RIZIKÁ KOMUNIKÁCIE NA SOCIÁLNYCH SIEŤACH

RISKS OF COMMUNICATION ON SOCIAL NETWORKS

Tatiana Hajdúková – Lucia Kurilovská – Samuel Marr

Abstract

One of the priorities of international and national politics today is to support the deployment and development of information and communication technologies in the public sector. The initiative to keep up with the times and remain competitive is manifested on a societal and personal level. The increasing flow of digital data complicates the conditions for ensuring security in the online environment. The aim of the article is to point out the dynamics of the implementation of digital progress in the EU and the Republic of Slovenia in the context of a common user who, even with ignorance, may not be sufficiently aware of the potential threats to which he is exposed when using technology. It is not in the power of the authorities involved in criminal proceedings to ensure individual protection of individuals without their responsibility. The training of individuals for the purpose of responsible správania sa in the online space must be realized parallel to the deployment and development of technologies.

Key words: communication, sensitive data, public administration, security, social networks,

JEL Code: K14, K24

Úvod

Zvyšovanie aktivity ľudí v online prostredí je za posledné desaťročia stúpajúcim trendom, ktorý skôr graduje, ako by bol na ústupe. Plnohodnotný život a fungovanie spoločnosti sa stávajú v plnom význame slova závislé na neustále využívanejších informačných a komunikačných technológiách (IKT) so službami, ktoré sú pomocou nich poskytované. Dotýka sa to prakticky všetkých procesov v spoločnosti, ktoré zabezpečujú jej funkčnosť v dynamicky a vzájomne prepojenom celku. Používanie IKT vo verejnom sektore je prioritou nadnárodných a národných politík, pretože vytvára množstvo pozitívnych efektov v celom verejnom sektore (Jeck, 2017). Podľa (Jeck, 2017) IKT stoja v epicentre štvrtej priemyselnej revolúcie a sú faktorom ekonomických a spoločenských zmien viac ako kedykoľvek predtým. Nemenej významnou mierou, ako pri verejných službách sú využívané na komerčné účely ako aj uspokojovanie

osobných potrieb jednotlivcov, či trávenie ich voľnočasových aktivít. Opodstatnenosť užitočnosti IKT pramení v ich rýchlosti, efektívnosti a masovom rozširovaní do nových oblastí. Ako uvádza (Ivančík, R., Andrassy, V., 2023) vzhľadom na konštatovanú nezvrátiteľnú realitu je dôležité súčasne s ich vymoženosťami uvedomovať si aj ohrozenia, ktorým sú užívatelia vystavení. Podľa (Kopencová, D., Felcan, M., Rak, R., 2020) ich dôležitosť si uvedomujeme najmä v nežiadúcich situáciách, keď dočasne stratia svoju funkčnosť.

Ako upozorňuje (Európska komisia, 2020) pandémia ochorenia COVID-19 ešte viac zviditeľnila existujúce nedostatky v digitálnom hospodárstve Slovenska a v slovenskej spoločnosti, a to aj v oblasti pripojiteľnosti, získavania digitálnych zručností a digitalizácie škôl, domácností, podnikov a verejných služieb. Informačné systémy v nemocniciach, školách a verejných inštitúciách neboli pripravené na náhly prechod na online a diaľkové fungovanie.

Predmetný príspevok kontrastuje veľké očakávania od využívania IKT v ekonomickej, politickej, hospodárskej a kultúrnej sfére spoločnosti so slobodou prejavu a z nej vyplývajúcej nedostatočnej regulácie šírenia škodlivého obsahu. Pretože online prostredie sa pre ľudí stalo významným zdrojom informácií a determinuje tvorbu názorov a zmýšľanie obyvateľstva, cieľom príspevku je meraním posúdiť mieru ich negatívneho vplyvu na správanie ľudí z pohľadu šírenia dezinformácií. Popri štúdiu odbornej literatúry, analýzy a syntézy sme v empirickej časti zrealizovali dotazníkový prieskum.

1 Digitálny kompas pre digitálne desaťročie EÚ

Od roku 2014 Európska komisia každoročne monitoruje digitálny pokrok členských štátov EÚ. Monitorovanie uskutočňuje pomocou tzv. indexu digitálnej ekonomiky a spoločnosti (DESI). Prostredníctvom indexu je sledovaný pokrok v konkurencieschopnosti členských štátov EÚ v kľúčových oblastiach a to: ľudský kapitál, širokopásmová pripojiteľnosť, integrácia digitálnych technológií v podnikoch a digitálne verejné služby. S cieľom zabezpečiť komplexnú a udržateľnú digitálnu transformáciu na úrovni EÚ vo všetkých sektoroch hospodárstva, sú podľa aktuálneho stavu priebežne stanovované ciele, ktoré sa majú dosiahnuť do roku 2030.

