32,48 % spíše ano). Názor, že dezinformace jsou částečně ano a částečně ne součástí hybridních hrozeb a hybridní války, sdílí v ČR poměrně vysoký počet 20,7 % respondentů oproti 14,65 % respondentů v SR. Nesouhlas vyjádřil minimální počet respondentů (1,56 % spíše ne a 0,39 % rozhodně ne v ČR a 0,96 % spíše ne a 0,32 % rozhodně ne v SR). Názor respondentů koresponduje se závěry řady studií, že dezinformace hrají klíčovou roli v rámci hybridních hrozeb a hybridních válek.

Dezinformace mohou být klíčovým prvkem v hybridních hrozbách a válkách z několika důvodů:

- Ovlivňování veřejného mínění: Cílem dezinformačních kampaní může být ovlivňování veřejného mínění, jak doma, tak i v cílových zemích. Účelem může být vytvoření deziluze, podkopání důvěry v instituce nebo destabilizace společnosti.
- Diskreditace protivníka: Dezinformace může být použita k diskreditaci politických představitelů, vojenských osobností nebo celých zemí. Falešné informace mohou být šířeny s cílem oslabit image nebo legitimitu protivníka.
- Rozpínání konfliktu: Informační války mohou být navrženy tak, aby zvyšovaly napětí a konflikty mezi různými skupinami nebo státy. Dezinformace mohou přispívat k eskalaci konfliktů a vytvářet nepřátelství.
- Vytváření chaosu: Cílem některých dezinformačních kampaní může být vytvoření chaosu a nejistoty. To může mít za následek politickou nestabilitu a oslabení ústředních institucí.
- Kybernetické operace: Dezinformace může být propojena s kybernetickými útoky a hybridními operacemi, kde jsou používány různé nástroje a prostředky k dosažení strategických cílů.

V důsledku toho je rozpoznání a boj proti dezinformacím stále důležitější součástí obrany státu proti hybridním hrozbám. V rámci dotazníkového šetření proto byla stěžejní

otázkou i zpětná vazba od studentů týkající se reflexe problematiky dezinformací a hybridních hrozeb v obsahu jejich vysokoškolského studia. Zde se bohužel prokazuje, že dle názoru studentů je jejich příprava v rámci studia nedostatečná. Pouze 23,44 % respondentů VŠERS a 25,32 % respondentů APZ deklaruje, že je o této problematice dostatečně informováno. 76,57 % respondentů VŠERS a 74,68 % respondentů APZ uvádí, že se s touto problematikou buď vůbec nesetkala, nebo jen na minimální, tzn. nedostatečné úrovni. Ambicí obou vysokých škol by tak mělo být při nejbližší reakreditaci promítnout tuto problematiku v míře co nejširší do studijních plánů vybraných studijních programů.

ZÁVĚR

Z dílčích výsledků dotazníkové šetření mezi studenty VŠERS a APZ vyplývají 3 základní zjištění:

- Setkání s dezinformacemi potvrzuje 99,61 %, respektive 98,42 % dotazovaných respondentů, tzn. téměř všichni respondenti.
- Jen 7,42 % respondentů VŠERS a 7,91 % respondentů APZ je však schopno kvalifikovaně rozpoznat dezinformace.
- Příprava odborníků v oblasti bezpečnosti se musí v oblasti dezinformací změnit a zlepšit, protože pouze 23,44 % respondentů VŠERS a 25,32 % respondentů APZ deklaruje, že je o této problematice dostatečně informováno.

Výsledky mezinárodního šetření mezi studenty obou vysokých škol, které vykazují u klíčových otázek pouze zanedbatelné rozdíly v řádu procent, jsou zajímavé a mohou být interpretovány několika způsoby:

- Podobnost vzdělávacího prostředí: Výsledky ukazují na možnou podobnost vzdělávacího prostředí mezi oběma školami. To může znamenat, že studenti obou institucí mají podobný přístup k učení, stejně jako podobné povědomí o daném tématu.
- Univerzálnost problému: Nízké rozdíly mohou také ukazovat na to, že problém, který byl předmětem šetření, je univerzální nebo alespoň široce sdílený mezi studenty nezávisle na jejich geografickém umístění nebo konkrétní instituci.
- Efektivita vzdělávacích programů: Výsledky mohou být také interpretovány jako známka (ne)efektivity vzdělávacích programů obou škol, které dokáží připravit studenty s podobným povědomím nebo postoji k dané problematice.
- Mezinárodní srovnávání: Výsledky mohou poskytnout cenný vhled pro mezinárodní srovnávání vzdělávacích systémů a studentů. Pokud jsou rozdíly zanedbatelné, mohou

tato zjištění poskytnout podporu pro přístup k internacionalizaci výzkumných a vzdělávacích aktivit.

- Limitace a reflexe: Při interpretaci výsledků je také důležité zvážit případné omezení šetření a zohlednit, zda je výsledek skutečně reprezentativní pro celkovou situaci.

Celkově lze konstatovat, že minimální rozdíly v řádu procent u klíčových otázek jsou pozoruhodným výsledkem a mohou poskytnout platformu pro další diskuzi a porovnání mezi oběma institucemi.

Boj proti dezinformacím na vysokých školách zaměřených na vzdělávání v oblasti bezpečnosti je mimořádně důležitý, zejména v kontextu narůstajících kybernetických hrozeb a hybridních konfliktů, je proto nutné přijmout specifické strategie a opatření, která mohou být implementována v rámci jednotlivých studijních programů či celých škol zaměřených na oblast vnitřní a vnější bezpečnosti. Jedná se například o:

- Vytváření specializovaných kurzů o dezinformacích a kybernetické bezpečnosti, které se zaměřují na konkrétní problémy spojené s dezinformacemi, manipulací s informacemi a kybernetickou bezpečností. Tato výuka by měla zahrnovat praktické dovednosti, jako jsou analýza digitálních stop, monitorování sociálních sítí a zajišťování kybernetické bezpečnosti.
- Zavedení interdisciplinárních programů, které zahrnují prvky zejména z oblastí informatiky, politologie, bezpečnostních studií, žurnalistiky a komunikačních věd.
- Simulace kybernetických útoků, kde studenti mohou v praxi testovat své schopnosti v odhalování a reagování na dezinformace a kybernetické hrozby.
- Navazování spolupráce s odborníky na kybernetickou bezpečnost, zpravodajskými službami a bezpečnostními firmami, kteří mohou přinést praktické zkušenosti a nové know-how.
- Analýzy konkrétních případů – případové studie dezinformačních kampaní a kybernetických útoků umožňující studentům hlouběji porozumět mechanismům a strategiím útočníků.
- Vývoj softwaru pro detekci dezinformací – projekty vytvářejících software nebo algoritmy pro detekci dezinformací a analýzu digitálních stop. Blíž viz např. studentský projekt Verifee, který rozšiřuje webový vyhledávač. Po jeho instalaci pak umělá inteligence na dostupných zpravodajských webech nabídne u článků číselné hodnocení a zdůvodnění případných technických nedostatků. Model informace spojí, vyhodnotí a ukáže pak skóre důvěryhodnosti od 0 do 100 společně s transparentním vysvětlením,

proč bylo toto skóre uděleno. Čím nižší skóre, tím je článek pravděpodobně manipulativnější a chce klamat čtenáře (BRAVANSKÝ, 2023).

- Bezpečnostní audity – provádění bezpečnostních auditů na sociálních sítích, které pomáhají identifikovat a analyzovat falešné účty, šíření dezinformací a kybernetické hrozby.
- Mezinárodní spolupráci – zapojení vysokých škol do mezinárodních iniciativ a spolupráce s s jinými univerzitami, institucemi a odborníky v oblasti kybernetické bezpečnosti a boje proti dezinformacím.

Implementace strategií a opatření zaměřených na vzdělávání v oblasti bezpečnosti a boje proti dezinformacím má klíčový význam v přípravě studentů na komplexní výzvy, které nám přináší současný digitální svět. S nárůstem digitálních technologií a přítomností internetu ve všedním životě se zvyšuje i riziko kybernetických hrozeb a šíření dezinformací. Odborníci v oblasti bezpečnosti musí dnes nejen mít hluboké znalosti o technických aspektech kybernetických hrozeb, ale také být schopni aktivně analyzovat a rozlišovat informace v prostředí, které je náchylné k dezinformacím. To zahrnuje schopnost identifikovat manipulativní obsah, rozpoznat dezinformační kampaně a efektivně komunikovat s veřejností o otázkách bezpečnosti. Vzdělávací strategie by měly studenty vybavit nejen s technickými dovednostmi, ale také s kritickým myšlením a schopností citlivě hodnotit a kontrolovat informace, které „konzumují“. To může zahrnovat i povědomí o různých formách manipulace a technikách šíření dezinformací, což studentům umožní lépe porozumět a reagovat na aktuální bezpečnostní výzvy. Důležitým aspektem vzdělávání v oblasti bezpečnosti je také podpora etického chování online a odpovědného používání digitálních médií. Studenti by měli být schopni rozpoznat etická dilemata spojená s kybernetickou bezpečností a dezinformacemi a být vybaveni nástroji pro správné rozhodování v těchto situacích. Celkově lze říci, že vzdělání v oblasti bezpečnosti a boje proti dezinformacím by mělo být komplexní a multidisciplinární, aby studenti získali nejen technické, ale i společenské a etické kompetence potřebné k úspěšnému působení v digitálním prostředí.

POUŽITÁ LITERATURA A INFORMAČNÍ ZDROJE:

1. ALLCOTT, H. – GENTZKOW, M. (2017): Social Media and Fake News in the 2016 Election. *Journal of Economic Perspectives,* Vol. 31, No. 2. ISSN 0895-3309. pp. 211–236.
2. ALLEA. (2021): *Fakt, nebo fake? Jak čelit vědeckým dezinformacím*. Berlín: ALLEA – Celoevropské sdružení akademií.

3. BAHENSKÝ, V. (2018): Paradox hybridní války: O příčinách a následcích pragmatismu v debatě. *Obrana a strategie*, Vol. 2018, No. 2. ISSN 1802-7199. pp. 89–100.
4. BAHENSKÝ, V. *Radikalizace a „fake news" – stav expertního poznání* (2023). [online]. [cit. 2024-01-07]. Dostupný z <https://www.iir.cz/radikalizace-a-fake-news-stav-expertniho-poznani>
5. BAKIR, V. – MCSTAY, A. (2018): Fake News and the Economy of Emotions: Problems, Causes, Solutions. *Digital Journalism*, Vol. 6, No. 2. ISSN 2167-0811. pp. 154–175.
6. BENKLER, Y. – FARIS, R. – ROBERTS, H. (2018): *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. Oxford: Oxford University Press.
7. BILAL, A. *Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote* (2021). [online]. [cit. 2024-01-07]. Dostupný z <https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html>
8. BRAVANSKÝ, M. *Verifee – Vaše rozšíření proti fakenews* (2023). [online]. [cit. 2024-01-08]. Dostupný z <https://verifee.ai/>
9. DFRLAB. *Digital Forensic Research Lab* (2023). [online]. [cit. 2024-01-07]. Dostupný z <https://dfrlab.org/>
10. DIRESTA, R. – SHAFFER, K. – RUPPEL, B. – SULLIVAN, D. – MATNEY, R. – FOX, R. – ALBRIGHT, J. – JOHNSON, B. *The Tactics & Tropes of the Internet Research Agency* (2018). [online]. [cit. 2024-01-07]. Dostupný z <https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/12/The_Tactics__Tropes_of_the_Internet_Research_Agency.pdf>
11. EEAS. *EU vs Disinfo* (n.d.). [online]. [cit. 2024-01-07]. Dostupný z <https://euvsdisinfo.eu/>
12. FRIDMAN, O. (2018): *Russian „Hybrid Warfare": Resurgence and Politicization*. Oxford: Oxford University Press.
13. GIANNOPOULOS, G. – SMITH, H. – THEOCHARIDOU, M. *The Landscape of Hybrid Threats: A Conceptual Model (Public Version)* (2021). [online]. [cit. 2024-01-07]. Dostupný z <https://www.hybridcoe.fi/publications/the-landscape-of-hybrid-threats-a-conceptual-model/>
14. HAVLÍK, M. (2022): Inovativní pohled na metodický proces čelení dezinformacím. *Vojenské rozhledy*, Vol. 31, No. 4. ISSN 1210-3292. pp. 23–36.

15. HAVLÍK, M. (2022): Inovativní pohled na metodický proces čelení dezinformacím. In *Vojenské rozhledy*, Vol. 31, No. 4. ISSN 1210-3292. pp. 23–36. na základě HELVOORT, J. van, HERMANS, M. (2020): Effectiveness Of Educational Approaches To Elementary School Pupils (11 Or 12 Years Old) To Combat Fake News. *Media Literacy and Academic Research,* Vol. 3, No. 2. ISSN 2585-9188. pp. 38–47.
16. IVANČÍK, R. (2022): *Bezpečnosť. Teoreticko-metodologické východiská*. Plzeň: Aleš Čeněk.
17. 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. 2024-01-07]. Dostupný z <https://doi.org/10.52651/vr.a.2023.3.38-58>
18. KOPECKÝ, K. – SZOTKOWSKI, R. (2019): *Dezinformace a fake news*. Olomouc: Univerzita Palackého v Olomouci.
19. KURFÜRST, J. – PAĎOUREK, J. (eds.) (2022): Za zrcadlem hybridní válka jako staronový fenomén mezinárodních vztahů. Praha: Academia.
20. MILLER, C. – WILDE, G. *Focusing on 'Disinformation' Creates More Problems Than It Solves* (2022). [online]. [cit. 2024-01-07]. Dostupný z <https://www.worldpoliticsreview.com/misinformation-vs-disinformation-define/>
21. MINISTERSTVO VNITRA ČR. *Dezinformace na sociálních sítích a EU – poučení z krize?* (2020). [online]. [cit. 2024-01-07]. Dostupný z <https://www.mvcr.cz/chh/clanek/dezinformace-na-socialnich-sitich-a-eu-pouceni-z-krize.aspx>
22. MINISTERSTVO VNITRA ČR. *Trestněprávní úprava* (2023). [online]. [cit. 2024-01-07]. Dostupný z <https://www.mvcr.cz/chh/clanek/dezinformacni-kampane-trestnepravni-uprava-trestnepravni-uprava.aspx>
23. PENNYCOOK, G. – BEAR, A. – COLLINS, E. T. – RAND, D. G. (2018): The Implied Truth Effect: Attaching Warnings to a Subset of Fake News Headlines Increases Perceived Accuracy of Headlines Without Warnings. *Management Science,* Vol. 66, No. 11. ISSN 0025-1909. pp. 4944–4957.
24. PENNYCOOK, G. – RAND, D. G. (2020): Who Falls for Fake News? The Roles of Bullshit Receptivity, Overclaiming, Familiarity, and Analytic Thinking. *Journal of Personality,* Vol. 88, No. 2. ISSN 1467-6494. pp. 185–200.
25. SALING, L. L. – MALLAL, D. – SCHOLER, F. – SKELTON, R. – SPINA, D. (2021): No One is Immune to Misinformation: An Investigation of Misinformation Sharing by Subscribers to a Fact-checking Newsletter. *Plos One*, Vol. 16, No. 8. ISSN 1932-6203.

26. STARBIRD, K. – PALEN, L. (2017): (How) Will the Revolution be Retweeted?: Information Diffusion and the 2011 Egyptian Uprising. In *Proceedings of the ACM 2012 Conference on Computer Supported Cooperative Work (CSCW 2012*). New York: Association for Computing Machinery. pp. 7–16.
27. TANDOC, E. C., Jr. – LIM, Z. W. – LING, R. (2018): Defining "Fake News": A Typology of Scholarly Definitions. *Digital Journalism*, Vol. 6, No. 2. ISSN 2167-0811. pp. 137–153.
28. VOSOUGHI, S. – ROY, D. – ARAL, S. (2018): The Spread of True and False News Online. *Science*, Vol. 359, No. 6380. ISSN 1095-9203. pp. 1146–1151.
29. WARDLE, C. – DERAKHSHAN, H. (2017): Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making. Strasbourg: Council of Europe.
30. ŽABKA, J. *Špína na Piráty a podpora pro Babiše a „vlastence". Jak vidí svět před volbami příjemci řetězových mailů* (2021). [online]. [cit. 2024-01-07]. Dostupný z <https://hlidacipes.org/spina-na-piraty-a-podpora-pro-babise-a-vlastence-jak-vidi-svet-pred-volbami-prijemci-retezovych-mailu/>

Tento článek byl zpracovaný v rámci mezinárodní vědeckovýzkumné úlohy č.: APZ-OVVP-14-2023 „Dezinformácie ako súčasť hybridních hrozieb pre demokratickú spoločnosť a ich vnímanie študentmi vysokých škôl" (VÝSK 268).

ADDRESS & ©

doc. Ing. Jiří DUŠEK, Ph.D.
Katedra managementu veřejné správy
Vysoká škola evropských a regionálních studií, z. ú.
Žižkova tř. 1632/5b, 370 11 České Budějovice
Czech Republic
dusek@vsers.cz
ORCID iD – 0000 0002 0687 8311

PhDr. Štěpán KAVAN, Ph.D.
Katedra právních oborů a bezpečnostních studií
Vysoká škola evropských a regionálních studií, z. ú.
Žižkova tř. 1632/5b, 370 11 České Budějovice
Czech Republic
stepan.kavan@email.cz
ORCID iD – 0000 0001 7997 8711

BEZPEČNOST • SAFETY

DOI: 10.36682/a_2024_1_2

DEZINFORMÁCIE AKO BEZPEČNOSTNÁ HROZBA ŠÍRENÁ NA INTERNETE

Disinformation as a security threat spread on the Internet

Radoslav IVANČÍK

Bratislava, Slovak Republic

ABSTRAKT: V súčasnej modernej informačnej spoločnosti je online prostredie už prirodzenou, všadeprítomnou a v mnohých prípadoch nenahraditeľnou súčasťou pracovného, spoločenského i súkromného života. Internet sa v posledných rokoch globálne rozšíril a dnes je dostupný pre prevažnú väčšinu ľudskej populácie. Neustále sa dynamicky vyvíja a vo väčšej či menšej miere ovplyvňuje všetky oblasti, sféry či sektory ľudskej spoločnosti i samotného ľudského života, vrátane komunikácie. Ľudstvu prináša na jednej strane mnoho pozitív, ale na druhej strane aj mnoho negatív v podobe možností, ako ho zneužívať a prostredníctvom neho šíriť nepravdivé, zavádzajúce, skreslené, neúplné a/alebo vymyslené informácie v podobe dezinformácií. Z uvedeného dôvodu sa autor v predloženom článku, s využitím relevantných vedeckých metód a prístupov v rámci realizovaného interdisciplinárneho výskumu, zaoberá dezinformáciami ako bezpečnostnou hrozbou šírenou na internete, pretože prostredníctvom nich je možné ovplyvňovať jednotlivcov, sociálne skupiny i širokú časť verejnosti, formovať ich postoje, správanie a vnímanie reality.

Kľúčové slová: Dezinformácie – informácie – internet – spoločnosť – bezpečnostná hrozba.

ABSTRACT: In today's modern information society, the online environment is a natural, ubiquitous and often irreplaceable part of working, social and private life. The Internet has spread globally in recent years and is now accessible to the vast majority of the human population, developing constantly, dynamically, and affecting, to a greater or lesser extent, all areas, spheres or sectors of human society and human life in general, including communication. On the one hand, it offers many positives to mankind, but on the other hand, it also brings many negatives in the form of its potential misuse and dissemination of false, misleading, distorted, incomplete, and/or fabricated information - misinformation. For this reason, the author of the present article uses relevant scientific methods and approaches, and as part of the interdisciplinary research, deals with disinformation as a security threat spreading on the Internet, since it enables influencing individuals, social groups, and a large part of the public, shaping their attitudes, behaviour, and perception of reality.

Key words: Disinformation – information – internet – society – security threat.

ÚVOD

V súčasnej modernej informačnej spoločnosti je online prostredie už prirodzenou, všadeprítomnou a v mnohých prípadoch nenahraditeľnou súčasťou pracovného, spoločenského i súkromného života. Internet sa stal v posledných rokoch globálne rozšíreným a všeobecne dostupným pre prevažnú väčšinu ľudskej populácie. Neustále sa dynamicky vyvíja a vo väčšej či menšej miere ovplyvňuje všetky oblasti, sféry či sektory ľudskej spoločnosti[1] i samotného ľudského života.

Vďaka internetu je dnes jednoduché komunikovať a vymieňať si či zdieľať informácie s ľuďmi zo všetkých kútov planéty, absolvovať online pracovné porady, pohovory či súkromné stretnutia s rodinou, priateľmi a známymi, vzdelávať sa, získavať nové vedomosti a zručnosti, mať prehľad o aktuálnom svetovom dianí atď. Na druhej strane, na rozdiel od vyššie uvedených, ale aj mnohých ďalších pozitív, vývoj nových infraštruktúr[2] a moderných technológií – internet nevynímajúc – prinášajú aj pomerne širokú škálu možností, ako ich zneužívať a cestou nich šíriť nepravdivé, zavádzajúce, skreslené, neúplné a/alebo vymyslené informácie v podobe rôznych dezinformácií.

V tejto súvislosti je možné dodať, že dezinformácie sú svojím spôsobom prirodzenou súčasťou demokratických spoločností, v ktorých sa uznáva sloboda slova a ktoré nepresadzujú jediný správny uhol pohľadu (Európsky parlament, 2021). Dnes už tradičné médiá nie sú jedinými, ktoré určujú, ktoré správy sú pre publikum relevantné a ktoré nie. Užívatelia tvoriaci obsah na internete nemusia dodržiavať etiku (Sapík, 2022) a profesijné zásady platiace pre novinárov a sú sami sebe editormi. Nezväzuje ich legislatíva regulujúca tradičné médiá (Kavan, 2021).

V nadväznosti na uvedené možno dodať, že za kľúčový moment sú často označované americké prezidentské voľby v roku 2016, počas ktorých dochádzalo k hromadnému šíreniu dezinformácií z táborov oboch kandidátov – republikánskeho i demokratického. Všeobecne ale

[1] Rýchly vývoj v oblasti internetu a výpočtovej techniky spôsobil, že aj úrady začali vytvárať vlastné informačné systémy pre svoju internú komunikáciu a výmenu dát a informácií, čo súvisí so začiatkom e-Governmentu v Českej republike i Slovenskej republike (Dušek, 2023).