Slovensko sa v roku 2022 nachádzalo v indexe digitálnej ekonomiky a spoločnosti (DESI) na nelichotivom 23. mieste spomedzi 27 štátov EÚ, čím sa o 1 miesto zhoršila jeho pozícia z roku 2021. V rámci ukazovateľov v oblasti ľudského kapitálu je situácia indexu DESI na Slovensku najpriaznivejšia, pretože základné digitálne zručnosti vykazuje 55 % Slovákov, čo je o 1 % viac, ako bol dosiahnutý priemer EÚ. Porovnanie DESI upozorňuje na pokračujúce

zaostávanie Slovenska napríklad v nedostatočnom využívali potenciál veľkých dát, umelej inteligencie a systémov elektronického zdieľania informácií (Európska komisia, 2023).
Európska komisia 9. marca 2021 predstavila víziu a spôsoby, ako dosiahnuť digitálnu transformáciu Európy do roku 2030. Komisia navrhuje Digitálny kompas pre digitálne desaťročie EÚ, ktorý sa vyvíja okolo štyroch základných bodov:

- Zručnosti.
- Infraštruktúra.
- Podnikanie.
- Štátna správa.

Dňa 26. januára 2022 Európska komisia navrhla medziinštitucionálne vyhlásenie o digitálnych právach a zásadách digitálneho desaťročia pozostávajúce z nasledovných oblastí:

- Ľudia v centre pozornosti. Digitálne technológie by mali chrániť práva ľudí, podporovať demokraciu a zabezpečovať, aby všetci aktéri v digitálnej oblasti konali zodpovedne a bezpečne. EÚ tieto hodnoty presadzuje na celom svete.
- Solidarita a inklúzia. Technológia by mala ľudí zjednocovať. Každý by mal mať prístup k internetu, digitálnym zručnostiam, digitálnym verejným službám a spravodlivým pracovným podmienkam.
- Slobodná voľba. Ľudia by mali mať k dispozícii spravodlivé online prostredie, byť chránení pred nezákonným a škodlivým obsahom a mať posilnené postavenie pri interakcii s novými a vyvíjajúcimi sa technológiami, ako je umelá inteligencia.
- Participácia. Občania by mali mať možnosť zapojiť sa do demokratického procesu na všetkých úrovniach a mať kontrolu nad svojimi vlastnými údajmi.
- Bezpečnosť a ochrana.

Digitálne prostredie by malo byť bezpečné a chránené. Všetci používatelia by od detstva až po starobu mali požívať posilnené postavenie a byť chránení.

- Udržateľnosť. Digitálne zariadenia by mali podporovať udržateľnosť a zelenú transformáciu. Ľudia musia vedieť o vplyve svojich zariadení na životné prostredie a o ich spotrebe energie.

Digitálne práva a zásady uvedené vo vyhlásení doplnia existujúce práva, ako sú práva zakotvené v Charte základných práv EÚ, a právne predpisy v oblasti ochrany údajov a súkromia. Poskytnú občanom referenčný rámec v oblasti ich digitálnych práv, ako aj

usmernenie pre členské štáty EÚ a spoločnosti pre prácu s novými technológiami. Majú slúžiť na to, aby bol každý v EÚ schopný vyťažiť z digitálnej transformácie čo najviac.

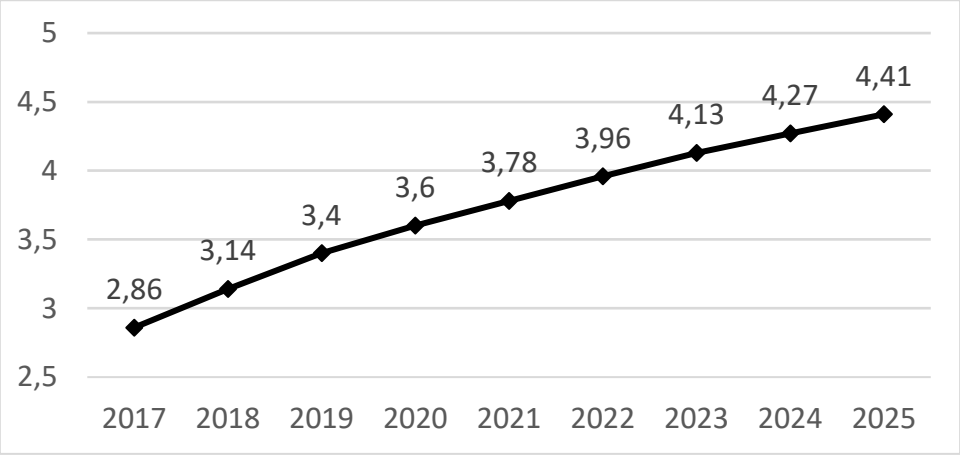
2 Trendy technologického pokroku zdieľanej online komunikácie

Pokrytie internetovou sieťou je aj v súčasnosti dostupnejšie ako kedykoľvek predtým, so zanedbateľnými finančnými nákladmi. (Schwab, 2016) vytipoval niekoľko prelomových technologických a systémových trendov, ktoré by v ekonomike štvrtej priemyselnej revolúcie mali zohrať kľúčovú úlohu:

- digitálna prítomnosť na internete (sociálne médiá);
- rozšírenie zmyslov pomocou internetu (napr. Google Glass);
- umelá inteligencia v rozhodovaní podnikov;
- ekonomika zdieľania, superpočítač do vrecka;
- rozšírenie digitálnych kryptomien;
- 3D tlač (napríklad v zdravotníctve);
- big data;
- neobmedzená a bezplatná pamäťová kapacita;
- autonómne vozidlá;
- využívanie robotov;
- všadeprítomnosť počítačov;
- internet v oblečení a doplnkoch;
- internet všetkého (napríklad zosieťovaná domácnosť);
- . smart mestá.

Využívanie internetového pripojenia neprináša len zvýšenie dynamiky a zjednodušenie procesov v spoločnosti, pozitívne ho možno vnímať v spojitosti s uspokojovaním potrieb ľudí v osobnom živote. Internet vynútil zmeniť tradičné komunikačné médiá na zrýchlené formy ľudskej interakcie prostredníctvom online fór, okamžitých správ a sociálnych sietí. Vzostup digitálnych sociálnych médií potláča rozlišovanie osobného a verejného online priestoru. Mainstreaming internetových funkcií, digitálna hudba a video, obsah vytvorený používateľmi, predaj digitálnych médií, spôsobili pokles spotreby tradičných médií Napriek širokej škále sociálnych médií, v dnešnej dobe sú výrazne najviac obľúbené sociálne siete. Podľa vývoja počtu používateľov sociálnych sietí na celom svete sa odhad budúcnosti vyznačuje zjavným optimizmom narastajúceho trendu, grafe č. 1. Pri odhade vývoja počtu používateľov sociálnych sietí na celom svete od roku 2017 dávame do pozornosti predpoklad nárastu na úrovni približne dvojnásobného počtu používateľov, ktorý by sa mohol dosiahnuť v priebehu desať rokov. Oblasť zdieľanej online komunikácie si vyžaduje globálne aj lokálne strategické plány.

Graf 1 Odhad počtu používateľov (v biliónoch) sociálnych sietí celosvetovo, 2017-2025



Zdroj údajov: Výskumné oddelenie Statista[1]

Medzi rôznorodé najpopulárnejšie činnosti umožňované súčasnou podobou sociálnych sietí patria komunikácia s priateľmi (napríklad Facebook, Twitter a LinkedIn), výmena a zdieľanie fotografií a videí (napríklad Instagram a YouTube), sledovanie noviniek, rozšírenie svojej obchodnej siete prostredníctvom online shopov, blogovacie siete, vizuálne zamerané siete (Pinterest), miesta, kde používatelia zdieľajú záujmy, posielanie textových správ (Facebook Messenger, WhatsApp).

3 Škodlivý obsahu online komunikácie a jeho negatívny dopad na užívateľov

Skúsenosti dokazujú, že ruka v ruke s vývojom technológií a širším využívaním digitálnych technológií a služieb je nevyhnutné súčasne riešiť aj ich ochranu ako aj ochranu ich užívateľov. Želaným stavom je zvyšovanie bezpečnosti a ochrany v protiklade s dostupnejším a intenzívnejšie využívaným internetom. Rozvoj spoločnosti v každej oblasti je determinovaný dosiahnutím stavu bezpečnosti, obzvlášť pri prebiehajúcich intenzívnych snahách o integráciu a globalizáciu. Viacerí autori sa zhodujú (Ivančík, R, Nešas, P., 2023), (Kuchtová, 2022), (Lisoň, M., Hullová, M., 2020) že všetky štáty, organizácie či akékoľvek iné entity sa snažia zaistiť svoju bezpečnosť na čo najvyššej úrovni prostredníctvom efektívneho, účelného a najmä funkčného bezpečnostného systému.