[2] Rýchly a takmer neriadený a živelný rozvoj existujúcich infraštruktúr s internetovými technológiami sa stal zdrojom problémov aj v oblasti zaisťovania kybernetickej bezpečnosti v podobe kybernetických hrozieb (Dušek, 2020). Kým v minulosti sa o kybernetických hrozbách hovorilo nanajvýš v kontexte bezpečnosti osobných a firemných počítačov a serverov, v uplynulých rokoch sa situácia dramaticky zmenila. Kybernetickú hrozbu už nemožno chápať len ako potenciálny útok hackerov, pri ktorom sú ľuďom, firmám a korporáciám odcudzené dáta a citlivé údaje. Hrozby sa presunuli prakticky do všetkých oblastí spoločnosti, počnúc ekonomikou, politikou, verejným aj súkromným sektorom a vojenskou a civilnou oblasťou. Prítomné sú tak na národnej úrovni, ako aj v medzinárodnom kontexte. Ich cieľom môže byť kritická infraštruktúra, ako sú telekomunikačné alebo energetické siete, ale aj bežné zariadenia používané v domácnostiach (Andrassy – Grega, 2015; Kollár, 2019; Nečas – Kollár, 2021; Jurčák a kol., 2023).

panuje zhoda na tom, že dezinformácie šírené z tábora Donalda Trumpa mali oveľa výraznejší vplyv na voličov a prispeli k jeho víťazstvu (Allcot – Gentzkow, 2017, s. 212). Aké závažné nebezpečenstvo predstavujú dezinformácie ukázali aj posledné dve veľké krízy: pandémia koronavírusu a invázia ruských vojsk na Ukrajinu, v súvislosti s ktorými sa šírilo a neustále šíri množstvo nepravdivých, zavádzajúcich, skreslených, neúplných a/alebo vymyslených informácií.

METODIKA A CIEĽ

Napriek pomerne značnému množstvu poznatkov, ktoré sa v priebehu niekoľkých uplynulých rokov nazbierali, a záujmu odbornej i laickej verejnosti o problematiku dezinformácií, dosiaľ bolo zaznamenaných len málo pokusov o všeobecné predstavenie tohto fenoménu a jeho jednotlivých aspektov. Jednou z hlavných príčin je skutočnosť, že výskumníci, ktorí sa problematikou dezinformácií zaoberajú, prirodzene rešpektujú určité hranice a nechcú rozšíriť skúmanie za hranice svojej vednej disciplíny, prípadne dezinformácie nie sú tou hlavnou prioritou v ich vedeckovýskumnej činnosti a pod. Viditeľne sa to prejavuje v tom, že napríklad v prácach patriacich do oblasti spoločenských vied sa veľmi zriedkavo vyskytujú odkazy na nejaký politologický alebo bezpečnostný výskum týkajúci sa dezinformácií.

Aj preto je primárnym cieľom autora článku, s využitím relevantných vedeckých metód (najmä teoretickej analýzy a syntézy, kvalitatívnej a obsahovej analýzy, metódy štúdia dokumentov, vedeckej metódy teoretického zovšeobecňovania poznatkov a skúseností) v rámci realizovaného kvalitatívneho teoretického interdisciplinárneho vedeckého výskumu a vychádzajúc z diel renomovaných zahraničných i domácich autorov, prispieť k akademickej diskusii a prehĺbeniu teoretických poznatkov o dezinformáciách. Zároveň je cieľom autora priniesť čitateľom z radov odbornej i laickej verejnosti najnovšie poznatky o dezinformáciách ako bezpečnostnej hrozbe šírenej na internete.

VÝSLEDKY A DISKUSIA

Dezinformácie sú, podobne ako mnohé iné pojmy, definované rôzne. V súčasnosti neexistuje žiadne ich jednotné, unifikované a všeobecne akceptované definičné vymedzenie, a preto sa v literatúre možno stretnúť s pomerne veľkým množstvom definícií líšiacich sa predovšetkým tým, kto je ich tvorcom, v akej sfére pôsobí a v akom odvetví či oblasti spoločnosti sa dezinformácie vyskytujú, resp. aplikujú. Napriek ich väčšej či menšej odlišnosti, spoločným rysom všetkých používaných definícií je fakt, že v prípade dezinformácií ide

o úmyselnú modifikáciu poskytovaných informácií so zámerom ovplyvniť, oklamať či uviesť adresátov týchto informácií do omylu.

DEFINIČNÉ VYMEDZENIE POJMU DEZINFORMÁCIE

V slovenskom prostredí sú pomerne často využívané definície nachádzajúce sa v príslušných slovníkoch. Napríklad v Slovníku cudzích slov je dezinformácia vymedzená veľmi stručne ako *„nesprávna, vedome skreslená informácia“* (Slovník cudzích slov, 2023). V Slovníku súčasného slovenského jazyka je už dezinformácia definovaná obšírnejšie ako *„nepravdivá, vedome skreslená informácia, ktorej cieľom je ovplyvniť určitú skupinu ľudí, prípadne celú populáciu“* (Slovník súčasného slovenského jazyka. 2023). V Slovníku pojmov z mediálnej výchovy sa uvádza, že *„dezinformácia je úmyselne nesprávna či skreslená informácia tajne implantovaná do informačnej sústavy oponenta so zámerom ovplyvniť potrebným smerom jeho aktivity“* (Slovník pojmov z mediálnej výchovy, 2020).

Podľa Krátkeho slovníka hybridných hrozieb, ktorý vznikol z iniciatívy Národného bezpečnostného analytického centra: *„Dezinformácia je overiteľne nepravdivá, zavádzajúca alebo manipulatívne podaná informácia, ktorá je zámerne vytvorená, prezentovaná a šírená s jednoznačným úmyslom klamať alebo zavádzať, spôsobiť nejakú ujmu alebo zabezpečiť nejaký zisk (napríklad politický či hospodársky). 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 paródia, ani správy a komentáre naklonené jednej strane, ktoré sú takto zreteľne označené“* (Krátky slovník hybridných hrozieb, 2023).

V českom prostredí, Centrum proti hybridným hrozbám Ministerstvo vnútra Českej republiky na svojich webových stránkach označuje dezinformáciu za *„šírenie zámerne nepravdivých informácií, najmä štátnymi aktérmi alebo ich odnožami voči cudziemu štátu alebo voči médiám, s cieľom ovplyvniť rozhodovanie alebo názory tých, ktorí ich prijímajú“* (MV ČR, 2020).

Na európskej úrovni, podľa Akčného plánu proti dezinformáciám, ktorý bol prijatý na pôde Európskeho parlamentu *„dezinformácie predstavujú preukázateľne nepravdivé alebo zavádzajúce informácie, vytvorené, prezentované a šírené za účelom ekonomického zisku alebo zámerného klamania verejnosti a môžu spôsobiť verejné škody“* (Európska komisia, 2018). Kľúčovým prvkom, ktorý sa v tejto súvislosti v predmetnom dokumente zdôrazňuje, je úmysel. Severoatlantická aliancia vníma dezinformácie ako *„zámerné vytváranie a šírenie*

nepravdivých a/alebo manipulovaných informácií s úmyslom klamať a/alebo zavádzať, pričom aktéri šíriaci dezinformácie sa snažia prehĺbiť rozdiely v rámci spojeneckých krajín a medzi nimi a podkopať dôveru ľudí vo zvolené vlády" (NATO, 2020).

INTERNET A JEHO ÚLOHA PRI ŠÍRENÍ DEZINFORMÁCIÍ

Dezinformácie tu boli aj pred nástupom internetu a sociálnych sietí. Premena spôsobu produkcie a konzumácie správ, ktorú spôsobil vzostup internetu a sociálnych sietí, však výrazným spôsobom uľahčila ich šírenie. Internet znížil náklady na vstup na mediálny trh. Dnes už jednotlivec nepotrebuje mať prístup do tradičných médií na šírenie vlastných myšlienok a názorov. Stačí mať vlastný blog alebo účet na sociálnych sieťach s dostatkom sledovateľov. Tradičné médiá tak stratili svoju výsadnú úlohu tzv. gatekeeperov[3] (Groshec – Tandoc, 2017, s. 201).

Vďaka všadeprítomnosti internetu sa celý mediálny cyklus zrýchlil, čerstvé správy sú dostupné v akúkoľvek hodinu dňa, nielen v ranných novinách alebo vo večernom spravodajstve. Internet zároveň umožnil svojim používateľom slobodu rozhodovať sa, kedy a aké informácie budú konzumovať, ako aj možnosť na ne bezprostredne a verejne reagovať. Mediálne prostredie sa stalo fragmentovaným, internetoví tvorcovia sú sami sebe editormi a nemusia dodržiavať žurnalistické štandardy, etiku a pravidlá (Lazer a kol., 2018, s. 1094).

Dôvera v tradičné médiá sa s nástupom internetu znížila, a to aj kvôli spomínanej fragmentácii mediálneho prostredia, ktoré umožňuje politickým aktérom odovzdávať svoje oznámenia mimo tradičných médií, ktoré si ich výroky overujú, zasadzujú do kontextu a komentujú. Tradičné médiá môžu politici označovať za nedôveryhodné alebo nadŕžajúce politickým konkurentom bez obáv, že stratia prístup k svojmu publiku (Lazer a kol., 2018, s. 1095).

Obrovské množstvo zdrojov a fragmentácia mediálneho prostredia je jedným z hlavných dôvodov toho, prečo sú internet a sociálne siete ideálnym podhubím na šírenie dezinformácií (Kuchtová, 2018). S rastúcim množstvom zdrojov informácií a ich šírením na internete a sociálnych sieťach sa stáva posudzovanie dôveryhodnosti zdrojov náročnejším (Kuchtová, 2019). Druhým hlavným dôvodom je vytváranie tzv. echo komôr[4], pretože ľudia väčšinou vyhľadávajú podobne zmýšľajúcich jedincov (Baum a kol., 2017). Navyše, kvôli možnosti distribuovať internetový obsah na základe osobných preferencií užívateľa, svojou

[3] Gatekeeperom je ten, kto rozhoduje o výbere tém a udalostí, ktoré sa budú spracovávať na mediálne obsahy.

[4] Echo komora je pojem, ktorý označuje situáciu, keď určité myšlienky, presvedčenia alebo údajové body sú posilnené opakovaním uzavretého systému, ktorý neumožňuje voľný pohyb alternatívnych alebo konkurenčných myšlienok alebo konceptov.

funkcionalitou sa stihol stať mocným nástrojom, pomocou ktorého je možné manipulovať verejnou mienkou a polarizovať spoločnosť (Hajdúková – Bindas, 2023).

Internet umožňuje svojim užívateľom združovať sa v uzavretých skupinách osôb s podobnými názormi (Hajdúková – Hruška, 2018), kde si navzájom zdieľajú informácie, ktoré interpretujú prostredníctvom zdieľaného systému významov a spoločne ich zasadzujú do svojho videnia sveta (Bessi a kol., 2016, s. 554). Bez akýchkoľvek alternatívnych informácií sa jedinci v skupinách utvrdzujú vo svojich názoroch. Echo komory môžu ovplyvňovať politické (Trifunović a kol., 2021) a/alebo ekonomické rozhodovanie (Sabayová, 2018; Sabayová – Červená, 2023) ľudí a taktiež poskytovať priestor na manipuláciu s verejnou mienkou (Šišulák – Cíchová, 2019) a normalizáciu nenávistných a extrémistických postojov alebo predsudkov a prehlbovať rozdelenie spoločnosti (Baum a kol., 2017; Danics – Tejchmanová, 2017). Aj šírenie dezinformácií je v nich oveľa jednoduchšie a efektívnejšie (Bessi a kol., 2016, s. 558).

Z jednej z najrozsiahlejších štúdií o šírení dezinformácií na internete vyplýva, že dezinformácia sa šíri oveľa rýchlejšie a medzi väčším počtom príjemcov ako pravdivá informácia a aj šanca, že dezinformácia bude ďalej zdieľaná, je až o 70 % vyššia. Možným vysvetlením je, že dezinformácie častejšie obsahujú výrazne nové a prekvapivé informácie, preto majú väčšiu šancu upútať pozornosť publika, ktoré ich ďalej zdieľa. Dezinformácie zároveň v publiku prebúdzajú emócie, ako sú prekvapenie a/alebo znechutenie,[5] ktoré tiež posilňujú snahu ďalej ich zdieľať (Aral a kol., 2018, s. 1149).

Navyše, inzercia v online prostredí internetu umožňuje dezinformátorom na šírení svojho obsahu zarábať (Lazer, 2018, s. 1096). Allcot a Gentzkow (2017, s. 217) v tejto súvislosti identifikujú dva hlavné dôvody vytvárania falošných správ a dezinformácií. Prvým z nich je ideológia, pretože ich vytváraním a šírením je možné jednak očierniť politických rivalov, médiá, osobnosti a jednak ovplyvniť verejnosť. Druhým dôvodom je práve finančný zisk. Z uvedeného vyplýva, že internet je ideálnym nástrojom na šírenie dezinformácií, preto je nutné brať to do úvahy pri akejkoľvek debate o nástrojoch boja proti dezinformáciám.

[5] Pravdivé informácie, naopak, prebúdzajú skôr pocit dôvery, očakávania, smútku alebo radosti.

ZÁVER

Využívanie internetu na šírenie dezinformácií je najmä v posledných rokoch typickým príkladom zneužívania moderných technológií, predovšetkým informačných a komunikačných technológií, systémov a prostriedkov za účelom dosiahnutia vopred stanovených politických, ideologických, ekonomických alebo iných cieľov. V mnohých prípadoch predstavuje šírenie dezinformácií prostredníctvom internetu bezpečnostnú hrozbu, ktorej šírenie je súčasťou vedenia informačných a psychologických operácií v rámci hybridných hrozieb nasmerovaných voči demokratickým spoločnostiam (Kavan, 2020; Ivančík, 2022; 2023). Pomocou týchto operácií je totiž možné ovplyvňovať jednotlivcov, sociálne skupiny i širokú časť verejnosti, formovať ich postoje, správanie a vnímanie reality. Vedené operácie je nutné vnímať ako súčasť aktérmi vyvíjaných aktivít, ktorých cieľom je poškodiť protivníka.

Dezinformácie môžu šíriť štáty (štátni aktéri), ale aj na štáty napojení neštátni aktéri. Využívajú ich ako súčasť aktivít smerujúcich k oslabeniu pozícií jednotlivých politických súperov, k narušovaniu chodu a fungovania demokratickej spoločnosti, k napádaniu súčasného demokratického systému i pravidiel, princípov a zásad na ktorých je demokratická spoločnosť postavená, k narušovaniu spoločenskej súdržnosti a k zvyšovaniu neistoty v nej. Dezinformácie zároveň pomáhajú prehlbovať už existujúce rozpory a polarizáciu v spoločnosti, radikalizujú nielen postoje publika, ale aj prebiehajúcu diskusiu v spoločnosti. Publikum ovplyvnené dezinformáciami je menej ochotné si prijímané informácie overovať a uchyľuje sa k alternatívnym zdrojom informácií. Ľahšie sa radikalizuje, pričom radikalizovaní jedinci majú oveľa silnejšie sklony k násiliu. Šírenie dezinformácií môže tiež narúšať diplomatické vzťahy medzi krajinami. Aj preto sú dezinformácie považované za bezpečnostnú hrozbu.

POUŽITÁ LITERATÚRA A INFORMAČNÉ ZDROJE:

1. ALLCOTT, H. – GENTZKOW, M. (2017): Social Media and Fake News in the 2016 Election. In *Journal of Economic Perspectives*, 2017, roč. 31, č. 2, s. 211-236. ISSN 1944-7965. [online] [cit. 15-11-2023]. Dostupné na internete: <https://pubs.aeaweb.org/doi/pdfplus/10.1257/jep.31.2.211>.
2. ANDRASSY, V. – GREGA, M. (2015): Možnosti optimalizácie informačných systémov v bezpečnostnom systéme. In Košická bezpečnostná revue, 2015, roč. 5, č. 2, s. 11-18. ISSN 1338-4880.

3. ARAL, S. – ROY, D. – VOUSOUGHI, S. (2018): The spread of true and false news online. In *Science*, 2018, roč. 359, č. 6380, s. 1146-1151. ISSN 2780-8971. [online] [cit. 17-11-2023] Dostupné na: <https://www.science.org/doi/10.1126/science.aap9559>.
4. BAUM, M. – LAZER, D. – MELE, N. (2017): Combating Fake News: An Agenda for Research and Action. In *Harvard Kennedy School, Shorenstein Center on Media, Politics and Public Policy*, 2017. [online] [cit. 17-11-2023] Dostupné na internete: <https://shorensteincenter.org/combating-fake-news-agenda-for-research/>.
5. BESSI, A. – CALDARELLI, G. – VICARIO, M. – PETRONI, F. – QUATTROCIOCCHI, W. – STANLEY, E. – ZOLLO, F. (2016): The spreading of misinformation online. In *PNAS*, 2016, roč. 113, č. 3, s. 554-559. ISSN 1091-6490.
6. DANICS, Š. – TEJCHMANOVÁ, L. (2017): *Extremismus, radikalismus, populismus a euroskepticismus*. Praha : Univerzita Jana Amose Komenského, 2017. 420 s. ISBN 978-80-7452-122-5.
7. DUŠEK, J. (2020): Smart City/Region – rozvojové a limitující faktory v Jihočeském kraji. In Cudlínová, E. (ed.): *Rozvoj Jihočeského kraje – potenciál pro aplikaci iniciativy Evropské komise Smart Region*. České Budějovice : Jihočeská univerzita, Ekonomická fakulta, 2020. s. 36-46. ISBN 978-80-7394-799-6.
8. DUŠEK, J. (2023): Data Boxes as a Part of the Strategic Concept of Computerization of Public Administration in the Czech Republic. In *Administrative Sciences*, 2023, roč. 13, č. 6, s. 154. ISSN 2076-3387. [online] [cit. 17-11-2023] Dostupné na internete: <https://doi.org/10.3390/admsci13060154>.
9. Európska komisia. (2018): Action Plan Against Disinformation. In *European Commission*, 2018. [online] [cit. 14-11-2023] Dostupné na internete: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52018JC0036>.
10. Európsky parlament. (2021): The impact of disinformation on democratic processes and human rights in the world. In *European Parliament – Policy Department for External Relations*, 2021. 64 s. ISBN 978-92-846-8014-6.
11. GROSHEK, J. – TANDOC, E. (2017): The affordance effect: Gatekeeping and (non) reciprocal journalism on Twitter. In *Computers in Human Behavior*, 2017, roč. 66, č. 2, s. 201-210. ISSN 0747-5632. [online] [cit. 17-11-2023] Dostupné na internete: <https://doi.org/10.1016/j.chb.2016.09.020>.
12. HAJDÚKOVÁ, T. – BINDAS, B. (2023): Možnosti ovplyvňovania verejnej mienky v on-line priestore pri volebnej kampani. In *Bezpečnosť elektronickej komunikácie 2023* –

zborník z vedeckej konferencie s medzinárodnou účasťou. Bratislava : Akadémia Policajného zboru, 2023, s. 31-44. ISBN 978-80-8040-631-8.

13. HAJDÚKOVÁ, T. – HRUŠKA, P. (2018): Prínos siete Internet pre rozvoj spoločnosti a jeho možnosti využitia v činnosti Policajného zboru. In *Tradície a dynamika vývoja manažmentu a informatiky z pohľadu univerzít s bezpečnostným zameraním*. Brati-slava: Akadémia Policajného zboru, 2018, s. 131-142. ISBN 78-80-8054-768-4.
14. HAJDÚKOVÁ, T. – ŠIŠULÁK, S. (2022): Abuse of modern means of communication to manipulate public opinion. In INTED 2022: 16th International Technology, Education and Development – Conference Proceedings. Barcelona : IATED, 2022, s. 1992-2000. ISBN 978-84-09-37758-9.
15. IVANČÍK, R. (2022): Dezinformácie ako hybridná hrozba. In *Dezinformácie a právo – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2020, s. 54-65. ISBN 978-80-8054-965-7.
16. 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.
17. IVANČÍK, R. (2023): Úvod do skúmania problematiky konšpiračných teórií. In *Auspicia*, 2023, roč. 20, č. 1, s. 56-70. ISSN 2464-7217. [online] [cit. 16-11-2023] Dostupné na: <https://vsers.cz/wp-content/uploads/2023/11/Auspicia_1_2023.pdf#page=56>.
18. KAVAN, Š. (2020): *Ochrana člověka a společnosti – vývoj vzdělávání v bezpečnostních tématech*. Praha : Nakladatelství Lidových novin, 2020. 271 s. ISBN 978-80-7422-753-0.
19. KAVAN, Š. (2021): Evaluation of the Current Approach to Education of Security Issues at Selected Universities Preparing Future Pedagogues. In *Sustainability*, roč. 13, čl. 10684. ISSN 2071-1050. [online] [cit. 16-11-2023] Dostupné na: <https://doi.org/ 10.3390/su131910684>.
20. 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, 2018, s. 90-98. ISBN 978-80-8054-773-8.
21. KUCHTOVÁ, J. (2019): Digitálna stopa ako základ kybernetickej bezpečnosti. In *Aktuálne výzvy kybernetickej bezpečnosti*. Bratislava : Akadémia Policajného zboru, 2019, s. 97-101. ISBN 978-80-8054-819-3.
22. LAZER, D. M. J. a kol. (2018): The science of fake news: Addressing fake news requires a multidisciplinary effort. In *Science*, 2018, roč. 359, č. 6380, s. 1094-1096. ISSN [online]

[cit. 17-11-2023] Dostupné na internete: <https://www.science.org/doi/ 10.1126/science.aao2998>.

23. MV ČR. (2020): *Definice dezinformací a propagandy*. In *Ministerstvo vnútra Českej republiky*, 2020. [online] [cit. 16-11-2023] Dostupné na: <https://www.mvcr.cz/cthh/ clanek/definice-dezinformaci-a-propagandy.aspx>.
24. NATO. (2020): NATO's approach to countering disinformation. In *North Atlantic Treaty Organisation*, 2020. [online] [cit. 16-11-2023] Dostupné na internete: <https://www.nato.int/cps/en/natohq/177273.htm>.
25. SABAYOVÁ, M. – ČERVENÁ, K. (2023): In *Digital Economy Financial Law Review*, 2023, roč. 31, č. 3, s. 71-85. ISSN 2299-6834.
26. SABAYOVÁ, M. (2018): K otázkam „Voluntary Tax Compliance". In *Societas et Iurisprudentia*, 2018, roč. 6, č. 1, s. 173-185. ISSN 1339-5467.
27. 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.
28. SAPÍK, M. (2022): Etika v prostředí moderní společnosti. In *Auspicia*, 2022, roč. 19, č. 1, s. 104-116. ISSN 2464-7217. [online] [cit. 15-11-2023] Dostupné na internete: <https://vsers.cz/wp-content/uploads/2022/10/Auspicia_1_2022.pdf#page=104>.
29. Slovník cudzích slov. (2023): Dezinformácia. In *Slovníkový portál Jazykovedného ústavu Ľ. Štúra Slovenskej akadémie vied*, 2023. [online] [cit. 10-07-2023] Dostupné na internete: <https://sdu.sk/7yDN>.
30. Slovník pojmov z mediálnej výchovy. (2020): Dezinformácia. In *Mediálna výchova*, 2023. [online] [cit. 15-11-2023] Dostupné na: <https://medialnavychova.sk/ dezinformacia/>.
31. Slovník súčasného slovenského jazyka. (2023): Dezinformácia. In *Slovníkový portál Jazykovedného ústavu Ľ. Štúra Slovenskej akadémie vied*, 2023. [online] [cit. 15-11-2023] Dostupné na internete: <https://sdu.sk/7rY>.
32. TRIFUNOVIĆ, D. – KAZANSKÝ, R. – NEČAS. P. (2021): Conceptualization of Terrorism as a Modern Form of Political Violence. In *Politické vedy*, 2021, roč. 24, č. 2, s. 108-124. ISSN 1335-2741.
33. JURČÁK, V. – ANDRASSY, V. – STOLÁRIKOVÁ, K. (2023): Kybernetické operácie ako súčasť kybernetických hrozieb. In *Národná a medzinárodná bezpečnosť 2023 – zborník vedeckých prác*. Liptovský Mikuláš : Akadémia ozbrojených síl generála M. R. Štefánika, 2023, s. 142-150. ISBN 978-80-8040-651-6.

34. NEČAS, P. – KOLLÁR, D. (2021): Cyber Security and Information Protection on the Transnational Level. In *Security Forum 2021 – zborník vedeckých prác*. Banská Bystrica : Interpolis, 2021, roč. 14, s. 258-267. ISBN 978-80-973394-5-6.
35. KOLLÁR, D. (2019): Trendy kybernetickej bezpečnosti a jej súčasné výzvy pre spoločnosť. In *Medzinárodné vzťahy 2019: Aktuálne otázky svetovej ekonomiky a politiky*. Bratislava : Ekonomická univerzita, Fakulta medzinárodných vzťahov, 2019, roč. 20, s. 565-571. ISBN 978-80-225-4686-7.

Tento článok bol spracovaný v rámci medzinárodnej vedeckovýskumnej úlohy č.: APZ OVVP-14-2023 „Dezinformácie ako súčasť hybridných hrozieb pre demokratickú spoločnosť a ich vnímanie študentmi vysokých škôl“ (VÝSK 268).

ADDRESS & ©

doc. Ing. Radoslav IVANČÍK, PhD. et PhD., MBA, MSc.
Akadémia Policajného zboru
Sklabinská 1
817 35 Bratislava
Slovenská republika
radoslav.ivancik@akademiapz.sk
ORCID: 0000-0003-2233-1014

BEZPEČNOST • SAFETY

DOI: 10.36682/a_2024_1_3

ZDROJE INFORMÁCIÍ ALEBO DEZINFORMÁCIÍ?

Sources of Information or Disinformation?

Tatiana HAJDÚKOVÁ

Bratislava, Slovak Republic

ABSTRAKT: Internet sa stal širokospektrálnym zdrojom informácií, kvantum ktorých je také, že sa oprávnene dostávajú do pozornosti nielen otázky ich kvality a vierohodnosti, ale aj schopnosti jednotlivca vyhodnocovať obsah. Zámerné rozširovanie zavádzajúcich, skreslených až klamlivých informácií sa stáva stále viac akútnym problémom spoločnosti Dezorientácia obyvateľstva je prekážkou pri presadzovaní konštruktívnych riešení existujúcich problémov. Cieľom príspevku je vytvoriť odhad aktuálneho stavu a upozorniť na význam vplyvu internetu a sociálnych sietí na vybranú časť obyvateľstva, u ktorých sa stali dominantným mienkotvorným zdrojom informácií. Zistenia príspevku sa opierajú o dotazníkový prieskum realizovaný v roku 2023 na Akadémii Policajného zboru v Bratislave na vzorke 298 respondentov, zväčša príslušníkov policajného zboru alebo iných bezpečnostných zborov.

*Kľúčové slová**:*** informácie – dezinformácie – sociálne siete.

ABSTRACT: Nowadays, the Internet provides such a wide range of information that it is necessary to address issues of the quality and credibility of the information, as well as the ability of an individual to assess and evaluate its content. Deliberate publication of misleading, out-of-context, or outright false information is becoming an increasingly pressing problem in society. Disinformation present among the population represents an obstacle to implementing constructive solutions to existing problems. The aim of this paper is to create an estimate of the current state, to highlight the importance of the influence of the Internet and social networks on a selected sample of the population, specifically Internet users who claim that the Internet and social networks are their main source of information. The findings in this paper are based on a questionnaire survey carried out in 2023 at the Academy of the Police Force in Bratislava, on a sample of 298 respondents, mostly members of police or security forces.

*Key words***:** Information – disinformation – social networks.

ÚVOD

V rámci evolúcie sa ľudské poznávanie vyznačuje vedomým nadväzovaním na znalosti a skúsenosti z minulosti. Kumuláciu poznatkov umožňuje využívanie rôznych spôsobov ich zaznamenávania, ktoré sú odrazom technickej vyspelosť danej doby. Staré jaskynné maľby boli postupne nahradené rukopismi, mapami a obrázkami na papieri, čiarovými kódmi, či v súčasnosti preferovanými pamäťovými médiami, ktoré slúžia na efektívne elektronické ukladanie digitálnych dát. Zvýšením kapacity priestoru na archiváciu dát sú verejnosti dostupnejšie odborné vedomosti a vedecké objavy, správy o udalostiach každodenného života napr. o počasí, kultúrnych či rodinných udalostiach, o známych osobnostiach, politických rozhodnutiach a množstvo ďalších druhov informácií z diania na celom svete. Zvýšené sýtenie informáciami je umožnené nielen vyššou produkciou dát, ale aj ich lepšou dostupnosťou sprostredkovanou informačnými a komunikačnými technológiami a počítačovými sieťami.

Nie je to tak dávno, keď správy občanom v podstate monopolne poskytovali tzv. tradičné médiá zastúpené tlačou, rozhlasom a televíziou, V dobe svojej najväčšej slávy predstavovali nenahraditeľný a integrálny prvok fungovania demokracie socialistickej spoločnosti, prostredníctvom ktorých bola uskutočňovaná aj kontrola moci. Rozvíjajúce sa komunikačné technológie donútili tieto dnes už prekonané klasické média urobiť zmeny vo svojom obchodnom modeli, nakoľko ľudia už nie sú ochotní za nich platiť, svoju prevádzku sú nútení finančne zabezpečiť z reklám v nízkorozpočtovom digitálnom prostredí. Cieľom článku je poukázať na návyky občanov pri vyhľadávaní zdrojov informácií a posúdenie kvality obsahu týchto zdrojov na základe výskytu dezinformácií. Nakoľko manipulácia s verejnou mienkou sa stáva stále viac naliehavým spoločenským problémom, je nevyhnutné spoznávať aktuálny stav a monitorovať potenciálne hrozby priebežne od prvých náznakov, aby nápravné opatrenia prichádzali včas a s dostatočnou silou vo fáze prevencie a nie represie.

INFORMÁCIE A ICH VPLYV NA JEDNOTLIVCA

Pojem informácia pochádza z latinského slova „informo“ čo v preklade znamená prenášanie správ, oznámenie, ale aj znázornenie, opísanie niečoho. Švarcová (2011, s. 20) definuje informáciu ako *„poznatok o určitej skutočnosti, predmetu alebo javu zachytenom v zrozumiteľnej forme, využiteľný pri prispôsobovaní sa človeka životnému prostrediu“*.

Jedným z významných atribútov demokratickej spoločnosti je slobodný prístup k informáciám, ktorý podporuje spoločenskú a individuálnu informovanosť. Podľa Zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov, *„informácia je obsah písomnosti, nákresu, výkresu, mapy, fotografie, grafu alebo iného*

záznamu, alebo obsah ústneho vyjadrenia, alebo obsah elektrického, elektromagnetického, elektronického alebo iného fyzikálneho transportného média". Najviac žiadané zvyknú byť informácie z prítomnosti, ktoré zachytávajú realistickú etapu. Už dávnejšie bolo skonštatované, že jednotlivec si nedokáže osvojiť všetky ani väčšinu existujúcich vedomostí. Dokonca nedokážeme spracovať ani všetky informácie, ktorým sme v modernom svete vystavení aj bez ich aktívneho vyhľadávania konkrétnych záujmových informácií. Hlad po informáciách spôsobuje aj skutočnosť, že neznalosť prináša konflikty, aroganciu a odsudzovanie.

Dôležitými atribútmi informácie sú jej význam a interpretácia pre príjemcu, ako aj jej vplyv na prijímateľa (Kuchtová. 2021). Aby človek dokázal pochopiť informáciu, musí byť schopný zachytiť podnet z okolia, zaznamenať ho v mozgu, subjektívne spracovať a prípadne následne poskytnúť reakciu do okolia. Každý príjemca informácie vníma zachytený impulz z okolia na základe iných kritérií a znalostí. V mysliach sa v konečnom dôsledku značne odlišujú. Jedna informácia obvykle vyvoláva spektrum reakcií od nezúčastnenej a ľahostajnej, až po prudko emotívnu alebo iracionálnu. Na využitie informácie je nevyhnutné zvnútornenie je obsahu, lebo ináč by zostala len ako nepochopený podnet z okolia bez odozvy. Ako uvádza (Povrazník, 2007, s. 42) *„informácie sú také oznámenia, ktoré príjemca vie interpretovať, považuje ich za pravdivé a kompletné v potrebnej miere a je kompetentný v konkrétnom čase a priestore ich využiť"*.

Predovšetkým zdroje dát, ktoré pochádzajú z overených a dôveryhodných zdrojov s definovanými kontrolnými mechanizmami, ktoré zodpovedajú za obsah, je možné považovať a to len do istej miery objektívnu pravdu. So stúpajúcou dostupnosťou informácií narastá potreba zameriavať sa na prostriedky a efektívne postupy hľadania relevantných informácií (Kaščák, 2019). V súčasnosti je šírenie informácií predovšetkým na internete, sociálnych sieťach či blogoch natoľko masívne a rýchle, že ich nadmernosť sťažuje reálne posúdenie ich pravdivosti širokou verejnosťou.

DEZINFORMÁCIE

Informačnú dezorientáciu a pochybnosti u obyvateľstva vyvolávajú rôzne dezinformácie, polopravdy, konšpirácie, hoaxy, alternatívne fakty. Vzájomne protirečiace si informácie obvykle vyvolávajú napätie, nedôveru a pochybnosti u jednotlivcov, v dôsledku ktorých môže dochádzať ku polarizácii významnej časti spoločnosti (Lisoň – Fidler, 2022; Grant 2019). Pre účely článku problematiku pôsobenia škodlivých informácií zúžime na dezinformácie. Rovnako ako pri mnohých iných pojmoch, ani pri dezinformáciách nedošlo ku zjednoteniu ich definície. Ako uvádza Ivančík (2021a, s. 166), *„napriek väčšej či menšej*

odlišnosti definícií dezinformácií, spoločným rysom všetkých je fakt, že ide o úmyselnú modifikáciu poskytovaných informácií so zámerom ovplyvniť, oklamať či uviesť adresátov týchto informácií do omylu. Účelmi zámerného rozširovania dezinformácií môže byť vyvolanie negatívnych akcií, manipulácia s obrazom verejnej mienky, spochybnenie súpera". Menší rádius vplyvu na zavádzanie verejnosti má misinformácia. Ivančík (2021b, s. 20) ju označuje ako *„nesprávnu alebo zavádzajúca informáciu, ktorá nie je šírená ani systematicky, ani úmyselne, ani s cieľom ovplyvniť rozhodovanie alebo názory tých, ktorí ju prijímajú"*.

Vzhľadom na neprimeraný výskyt škodlivého obsahu vo verejne dostupných zdrojoch sa stále viac nedostatkovým javí zrozumiteľné vysvetlenie a objektívne zasadenie skutočností do kontextu. Dezorientácia obyvateľstva je prekážkou pri presadzovaní konštruktívnych riešení prítomných problémov.

Vyhodnotenie prijatých informácií je medzi ľuďmi výrazne variabilné, a to aj vzhľadom na individuálne schopnosti a skúsenosti. Z hľadiska vnútornej bezpečnosti štátu môžeme ako tzv. nízko rizikové považovať marketingovo orientované informácie. Ich zámerom je ovplyvňovať predovšetkým spotrebu obyvateľstva na základe zbierania informácií o návykoch, záujmoch a potrebách. Rozvoj a dosah masovokomunikačných prostriedkov výrazným spôsobom ovplyvňuje mnohé a zásadné procesy v spoločnosti. Ako uvádzajú viacerí autori (Lisoň – Hullová, 2020; Ivančík, R., 2021a; Hudecová, 2022), negatívnym dopadom masovokomunikačných prostriedkov je rozširovanie rôznych nepravdivých a zavádzajúcich informácií s cieľom dezinformovať verejnosť. Tvorcovia dezinformácií sú si vedomí, že dopad je účinnejší v prostredí, kde sa nachádzajú aj čitatelia, preto zdroje dezinformácií sa bytostne viažu ku zdrojom informácií.

INTERNET AKO ZDROJ INFORMÁCIÍ

Sociálny rozmer rozvoja komunikácie s využitím informačno-komunikačných technológií preukázal, že existujú nástroje na efektívnejšiu, prehľadnejšiu a rýchlejšiu interakciu a spoluprácu medzi občanmi, inštitúciami a súkromnými spoločnosťami. Pre mnohých občanov sa online priestor stal hlavným zdrojom informácií a spôsobom zapojenia sa do procesu rozhodovania a uplatňovania politík verejnej správy. Globálne silnie tlak verejnosti na transparentnosť politiky, vlády, štátnej a verejnej správy, a poskytovanie prístupu k informáciám prostredníctvom otvorených údajov. Prístup k otvoreným údajom znamená, že informácie alebo údaje sú pre každého dostupné za rovnakých podmienok, bezplatne a na akýkoľvek účel. Kľúčovou myšlienkou otvorených údajov je proaktívne sprístupnenie týchto údajov a podpora ich zmysluplného využívania na ďalšie účely.

Verejné prezentovanie názorov a postojov jednotlivcov nikdy nebolo dostupnejšie ako v prostredí internetu a to hlavne v dôsledku vysokého počtu jeho používateľov. S príchodom internetu sa online médiá stali najrozšírenejším zdrojom informácií. Internet sa v tomto ohľade stal bezkonkurenčným širokospektrálnym zdrojom informácií, kvantum ktorých je také, že sa oprávnene dostávajú do pozornosti nielen otázky ich kvality a vierohodnosti, ale aj schopnosti jednotlivca vyhodnocovať obsah (Ivančík – Nečas, 2022). Z tohto uhla pohľadu Burkhard (2017, s. 11) označuje internet za skutočne demokratický a čestný spôsob zdieľania informácií, pretože svojím spôsobom obmedzuje silu držiteľov informačnej moci, napr. mediálnych magnátov, pričom kontrola obsahu dostupného prostredníctvom internetu je síce zložitá, ale nie je nemožná. S názorom možno súhlasiť pri presadení neúplatnosti a nekomerčnosti na internete, alebo vytvorení priestoru pre slobodné a verejné vyjadrenie sa tých, ktorých nie je počuť. Polemizovať možno pri odporovaní si dvoch základných tvrdení vyjadrenia. Demokratické zdieľanie informácií je v protiklade s kontrolou dostupného obsahu. Aplikačný problém kontroly obsahu spočíva nielen v definovaní, aký obsah by nemal byť zverejňovaný tak, aby zostala zachovaná Ústavou garantovaná sloboda slova a slobodný prístup k informáciám, ale aj určenie subjektu, ktorý by mal rozhodovať o vhodnosti obsahu a podľa akých kritérií.

METODIKA A CIEĽ

Cieľom článku je meraním kvantifikovať výber zdrojov na získavanie informácií u špecifickej skupiny obyvateľov Slovenskej republiky pre bežný každodenný život. Ako výskumná metóda bol zvolený dotazníkový prieskum, v ktorom nebol sledovaný dôvod získavania informácií, ani nebolo rozlišované, či ide o pracovné, služobné alebo súkromné účely. Oslovení na participáciu na výskume boli prevažne interní a externí študenti Akadémie Policajného zboru v Bratislave alebo účastníci vzdelávacích kurzov realizovaných na Akadémii Policajného zboru v Bratislave. Z uvedeného vyplýva, že išlo o príslušníkov Policajného zboru, zamestnancov štátnej alebo verejnej správy, ale okrajovo aj zo súkromného sektora. Elektronický dotazníkový prieskum bol realizovaný v druhej polovici roku 2023, zapojilo sa do neho a valídne odpovedalo 298 respondentov. Nakoľko v predmetnom príspevku nás zaujíma výlučne voľba používaných zdrojov informácií respondentov v kontraste so skúsenosťami so zdrojmi dezinformácií vo všeobecnosti, socio-demografické charakteristiky respondentov neuvádzame, ako ani reakcie na ostatné otázky prieskumu. Znenie analyzovaných otázok bolo:

1. Odkiaľ najčastejšie čerpáte informácie? (možnosť až troch odpovedí)[6]

[6] Alternatívy odpovedí na prvú otázku: internet, knihy (vedecké, odborné, učebnice), odborníci, vedci, televízia, tlač (noviny, časopisy), rozhlas, sociálne siete, rodina, priatelia, známi.

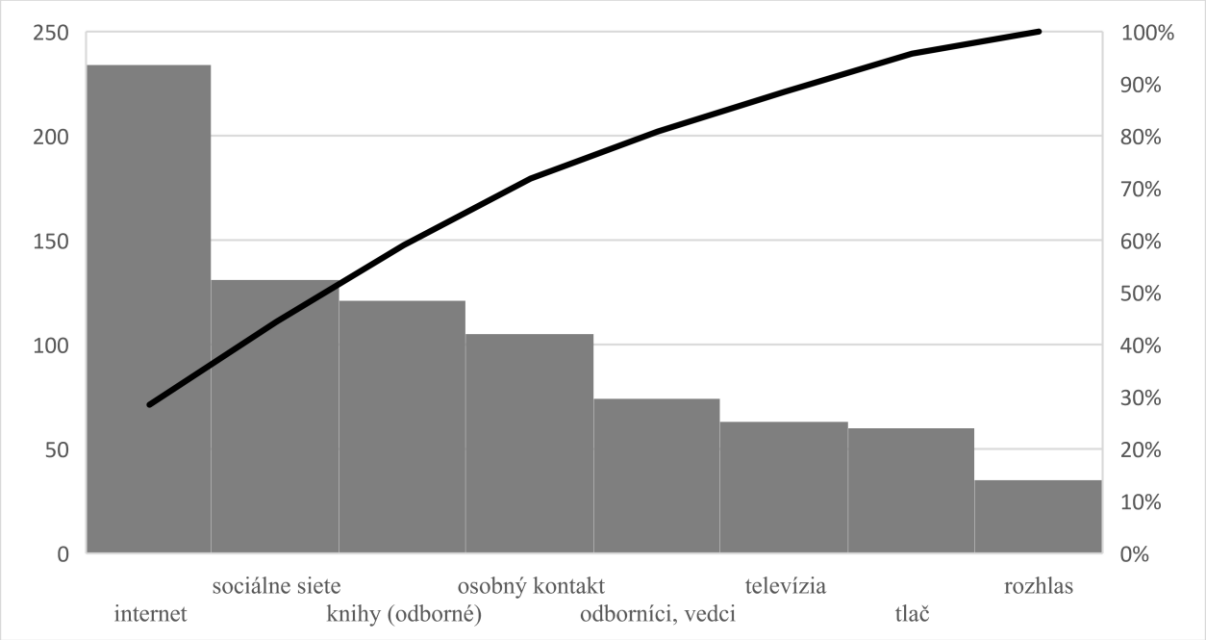
2. Kde ste sa stretli, resp. stretávate sa s dezinformáciami? (možnosť až troch odpovedí)[7]

Na vyhodnotenie výsledkov bola použitá komparácia, frekvenčná analýza a korelačná analýza vykonané pomocou softvérov MS Excel a SPSS 27.

VÝSLEDKY A DISKUSIA

V prvom priblížení sme sa zaujímali o kumulovaný názor všetkých zapojených respondentov aký zdroj si najčastejšie vyberajú na čerpanie informácií, zobrazené na grafe č. 1.

Graf 1: Paretov graf rozloženie odpovedí na najčastejší zdroj pre čerpanie informácií



Zdroj: Vlastné spracovanie z dát VVU Dezinformácie ako súčasť hybridných hrozieb pre demokratickú spoločnosť a ich vnímanie študentmi vysokých škôl.

Na vodorovnej osi grafu č. 1 sú rozlišované zdroje informácií, na zvislej početnosti ich odpovedí. Zobrazenie je vytvorené Paretovým grafom, t. j. sledované média sa usporiadané zľava doprava zostupne podľa frekvencie využívania respondentami. Vedľajšia os vpravo znázorňuje relatívne percentá z celkových získaných odpovedí[8] a čierna lomená krivka postupne kumulatívne percentá z informačných zdrojov.

[7] Alternatívy odpovedí na druhú otázku bola s mierne pozmenenou formuláciou a vynechaná možnosť odborníci, vedci: na internete, v televízii, na sociálnych sieťach, v osobnom styku (od rodiny, priateľov, známych, ...), v knihách (bez ohľadu na typ / druh knihy), v tlači (v novinách, časopisoch), v rozhlase.

[8] V inštrukcii otázky bola možnosť vyberať viacero odpovedí na danú otázku a väčšina respondentov označovala tri média ako svoj zdroj informácií. Na grafe je zobrazený relatívny podiel odpovedí na jednotlivé média zo všetkých obdržaných odpovedí.

Medzi všetkými respondentami vzniklo relatívne percentuálne zastúpenie jednotlivých médií nasledovne (tabuľka č. 1).

Tabuľka 1: Relatívne zastúpenie výberu médií, ako zdroja informácií pri jednotlivých osobách

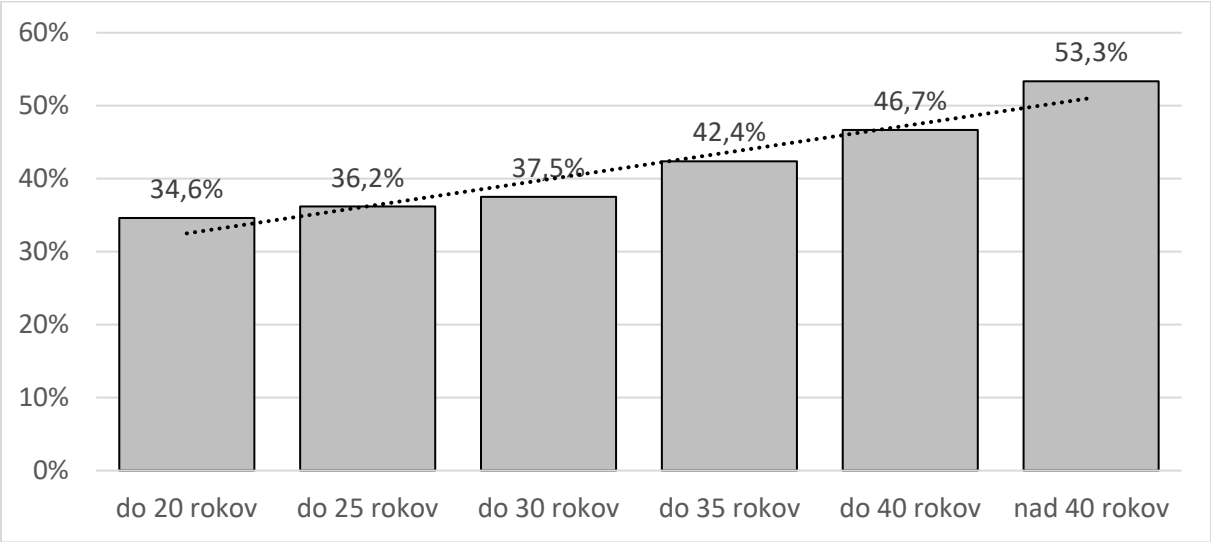
Médium	Podiel	Médium	Podiel
internet	78,1 %	odborníci, vedci	24,6 %
sociálne siete	43,6 %	televízia	21,1 %
knihy (vedecké, odborné, učebnice)	40,4 %	tlač (noviny, časopisy)	20,1 %
rodina, priatelia, známi	35,2 %	rozhlas	11,7 %

Zdroj: Vlastné spracovanie z dát VVU Dezinformácie ako súčasť hybridných hrozieb pre demokratickú spoločnosť a ich vnímanie študentmi vysokých škôl.