V online priestore ľudia dobrovoľne trávia svoj voľný čas, vzdelávajú sa, hľadajú odpovede, komunikujú, pozerajú videá, počúvajú hudbu, nadväzujú kontakty s novými ľuďmi, zverejňujú svoje postoje a prezentujú sa cez videá a fotky. Z pohľadu nebezpečnosti je obľuba,

[1] Medzinárodná platforma dát z viac ako 22500 zdrojov a 57 krajín sveta.

otvorenosť a verejnosť vystupovania v online priestore ich najväčším rizikom. Mnohým užívateľom sociálnych sietí imponuje sila ich hlasu, množstvo komunikujúcich a prakticky ich nepretržitá prítomnosť.

Jednou z hlavných príčin veľkej skupiny problémov v online priestore spočíva v toku obrovského množstva digitálnych dát, nad ktorými sa ťažko udržiava kontrola nielen z pohľadu ich obsahu ale aj identifikácie komunikujúcich. Skryť sa na otvorenom priestranstve je oveľa náročnejšie až nemožné, v porovnaní s podmienkami v hustom neprehľadnom dave ľudí. Masa ľudí vo väčších vzdialenostiach navzájom splýva a ťažko sa rozlišuje. Limitujúcim faktorom počtu osôb prítomných na konkrétnom mieste je fyzický priestor, pretože každá osoba v prostredí zaberá určitý objem, ktorý obmedzuje hustotu a tým aj počet osôb. Uvedené priestorové obmedzenia neexistujú v online prostredí. Na realizáciu vzdialenej komunikácie stačí mať k dispozícií pripojovací bod do internetu prakticky bez akýchkoľvek priestorových nárokov. Spomenutá argumentácia sa v online prostredí umocňuje, pretože v bežných komunikačných fórach absentuje kontrola o správne vyplnených registračných údajoch, tým sa jednoduchšie utajuje identita a ťažšie sa personifikuje činnosť.

Súbežne s narastajúcim počtom užívateľov sa zvyšuje aj množstvo osobných a citlivých informácií, ktoré používatelia sprístupňujú. Aj zdanlivo opatrnejší si často krát neuvedomia, ako postupne zverejňujú svoje osobné informácie, spojením ktorých sa dá získať ich jednoznačný identifikátor. Deje sa tak aj mimovoľne, napríklad pri registrovaní sa na poskytnutie určitej služby. Riziká pre jednotlivcov, spoločnosti, organizácie a vlády neboli nikdy väčšie, ako sú počas posledných rokov, napriek viacerým legislatívnym iniciatívam. Za posledné roky sa neprehliadnuteľne zintenzívnila vedomá manipulácia s obsahom informácií. Dezinformácia, klamstvo, hoax, manipulácia a propaganda, to všetko sú fenomény staré stovky rokov. Rôzne varianty propagandy a šírenia nepravdivých, skreslených, informácií bolo súčasťou svetových vojen, sú súčasťou mnohých politických systémov, predvolebného aj povolebného boja. V minulosti sa informácie šírili pomalšie a s menším rádiusom ako v súčasnosti, pretože k nim bol prístup sprostredkovaný prevažne tlačou, rozhlasom a televíziou, ku ktorým ani nemal prístup každý. Zásadnejší prelom nastal v 90. rokoch minulého storočia, keď sa k šíreniu správ začal aktívne využívať e-mail a internet. S príchodom nových online médií sa informácie začali šíriť podstatne rýchlejšie a masovejšie, než kedykoľvek v minulosti. Medzi pravdivé informácie ľahko prenikli aj nepravdivé alebo manipulatívne informácie a dostali sa fakticky k miliónom užívateľov internetových služieb. Za účelom príspevku so problematiku šírenia potenciálne škodlivých správ zúžime len na skúsenosti občanov so zdrojmi dezinformácií na sociálnych sieťach. Pojem dezinformácia na