Z výsledkov rezonuje zdôraznenie významu internetu, ktorý je dominantným zdrojom informácií aj pre študentov, od ktorých by sa dalo očakávať intenzívnejšie využívanie napr. odbornej, vedeckej literatúry a učebníc, ako pri bežnej populácii. Vo vzťahu ku využívaniu informačných zdrojov z odborných a vedeckých kníh je povšimnutia hodná zreteľná kladná asociácia s vekom pri dospelých osobách vo veku do cca päťdesiat rokov, zobrazené v relatívnej mierke na grafe č 2. Vzťah veku osôb a využívanie vedeckých a odborných kníh týmito osobami ako zdroj informácií veľmi dobre modeluje lineárna závislosť, viditeľné na priamke preloženej nameranými hodnotami s rovnicou:

$$y = 0{,}0371x + 0{,}2879$$

Graf 2: Podiel vedeckých a odborných kníh na zdrojoch informácií podľa veku respondentov



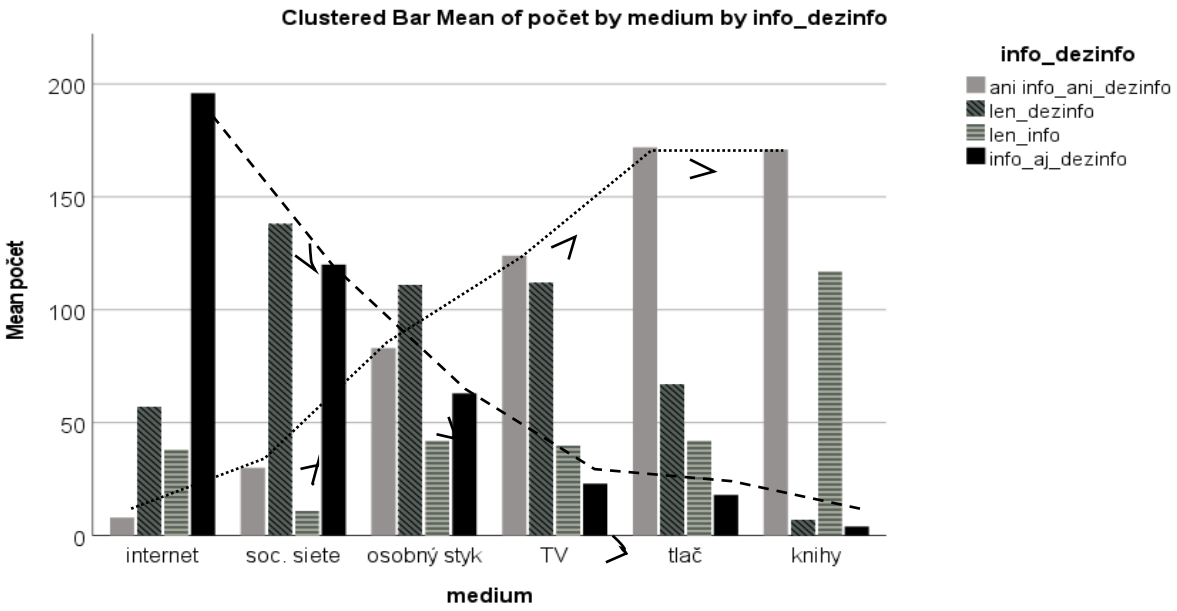
Zdroj: Vlastné spracovanie z dát VVU Dezinformácie ako súčasť hybridných hrozieb pre demokratickú spoločnosť a ich vnímanie študentmi vysokých škôl.

Hoci malý, ale kladný koeficient pre premennej *x* poukazuje v rámci sledovaného vekového intervalu medzi 20 až cca 50 rokov na nárast využívania odbornej a vedeckej literatúry s vekom, resp. jeho nepriaznivé klesanie u mladých ľudí. Koeficient spoľahlivosti takto vytvoreného modelu je vysoký, 93,2 %. Výsledok nie je možné vnímať ako pozitívny, pretože vedecké a odborné časopisy predstavujú nezastupiteľný informačný kanál nielen vo vedeckej komunikácii. Ich spoločenská, vedecká a odborná hodnota sa odráža v aplikovaní poznatkov z týchto zdrojov nielen v ďalšom vedeckom bádaní a napredovaní, ale aj v bežnom živote čitateľov. Zastúpenie vedeckých a odborných časopisov na internete neustále narastá, ale v menšej miere, ako neželaný škodlivý obsah. Rozhodne je v záujme spoločnosti proaktívne vytvárať podmienky pre popularizáciu vedeckých a odborných informácií.

Následne sme pokračovali sledovaním odpovedí jednotlivých respondentov na kombináciu dvoch otázok, a to aké zdroje informácií používajú najčastejšie a kde sa stretli, resp. stretávajú s dezinformáciami najčastejšie. Zistenia sú prezentované skupinovým stĺpcovým grafom č. 3. Na zvislej osi sú zobrazované početnosti jednotlivých skupín odpovedí respondentov. Sledované zdroje informácií/dezinformácií sú zobrazené na vodorovnej osi, pritom každé médium je popísané pomocou štyroch skupín možných vyjadrení respondentov. Každý respondent je uvedený pri každom médiu práve raz a to vždy v jednej zo skupín:

- Dané médium nebolo označené pri žiadnej odpovedi, to znamená, že ho respondent nevyužíva ako zdroj svojich informácií, a teda ani nemá osobné skúsenosti s dezinformáciami v ňom sa nachádzajúcimi (v skupine ľavý stĺpec so sivou výplňou).

Graf 3: Rozloženie odpovedí na používanie zdrojov informácií verzus skúsenosti s dezinformáciami v danom médiu



Zdroj: Vlastné spracovanie z dát VVU Dezinformácie ako súčasť hybridných hrozieb pre demokratickú spoločnosť a ich vnímanie študentmi vysokých škôl.

- Druhý stĺpec v skupine zľava so šikmou vzorkou znázorňuje médium považované len za zdroj dezinformácií, t. j. respondent ho nepoužíva ako svoj zdroj informácií a tak jeho presvedčenie, že sa v médiu nachádzajú dezinformácie je pozostatok z minulosti alebo je sprostredkované z iného zdroja.
- Tretí stĺpec v skupine zľava s vodorovnou vzorkou znázorňuje médium využívané ako zdroj informácií, na ktorom sa respondent nestretol s dezinformáciami.
- Štvrtý stĺpec v skupine zľava s čiernou výplňou zobrazuje médium označené ako zdroj informácií v jednej otázke a opäť označené ako zdroj dezinformácií v druhej otázke.

Média na grafe č. 3 sú usporiadané zľava doprava zostupne podľa celkovo najpočetnejšej kategórie, ktorou je médium vnímané ako zdroj informácií aj dezinformácií súčasne, t. j. internet (prvé médium zľava), pri ktorom si respondenti uvedomujú, že je silný zdroj informácií, a preto ho používajú, avšak je nutné selektovanie aj dezinformácií.

Na sociálnych sieťach a pri osobnom styku s rodinou, známymi či priateľmi sa ako najčastejší názor vyprofilovali negatívne skúsenosti s vnímaním ako častým zdrojom

dezinformácií. Uvedený postoj je znepokojivý hlavne pri osobnom styku, ktorý ešte v nedávnej minulosti tvoril základ pre vnímanie a zmýšľanie diania v okolí a budovanie názorovej orientácie mladého človeka. Pri osobnom styku sú skúsenosti zastúpené pri všetkých postojoch ku zdrojom informácií aj dezinformácií spomedzi sledovaných médií najrovnomernejšie. Podobne negatívne skúsenosti so šírením dezinformácií ako na sociálnych sieťach a pri osobnom styku sa prejavil aj pri televízii, ktorá však oproti predchádzajúcim dvom má ako poskytovateľ informácií vo všeobecnosti nižšiu sledovanosť. Nevýhodou týchto médií je skutočnosť, že ich označujú za zdroje dezinformácií osoby, ktoré ich nepoužívajú za svoje informačné zdroje, a teda ich názor bol vytvorený viac menej sprostredkovane.

Pri posledných troch médiách na grafe č. 3 vpravo, t. j. odborná literatúra televízia tlač (noviny a časopisy) a knihy (vedecké a odborné knihy, učebnice) dominuje stĺpec so sivou výplňou, ktorý vo všeobecnosti poukazuje na nízky záujem o tieto média ako o informačný zdroj. Pretože tieto média obvykle nie sú využívané ako zdroj informácií, prirodzene je u týchto jednotlivcov vytváraný chudobný priestor na konfrontovanie dezinformácií s odborným stanoviskom. Nezáujem o tlač a knihy ako o zdroje akýchkoľvek informácií bol podľa respondentov porovnateľne najmenší. Podstatný rozdiel medzi tlačou a knihami videli respondenti v častejšom výskyte dezinformácií v tlači (cca 70 respondentov), kým pri knihách to boli skutočne ojedinelé vyjadrenia. Povšimnutia hodné je, že knihy boli v porovnaní so všetkými ostatnými sledovanými médiami s výraznou prevahou posúdené ako najčastejší zdroj informácií ako takých, a teda výskyt dezinformácií v knihách je výnimočný.

Poradie médií na vodorovnej osi je súčasne aj vzostupným usporiadaním z pohľadu nevyužívania daného média ako informačného zdroja a teda aj dezinformačného zdroja (bodkovaná krivka). Vizuálny odhad sme potvrdili pomocou Pearsonovho korelačného koeficientu spočítaný z odpovedí respondentov z prvej a štvrtej kategórie.

Tabuľka 2: Pearsonov koeficient korelácie medzi médiami, ktoré sú zdrojom informácií / dezinformácií a frekvenciou ich využívania

Correlations

		počet	info_dezinfo
počet	Pearson Correlation	1	-,203
	Sig. (2-tailed)		,527
	N	12	12
info_dezinfo	Pearson Correlation	-,203	1
	Sig. (2-tailed)		
	N	12	12

Výsledok potvrdil slabú zápornú koreláciu, ktorá indikuje nepriamu závislosť a teda médium častejšie využívané ako zdroj informácií vrátane dezinformácii je v opozite s médiami, ktorým respondenti nevenujú pozornosť a nesledujú ich obsah, hoci sa v nich nachádzajú hodnotné informácie bez zavádzajúceho obsahu.

ZÁVER

Vzhľadom na prebiehajúce štúdium oslovených osôb alebo účasť respondentov na kurze celoživotného vzdelávania príslušníkov Policajného zboru na Akadémii Policajného zboru v Bratislave, všetci participujúci mali ukončené stredoškolské vzdelanie s maturitou a absolvovanú istú časť alebo ukončené vysokoškolské vzdelanie. Ďalším špecifikom zapojených respondentov vzhľadom na bežnú populáciu bola ich profilácia na bezpečnostno-právne služby. Uvedené skutočnosti predikujú väčšiu senzitivitu respondentov na riziká v spojitosti bezpečnosťou, uvedomením si dôležitosti informácií, dôsledky rozhodovania na základe nesprávnych, nedostatočných alebo neúplných informácií. V neposlednom rade obozretnejšími ich robia aj skúsenosti s prácou s občanmi, ktorí nie vždy konajú zodpovedne a v medziach zákona. Vzhľadom na uvedené je možné očakávať, že výsledky prieskumu na bežnej populácii by mohli viac inklinovať k využívaniu internetu, ako pri oslovenej vzorke.

Informácie tvoria základ pre rozhodovacie procesy. Zistenia prieskumu naznačujú jednostrannosť využívania zdrojov informácií obmedzených na internet obzvlášť u mladých ľudí. Pokles záujmu o čítanie beletrie je nezvrátiteľný fakt posledných rokov. Najmä pri detskej populácii chýba prirodzený návyk, podobne ako pri súčasných mladých ľuďoch, ktorí už vyrastali spolu s internetom. Internet ako všade a vždy prítomný, sa v dnešnej spoločnosti stal prakticky neobíditeľný. Dezinformácie v obsahu média neodrádzajú jeho používateľov od sledovania obsahu. Na oslovenej vzorke špecifických respondentov sa stal výsledok prieskumu jednoznačný. Ľudia preferujú internet ako informačný zdroj s vedomím, že sa v ňom nevyhnú dezinformáciám. Úloha spoločnosti do budúcnosti je pomerne jednoznačná a naliehavá, hoci nie ľahko dosiahnuteľná. Nevyhnutné je zlepšiť kontrolu a reguláciu obsahu na internete, účinnejšie a rýchlejšie odstraňovať škodlivý obsah a vytvoriť účinné mechanizmy na udeľovanie sankcií, ktoré by mali nielen nápravný, ale hlavne preventívny účinok.

POUŽITÁ LITERATÚRA A INFORMAČNÉ ZDROJE:

1. KALINSKÝ, V. (2018b): Ako eliminovať dezinformácie? In *Aktuálne problémy vo sfére bezpečnosti – zborník z medzinárodnej vedeckej konferencie*. České Budějovice : Vysoká škola evropských a regionálních studií, 2018, s. 91-101. ISBN 978-80-5020-676-1.
2. BUENTING, J. – TAYLOR, J. (2010): Conspiracy Theories and Fortuitous Data. In Philosophy of the Social Sciences, 2010, roč. 40, č. 4, 567-578. [online] [cit. 20-12-2023] Dostupné na internete: <https://journals.sagepub.com/doi/pdf /10.1177/0048393109350750>.
3. FLYNN, D. J. – NYHAN, B. – REIFLER, J. (2017): The Nature and Origins of Misperceptions: Understanding False and Unsupported Beliefs About Politics. In *Advances in Political Psychology*, 2017, roč. 38, č. 1, s. 127-150. ISSN 1479-0661.
4. GALLIFORD, N. – FURNHAM, A. (2017): Individual difference factors and beliefs in medical and political conspiracy theories. In *Scandinavian Journal of Psychology*, 2017, roč. 58, č. 5, s. 422-428. ISSN 1467-9450. [online] [cit. 20-12-2023] Dostupné na internete: <https://onlinelibrary.wiley.com/doi/abs/10.1111/sjop.12382>.
5. GRANT, M. L. (2019): Updating security and defence policy. In *National Institute Economic Review*, 2019, roč. 250, č. 1, s. 40-46. ISSN 1741-3036. Dostupné na internete: <http://doi.org/10.1177/002795011925000116>.
6. HUDECOVÁ, V. (2022): Crisis development and its management. In *Entrepreneurship and Sustainability Issues*, 2022, roč. 9, č. 3, s. 414-428. ISSN 2345-0282.
7. IVANČÍK, R. (2021): Základné teoretické a terminologické východiská skúmania problematiky dezinformácií. In *Národná a medzinárodná bezpečnosť 2021 – zborník vedeckých príspevkov z 12. medzinárodnej vedeckej konferencie*. Liptovský Mikuláš : Akadémia ozbrojených síl generála M. R. Štefánika, 2021, s. 165-172. ISBN 978-80-8040-606-6.
8. IVANČÍK, R. (2021): Dezinformácie ako bezpečnostná hrozba pre demokratickú spoločnosť. In *Právo a bezpečnost*, 2021, roč. 15, č. 3, s. 16-33. ISSN 2336-5323.
9. IVANČÍK, R. – NEČAS, P. (2022): On disinformation as a hybrid threat spread through social networks. In *Entrepreneurship and Sustainability Issues*, 2022, roč. 10, č. 1, s. 344-357. ISSN 2345-0282. Dostupné na internete: <http://doi.org/10.9770/jesi.2022.10.1(18)>.
10. JENČO M. – VYHNAL P. (2012): Informácie a informačné systémy. Poprad : 2008. 254 s. ISBN 978-80-88680-44-4.
11. KAŠČÁK, M. (2019): Medzinárodná policajná spolupráca v európskom priestore na príklade Stredoeurópskej policajnej akadémie. In *Aktuálne problémy rezonujúce Európou*

(Právno-bezpečnostné aspekty) – zborník príspevkov z medzinárodnej vedeckej konferencie. Bratislava : Akadémia Policajného zboru, 2019, s. 171-178. ISBN 978-80-8054-826-1.

12. KUCHTOVÁ, J. (2021): Vybrané informačné a komunikačné technológie využívané počas pandémie Covid-19. In *Policajná teória a prax*, roč. 29, č. 1, s. 5-22. ISSN 1335-1370.
13. LEVY, R. (2020): Social media, news consumption, and polarization: evidence from a field experiment. In *American Economic Review*, 2020, roč. 111, s. 831–870. ISSN 0002-8282.
14. LISOŇ, M. – FIDLER, Ľ. (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.
15. LISOŇ, M. – HULLOVÁ, M. (2020): Klasifikácia kriminality. In Policajná teória a prax. ISSN 1335-1370, 2020, roč. 28, č. 1, s. 59-79. ISSN 1335-1370.
16. POVRAZNÍK, J. a kol. (2007): *Celostný manažment*. Žilina : Poradca podnikateľa. 2007. 540 s. ISBN 978-80-88931-73-7.
17. ŠVARCOVÁ, I. – RAIN, T. (2011): *Informační management*. Praha : Alfa. 2011. 183 s. ISBN 978-80-87197-40-0.
18. Zákon č. 215/2004 Z. z o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov.

ADDRESS & ©

doc. RNDr. Tatiana HAJDÚKOVÁ, PhD.
Akadémia Policajného zboru
Sklabinská 1, 817 35 Bratislava
Slovenská republika
tatiana.hajdukova@akademiapz.sk
ORCID: 0000-0002-2313-4568

BEZPEČNOST • SAFETY

DOI: 10.36682/a_2024_1_4

DEZINFORMÁCIE AKO HROZBA PRE SPOLOČNOSŤ A SNAHY O ICH ELIMINÁCIU

Disinformation as a threat to society and efforts to eliminate them

Magda RUŽBACKÁ

Bratislava, Slovak Republic

ABSTRAKT: S rozvojom širokej škály moderných technológií, rýchlym rozšírením a širokou dostupnosťou internetu, ako aj rozsiahlym využívaním rôznych informačných a komunikačných nástrojov a zariadení sa objavila pred ľuďmi nová paleta možností, akými sú vyhľadávanie, spracovanie a šírenie informácií. Zároveň sa však objavila nová paleta možností šírenia falošných, zavádzajúcich, klamlivých a nepravdivých informácií – dezinformácií – zo strany štátnych aj neštátnych aktérov s cieľom ovplyvniť fungovanie demokratickej spoločnosti a konanie ľudí. Šírenie dezinformácií tak dnes predstavuje mimoriadne nebezpečnú hrozbu, ktorá môže mať veľmi nepriaznivé dôsledky pre jednotlivcov, organizácie i celú spoločnosť. Z uvedeného dôvodu sa autorka v článku, v rámci realizovaného bezpečnostného výskumu, zaoberá problematikou dezinformácií, poukazuje na nebezpečenstvo ich šírenia, vymedzuje pojem dezinformácie a súčasne sa zaoberá možnosťami eliminácie dôsledkov šírenia dezinformácií.

Kľúčové slová: Dezinformácie – hrozba – demokratická spoločnosť – moderné technológie.

ABSTRACT: With the development of a wide range of modern technologies, the rapid spread and wide availability of the Internet, as well as the extensive use of various information and communication tools and devices, a new range of possibilities have emerged for people, such as information retrieval, processing, and dissemination. However, at the same time, a new range of opportunities has emerged for the spread of misleading, deceptive and false information – disinformation –spread by state and non-state actors with the aim of influencing the functioning of democratic society and people's behaviour. The spread of disinformation thus currently represents an extremely dangerous threat that can have very negative consequences for individuals, organisations, and the entire society. For this reason, as part of the conducted security research, the author of this paper, deals with the issue of disinformation, points out the danger of its spread, defines the concept of disinformation and at the same time, discusses the possibilities of eliminating the consequences of the spread of disinformation.

Key words: Disinformation – threat – democratic society – modern technology.

ÚVOD

Dosiahnutý výrazný pokrok v oblasti informačných a komunikačných technológií, systémov a prostriedkov umožnil v prvých dvoch desaťročiach tretieho tisícročia miliónom ľudí na celom svete prístup k nespočetnému množstvu informácií (Nečas, Ivančík, 2019), z ktorých ale mnohé sú klamlivé, zavádzajúce, skreslené, úmyselne pozmenené alebo nepravdivé (Gregor a kol., 2018; Ivančík, 2022). S rôznymi takýmito informáciami, resp. dezinformáciami sa nanešťastie v súčasnosti stretávame oveľa častejšie ako v minulosti, v podstate takmer denne, či už ide o rôzne vyššie zmienené klamlivé, zavádzajúce, pozmenené, úplne vymyslené alebo z kontextu vytrhnuté informácie, upravené fotografie alebo videá, články alebo „zaručene pravdivé“ správy preposielané prostredníctvom internetu v reťazových e-mailoch alebo šíriace sa cestou platforiem rôznych sociálnych sietí (Ivančík, 2023, s. 45). Žiaľ, šírenie dezinformácií – ako súčasti šírenia hybridných hrozieb – štátnymi aj neštátnymi aktérmi za účelom získania určitého politického, ideologického alebo ekonomického profitu je v dnešnej dobe veľmi častým javom, ktorý negatívne ovplyvňuje bezpečnosť krajín (Jurčák a kol., 2016; Kollár, 2022; Ivančík, 2022, s. 56).

Výskyt najrôznejších dezinformačných kampaní, ako jedného z prostriedkov vedenia tzv. hybridnej vojny, sa v posledných rokoch neustále zvyšuje (Jurčák, Turac, 2018; Kollár, 2022; Ivančík, 2022, 2023). Hoci dezinformácie nie sú novým javom v spoločnosti, ich význam z hľadiska bezpečnosti štátu sa zvýšil najmä v súvislosti s dynamickým vývojom moderných technológií a novších a efektívnejších techník ich šírenia. Hlavne zahraniční štátni aj neštátni aktéri čoraz viac využívajú dezinformačné stratégie na to, aby mohli ovplyvňovať verejné diskusie, spochybňovať demokratické pravidlá, zásady a princípy, podporovať polarizáciu spoločnosti, podnecovať chaos, vzbudzovať v ľuďoch neistotu, strach a zasahovať do demokratického rozhodovania v demokratických krajinách Európy i sveta (Ivančík, 2020). Pre bezpečnosť štátov sú hrozbou predovšetkým preto, že šírenie dezinformácií oslabuje dôveru občanov v demokratické inštitúcie a demokratické procesy prebiehajúce v demokratických spoločnostiach, čo môže v extrémnych prípadoch viesť až k prevratu a následnej zmene režimu – z demokratického na autokratický. Úlohou, resp. povinnosťou demokratických štátov a ich kompetentných zložiek (ozbrojených síl, ozbrojených bezpečnostných zborov, spravodajských služieb a ďalších úradov a inštitúcií) je v rámci zaisťovania ich bezpečnosti a obrany bojovať s dezinformačnými kampaňami jednak na národnej úrovni a jednak na medzinárodnej úrovni (Ivančík, Nečas, 2020).

METODIKA A CIEĽ

Hlavným cieľom článku, ktorý sa zaoberá problematikou dezinformácií, je skúmať dezinformácie ako hrozbu pre demokratickú spoločnosť, poukázať na nebezpečenstvo ich šírenia v rámci šírenia hybridných hrozieb, resp. vedenia hybridnej vojny, vymedziť pojem dezinformácie a súčasne zamerať pozornosť na potrebu a možnosti eliminácie negatívnych dôsledkov šírenia dezinformácií. Zistenia uvádzané v článku vychádzajú z realizovaného bezpečnostného výskumu zameraného na problematiku dezinformácií. Pri spracovaní článku boli použité základné vedecké metódy a postupy, vhodné pre riešenie skúmanej problematiky. Využité boli viaceré druhy analýzy (najmä obsahová, sémantická a teoretická analýza), syntéza, komparácia, dedukcia a indukcia, a taktiež vedecké metódy štúdia dokumentov a teoretického zovšeobecňovania získaných poznatkov. Pokiaľ ide o literatúru a zdroje, tak autorka pri spracovaní článku využila predovšetkým vedecké články a príspevky z medzinárodných vedeckých konferencií autorov, ktorý sa skúmanou problematikou zaoberajú vo svojej výskumnej činnosti.

VÝSLEDKY A DISKUSIA

Pojem dezinformácie je najmä v posledných rokoch často používaný, ale zatiaľ nebol presne a jednotne vymedzený (Ivančík, 2022; Ivančík, Müllerová, 2022; Kollár, 2022). Často sa používa v súvislosti s ďalšími výrazmi s podobným významom, preto je vhodné odlíšiť tento termín od tých, s ktorými sa často prekrýva. Ide najmä o falošné správy, hoaxy a propagandu.

Falošné správy sú informácie, ktoré zámerne napodobňujú formát spravodajstva alebo iného produktu žurnalistiky, pričom ich tvorcovia úmyselne alebo neúmyselne zavádzajú svoje publikum skresľovaním reality (Národný bezpečnostný úrad, 2023).

Hoax je podvod, žart, virálne rozšírená poplašná správa. Zväčša má tri typické znaky: naliehavosť, odkaz na iluzórnu autoritu (policajný zdroj, neexistujúce vedecké výsledky) a žiadosť o šírenie ďalej. Môže však aj ísť napríklad o falošné nahlásenie bomby (Národný bezpečnostný úrad, 2023).

Propaganda je aktivita, ktorá je zameraná na šírenie určitej myšlienky, zdôrazňujúca jej pozitívne aspekty a šírená s cieľom presvedčiť publikum o jej správnosti. Má spravidla ideologickú, náboženskú alebo politickú konotáciu. Na rozdiel od reklamy či propagácie propaganda nemá komerčný rozmer (Národný bezpečnostný úrad, 2023).

Okrem týchto pojmov, ktoré možno považovať do určitej miery za podmnožiny dezinformácii, existujú aj pojmy misinformácia a malinformácia, ktoré sú definične vymedzené nasledovne:

Misinformácia je informácia, ktorá je nesprávna, nepravdivá alebo zavádzajúca, avšak zámerom jej šírenia nie je úmyselne spôsobiť niekomu ujmu (na rozdiel od dezinformácie). Napríklad ide o prípady, kedy jednotlivci na sociálnych sieťach v dobrej viere šíria informácie bez toho, aby vedeli o tom, že sú nepravdivé (Národný bezpečnostný úrad, 2023).

Malinformácia je informácia založená na realite, ktorá je šírená úmyselne s cieľom spôsobiť niekomu ujmu, poškodiť povesť inej osoby, alebo sú to napríklad nenávistné prejavy (Národný bezpečnostný úrad, 2023).

Pokiaľ ide o samotný pojem dezinformácia, tak možno ju definovať ako akúkoľvek formu overiteľne nepravdivej, zavádzajúcej alebo manipulatívne podanej informácie, 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 (Národný bezpečnostný úrad, 2023).

Okrem tohto definičného vymedzenia existujú aj iné definície. Napríklad Európska únia definuje dezinformácie ako preukázateľne nepravdivé alebo zavádzajúce informácie, ktoré boli alebo sú vytvorené, prezentované a šírené za účelom ekonomického zisku alebo zámerného klamania verejnosti a ktoré môžu spôsobiť verejné škody (Európska únia, 2018). Organizácia severoatlantickej zmluvy vymedzuje dezinformácie ako zámerné vytváranie a šírenie nepravdivých a/alebo manipulovaných informácií s úmyslom klamať a/alebo zavádzať, pričom aktéri šíriaci dezinformácie sa snažia prehĺbiť rozdiely v rámci spojeneckých krajín a medzi nimi a podkopať dôveru ľudí vo zvolené vlády (NATO, 2020).

SNAHY O ELIMINÁCIU DEZINFORMÁCIÍ

Vďaka rozvoju internetu a moderných technológií sa prístup k vedomostiam v priebehu posledných rokov značne zjednodušil. Informácie, ale aj dezinformácie sa šíria oveľa rýchlejšie a jednoduchšie, a tým sa aj schopnosť zavadzajúco, klamlivo alebo nepravdivo informovať výrazne zjednodušila a zefektívnila. Z tohto dôvodu je nutné vypracovať vhodné postupy zamerané na elimináciu dezinformácií, prijímať účinné opatrenia a využívať adekvátne

prostriedky na elimináciu negatívnych účinkov šírenia dezinformácií (Táborský, 2019; Ivančík, Müllerová, 2022; Kollár, 2022). Aby však v rámci úsilia o elimináciu dezinformácií boli využívané efektívne a účinné techniky a prostriedky, je potrebné identifikovať cieľ, ktorý štátni alebo neštátni aktéri – šíritelia dezinformácií – pri tom sledujú. Nakoľko informačný priestor obsahuje nespočetné množstvo falošných, zavádzajúcich, klamlivých a skreslených informácií (Ivančík, 2022), nie je možné reagovať na každú z nich, ale iba na tie, ktoré majú potenciál negatívne pôsobiť a v rámci tohto pôsobenia spôsobiť škody štátom, organizáciám a/alebo jednotlivcom. Pre zvolenie efektívnych a účinných spôsobov, techník a prostriedkov v boji proti dezinformáciám je vhodné v kontexte eliminácie ich negatívnych dôsledkov uvažovať o nasledujúcich atribútoch:

- závažnosti, to znamená, či ide o viac (nebezpečné, vysoko nebezpečné) alebo menej závažné dôsledky šírenia dezinformácií;
- rozsahu, to znamená odhadnúť k akému množstvu ľudí sa dezinformácia dostane a či sa bude šíriť ďalej;
- cieli (zámere), to znamená, či aktér šírením dezinformácie sleduje politický, finančný alebo iný profit;
- pôvodcovi, to znamená zistiť, či ide o zahraničného alebo domáceho aktéra; štátneho alebo neštátneho aktéra, organizáciu (skupinu) alebo jednotlivca a pod.;
- spôsoboch (prostriedkoch) šírenia, to znamená zistiť, či sú dezinformácie šírené v tlači, televízii, rozhlase, internetom, sociálnymi sieťami a pod.

Aktuálne sa na šírenie dezinformácií čoraz viac využívajú, resp. zneužívajú najmä sociálne siete a rôzne moderné technológie, systémy a zariadenia (Hajdúková – Šišulák, 2022; Kuchtová, 2022; Ivančík, 2023). V súčasnej dobe používané techniky zahŕňajú napríklad videomanipuláciu (tzv. deepfakes), falšovanie údajov a úradných dokumentov, používanie internetového automatizovaného softvéru (tzv. botov) na šírenie a znáso-bovanie kontroverzného obsahu a diskusií v sociálnych médiách, útoky prostredníctvom trollov na profily na sociálnych sieťach, krádeže informácií a osobných údajov atď. Zároveň však naďalej zohrávajú dôležitú úlohu aj tradičné metódy s využitím napríklad televízie, tlače (knihy, časopisy, noviny), internetových portálov a reťazových e-mailov (Hajdúková – Šišulák, 2022; Kuchtová, 2022; Ivančík, 2023). Používané nástroje a techniky šírenia dezinformácií sa menia veľmi rýchlo, a preto reakcia nesmie zaostávať.

V súčasnosti už existuje viacero spôsobov ako overovať pravdivosť správ, či už manuálne alebo automaticky prostredníctvom vytvorených programov a algoritmov. Niektoré detektory falošných správ dokážu identifikovať internetovú stránku alebo profil na sociálnej sieti, ktoré pravidelne produkujú nepravdivé alebo zavádzajúce informácie. Hoci tieto doplnky sú užitočné, stále je dôležité zvyšovať aj odolnosť spoločnosti voči dezinformáciám. To možno dosiahnuť rozvíjaním kritického myslenia, vzdelávania a mediálnej či informačnej gramotnosti. Uvedené zahŕňa predovšetkým:

- vzdelávanie ku kritickému mysleniu na všetkých stupňoch škôl;
- overovanie informácií a uvádzaných faktov;
- čerpanie informácií z overených zdrojov;
- identifikácia dezinformačných médií a vytváranie ich zoznamu;
- vysvetľovanie ako dezinformácie fungujú na konkrétnych príkladoch;
- zavedenie funkčných právnych noriem, ktoré postihnú dezinformačné média;
- transparentnosť a budovanie dôveryhodnosti;
- využívanie strategickej komunikácie a vlastných naratívov, vrátane preventívnej funkcie, v snahe byť produktívny, ale nie reaktívny;
- využívanie moderných technológii a aplikácii, vrátane počítačových hier, vytvorených s cieľom podporiť kritické myslenie, rozlišovanie pravdivých a nepravdivých informácii, ako aj možnosti uplatňovania umelej inteligencie na odhaľovanie falošných správ;
- aktívna občianska spoločnosť (Gregor a kol., 2018; EÚ, 2018; Táborský, 2019; Hajdúková – Šišulák, 2022; Kuchtová, 2022; Ivančík – Müllerová, 2022; Kollár, 2022; Ivančík, 2023).

ZÁVER

Aj napriek existencii viacerých techník a nástrojov, vďaka ktorým možno negatívny vplyv dezinformácii obmedziť, zostáva efektívne a účinné riešenie problémov spojených so šírením dezinformácií a snahami o ich čo najširšiu elimináciu aj naďalej obrovskou výzvou pre celý demokratický svet. Dezinformácie sú totiž namierené hlavne voči demokratickým štátom. Cieľom aktérov šíriacich dezinformácie je prostredníctvom nich a následných negatívnych vplyvov s tým súvisiacich narušiť a oslabiť fungovanie demokratických spoločností. Aj preto problematika dezinformácií predstavuje veľmi zložitú oblasť, v ktorej sa prelína veľa rôznych tém. Aktuálne šírenie dezinformácií predovšetkým prostredníctvom internetu a sociálnych sietí je extrémne nebezpečnou hrozbou, ktorá môže mať pre jednotlivcov, organizácie i celú

demokratickú spoločnosť veľmi nepriaznivé dôsledky. Je preto veľmi dôležité zo strany štátu a jeho kompetentných inštitúcií podporovať prevenciu, kritické myslenie a vzdelávanie v oblasti mediálnej gramotnosti a práce s informáciami. Zvýšenie povedomia o dezinformáciách, zlepšenie schopnosti rozoznávať a odhaľovať ich, ako aj eliminovať ich šírenie v čo najväčšej miere by určite znamenalo menej príležitostí napríklad pre populizmus, radikalizmus, extrémizmus, xenofóbiu či rozdeľovanie spoločnosti. Angažovanie štátu v tejto problematike je z toho dôvodu nielen žiaduce, ale nevyhnutné. Na druhej strane si ale všetci občania musia uvedomiť, že možnosti štátu nie sú nekonečné, nie všetko za nich vyrieši štát, a tak je nutné, aby aj oni sami prispeli k potláčaniu množstva, sily a vplyvu dezinformácií a ich šíriteľov na ich životy.

POUŽITÁ LITERATÚRA A INFORMAČNÉ ZDROJE:

1. EÚ. (2018): Akčný plán boja proti dezinformáciám. In *Európska únia,* 2018. [online] [cit. 10-12-2023] Dostupné na internete: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52018JC0036>.
2. GREGOR, M. a kol. (2018): *Nejlepší kniha o Fake News, dezinformacích a manipulacích!!!* Brno: CPress, 2018. 143 s. ISBN 978-80-264-1805-4.
3. HAJDÚKOVÁ, T. – ŠIŠULÁK, S. (2022): Abuse of modern means of communication to manipulate public opinion. In *INTED 2022: International Technology, Education and Development Conference – Conference Proceedings*. Barcelona : IATED, 2022, s. 1992-2000. ISBN 978-84-09-37758-9.
4. 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.
5. IVANČÍK, R. – NEČAS, P. (2020): Kybernetická moc v kontexte zaisťovania kybernetickej bezpečnosti a obrany na národnej a aliančnej úrovni. In *Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie s medzinárod-nou účasťou*. Bratislava : Akadémia Policajného zboru, 2020, s. 47-58. ISBN 978-80-8054-819-3.
6. IVANČÍK, R. (2020): Analýza prístupov k definovaniu a vymedzeniu hybridnej vojny. In *Národná a medzinárodná bezpečnosť 2020 – zborník príspevkov z medzinárodnej vedeckej konferencie*. Liptovský Mikuláš : Akadémia ozbrojených síl generála M. R. Štefánika. 2020. s. 174-184. ISBN 978-80-8040-589-2.

7. IVANČÍK, R. (2022): Dezinformácie ako hybridná hrozba. In *Dezinformácie a právo (úlohy a postavenie bezpečnostných zložiek) – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2022, s. 54-65. ISBN 978-80-8054-965-7.
8. 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.
9. IVANČÍK, R. (2023): Šírenie hoaxov cestou sociálnych sietí – hrozba pre súčasnú demokratickú spoločnosť. In *Bezpečnosť elektronickej komunikácie – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2023, s. 45-56. ISBN 978-80-8054-997-8.
10. JURČÁK, V. – JURČÁK, J. – SASARÁK, J. (2016): Hybridné hrozby – výzva pre Európsku úniu. In *Medzinárodné vzťahy – aktuálne otázky svetovej ekonomiky a politiky*. Bratislava : Ekonomická univerzita, Fakulta medzinárodných vzťahov, 2016, s. 542-550. ISBN 978-80-225-4365-1.
11. JURČÁK, V. – TURAC, J. (2018): Hybridné vojny – výzva pre NATO. In *Bezpeč-nostné fórum 2018 – zborník vedeckých prác z medzinárodnej vedeckej konferencie*. Banská Bystrica : Interpolis, 2018. s. 177-184. ISBN 978-80-972673-5-3.
12. KOLLÁR, D. (2022): Dezinformácie ako kľúčová bezpečnostná výzva súčasnosti v kontexte rusko-ukrajinského konfliktu. In *Politické vedy*, 2022, roč. 25, č. 3, s. 87-109. ISSN 1335-2741.
13. KUCHTOVÁ, J. (2023): Bezpečnosť na sociálnych sieťach. In *Bezpečnosť elektro-nickej komunikácie – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru v Bratislave, 2022, s. 237-247. ISBN 978-80-8054-968-8.
14. Národný bezpečnostný úrad. (2021): Dezinformácie. In *Národné bezpečnostné analytické centrum - Krátky slovník hybridných hrozieb*, 2021. [online] [cit. 11-12-2023] Dostupné na internete: <https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/kratky-slovnik-hybridnych-hrozieb/index.html>.
15. Národný bezpečnostný úrad. (2021): Falošné správy. In *Národné bezpečnostné analytické centrum - Krátky slovník hybridných hrozieb*, 2021. [online] [cit. 11-12-2023] Dostupné na internete: <https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/kratky-slovnik-hybridnych-hrozieb/index.html>.
16. Národný bezpečnostný úrad. (2021): Hoax. In *Národné bezpečnostné analytické centrum - Krátky slovník hybridných hrozieb*, 2021. [online] [cit. 11-12-2023] Dostupné na internete:

<https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/kratky-slovnik-hybridnych-hrozieb/index.html>.

17. Národný bezpečnostný úrad. (2021): Malinformácie. In *Národné bezpečnostné analytické centrum - Krátky slovník hybridných hrozieb*, 2021. [online] [cit. 11-12-2023] Dostupné na internete: <https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/kratky-slovnik-hybridnych-hrozieb/index.html>.
18. Národný bezpečnostný úrad. (2021): Misinformácie. In *Národné bezpečnostné analytické centrum - Krátky slovník hybridných hrozieb*, 2021. [online] [cit. 11-12-2023] Dostupné na internete: <https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/kratky-slovnik-hybridnych-hrozieb/index.html>.
19. NATO. (2020): NATO's approach to countering disinformation. In *North Atlantic Treaty Organisation*, 2020. [online] [cit. 10-12-2023] Dostupné na internete: <https://www.nato.int/cps/en/natohq/177273.htm>.
20. NEČAS, P. – IVANČÍK, R. (2019): Aktuálny vývoj v oblasti zaisťovania kyber-netickej bezpečnosti a ochrany informácií na národnej a nadnárodnej úrovni. In *Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konfe-rencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2019, s. 125-137. ISBN 978-80-8040-819-3.

ADDRESS & ©

JUDr. Magda RUŽBACKÁ
Prezídium Policajného zboru
Račianska 45, 831 02 Bratislava
Slovenská republika
magda.ruzbacka@minv.sk

BEZPEČNOST • SAFETY

DOI: 10.36682/a_2024_1_5

SEBAVNÍMANIE ODOLNOSTI VOČI DEZINFORMÁCIÁM VO VYSOKOŠKOLSKOM PROSTREDÍ

Self-perception of resistance to misinformation in the university environment

Mária SABAYOVÁ

Bratislava, Slovak Republic

ABSTRAKT: Schopnosť identifikovať nepravdivé, vymyslené, klamlivé, pozmenené, či skreslené informácie, ktoré sú v súčasnosti vo väčšej, alebo menšej miere šírené takmer všetkými typmi sociálnych médií bude kľúčovou v snahách eliminovať ich vplyv na spoločenské dianie pro futuro. Predkladaná štúdia ako výstup pilotného sociologického prieskumu medzi študentmi Vysokej školy európskych a regionálnych štúdií (CZ) a Akadémie Policajného zboru v Bratislave (SK),odhaľuje sebavnímanie vysokoškolských študentov vo vzťahu k problematike dezinformácií, ktorý vytvorí novú výskumnú bázu smerujúcu k potrebe nastavenia vzdelávania v tejto oblasti. Cieľom bolo zodpovedať na otázku, či sú študenti schopní overovaním si obsahu informácií, okolností za akých sú im podávané, resp. záujmu autora informácie, v konečnom dôsledku rozpoznať že ide o dezinformáciu, a či sa o to aj snažia. Opatrnosť pri prijímaní informácií sa síce potvrdila, na druhej strane však naznačuje, že aj keď študenti neprijímajú informácie nekriticky, majú v podstate pochybnosti o tom, že sú schopní dezinformáciu rozpoznať.

Kľúčové slová: dezinformácie – médiá – prieskum – gramotnosť.

ABSTRACT: The ability to identify false, fabricated, deceptive, altered, or distorted information that is currently being disseminated to a greater or lesser extent by almost all types of social media will be key in efforts to eliminate its influence on social events pro futuro. The present study is an output of a pilot sociological survey among students of the College of European and Regional Studies (CZ) and the Academy of the Police Force in Bratislava (SK), determining the self-perception of university students in relation to the issue of disinformation, which provides a new research base oriented towards the need to adjust education in this area. The aim was to answer the question of whether students are able to verify the content of information, the circumstances in which it is given to them, or the interests of the author of the information, as well as whether they are ultimately able to recognize it as disinformation, and whether they even try to do so. Although some caution while receiving information has been proven, the results suggest that even if students do not take in information mindlessly, they actually doubt their ability to recognize disinformation.

Key words: disinformation – media – survey – literacy.

ÚVOD

Štandardne sa ľudia líšia v názoroch na politiku a politikov, na potraty, či vyučovanie náboženstva na základných školách. Antagonizmy ako dôsledok objektívnej rozdielnosti záujmov tak môžu za určitých podmienok vyústiť do konfliktu názorov na akékoľvek politické alebo sociálne otázky. Aj keď sú zdanlivo uvedené konštrukty odlišné, majú rovnakú motiváciu, a to nakloniť si isté sociálne skupiny v čo najširšej miere na svoju stranu. A práve v tomto výraznú úlohu zohrávajú informácie.

Čoraz častejšie a v čoraz väčšom rozsahu nás atakujú cielené informácie, ktorých primárnou úlohou je podpora istých konkrétnych ekonomických, politických, sociálnych a iných záujmov. To znamená, že majú za cieľ bezprostredne ovplyvňovať presvedčenie a rozhodnutia tých, ktorým sú adresované. Popri pravdivých správach sa tak objavujú rôzne dezinformácie a falošné správy. Ich neustále rastúci objem a rýchlosť ich distribúcie, ako aj globálny dosah vyvolávajú pochybnosti a obavy tak u autorít, ako aj u laickej verejnosti. Snahy pokiaľ možno čo najefektívnejšie na tento jav reagovať, či už ako súčasť boja proti hybridným hrozbám, alebo snahou o objektívnosť spravodajstva, narážajú na neexistenciu jednotného typologického rámca, alebo aspoň istých konsenzuálnych kategorizačných kritérií (napr. zámer zavádzať, úmysel ublížiť, autentickosť, resp. overiteľnosť), ktoré by mohli byť všeobecne akceptovaným právnym a regulačným východiskom. Veľké množstvo pojmov, a konceptov, ktoré sa v tejto súvislosti aj v odbornej literatúre objavuje i samotných charakter javu dáva tušiť, že neexistuje univerzálna zhoda na to, čo dezinformácia je alebo nie je. Nie je možné vymedziť jasné hranice. Diskusie k samotnému obsahu pojmu dezinformácia tak prinášajú problém nie len vo vedeckom výskume, ale aj vo vzdelávacom procese. Obzvlášť v odbore bezpečnostných vied kde problematika nadobúda úplne iný rozmer. Napriek tomu je pojem dezinformácia frekventovaný,[9] pričom najmä v laickej verejnosti sú predstavy o obsahu tohto pojmu pomerne diverzifikované.