Slovensku doposiaľ nebol terminologicky presne špecifikovaný, obvykle sú preberané definície z odborných publikácií či oficiálnych európskych dokumentov. V príspevku vychádzame z vymedzenia Národným bezpečnostným úradom Slovenskej republiky, ktorý dezinformáciou označuje nepravdivú alebo zmanipulovanú informáciu, ktorá je šírená zámerne s cieľom zavádzať a uškodiť. Dezinformácie môžu mať podobu nepravdivého alebo zmanipulovaného textu, obrázku, videa alebo zvuku, pričom môžu byť použité na šírenie pochybností a diskreditáciu pravdivých informácií či jednotlivcov, organizácií až polarizáciu spoločnosti. Ako uvádza (Lisoň, M, Fidler, Ľ., 2022) aj pravdivá informácia môže byť považovaná za dezinformáciu, ak je podaná manipulatívnym spôsobom. Naopak, neúmyselné chyby v spravodajstve, satira, paródia ani správy a komentáre naklonené jednej strane, ak sú takto zreteľne označené, sa nepovažujú za dezinformácie.

4 Prieskum vnímania zdrojov dezinformácií

Úspešnú obranu proti šíreniu dezinformácií nie je možné účelne vytvoriť bez znalosti ich zdrojov. V rámci dotazníkového prieskumu realizovaného na Akadémii Policajného zboru v Bratislave v roku 2023 v oblasti šírenia dezinformácií bola respondentom položená základná otázka, či sa už v živote stretli alebo stretávajú s dezinformáciami. Spomedzi 299 respondentov, ktorí sa do prieskumu zapojili len dvaja, t.j. 0,63 % odpovedali negatívne, že sa s dezinformáciami ešte nestretli. Ďalšia otázka skúmania znela „*Kde ste sa stretli, resp. stretávate sa s dezinformáciami*?“. Respondenti si podľa vlastného uváženia odpovede vyberali z nasledovných možností:

> na internete, v televízii, v tlači (v novinách, časopisoch), na sociálnych sieťach, v knihách (bez ohľadu na typ / druh knihy), v osobnom styku (s rodinou, známymi, priateľmi), v rozhlase.

Počet položiek v odpovedi na otázku nebol presne stanovený, rozhodovali o ňom respondenti.

Tabuľka 1 Sumár odpovedí na zdroje dezinformácií

Case Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
$všetky zdroje[a]	298	99,7%	1	0,3%	299	100,0%

a. Dichotomy group tabulated at value 1.

Zdroj: vlastné spracovanie

Tabuľka 2 Frekvenčná tabuľka odpovedí na zdroje dezinformácií

		Responses		
		N	Percent	Percent of Cases
všetko[a]	na_sociálnych_sieťach	258	27,3%	86,6%
	na_internete	253	26,8%	84,9%
	v_osobnom_styku	174	18,4%	58,4%
	v_televízii	135	14,3%	45,3%
	v_tlači	85	9,0%	28,5%
	v_rozhlase	29	3,1%	9,7%
	v_knihách	11	1,2%	3,7%
Total		945	100,0%	317,1%

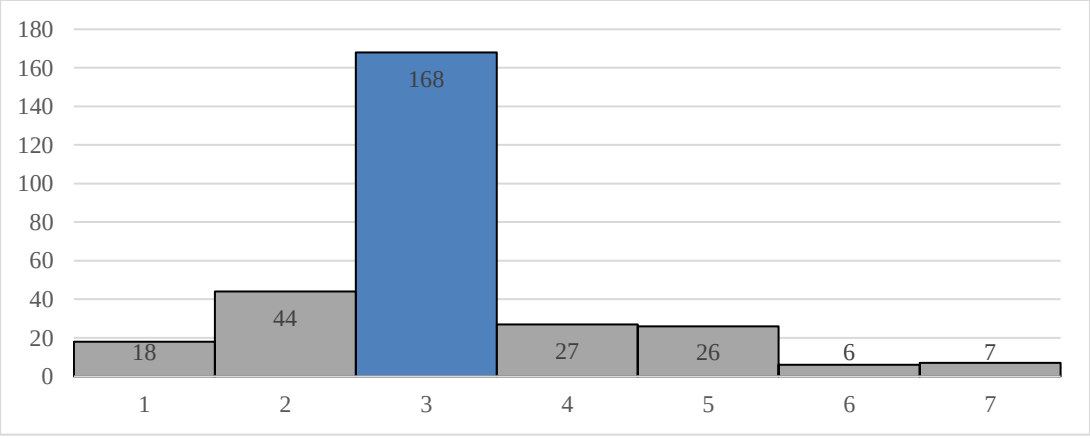
a. Dichotomy group tabulated at value 1.