Pre účely štúdie chápeme pojem „dezinformácia“ ako nepravdivé, nepresné, alebo zavádzajúce informácie, ktoré boli navrhnuté a prezentované *s úmyslom spôsobiť škodu* – ekonomickú, politickú či ideologickú. Literatúra spravidla pracuje s dvomi rovinami takýchto šírených dezinformácií. Buď sú imanentnou súčasťou správ o reálnych udalostiach (už neaktuálne, také ktoré sa pôvodne považovali za pravdivé ale už boli vyvrátené, technicky síce

[9] Pojem dezinformácia v slovenskom jazyku k dátumu písania článku vyhľadávaný Googlom priniesol 679 tisíc odkazov a v anglickom jazyku 90 miliónov odkazov. Pokiaľ ide výlučne len o vedecké články v anglickom jazyku, tak Googlescholar pri pojme disinformation ponúkol 225 tisíc výsledkov, pri slove misinformation 513 tisíc odkazov.

pravdivé, no zavádzajúce polopravdy a pod.), alebo sú celé správy fiktívne a vytvorené prostredníctvom dezinformačných techník, v súčasnosti dokonca aj prostredníctvom umelej inteligencie. Ich využívanie sa nevyhýba komukoľvek, kto sa snaží presvedčiť čo najširšiu verejnosť, alebo nakloniť si isté sociálne skupiny (používajú ich aj politici, obchodníci, finanční sprostredkovatelia pod.). Vo vlastnom (zištnom) záujme tak majú tendenciu skresľovať, zveličovať či zahmlievať.

Rozpoznanie samotnej dezinformácie, či dokonca jej typu a faktorov, ktoré uľahčujú jej šírenie nie je vždy bez dostatočných vedomostí o konkrétnom probléme, alebo jeho politickom, ekonomickom, či sociálnom kontexte jednoduché. Takisto vedci upozorňujú, že stratégie, ktoré sa môžu ukázať ako účinné pri eliminácii jedného typu dezinformácií, nemusia fungovať proti iným. Najmä ak vezmeme do úvahy konkrétne kombinácie sociálnych, politických a ekonomických faktorov a dostupné technológie, ktoré vznik a šírenie rôznych typov dezinformácií uľahčujú (McCright, Dunlap, 2017).

Overovanie faktov v relevantných zdrojoch by dnes malo byť výbavou každého, kto sa o čokoľvek konkrétne zaujíma. Znamená to pozerať sa na svet skeptickou optikou. Užívatelia správ/informácií sa však často spoliehajú, že médiami ponúkané informácie sú a priori korektné, a to aj bez toho aby bolo zrejmé, či prešli internými verifikačnými procesmi a bez toho, aby médiá ručili za pravdivosť a presnosť informácií ktoré zverejňujú. Nezriedka napríklad aj v politických diskusných reláciách sme svedkami, že médiá nie sú schopné zaručiť objektivitu toho čo odznie, a žiaľ nie je výnimkou aj to, že sa ich zástupcovia priamo zapájajú do politických argumentov, alebo neskrývajú osobnú zaujatosť.

METODIKA A CIEĽ

Ak sa hranice medzi skutočnosťou a fikciou začnú stierať, možnosť zdieľania obsahu vo veľmi krátkom čase ho často povýši na virálny. Potom žiaľ, aj v prípade že sa zistí jeho nepravdivosť, zvyčajne už žije svojím vlastným životom a snahy zastaviť, alebo uviesť informácie na pravú mieru sa v konečnom dôsledku minú účinku.

Podľa autorov knihy The Debunking Handbook 2020, čím viac sa ľudia stretávajú s dezinformáciou, ktorú nespochybnia oni sami, alebo niekto iný, tým viac sa dezinformácia javí ako pravdivá. A to aj napriek pochybnostiam o samotnom zdroji informácie. Opakované vystavenie takýmto informáciám napokon vedie k tomu, že predmetným tvrdeniam uveria. Tento jav je označovaný ako „*efekt iluzórnej pravdy*“. (Lewandowsky a kol., 2020; Vellani a kol., 2023; Newman a kol., 2020; Smelter, Calvillo, 2020 ai.). Skutočnosť že opakované tvrdenia sú subjektívne hodnotené ako pravdivejšie, než porovnateľné nové tvrdenia, a to aj v

prípade keď samotné opakovanie neposkytuje žiadne nové dôkazné informácie, využívajú často najmä sociálne médiá. Aj preto si dovolíme tvrdiť, že sociálne médiá umožňujú legitimizáciu dezinformácií.

Študenti využívajú sociálne médiá vo veľkej miere a v tejto súvislosti si kladieme otázku či sú tiež schopní overovaním si obsahu informácií, okolností za akých sú im podávané, či okolnosti záujmu autora informácie rozpoznať (dez)interpretáciu reality, identifikovať rozdiel medzi (ne)profesionálnym štandardom a (ne)overiteľnosťou informácií alebo interpretáciu reality s istým „žiadúcim" naratívom. A tiež či to v skutočnosti aj robia. Prístup k takému rozsiahlemu spektru médií a komunikačných technológií je síce zdrojom veľkého množstva informácií v krátkom čase, automaticky to však neznamená, že im ľudia aj rozumejú a dokážu prijímať ich obsah s primeranou dávkou kritického myslenia. Máme tým na mysli čerpanie informácií z rôznych zdrojov, ich porovnávanie, akceptovanie aj alternatívnych pohľadov na problematiku a samozrejme nespoliehanie sa na jediný zdroj, bez ohľadu na to, že sa zdá byť akokoľvek dôveryhodný, autentický, či pravdivý. V tomto kontexte je dôležitá najmä dôslednosť pri rozlišovaní faktov a názorov (Vrabec, Petranová, 2015). Zaujímalo nás teda, či si študenti myslia, že dokážu rozpoznať špecifické techniky používané a v mediálnom priestore a ich skutočný účel. Či vždy hľadajú aj alternatívne zdroje informácií, bez problémov odhalia zavádzajúci obsah a sú schopní krížovou kontrolou si informácie overovať a dekódovať. Spochybňovanie a zdravý skepticizmus vo vzťahu k informáciám (či už ide o správy, fotografie, audio/video obsah, alebo aj infografiky a štatistiky) by mal byť nevyhnutnou výbavou každého jednotlivca, a u študentov, ktorí sa v mnohých sférach života iba začínajú orientovať je to priam nevyhnutné. Je teda ich prirodzenou výbavou uisťovanie sa o pravdivosti informácií napríklad aj uvedomovaním si autentickosti prijímaného obsahu vo vhodných kontextoch, či o spôsobe používania jazyka? Všímajú si, na čo je kladený pri informovaní dôraz, čo sa (zámerne) vynecháva, kto čo hovorí, aká spoľahlivá je osoba ktorá obsah ponúka, či „náhodou" nenapĺňa určitú agendu? Aký môžu prezentované informácie mať prípadný dopad a ako vnímajú a preberajú takéto správy ostatní (Ireton, Posetti, 2018).

Tento problém indikoval voľbu metodologického prístupu a náš cieľ, a to identifikovať potenciálnu odolnosť vysokoškolských študentov voči dezinformáciám. Na základe teoretických poznatkov získaných historickou metódu, ktorá v danom kontexte umožňuje poznávanie vecí a javov v ich vzniku, vývine, a vo vzájomných súvislostiach s podmienkami, ktoré vyvolávajú ich vznik, sme dospeli k výskumnej otázke, a to, či si študenti uvedomujú nové riziká, ktoré dezinformácie so sebou prinášajú, resp. či tejto problematike vôbec venujú pozornosť. Charakter skúmaného objektu determinuje formy analýzy, t.j. rozčlenenie celku na

časti, oddelenie podstatného od nepodstatného, redukciu zložitého na jednoduché a odhalenie štruktúry predmetu. Analyzovali sme preto jednotlivé aspekty, ktoré vstupujú do stanoveného výskumného objektu a predmetu prostredníctvom myšlienkového rozkladu skúmaného predmetu, ktorým je v našom prípade sebavidenie študentov ako potenciálnych konzumentov dezinformácií, resp. špecifikáciou aspektov, ktoré predstavovali potenciál vplyvu. Syntézou teoretických východísk a výsledkov prieskumu sme sa pokúsili o zovšeobecnenie nadobudnutých poznatkov. Základom pre dedukciu boli predovšetkým argumentačne nevyvážené reakcie študentov na niektoré odborné otázky v rámci vyučovaných predmetov a indukcia - prechod od jednotlivých faktov ku všeobecným tvrdeniam základe logických pravidiel, sa opiera o výstupy z dotazníkového prieskumu realizovaného medzi študentami Akadémie Policajného zboru v Bratislave. Zber údajov prebiehal v mesiacoch september a október 2023, ako súčasť vedeckovýskumnej úlohy VÝSK 268: *Dezinformácie ako súčasť hybridných hrozieb pre demokratickú spoločnosť a ich vnímanie študentmi vysokých škôl* a zúčastnilo sa ho na základe on-line dotazníkov celkom 299 študentov rôznych vekových kategórií v rámci všetkých troch stupňov denného štúdia a externého štúdia, a tiež v rámci účastníkov celoživotného vzdelávania. Najväčšiu časť respondentov tvorili študenti magisterského štúdia (52%) a bakalárskeho štúdia (34%), zvyšok dopĺňali študenti doktorandského štúdia a štúdia v rámci celoživotného vzdelávania (odborný kurz a pod.) na Akadémii Policajného zboru v Bratislave, pričom 60 % respondentov tvorili ženy. Dve tretiny respondentov boli študenti vo veku do 30 rokov, respondenti nad 41 rokov tvorili jednu desatinu výskumnej vzorky. Získané výstupy boli štatisticky spracované prostredníctvom programu Excel a v kontexte výskumnej otázky nás zaujímali najmä hraničné odpovede, vyjadrujúce jednoznačný postoj.

Všetci respondenti uviedli, že aktívne využívajú internet bez ohľadu na účel využitia. Z hľadiska *dĺžky využívania internetu*, trávia podľa vlastných vyjadrení v priemere viac ako 113 minút denne a aktívne *využívajú sociálne siete* bez ohľadu na účel využitia v priemere denne viac ako 90 minút. Muži pritom používajú internet a sociálne siete o viac ako jednu tretinu času dlhšie ako ženy.

Bez ohľadu na to, že nebola študentom problematika obsahu pojmu *dezinformácia* nijako ponúknutá, na otázku či sa už s dezinformáciou stretli, odpovedalo kladne 98% študentov, pričom rozsah pozornosti venovanej médiami danej téme sa premieta aj v percente odpovedí v nasledujúcej tabuľke.

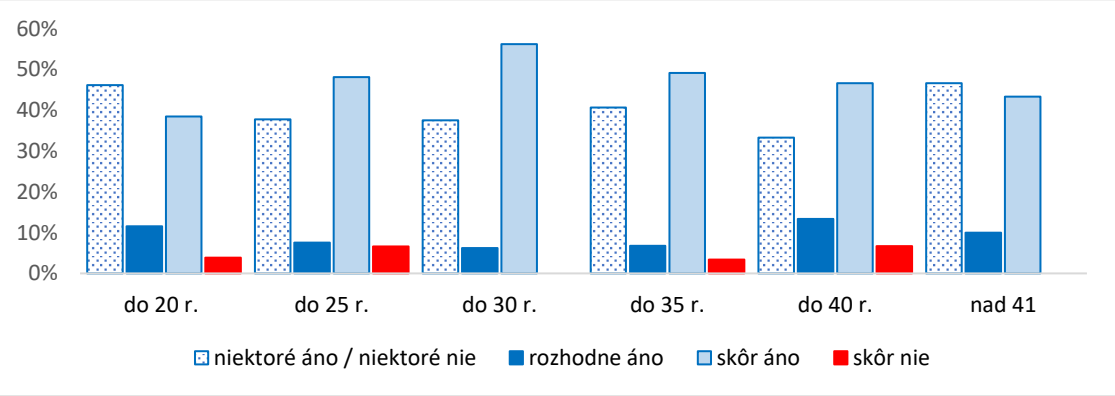
Tabuľka 1: Oblasť dezinformácií s ktorými sa respondenti stretli v posledných troch rokoch najčastejšie

Oblasť	Odpovedí
Vakcinácia (očkovanie) a liečba ochorenia Covid-19	87%
Vznik / pôvod koronavírusu spôsobujúceho ochorenie Covid-19	86%
Vypuknutie a priebeh konfliktu na Ukrajine	84%
Domáca politická scéna	59%
Rusko	55%
Spojené štáty americké	35%
Zahraničná politická scéna	25%
Snaha/úsilie o ovládnutie sveta určitými jednotlivcami alebo skupinami	22%
Európska únia	22%
Čína	20%
Severoatlantická aliancia	18%
Iné	8%

Zdroj: Vlastné spracovanie.

Len jeden z desiatich respondentov je presvedčený, že *rozhodne je schopný kvalifikovane rozpoznať dezinformáciu* a necelá polovica si myslí že to skôr dokáže, ako nie. V rámci vlastných vekových kategórií sú o svojich schopnostiach odhaliť dezinformáciu presvedčení najviac študenti od 25 do 30 rokov a najmenej študenti od 31 do 35 rokov. To že najväčší podiel odpovedí vo všetkých vekových kategóriách osciluje okolo *niektoré áno /niektoré nie* a *skôr áno*, naznačuje, že študenti neprijímajú informácie nekriticky a majú pochybnosti o tom, že sú schopní dezinformáciu rozpoznať.

Graf 1: Schopnosť kvalifikovane rozpoznať dezinformáciu



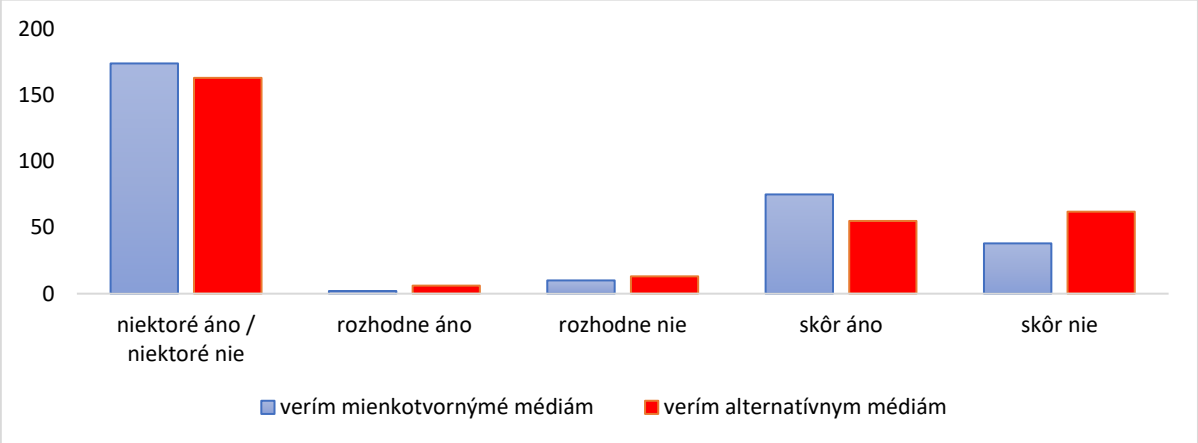
Zdroj: Vlastné spracovanie.

Podľa vyjadrení v dotazníkovom prieskume si informácie s ktorými sa študenti stretnú cca 96% z respondentov viac alebo menej overuje. Skutočne každú informáciu si však overuje len 13% opýtaných. V rámci svojej vekovej kategórie si *rozhodne,* alebo *skôr áno* informácie overujú najmä študenti od 25 do 30 rokov, najmenej respondenti do 20 rokov, pričom obe skupiny najviac posudzujú dôveryhodnosť informácie *podľa obsahu* informácie a *autora* informácie.

Najviac dezinformácií je podľa opýtaných šírených cez *internet* (42%), cez *sociálne siete* (39%) a *televíziu* (38%). Zaujímavé je, že za prostriedok šírenia informácií uvádzajú študenti aj *vedecké knihy, odborné knihy* a *učebnice* (30%) a tiež informácie osobne *šírené odborníkmi* a *vedcami* (28%). *Rodine, priateľom, známym* a *tlači* (noviny, časopisy) prisudzuje šírenie dezinformácií menej ako 20% respondentov.

Opatrnosť pri prijímaní informácií, ktoré poskytujú *alternatívne médiá* (tzv. nezávislé spravodajstvo, nezávislé weby, …) z hľadiska ich pravdivosti a objektivity sa potvrdila. Zaujímavým však bolo zistenie, že štvrtina respondentov považuje informácie ponúkané týmito médiami skôr za pravdivé a 58% uviedla že niektoré sú pravdivé a niektoré nepravdivé. Pri otázke, či považujú informácie uvádzané *v mienkotvorných (tzv. mainstreamových) médiách* za pravdivé a objektívne, 3 % opýtaných odpovedala že ich za pravdivé rozhodne nepovažuje, skôr áno odpovedalo 13 % respondentov a tak ako vo väčšine otázok sa opäť najčastejšie objavuje nevyhranené vyjadrenie.

Graf 2: Porovnanie dôvery voči mienkotvorným a alternatívnym médiám



Zdroj: Vlastné spracovanie.

Celkom 34 respondentov (11%) nedôverujúcich mienkotvorným médiám súčasne verí alternatívnym médiám. Tiež 25 respondentov (8%) neverí alternatívnym médiám a súčasne verí

mienkotvorným a 9 respondentov (3%) súčasne neverí ani mienkotvorným, ani alternatívnym médiám.

Tabuľka 2: Krížové porovnanie dôvery voči mienkotvorným a alternatívnym médiám

		vzťah k alternatívnym médiám		
		verím/skôr verím	niekedy verím, niekedy nie	neverím/skôr neverím
vzťah k mienkotvorným médiám	verím/skôr verím	3%	9%	8%
	niekedy verím, niekedy nie	11%	39%	5%
	neverím/skôr neverím	11%	11%	3%

Zdroj: Vlastné spracovanie.

Za vznikom a šírením dezinformácií sú podľa ***58%*** respondentov predovšetkým ***politické dôvody*** (zisk politických preferencií, zisk väčšieho počtu hlasov vo voľbách, očierňovanie politických konkurentov, ospravedlňovanie alebo skrývanie vlastných chýb pri vykonávaní verejných funkcií, spochybňovanie demokratického zriadenia, systému, poriadku, a pod.) a ***geopolitické dôvody*** (***18%***) týkajúce sa konfrontácie, napätia, nezhôd, konfliktov medzi štátmi, narušenie bezpečnostných systémov štátov, zoskupení ako napr. Európskej únie, Severoatlantickej aliancie, snaha o narušenie súdržnosti a dobrých vzťahov medzi krajinami, a pod. ***12%*** vidí za dezinformáciami ***societálne dôvody*** (ohováranie / očierňovanie určitej skupiny ľudí napr. inej národnosti, rasy, vierovyznania, politického zmýšľania a pod***., 9% ekonomické dôvody*** (dosiahnutie vyšších ziskov, snaha ovplyvniť ľudí, aby uprednostňovali určité výrobky na úkor konkurenčných výrobkov, očierňovanie konkurencie a jej produktov, a pod.) alebo ***iné dôvody (3%).***

Celkom 71% respondentov ktorí tvrdili, že si vždy alebo zväčša informácie overujú, rovnako videli za vznikom najmä politické dôvody (41%), pričom súčasne tvrdili, že si informácie overujú v poradí:

i.) obsah informácie, ii.) autor informácie, iii.) aktuálnosť informácie, iv.) iné faktory a *v.) vizuálny vzhľad informácie.*

VÝSLEDKY A DISKUSIA

Problémy dezinformácií sú hlboko prepojené s rozvojom digitálnych médií a v súčasnosti sú už bezprostredne vnímané ako súčasť hybridných hrozieb. V tomto kontexte sa otázke dezinformácií a ich typológii venujú mnohí autori, napr. Ivančík, Müllerová, 2022; Ivančík, 2021; Šišulák, Cichová, 2019; Byford, 2011; Dragomir, 2017; Zalewski, 2022; Vogel a kol., 2020 ai. Viacrozmerný prístup k skúmaniu dezinformácií tiež zvolila nezávislá skupina odborníkov zriadená Európskou komisiou (2018).

Záujem pochopiť prediktory šírenia dezinformácií a náchylnosť veriť im sa v posledných rokoch dostáva aj do pozornosti vedcov v spoločenských a predovšetkým behaviorálnych vedách. Za mnohých napr. Roozenbeek a kol.,2022; Pennycook,Rand,2021; ESMH, 2020. V rámci európskej politiky boja proti hybridným hrozbám sa špeciálne problematike dôverčivosti študentov voči dezinformáciám vo vede venovalo i Európske centrum pre vedu a médiá (ESMH, 2020). Objavujú sa dokonca snahy vytvoriť štandardizované nástroje na meranie citlivosti na dezinformácie. (pozri napr. Maertens a kol., 2023) Avšak príliš veľké rozdiely v metodológiách pokiaľ ide o štúdium dezinformácií sťažujú prípadnú komparáciu, či zovšeobecňovanie záverov nad rámec predmetných vedeckých prác. Aj v našom prípade prezentácia záverov hodnotí skôr sebavnímanie respondentov ako ich skutočnú schopnosť identifikovať dezinformácie a schopnosť odolať im.

Výsledkom prieskumu je vysoká miera neistoty, resp. pochybností, čo prirodzene korešponduje s tým, že väčšina respondentov je v životnej fáze, kedy vzdelanie v niektorých oblastiach (politika, právo a pod.) a ich orientácia v obsahu informácií, ktoré sprostredkúvajú tieto témy nie je na takej úrovni, aby spoľahlivo dezinformácie odhalili.

Tendencie vývoja dnešnej spoločnosti, pretkané spoločenskou anómiou a individualizmom, neistotou a dezilúziami postmodernej spoločnosti, ako aj prehlbujúca sa ekonomická nerovnosť, neriadená migrácia, zlyhania elít v zásadných spoločenských ale aj etických otázkach sú síce realitou súčasnosti, avšak prezentácia s tým súvisiacich faktov naráža v bežnom živote na absentujúce hlbšie vedomosti a bežnú ľudskú pochybovačnosť. Preto v prípade, ak oproti sebe stoja konzistentné nepravdivé informácie a nekonzistentné pravdivé informácie, navyše umocnené emotívnymi naratívmi je prirodzené podľahnúť (v zmysle sympatií a antipatií) ponúkanému obsahu, autorite a pod.. Populárne je dnes tiež uspokojiť sa so skratkovitými závermi vo vzťahu k problematike ktorej čelíme. Nie len preto, že na podrobnejšie analýzy nezostáva čas, ale aj preto že instantné informácie o javoch a udalostiach,

po ktorých je dopyt aj medzi študentmi, neumožňujú pochopenie vzájomných súvislostí a teda ani odhalenie skutočného zámeru autora.

Z osobných skúseností pedagóga však nemožno zároveň nekonštatovať, že študenti pristupujú k štúdiu z roka na rok povrchnejšie, čo v kontexte skúmanej problematiky spochybňuje ich schopnosť triezvo sa pohybovať v spleti faktov, ktoré sú im ponúkané. Napriek tomu tretina z našich respondentov uviedla ako prostriedok šírenia dezinformácií vedecké knihy, odborné knihy a učebnice a tiež informácie osobne šírené odborníkmi a vedcami, čím nespochybňujeme existenciu účelových, falšovaných alebo úplne vymyslených „výskumov“, nie je však zrejmé z čoho tento názor vychádza, či z reálnych dôkazov, alebo čo je tiež jednou z alternatív – z dezinformácií. Mnohé z uvedeného vyvoláva ďalšie otázky, o ktoré by sa mohol prieskum rozšíriť, alebo vyprecizovať.