Zdroj: vlastné spracovanie

Jednoznačné vyjadrenie respondentov ako celok sa nachádza v dvoch vrchných a dvoch spodných riadkoch tabuľky č. 2. Najčastejšie skúsenosti s výskytom dezinformácii boli uvedené pri sociálnych sieťach (86,6 % opýtaných) a na internete (takmer 85 %). Naopak ako ojedinelý zdroj dezinformácií bol zistený pri tradičných médiách ako sú knihy (3,7 %) a rozhlas (9,7 %). Na základe výsledkov nízkeho výskytu dezinformácií v knihách a rozhlase sa nedá jednoznačne posúdiť, či je indikovaný na reálne nízkom výskyte dezinformácií na týchto tradičných médiách alebo ich nízkou sledovanosťou. Dlhodobo je známe, že tradičné média sú existenčne vytláčané do úzadia modernými IKT.

Ako odlišný pohľad na výsledky prieskumu ponúkame cez rozdiely, ktoré sú identifikovateľné pri porovnaní rozloženia odpovedí vzhľadom na počet zvolených odpovedí jednotlivými respondentami.

Graf 2 Histogram početností odpovedí respondentov

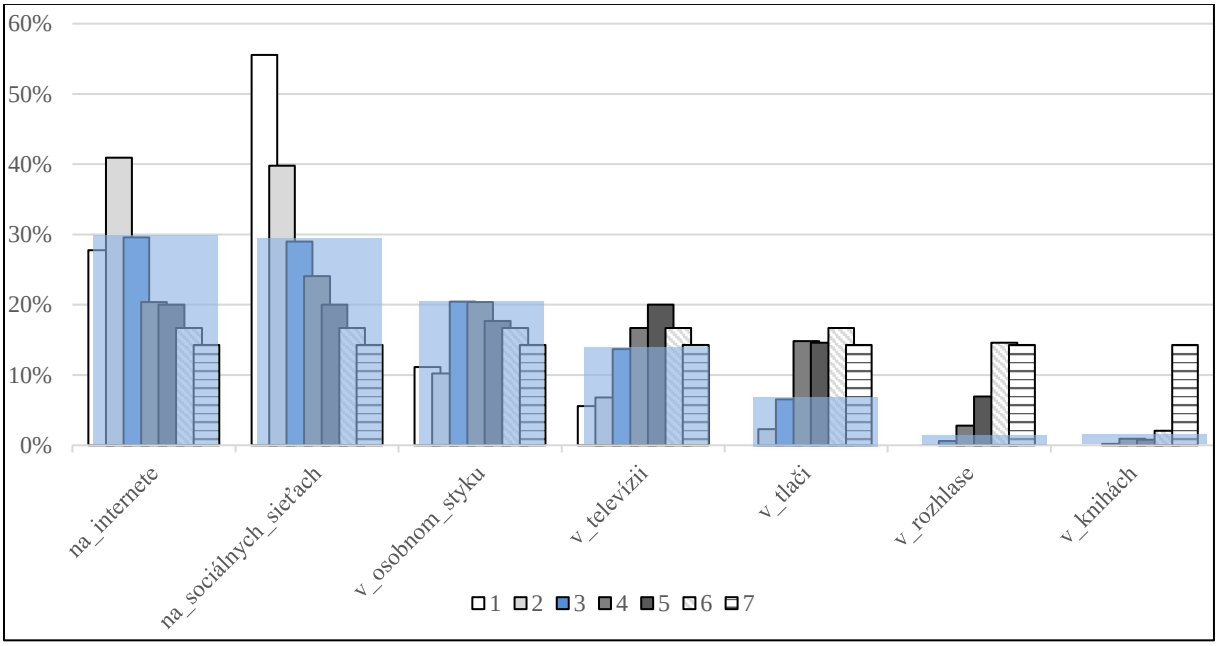


Zdroj: vlastné spracovanie

Zastúpenie respondentov podľa počtu odpovedí nebolo rovnomerné, výrazne najviac boli označené tri zdroje dezinformácií, ktoré sme si zvolili ako referenčnú skupinu a farebne odlíšili aj na grafe č. 3.

Na porovnanie rozloženia odpovedí podľa početnosti označených zdrojov dezinformácií sme použili relatívne početnosti pre každú početnosť odpovedí ako samostatný 100 %-ný celok, nakoľko absolútne početnosti predstaviteľov týchto skupín boli výrazne rozdielne, viditeľné z grafu č. 2.

Graf 3 Rozloženie odpovedí respondentov na osobné skúsenosti so zdrojmi dezinformácií



Zdroj: vlastné spracovanie z údajov prieskumu realizovaného na APZ v Bratislave

Ako jediný zdroj dezinformácií uviedlo 18 respondentov s výraznou prevahou označenia sociálnych sietí. Pri uvedení dvoch zdrojov dezinformácií (44 respondentov) porovnateľne dominoval ako zdroj dezinformácií internet v kombinácii so sociálnymi sieťami. Pri označení práve troch zdrojov dezinformácií sa potvrdila prevaha internetu a sociálnych sietí, s pomerne výrazným zastúpením aj pri osobách s ktorými komunikujú osobne alebo vzdialene prostredníctvom informačných a komunikačných technológií v rámci rodiny, s priateľmi a známymi. Jedná sa o každodenné interakcie a konfrontácie názorov, ktoré sú prirodzenou súčasťou bežného života. Spoločným znakom uvedených troch najpočetnejších zdrojov dezinformácií podľa vnímania respondentov je otvorená možnosť byť tvorcom ich obsahu širokou verejnosťou, ako aj ich ľahká dostupnosť cez všadeprítomné siete a obmedzené možnosti ich regulácie.

Pri štyroch a viacerých odpovediach sa vytrácajú rozdiely hodnotenia jednotlivých zdrojov dezinformácií, stúpajú do pozornosti tradičné masmédiá ako televízia, tlač (noviny a časopisy), rozhlas a knihy a naopak ustupujú z pozornosti internet a sociálne siete, ktoré boli väčšinou považované za hlavné zdroje dezinformácií. Rozhlas a knihy (bez ohľadu na typ / druh knihy) boli vo všeobecnosti vyhodnotené ako takmer bezchybné a dôveryhodné zdroje informácií. Detailným porovnaním výsledkov podľa počtu odpovedí poukazujeme na význam počtu odpovedí ako faktora, ktorý by mohol determinovať celkový výsledok. Z hľadiska hodnovernosti výsledkov by mohlo byť vhodnejšie, zjednotiť počet odpovedí pre všetkých respondentoch, nech sa vyrovná váha každého hlasu. Pri 7 odpovediach je zreteľné automatické označenie všetkých ponúkaných zdrojov dezinformácií. Pomerne nízka rozlišovacia schopnosť respondentov s väčším počtom odpovedí znižuje výpovednú hodnotu ich vyjadrenia.

Záver

Cieľom príspevku bolo poukázať na niektoré negatívne skutočnosti, ktoré sú prítomné pri zdieľanej online komunikácii, obzvlášť na sociálnych sieťach. Zisteniami prieskumu realizovaného na APZ v Bratislave v oblasti šírenia dezinformácií môžeme konštatovať, že väčšina obyvateľstva bez ohľadu na vek a pohlavie sa musela vysporiadať s dezinformáciami a to hlavne v prostredí sociálnych sietí, na internete a pri komunikácii s rodinou, známymi či priateľmi. Sloboda prejavu je jedna zo základných slobôd v demokratickej spoločnosti. Predstavuje právo každého vyjadrovať svoje názory slovom, písmom, tlačou, obrazom alebo iným spôsobom, ako aj slobodne vyhľadávať, prijímať a rozširovať idey a informácie bez ohľadu na hranice štátu. Nespochybniteľne sa jedná o jednu z najdôležitejších slobôd jedinca žijúceho v demokratickom a právnom štáte súčasnosti. Ako uvádza (Janko, 2022), aktuálna právna úprava zatiaľ neposkytuje dostatočnú ochranu spoločnosti proti šíreniu dezinformácií s primeraným rešpektovaním ústavou garantovaných práv ako napr. slobody prejavu. Vládne politiky pri sociálnych sieťach vytvárajú uzavretý kruh, v ktorom sa tento režim v podstate toleruje a ponecháva nezávislé skupiny a bežných občanov svojmu osudu.

Tvorenie a presadzovanie pravidiel autoritami tak, aby boli rešpektované a dodržiavané, ako aj prevádzkovanie mechanizmov kontroly represívnymi orgánmi sú v online prostredí náročnejšie, ako fungujú v reálnom svete. Pretože radikálne rýchle riešenie blokovaním nie je akceptovateľné, treba byť trpezlivejší a presadzovať inkluzívne riešenia, široké zapojenie zainteresovaných subjektov, spoluprácu verejných orgánov, online platforiem, reklamných agentúr, dôveryhodných oznamovateľov škodlivého obsahu, novinárov a mediálnych skupín.

V neposlednom rade jeden z významných spôsobov zvýšenia bezpečnosti užívateľov v online priestore je zlepšenie ich povedomia, kritického myslenia, zodpovednosti a budovanie informačnej imunity.