ZÁVER

Rozpoznanie samotnej dezinformácie, či dokonca jej typu a faktorov, ktoré uľahčujú jej šírenie nie je vždy bez dostatočných vedomostí o konkrétnom probléme, a súčasne o jeho politickom, ekonomickom, či sociálnom kontexte jednoduché. Samotný obsah informácie, či autor, tak ako im prisudzujú (ne)dôveryhodnosť študenti z nášho prieskumu nie sú vždy tou správnou cestou. Obzvlášť ak sami respondenti priznávajú ich šírenie najmä cez internet, sociálne siete a televíziu. Ako riešenie ponúkajú mnohí čo najširšiu podporu kritického myslenia a zvyšovania mediálnej gramotnosti, aj medzi žiakmi a študentmi.

Kritické myslenie vyžaduje byť neustále v obraze v danej problematike, ale súčasne aj otvorenosť iným názorom a schopnosť veľmi rýchlo vyhodnotiť ponúkané alternatívy byť schopný revidovať vlastný názor, bez predsudkov a spoločenských stereotypov. Pokiaľ ide o mediálnu gramotnosť, nemožno nesúhlasiť s tým, že „*nadobudnutie zručností v oblasti mediálnej gramotnosti posilní v ľuďoch kritické myslenie a podporí kreatívne schopnosti v prostredí neustále rastúceho množstva mediálnych posolstiev používajúcich obraz, slovo a zvuk*.“(Vrabec, 2007) Obávame sa však, že súčasný systém povrchného vzdelávania, kedy prioritou škôl nie je kvalitný výber, ale počty študujúcich (čo podmieňuje výšku finančných zdrojov ktoré škola získa) a na druhej strane neodškriepiteľný fakt, že pre mnohých študentov často nie je cieľom byť odborníkom v danom odbore, ale primárne získať titul, nebude schopný vybudovať v nich dostatočné kompetencie a eliminovať prijímanie šírených dezinformácií. Rovnako by bolo naivné veriť, že čokoľvek smerované voči tomuto negatívnemu javu dokáže konkurovať rýchlosti a rozsahu šírenia (dez)informácií. Práve preto majú výskumy v tejto oblasti, a hľadanie hoc aj len parciálnych riešení nespochybniteľný zmysel.

POUŽITÁ LITERATÚRA A INFORMAČNÉ ZDROJE:

1. BYFORD, J. (2011): Conspiracy Theories. A Critical Introduction. London : Palgrave Macmillan, 2011. 179 s. ISBN 978-1-349-32350-0.
2. DRAGOMIR, A. M. (2017): The Fake News Phenomenon in the Social Media Era. In Strategic Impact, 2017, č. 64/65, s. 54-65. ISSN 18415784.
3. ESMH. (2020): *Disinformation and Science. A survey of the gullibility of students with regard to false scientific news*. Brussels. European Union, 2020. ISBN: 978-92-846-7020-8. doi:10.2861/411673.
4. European Commission, (2018): *A multi-dimensional approach to disinformation – Report of the independent High level Group on fake news and online disinformation,* Publications Office, 2018, https://data.europa.eu/doi/10.2759/739290.
5. IRETON, Ch. – POSETTI, J. (2018): *Journalism, 'Fake News' & Disinformation Handbook for Journalism Education and Training*. UNESCO. 128p. ISBN:978-92-3-100281-6. 2018. [online] [cit. 3-11-2023]. Dostupné na internete: https://unesdoc.unesco.org/ark:/48223/pf0000265552 p.80.
6. IVANČÍK, R. (2021): *Dezinformácie ako bezpečnostná hrozba pre demokratickú spoločnosť.* In Právo a bezpečnost, 2021, roč. 15, č. 3, s. 16-33. ISSN 2336-5323.
7. IVANČÍK, R. – MÜLLEROVÁ, J. (2022): *Dezinformácie ako hybridná hrozba šírená prostredníctvom sociálnych sietí.* In: Policajná teória a prax. - ISSN 1335-1370 - Roč. 30, č. 3(2022), - s. 22-42.
8. LEWANDOWSKY, S. – COOK, J. – LOMBARDI, D. (2020): *Debunking Handbook 2020.* [online] [cit. 3-11-2023]. Dostupné na internete: Databrary. 10.17910/b7.1182.
9. MAERTENS, R., et al. (2023): *The Misinformation Susceptibility Test (MIST*): A psychometrically validated measure of news veracity discernment. Behav Res (2023). https://doi.org/10.3758/s13428-023-02124-2.
10. McCRIGHT, A. M. – DUNLAP, R. E. (2017): *Combatting misinformation requires recognizing its types and the factors that facilitate its spread and resonance.* In: Journal of Applied Research in Memory and Cognition, 6(4), 389–396. 2017. [online] [cit. 3-11-2023]. Dostupné na internete: https://doi.org/10.1016/j.jarmac.2017.09.005.
11. NEWMAN, E. J. – JALBERT, M. C. – SCHWARZ, N. – LY, D. P., (2020): *Truthiness, the illusory truth effect, and the role of need for cognition.* Consciousness and Cognition, 2020. [online] [cit. 3-11-2023]. Dostupné na internete: https://www.sciencedirect.com/science/article/abs/pii/S1053810019301977.

12. PENNYCOOK, G. – RAND, D. G. (2021): *The psychology of fake news. Trends in Cognitive Sciences,* 25(5), 388–402. https://doi.org/10.1016/j.tics.2021.02.007.
13. ROOZENBEEK, J., et al (2022): *Susceptibility to misinformation is consistent across question framings and response modes and better explained by myside bias and partisanship than analytical thinking.* Judgment and Decision Making, 17(3), 547–573. http://journal.sjdm.org/22/220228/jdm220228.pdf.
14. SMELTER, T. J. – CALVILLO, D. P. (2020): *Pictures and repeated exposure increase perceived accuracy of news headlines.* In: Aplied Kognitive Psychology. 34 (5), 1061–1071. 2020. [online] [cit. 3-11-2023]. Dostupné na internete: https://doi.org/10.1002/acp.3684.
15. ŠIŠULÁK, S. – CICHOVÁ, M. (2019): Fake news a propaganda v kybernetickom priestore In: *Aktuálne výzvy kybernetickej bezpečnosti v podmienkach bezpečnostných zložiek*: Bratislava: Akadémia PZ - K informatiky a manažmentu, 2019. - S. 156.
16. VELLANI, V. – ZHENG, S. – ERCELIK, D. – SHAROT, T. (2023): *The illusory truth effect leads to the spread of misinformation,* Cognition, Volume 236, 2023, ISSN 0010-0277, 2023. [online] [cit. 3-11-2023]. Dostupné na internete: https://doi.org/10.1016/j.cognition.2023.105421.
17. VOGEL, I. – HALVANI, O. a kol. (2020): *Desinformation aufdecken und bekämpfen. Interdisziplinäre Ansätze gegen Desinformationskampagnen und für Meinungspluralität*. 10.5771/9783748904816.
18. VRABEC, N. (2007): *Úroveň mediálnej gramotnosti mladých ľudí na Slovensku.* Výskumná správa vypracovaná pre organizáciu IUVENTA 2007. [online] [cit. 3-11-2023]. Dostupné na internete: https://www.iuventa.sk/files/documents/7_vyskummladeze/spravy/davm018/zver_spravadavm018.pdf.
19. VRABEC, N. – PETRANOVÁ, D. (2015): *Mediálna gramotnosť dospelej populácie v SR.* Univerzita sv. Cyrila a Metoda v Trnave, Fakulta masmediálnej komunikácie, Trnava 2015 S.179. ISBN: 978-80-8105-759-5.
20. ZALEWSKI, P. (2022): *New Technologies, Information, Disinformation, Fake News, Deepfake, Hate. Mechanisms of Manipulation in the Digital Space as a Threat to Security in the 21st Century* In: Przegląd Policyjny - The Police Review. - ISSN 2719-9614 - Roč. 146, č. 2(2022), - s. 293-317.

Tento článok bol spracovaný v rámci medzinárodnej vedeckovýskumnej úlohy č.: APZ-OVVP-14-2023 „Dezinformácie ako súčasť hybridných hrozieb pre demokratickú spoločnosť a ich vnímanie študentmi vysokých škôl“ (VÝSK 268).

ADDRESS & ©

doc. Ing. Mária SABAYOVÁ, PhD.
Akadémia Policajného zboru
Sklabinská 1
817 35 Bratislava
Slovenská republika
maria.sabayova@akademiapz.sk
ORCID: 0000-0003-3870-5500

BEZPEČNOST • SAFETY

DOI: 10.36682/a_2024_1_6

BEZPEČNOSTNÉ RIZIKÁ ŠÍRENIA DEZINFORMÁCIÍ NA INTERNETE PROSTREDNÍCTVOM NÁSTROJOV UMELEJ INTELIGENCIE

The security risks of creating and distributing disinformation on the internet using artificial intelligence tools

Jana ZACHAR KUCHTOVÁ

Bratislava, Slovak Republic

ABSTRAKT: Implementácia umelej inteligencie do internetových procesov má okrem svojich nepopierateľných pozitív aj výrazné negatíva, ktoré sa prejavujú predovšetkým v bezpečnosti na internete. Hlavným cieľom článku je identifikácia možného zneužitia umelej inteligencie prostredníctvom tvorby a šírenia obsahu za účelom nekalých praktík smerovaných na konečného internetového používateľa a návrh odporúčaní, ktoré týmto rizikám pomôžu predísť alebo ich minimalizujú. Pre dosiahnutie hlavného cieľa článku bol realizovaný hĺbkový rozhovor s odborníkom na produkciu a šírenie obsahu na internete. Výsledky článku identifikujú tri kľúčové oblasti, ktoré pomôžu s prevenciou a minimalizáciou škôd spôsobených konzumáciou obsahu vyprodukovaného a šíreného umelou inteligenciou.

Kľúčové slová: bezpečnosť – bezpečnostné riziká – internet – šírenie obsahu – dezinformácie – umelá inteligencia.

ABSTRACT: The implementation of artificial intelligence in Internet processes has undeniable positives, but also significant negatives, which are mainly manifested in the area of Internet security. The main objective of the paper is to identify possible misuse of AI through the creation and dissemination of content for the purpose of unfair practices targeted at the end Internet user and to propose recommendations that will help prevent or minimize these risks. To achieve the main objective of the paper, an in-depth interview was conducted with an expert in content creation and dissemination on the Internet. The results of the paper enable identifying three key areas that will help prevent and minimize the damage caused by consuming content created and disseminated by artificial intelligence.

Key words: security – security risks – internet – content distribution – disinformation – artificial intelligence.

ÚVOD

Internetoví používatelia využívajú celosvetovo stovky miliónov zariadení, ktoré sú pripojené k internetu, a ktoré sú prostredníctvom zdieľaných sietí dostupné komukoľvek s prístupom (Yang et al., 2019). Nakoľko neustále dochádza k rozvoju nových technologických oblastí, odborníci strácajú schopnosť reagovať v takom rozsahu a dostatočnou rýchlosťou, ako by bolo potrebné, či už výskumne, intervenčne alebo preventívne (Hajdúková, 2022). Tieto zariadenia môžu byť kompromitované s cieľom negatívne ovplyvniť konkrétnu osobu alebo organizáciu, alebo dokonca celú krajinu. Do nedávna bol na monitorovanie týchto zariadení využívaný manuálny prístup, ktorý bol časovo a finančne náročný (Lavrenovs et al., 2020). Súčasná umelá inteligencia však umožňuje automatizáciu týchto procesov, čo vytvára nové riziká pre používateľov internetu (Zhang & Yang, 2023). Zber dát o aktivitách používateľov prostredníctvom nových prístupoch založených na strojovom učení a umelej inteligencii na internete je bežnou praktikou, ktorá je v už dlhšiu dobu využívaná primárne pre marketingové účely (Guha et al., 2008). V nesprávnych rukách však tieto technologické prístupy môžu predstavovať výrazné bezpečnostné riziká.

Okrem štandardných zariadení určených na konzumáciu internetu sa inteligentné prvky dostávajú aj do ďalších zariadení, ktoré sumárne možno nazvať Internet vecí. Zariadenia, ktoré využívajú internet čelia kvôli umelej inteligencii štyrom základným rizikám, ktorými sú: overovanie zariadení, obrana proti útokom typu DoS (Denial of Service) a DDoS (Distributed Denial of Service), prieniky do zariadení a malvér (Wu et al., 2020). Uvedené zároveň znamenajú slabé miesta, ktorých narušenie predstavuje bezpečnostné riziká internetových používateľov. Pre nalomenie bezpečnosti sú v súčasnej dobe frekventovane využívané metódy strojového učenia a hĺbkového učenia (Al-Garadi et al., 2020). Podľa štúdií jedinou možnosťou ako sa týmto útokom brániť je implementovať bezpečnostné procesy a softvéry založené totožne na procesoch umelej inteligencie (Chen et al., 2017). Práve tieto prístupy majú najvyšší potenciál znížiť bezpečnostné riziká a zabezpečiť bezpečnejšie používanie zariadení pripojených k internetu (Demontis et al., 2019).

Bezpečnosť na internete sa pri súčasnom trende využívania prístupov založených na veľkých dátach, ktoré sú procesované strojovým a hĺbkovým učením a ďalšími prístupmi založenými na umelej inteligencia stáva ešte väčšou témou pre bezpečnostné zložky krajín a relevantné organizácie (Bertino, 2016). To vytvára priestor pre nové prístupy, ktoré štandardné pohľady na vývoj intenretových aplikácii typu SaaS (Software as a Servise) a pod. Obohacujú o nový prístup SecaaS – Security as a Service (Bhattasali & Chaki, 2016). Umelá inteligencia a jej prístupy sú predmetom výskumu a praktickej aplikácie predovšetkým

softvérových inžinierov. Dopady nekalého využitia umelej inteligencie však znášajú koneční internetoví používatelia.

Umelá inteligencia môže byť zneužitá napríklad pri šírení rôznych druhov dezinformácií v podobe zavádzajúcich, skreslených, pozmenených a/alebo úmyselne nepravdivých informácií za účelom získania určitého politického, ekonomického alebo iného profitu (Ivančík – Müllerová, 2022). Taktiež môže byť zneužitá pri šírení hybridných hrozieb zvlášť nebezpečných pre demokratické spoločnosti (Ivančík, 2022), ale aj pri zneužití autorských práv týkajúcich sa obsahu na internete, na analýzu písaného textu (Lee et al., 2020), manipuláciu obrazu prostredníctvom tzv. deep fake prístupov (Kunkel, 2023), imitáciu a rozpoznávanie reči a ďalšieho zvuku (He et al., 2023) a mnoho ďalších. Je preto nevyhnutné poznať všetky druhy obsahu, možnosti ich šírenia k finálnym konzumentom a identifikovať prevenčné opatrenia, ktoré úplne zabraňujú alebo minimalizujú negatívne efekty spôsobené využitím umelej inteligencie pri tvorbe a distribúcii obsahu.

METODIKA A CIEĽ

V úvode výskumnej práce bol realizovaný rešerš teoretických zdrojov so zameraním na domáce a zahraničné časopisecké a internetové zdroje renomovaných autorov. Rešerš prebiehal na tému umelej inteligencie, jej prítomnosti a využitia na internete a možností využitia umelej inteligencie na internete na nekalé účely, vrátane šírenia dezinformácií. Pri teoretickom rešerši bola vytvorená poznatková báza, ktorá pomohla identifikovať tematické okruhy v oblasti umelej inteligencii a bezpečnosti, ktorým v doterajšom výskume a v doterajších publikáciách bolo venované limitované množstvo pozornosti. Hlavným cieľom článku je identifikovať možné zneužitie umelej inteligencie na internete za účelom nekalých praktík smerovaných na konečného používateľa a navrhnúť odporúčania ako týmto hrozbám prechádzať alebo minimalizovať ich negatívne dopady. Pre dosiahnutie identifikovaného cieľa článku boli identifikované formy médií využívané na internete a boli pomenované nástroje umelej inteligencie, ktoré sú tieto formáty schopné produkovať. Za účelom identifikácie internetových kanálov distribúcie týchto formátov bol realizovaný hĺbkový rozhovor s manažérom digitálno-technologického oddelenia firmy, ktorá pôsobí ako prevádzkovateľ slovenských internetových médií a e-shopov. Realizovaný hĺbkový rozhovor mal trvanie približne tridsať minút, prebiehal voľnou diskusiou, ktorá bola tematicky koordinovaná zo strany autorky článku. Tematicky bola diskusia smerovaná k produkcii a distribúcii obsahu na internete, k využitiu umelej inteligencie v týchto procesoch a k možnostiam zneužívania umelej inteligencie na internete za účelom nekalých aktivít ohrozujúcich bezpečnosť jednotlivcov alebo celých organizácií. Výsledkom

diskusie je konštrukcia odporúčaní, ktoré pomôžu predchádzať úspešným útokom ohrozujúcich bezpečnosť na internete vytvorených umelou inteligenciou.

VÝSLEDKY A DISKUSIA

Výsledky realizovanej diskusie s respondentom počas hĺbkového rozhovoru odhalili nasledujúce zistenia, ktoré autorka článku systematizovala a kategorizovala pre dosiahnutie uceleného pohľadu na predmetnú problematiku. Vybrané časti ďalšieho textu boli doplnené o vlastné poznatky nadobudnuté pedagogickou činnosťou a doterajšou výskumnou činnosťou autorky.

V súčasnosti existujú stovky až tisíce internetových nástrojov, ktoré pracujú na základe umelej inteligencie a sú schopné vytvárať a distribuovať obsah na Internete. Pre vytvorenie prehľadu týchto nástrojov je nevyhnutné vytvoriť kategórie, do ktorých budú tieto internetové nástroje zaradené:

- *Produkcia a distribúcia obsahu na internete* – webstránky a obsah na internete sú v dnešnej dobe kvôli vysokej konkurencii a saturácii internetového priestoru webstránkami a obsahom neviditeľné. Je preto nevyhnutné poznať obsahové formáty a možnosti ich distribúcie k cieľovým skupinám. Základné formy obsahu využívané na internete sú:
    - *Text* – nástroje umelej inteligencie, ktoré dokážu generovať text, ktorý je použitý na internete ako článok, reklamná správa, správa v komunikačnej aplikácii atď.. Azda najznámejším nástrojom je ChatGPT. Existuje aj mnoho ďalších, napríklad Copy.ai, Wordtune, Writesonic atď.
    - *Obrázky* — nástroje umelej inteligencie, ktoré dokážu generovať obrázky vo forme fotografií alebo animácií. Tieto obrázky môžu byť generované v rôznych formátoch (najpoužívanejšie .jpg, .png a pod.). Tieto obrázky môžu byť následne použité v profiloch na sociálnych sieťach v článkoch, v súkromných správach, v emailovej komunikácii atď. Najznámejšie a najpoužívanejšie nástroje na generovanie obrázkov na základe umelej inteligencie sú Dall-e, Midjourney, Craiyon, a mnoho ďalších.
    - *Videá* – nástroje umelej inteligencie, ktoré dokážu generovať videá vo forme animácií alebo kamerových záznamov. Tieto videá môžu byť podobne ako obrázky použité ako obsah v článkoch, súkromných správach, emailovej komunikácii atď.. Za najznámejšie a najrozšírenejšie nástroje umelej

inteligencie dedikované produkcii video obsahu možno označiť Veed.io, InVideo, Elai.io a mnoho ďalších. Výstupy nástrojov umelej inteligencie v oblasti videa sú v súčasnosti najmenej dôveryhodné. Môže zato komplexnosť video výstupu, ktorá pracuje s veľkým množstvom obrázkov, ktoré sa vo vysokej rýchlosti premietajú a vytvárajú dynamický video efekt a s audio súbormi.

- *Audio* – nástroje umelej inteligencie, ktoré dokážu generovať audio súbory a zvukové záznamy. Tieto výstupy môžu byť použité vo videách, v súkromných správach používateľov, v emailovej komunikácii, na sociálnych sieťach atď.. Najznámejšie a najpoužívanejšie nástroje umelej inteligencie využívané na produkciu zvukových záznamov sú Landr, Descript, Mubert a mnoho ďalších.
- *Kombinácia* – v praxi sa možno často stretnúť s kombináciou týchto formátov. Texty vygenerované prostredníctvom nástrojov umelej inteligencie sú doplnené o obrázky, videá alebo zvukové záznamy taktiež vytvorené umelou inteligenciou. Využívaním kombinácie týchto formátov možno vytvárať celé články, webstránky a ďalšie mediálne formáty a internetové platformy. V optimálnom prípade takéto služby prinášajú svojim používateľom osoh, ktorý uspokoj informačnú potrebu. V horších prípadoch sú tieto formáty a platformy využívané na naručenie bezpečnosti používateľov za účelom nekalých praktík.
- *Alternatívne reality* – technologický pokrok umožňuje vytvárať alternatívne reality, ktoré realitu rozširujú o ďalšie grafické prvky (augumentovaná realita – AR) alebo vytvárajú realitu úplne novú (virtuálna realita – VR). Aj tento formát pracuje so základnými formátmi (texty, obrázky, videá a zvuk) avšak pracujú s nimi na vysokej technologickej úrovni. AR a VR sú zatiaľ v počiatkoch, avšak už aj tu možno nachádzať nekalé praktiky, ktoré konzumentovi tohto typu média môžu narušiť bezpečnosť.

- *Programovanie* – súčasné programy umelej inteligencie môžu slúžiť ako asistent programátorov, ktorí s nápoveďou umelej inteligencie dokážu pracovať v programovacom jazyku rýchlejšie a efektívnejšie. Táto efektivita pomáha rýchlejšiemu spúšťaniu informácií, čím exponenciálne akceleruje technologický vývoj.

Na druhej strane však zefektívnenie programovacích schopností môže viesť k intenzívnejšiemu narúšaniu bezpečnosti z viacerých zdrojov, čím sa vytvorí pre ohrozeného používateľa ešte väčší zmätok ako doteraz. Medzi asistentov programátorov pracujúcich na základe umelej inteligencii možno zaradiť TabNine, Kite, DeepCode a mnoho ďalších.

- *Marketing* – možno sem zaradiť nástroje umelej inteligencie, ktoré pracujú s analýzou používateľského správania na internete, analýzou webstránky a ďalších internetových platforiem, zákazníckou podporou, optimalizáciou internetovej zákazníckej cesty atď. Medzi tieto nástroje možno zaradiť Jasper, SecondBrain, Chatguel, Kustomer a mnoho ďalších.

- *Práca s ľuďmi* – umelá inteligencia má svoje miesto aj v procesoch práce s ľuďmi. Nástroje umelej inteligencie dokážu byť nápomocné už pri identifikácií potenciálnych uchádzačov v náborovej fáze procesu, pomáha s identifikáciou a testovaním relevantných zručností a vedomostí uchádzačov, pomáha s nastavením odmeňovacieho procesu a s vyhodnocovaním reálnych schopností po uzatvorení pracovného pomeru. Podobne ako pri programovaní aj v HR procesoch v súčasnej dobe pôsobí umelá inteligencia ako asistencia k náborovým odborníkom.

Umelá inteligencia na Internete môže mať na bezpečnosť používateľov pozitívny alebo negatívny vplyv:

- *Pozitívny vplyv umelej inteligencie na internete na používateľov internetu* – umelá inteligencia na internete dokáže monitorovať a detekovať podozrivé správanie iných používateľov alebo internetových softvérov na internete a podozrenie dokáže interpretovať používateľovi internetu. Výstraha pred podozrivým správaním tak môže slúžiť ako prevencia pred nebezpečnými praktikami na internete. Umelá inteligencia ďalej dokáže efektívne pomáhať používateľom internetu bezpečnosťou prostredníctvom navigácie pre vytvorenie silných hesiel, správy hesiel do rôznych internetových platforiem a s ďalšou autentifikáciou, ktorá môže pracovať aj s behaviorálnymi alebo inými prvkami jednotlivca. Okrem prevencie dokáže umelá inteligencia pomáhať s bezpečnosťou aj formou okamžitej reakcie pri prebiehajúcich nekalých aktivitách, ktoré narušujú bezpečnosť na internete. Monitorovacie systémy založené na umelej inteligencii dokážu útok rozpoznať a okamžite implementovať bezpečnostné prvky, ktoré minimalizujú možné vzniknuté škody. Okrem prevencie a

minimalizácie bezpečnostných rizík umelá inteligencia dokáže zistiť rozsah škôd, ktoré možné internetové útoky jednotlivcom alebo celým organizáciám spôsobili. Pozitívne vplyvy tak možno kategorizovať na:

  - *prevenčné,*
  - *minimalizačné,*
  - *monitorovacie.*

- *Negatívny vplyv umelej inteligencie na internete na používateľov internetu* – umelá inteligencia vytvára príležitosti pre nekalé praktiky, ktorých cieľom je narušiť bezpečnosť používateľov internetu. Môže ísť predovšetkým o využitie umelej inteligencie na kybernetické útoky a synchronizáciu niekoľkých útokov, praktiky spojené s narušením súkromia, napríklad vo forme monitorovania a vyhodnocovania aktivít používateľa na sociálnych sieťach alebo sledovaním jeho aktivít v internetovom prehliadači alebo na iných internetových platformách, využívanie umelej inteligencie pre automatizovanú produkciu obsahu, ktorej účelom je diskriminácia, kyberšikana, poškodzovanie reputácie a ďalšie formy útokov, alebo na implementáciu a automatizáciu sociálneho inžinierstva, ktoré má spravidla priamy negatívny vplyv na finančné zázemie jednotlivca alebo celých organizácií a masové vytváranie a šírenie dezinformácií.

Medzi bezpečnostné riziká umelej inteligencii na internete patrí predovšetkým produkcia a distribúcia zámerne skresleného obsahu, ktorý je prispôsobený pre dosiahnutie nekalých aktivít na internete, ktorých cieľom je poškodiť konečného používateľa. Pre tvorbu obsahu sa používajú v predošlom texte spomenuté texty, obrázky, videá, zvukové záznamy a ich kombinácie. Pre dosiahnutie akejkoľvek dobre alebo zle myslenej aktivity na internete je nevyhnutné vyprodukovať obsah, ktorý aktivitu charakterizuje a vyzve používateľa k akcii. Umelá inteligencia môže mať pri troche snahy výrazný podpis na zneužitie tejto produkcie na nekalé účely a na ovplyvnenie názoru používateľa.

Ďalším krokom v procese využitia umelej inteligencie na nekalé úmysly a na poškodenia používateľa internetu je obsah nevyhnutné distribuovať internetovými kanálmi k používateľovi. Obsah k používateľovi možno dostať hneď niekoľkými internetovými kanálmi: prostredníctvom internetového prehliadača zadaním adresy webstránky do vyhľadávacieho poľa, prostredníctvom internetových vyhľadávačov prostredníctvom zadania vyhľadávaných pojmov do vyhľadávacieho poľa, prostredníctvom sociálnych sietí,

internetových blogov a diskusných fór, prostredníctvom email marketingu, prostredníctvom priamych správ v komunikačných aplikáciách a pomocou uverejňovania v médiách. Takmer všetky z uvedených majú organické a platené možnosti šírenia obsahu.

Negatívnym vplyvom umelej inteligencie na internete na jednotlivcov alebo organizácie možno predchádzať nasledujúcimi aktivitami:

- *Edukáciou* – informovanosť jednotlivcov a celých organizácií o možných hrozbách a možných negatívnych scenároch dokáže mať prevenčný efekt, vďaka ktorému internetoví používatelia dokážu rozoznať možne hrozby spôsobené umelou inteligenciou, kriticky hrozbu vyhodnotiť a limitovať alebo úplne stopnúť prebiehajúcu aktivitu, ktorá by mohla mať negatívny bezpečnostný efekt.
- *Technológiou* – organizácie, ktoré stoja za vývojom internetových aplikácií, softvérov a platforiem musia už pri návrhu, produkcii a testovaní týchto aplikácií poznať všetky bezpečnostné riziká spojené s umelou inteligenciou na internete a musia týmto rizikám podrobiť testovanie svojich internetových platforiem. Umelá inteligencia kontinuálne evolvuje, a preto je nevyhnutné pre prevádzkovateľov internetových platforiem neustále internetové platformy optimalizovať, monitorovať nové generácie umelej inteligencie a chrániť svojich používateľov vlastnými bezpečnostnými mechanizmami alebo mechanizmami tretích strán.
- *Reguláciou* – z mediálneho uhla pohľadu je internet takmer jediné neregulované (alebo len veľmi obmedzene regulované médium). Nástup umelej inteligencie absenciu tejto regulácie ešte viac zvýrazňuje. Je nevyhnutné aby relevantné orgány a inštitúcie na celosvetovej, európskej alebo minimálne lokálnej štátnej úrovni prevzali aspoň čiastočnú zodpovednosť za aktivity na internete a usmernili ich prostredníctvom zmysluplných regulácií v záujme bezpečnosti konečného internetového používateľa. Implementácia regulácii a direkcia v oblasti využívania bezpečnostných prvkov schopných pracovať s umelou inteligenciou.

ZÁVER

Implementácia nástrojov umelej inteligencie do internetových nástrojov a procesov predstavuje prirodzenú evolúciu internetu. Okrem pozitív, ktoré v súčasnej dobe prevyšujú negatíva, však vytvára umelá inteligencia priestor pre nový typ ohrozenia bezpečnosti internetových používateľov. Tieto riziká môžu mať pre jednotlivcov alebo celé organizácie často fatálne následky. Umelá inteligencia dokáže výrazne urýchliť produkciu a distribúciu dezinformácií vytvorených za účelom narušenia bezpečnosti, na základe čoho sú používatelia internetu vystavení nekalým praktikám častejšie a v dôveryhodnejšej forme ako doteraz. Napriek výraznej inovácii tak umelá inteligencia na internete vytvára mnohé etické, morálne a predovšetkým bezpečnostné dilemy, ktoré v súčasnej dobe nie sú predmetom verejnej spoločenskej diskusie. Umelá inteligencia má významný vplyv na vytváranie textu, obrázkov, videí a zvukového obsahu, dokáže asistovať programátorom, marketérom, personalistom a ľuďom z mnoho ďalších pracovných zameraní. Postupne sa stane súčasťou všetkých pracovných pozícií a postupne začne suplovať pracovnú náplň vybraných pracovných pozícií. Negatívne aspekty využívania umelej inteligencie na internete sú badateľné predovšetkým v šírení dezinformácií v podobe rôznych skreslených, pozmenených alebo zavádzajúcich informácií, kybernetických útokoch, monitorovaní digitálnych stôp a automatizácii a personalizácii produkcie a distribúcie obsahu na internete. V prípade zneužitia umelej inteligencie na nekalé praktiky môže dôjsť k manipulácii verejnej mienky, k poškodeniu reputácie jednotlivca alebo celej organizácie, zneužitiu osobných údajov, krádeži identity, neoprávnenému využitiu finančných prostriedkov atď. Umelá inteligencia dokáže dnes asistovať pri akejkoľvek nekalej praktike na internete a dokáže ju výrazne zefektívniť a urýchliť. Nachádzanie riešení v oblastí zneužitia umelej inteligencie na internete si vyžadujú systematický a komplexný prístup, ktorý zahŕňa edukáciu, technologickú pripravenosť a implementáciu regulácií. Pre bezpečné vykonávanie aktivít na internete v dobe umelej inteligencie je nevyhnutné, aby spoločnosť dosiahla rovnováhu medzi inováciami a bezpečnosťou.

POUŽITÁ LITERATÚRA A INFORMAČNÉ ZDROJE:

1. AL-GARADI, M. A. – MOHAMED, A. – AL-ALI, A. K. – DU, X. – ALI, I., –GUIZANI, M. (2020): A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security. In *IEEE Communications Surveys and Tutorials*, roč. 22, š. 3, 2020, s. 1646-1685. [online] [cit. 20-11-2023] Dostupné na: <https://doi.org/10.1109/COMST.2020.2988293>
2. BERTINO, E. (2016): Big Data Security and Privacy. In J. Joshi, G. Karypis, L. Liu, X. Hu, R. Ak, Y. Xia, W. Xu, A. H. Sato, S. Rachuri, L. Ungar, P. S. Yu, R. Govindaraju, & T. Suzumura (Eds.): *IEEE International Conference on Big Data*, 2016.
3. BHATTASALI, T. – CHAKI, N. (2016): Poster: Exploring Security as a Service for IoT Enabled Remote Application Framework. In *Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services Companion*, 2016, s. 15-15. [online] [cit. 20-11-2023] Dostupné na: <https://doi.org/10.1145/2938559.2948769>
4. DEMONTIS, A. – MELIS, M. – BIGGIO, B. – MAIORCA, D. – ARP, D. – RIECK, K. – CORONA, I. – GIACINTO, G. – ROLI, F. (2019): Yes, Machine Learning Can Be More Secure! A Case Study on Android Malware Detection. In *IEEE Transactions on Dependable and Secure Computing*, roč. 16, č. 4, 2019, s. 711-724. [online] [cit. 20-11-2023] Dostupné na: <https://doi.org/10.1109/TDSC.2017.2700270>
5. GUHA, S. – MUNAGALA, K. – SARKAR, S. (2008): Information Acquisition and Exploitation in Multichannel Wireless Networks.
6. HAJDÚKOVÁ, T. (2022): Zneužívanie elektronických služieb na sexuálne zneužívanie detí. In *Bezpečnosť elektronickej komunikácie : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava: Akadémia Policajného zboru, 2022, s. 71-85. ISBN 978-80-8054-968-8.
7. HE, Y. – SENG, K. P. – ANG, L. M. (2023): Generative Adversarial Networks (GANs) for Audio-Visual Speech Recognition in Artificial Intelligence IoT. In *Information*, roč. 14, č. 10. ISSN 1422-3988. [online] [cit. 20-11-2023] Dostupné na: <https://doi.org/10.3390/info14100575>
8. CHEN, L. – YE, Y. – BOURLAI, T. (2017): Adversarial Machine Learning in Malware Detection: Arms Race between Evasion Attack and Defense. In *2017 European Intelligence and Security Informatics Conference (EISIC)*, 2017, s. 99-106. [online] [cit. 16-11-2023] Dostupné na: <https://doi.org/10.1109/EISIC.2017.21>
9. IVANČÍK, R. (2022). Dezinformácie ako hybridná hrozba. In *Dezinformácie a právo (úlohy a postavenie bezpečnostných zložiek) – zborník príspevkov z vedeckej konferencie*

s medzinárodnou účasťou. Bratislava : Akadémia Policajného zboru, 2022, s. 54-65. ISBN 978-80-8054-965-7.

10. 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.
11. KUNKEL, M. (2023). Bildmanipulation durch künstliche Intelligenz – Risiken für Deepfakes in der Wissenschaft. In *Die MKG*, 2023, roč. 16, č. 1, s. 61-62. [online] [cit. 21-11-2023] Dostupné na: <https://doi.org/10.1007/s12285-022-00391-0>
12. LAVRENOVS, A. – GRAF, R. – HEINAARO, K. (2020): Towards Classifying Devices on the Internet Using Artificial Intelligence. In *12th International Conference on Cyber Conflict (CyCon)*, 2020, s. 309-325. [online] [cit. 20-11-2023] Dostupné na: <https://doi.org/10.23919/CyCon49761.2020.9131713>
13. LEE, L. W. – DABIRIAN, A. – McCARTHY, I. P. – KIETZMANN, J. (2020): Making sense of text: artificial intelligence-enabled content analysis. In *European Journal of Marketing*, roč. 54, š. 3, 2020, s. 615-644. ISSN 1758-7123. [online] [cit. 21-11-2023] Dostupné na: <https://doi.org/10.1108/EJM-02-2019-0219>
14. WU, H. – HAN, H. – WANG, X. – SUN, S. (2020): Research on Artificial Intelligence Enhancing Internet of Things Security: A Survey. In *IEEE Access*, 8, 2020, s. 153826-153848. [online] [cit. 21-11-2023] Dostupné na: <https://doi.org/10.1109/ACCESS.2020.3018170>
15. YANG, K. – LI, Q. – SUN, L. (2019): Towards automatic fingerprinting of IoT devices in the cyberspace. In *Computer Networks*, 2019, roč 148, s. 318-327. ISSN 1944-1568. [online] [cit. 21-11-2023] Dostupné na: <https://doi.org/10.1016/j.comnet.2018.11.013>
16. ZHANG, Y. – YANG, N. (2023): Internet Information and Collection and data Analysis based on Artificial Inteligence. In *Mechatronic Systems and Control*, 2023, roč. 51, č. 10, s. 1-9. ISSN 2561-178X. [online] [cit. 21-11-2023] Dostupné na: <https://doi.org/10.2316/J.2023.201-0348>

ADDRESS & ©

kpt. JUDr. Jana ZACHAR KUCHTOVÁ
Akadémia Policajného zboru
Sklabinská 1
817 35 Bratislava
Slovenská republika
jana.kuchtova@akademiapz.sk
ORCID: 0000-0003-2536-1057

RECENZNÍ ŘÍZENÍ PRO Č. 1/2024

Jednotliví oponenti (7) recenzovali 1–2 články. Redakce od nich obdržela na každý příspěvek 1–2 posudky, celkem 11 posudků.

doc. Ing. Vladimír **ANDRASSY**, PhD.	Katedra bezpečnosti a obrany, Akademie ozbrojených sil generála M. R. Štefánika, Liptovský Mikuláš, **SR**
doc. Ing. Roman **HORÁK**, PhD.	Katedra řízení zdrojů, Fakulta vojenského leadershipu, Univerzita obrany, Brno, **ČR**
doc. RNDr. Tatiana **HEJDÚKOVÁ**, PhD.	Katedra informatiky a manažmentu, Akadémia policajného zboru v Bratislavě, Bratislava, **SR**
doc. Ing. Radoslav **IVANČÍK**, PhD. et PhD., MBA	Katedra informatiky a manažmentu, Akademia policajného zboru v Bratislavě, Bratislava, **SR**
PhDr. Štěpán **KAVAN,** Ph.D.	Katedra právní oborů a bezpečnostních studií, Vysoká škola evropských a regionálních studií z. ú., České Budějovice, **ČR**
Dr.h.c. prof. Ing. Pavel **NEČAS**, PhD.	Katedra bezpečnostních štúdií, Fakulta politických vied a medzinárodných vzťahov, Banská Bystrica, **SR**
doc. Ing. Mária **SABAYOVÁ**, PhD.	Katedra společenských vied, Akadémia policajného zboru v Bratislavě, Bratislava, **SR**

POČET OBDRŽENÝCH VĚDECKÝCH ČLÁNKŮ:	6
POČET RECENZOVANÝCH VĚDECKÝCH ČLÁNKŮ:	6
POČET OBDRŽENÝCH RECENZNÍCH POSUDKŮ:	11
POČET PUBLIKOVANÝCH VĚDECKÝCH ČLÁNKŮ:	6

O ČASOPISU

Základní charakteristika

Časopis Auspicia je nezávislým recenzovaným vědeckým časopisem pro otázky společenských a humanitních věd. Obsah časopisu prezentuje původní vědecké příspěvky, které jsou orientované na stěžejní obory zaměření periodika a rovněž v současnosti významné a řešené problémy. Mnohé z nich podávají formou přehledových studií návrh na reálné řešení konkrétních problémů, polemik ve smyslu akademické plurality názorů.
Historicky je založen na 5 základních a respektovaných principech:

- řádné a přísné recenzní řízení;
- mezinárodnost;
- otevřenost;
- výběrovost;
- kontinuální zvyšování kvality.

Historie

Časopis Auspicia je vydáván od r. 2004 Vysokou školou evropských a regionálních studií (VŠERS) a Vysokou školou technickou a ekonomickou (VŠTE) dvakrát ročně, pouze elektronicky. V dosavadních 41 číslech bylo otištěno zhruba 860 příspěvků a recenzí.

Rada pro výzkum, vývoj a inovace jako odborný a poradní orgán vlády ČR zařadila časopis Auspicia (ISSN 1214-4967) pro léta 2008–2013 a znovu pro rok 2015 (http://www.vyzkum.cz/FrontClanek.aspx?idsekce=733439) mezi recenzované neimpaktované časopisy, které uvedla v oborech Národního referenčního rámce excelence (NRRE).

V roce 2016 byl recenzovaný vědecký časopis Auspicia zařazen do mezinárodní databáze ERIH PLUS a od roku 2024 do online knihovny pro střední a východní Evropu – CEEOL.

Tematické sekce

Na základě úspěšného recenzního řízení jsou jednotlivé vědecké příspěvky řazeny do sekcí:

1. Společenské vědy
2. Bezpečnost
3. Veřejná správa, řízení
4. Recenze

<u>Základní pokyny autorům</u>

Jazyk vědeckého příspěvku: angličtina, čeština; **recenze**: angličtina, čeština, Články mohou být psány v angličtině nebo češtině, ale vzhledem k mezinárodnímu rozměru časopisu jsou preferovány anglické články.

Požadovaný rozsah v sekcích 1–3: max.8 normostran (1NS – 1800 znaků včetně mezer).

Data uzávěrek: 1. číslo – 1. 2. • 2. číslo – 1. 8.

Použitá literatura: 25 % zdrojů indexovaných v databázích Web of Science a/nebo Scopus.

Recenzní řízení: oboustranně anonymní, nezávislé, objektivní.

Data vydání: 1. číslo – 1. 6. • 2. číslo – 1. 12.

Podrobný zdroj: https://vsers.cz/auspicia/
Jak citovat vědecký příspěvek: In.: Pro autora. Šablona článku – https://vsers.cz/auspicia/

Autorský poplatek: Za výdaje spojené s uveřejněním vědeckého příspěvku v českém jazyce (příspěvky v angličtině jsou do odvolání dočasně bezplatné) v délce **max. 8 normostran** v sekcích 1–3 hradí autor částku **1 000,- CZK** *(popř. částku zvýšenou o 200,- Kč za každou další normostranu)*, nebo příslušnou částku v EUR dle aktuálního přepočtu, a to nejpozději do uzávěrky příslušného čísla (tj. před recenzním řízením) převodem na účet vydavatele (VŠERS) u Fio banky, a. s. (pobočka České Budějovice) č. 2101783605/2010, účet EUR/IBAN: CZ71 2010 0000 0024 0178 3607, BIC kód: FIOBCZPPXXX (zahraniční plátci si poplatek za převod hradí sami), nebo v hotovosti na ekonomickém oddělení VŠERS. Variabilním symbolem je IČO autorova pracoviště a specifickým symbolem číselný kód 12342022. Do zprávy pro příjemce se uvede jméno autora / autorů a pracoviště.

Kontaktní adresa:
Vysoká škola evropských a regionálních studií, z. ú.
Žižkova tř. 1632/5b
370 01 České Budějovice
doc. PhDr. Miroslav Sapík, Ph.D.
Telefon: +420 386 116 839
E-mail: sapik@vsers.cz, https://vsers.cz/auspicia/

ABOUT THE JOURNAL

General description

Auspicia is an independent, peer-reviewed scientific journal on the social sciences and humanities. The journal presents original scientific contributions on core areas of its field of focus, as well as currently significant and solved problems. In the form of overview studies, many of them constitute proposals for a real solution to specific problems, polemics in the sense of academic plurality of opinions.

The journal is based on five respected principles:
- proper and rigorous review procedures;
- internationality;
- openness;
- selectivity;
- continuous improvement in quality.

History

Auspicia has been published since 2004 by the College of European and Regional Studies (VŠERS) and the Institute of Technology and Business (VŠTE) twice a year, in electronic form only. So far, 860 scientific contributions and reviews have been published in 42 issues.
The Innovation Council, being a professional and advisory board of the government of the Czech Republic, has included *Auspicia* (ISSN 1214-4967) among reviewed, non-impact scholarly journals involved in the topics of the National Reference Framework of Excellence (NRRE) in 2008–2013, and it was included there again in 2015 (http://www.vyzkum.cz/FrontClanek.aspx?idsekce=733439).

In 2016 *Auspicia* was listed in the international database ERIH PLUS and since 2024, it has been listed in the Central and Eastern Europe Online Library – CEEOL.

Thematic sections

After individual scientific papers successfully pass review, they are allocated towards one of the following sections:

1. Social Sciences
2. Safety
3. Public Administration, Management
4. Reviews

Basic instructions for authors

Language of the scientific paper: English, Czech; **reviews**: English, Czech. Articles can be submitted in either English or Czech, but English articles are preferred due to the international dimension of the journal.

Required range in sections 1–3: maximum 8 standard pages (1 standard page – 1800 characters including spaces).

Deadlines: 1st issue – 1 February, 2nd issue – 1 August.

Bibliography: 25% of resources indexed in Web of Science and/or Scopus databases.

Review process: double-blind, independent, objective.

Publishing dates: 1st issue – 1 June, 2nd issue – 1 December.

Detailed source: https://vsers.cz/recenzovany-vedecky-casopis-auspicia

How to cite a scientific paper: In: For the author. Article template -

https://vsers.cz/vedecky-casopis-auspicia/

Author's fee. Authors of the papers (contributions) are to pay the amount of CZK 1,000 for the expenses connected with publishing the scholarly contributions in the Czech language (contributions in English are temporary free of charge until further notice) of a maximum of 8 standard pages (or that amount plus CZK 200 per each subsequent standard page), or the appropriate amount in EUR in accordance with the current exchange rate in sections 1–3. This must be done by the closing date of the relevant volume (i.e., before the review process) either by means of bank transfer to the publisher's bank account No. 2101783605/2010**,** at Fio Banka, a. s. (České Budějovice branch), account EUR/IBAN code: CZ71 2010 0000 0024 0178 3607, BIC code: FIOBCZPPXXX (foreign payors pay the transfer charge by themselves), or they may pay it in cash at the Department of Economics of the College of European and Regional Studies. Registration numbers of authors' workplaces are variable symbols, the specific symbol is a code with the following digits: 12342022. The information regarding the payee should include the name of the author/authors and their workplace.

Contact address:
The College of European and Regional Studies
Žižkova tř. 1632/5b
370 01 České Budějovice
doc. PhDr. Miroslav Sapík, Ph.D., editor-in-chief
Telephone number: +420 386 116 839
E-mail: sapik@vsers.cz, https://vsers.cz/auspicia/