Poďakovanie

Príspevok vznikol s podporou projektu APVV-19-0102 Efektívnosť prípravného konania – skúmanie, hodnotenie, kritériá a vplyv legislatívnych zmien.

Referencie

Bond., R. M. et. al. (2.. 9. 2023). A 61-million-person experiment in social influence and political mobilization. Nature. doi:https://doi.org/10.1038/nature11421

Európska komisia. (16. jún 2023). Index digitálnej ekonomiky a spoločnosti (DESI) 2022 Slovensko. (E. komisia, Ed.) Dostupné na Internete: https://www.mirri.gov.sk/sekcie/informatizacia/jednotny-digitalny-trh/index-digitalnej-ekonomiky-a-spolocnosti/index.html

Ivančík, R, Nešas, P. (2023). Security and defense are truly a priority for the member states of European Union: Fact or hoax? *ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES, 10*(3), 73-83. doi:http://doi.org/10.9770/jesi.2023.10.3(6)

Ivančík, R., Andrassy, V. (2023). Insights into the development of the security concept. *Entrepreneurship and Sustainability Issues, 10*(4), 26-39. doi:http://doi.org/10.9770/jesi.2023.10.4(2)

Janko, S. (2022). Spolupráca so sociálnymi sieťami pri získavaní dôkazov použiteľných v trestnom konaní. *Dezinformácie a právo* (s. 67-73). Bratislava: Akadémia Policajného zboru v Bratislave.

Jeck, T. (2017). *JECK, T. (2017). Slovenská ekonomika a štvrtá priemyselní revolúcia: faktory a predpoklady*. Bratislava: Ekonomický ústav SAV.

Kathleen E Powers and Brian C Rathbun. (2023). When the Rich Get Richer: Class, Globalization, and the Sociotropic Determinants of Populism. *International studies quarterly, 67*(4), sqad083. doi:https://doi.org/10.1093/isq/sqad083

Khawlah M. Al-Tkhayneh, Hasan Awad Al-Tarawneh, Enas Abulibdeh, Moath Khalaf Alomery. (May 2023). Social and Legal Risks of Artificial Intelligence: An Analytical Study Academic. *Journal of Interdisciplinary Studies, 12*(3), 309-318. Dostupné na Internete: https://www.richtmann.org/journal/index.php/ajis/article/view/13320/12909

Kitagawa, R. (2023). From Political Violence to Political Trust? How Transitional Justice Affects Citizen Views of Government. *International studies quarterly, 67*(1), sqad013. doi:https://doi.org/10.1093/isq/sqad013

Kopencová, D., Felcan, M., Rak, R. (2020). Role and meaning of equilibrium and limit states in risk analysis, security and forensic science. In *Management and information technology: a new challenges* (1. vydanie. vyd., s. 121). Varšava, Poľsko: Wydawnictwo SGGW,.

Kopencová, D., Rak, R., Hudecová, V. (2021). Global phenomenon of threats and risk management in management and information technologies . *Issues in Information Systems,, 22*(1), 76-77.

Kuchtová, J. (2022). Bezpečnosť na sociálnych sieťach. *Bezpečnosť elektronickej komunikácie* (s. 237-247). Bratislava: Ajadémia Policajného zboru v Bratislave.

Lisoň, M, Fidler, ľ. (2022). Potreba a možnosti identifikácie rizík z realizácie hybridných hrozieb. *Policajná teória a prax., XXX*.(2), s. 38-53.

Lisoň, M., Hullová, M. (2020). Klasifikácia kriminality. *Policajná teória a prax., XXVIII,* (1), s. 59-79.

Schwab, K. (2016). The Fourth Industrial Revolution. San Francisco: World Economic Forum., (s. 172).

Kontakt

Tatiana Hajdúková

Katedra informatiky a manažmentu, Akadémia Policajného zboru v Bratislave

Sklabinská 1, 835 17 Bratislava

e-mail: tatiana.hajdukova@akademiapz.sk

Lucia Kurilovská

Katedra trestného práva, kriminológie a kriminalistiky, Právnická fakulta UK Bratislava

Šafárikovo námestie č. 6, P.O.BOX 313, 810 00 Bratislava,

e-mail: lucia.kurilovska@uniba.sk

Samuel Marr

Katedra trestného práva, kriminológie a kriminalistiky, Právnická fakulta UK Bratislava

Šafárikovo námestie č. 6, P.O.BOX 313, 810 00 Bratislava,

e-mail: samuel.marr1@uniba.sk