



# Právo a bezpečnost

# OBSAH

PRÁVO A BEZPEČNOST, ČÍSLO 3, ROČNÍK 2021

## Editorial

<i>Zdeněk Koudelka</i> Pokrytectví Bruselu k polskému Ústavnímu tribunálu	5
--	---

## Články

<i>Iveta Klementová</i> Připravenost zdravotnických zařízení středočeského kraje na dlouhodobé přerušení dodávky pitné vody	7
--	---

<i>Radoslav Ivančík</i> Dezinformácie ako bezpečnostná hrozba pre demokratickú spoločnosť	16
--	----

<i>Petr Průcha</i> Nový stavební zákon	34
---	----

<i>Petr Kolman</i> Nahrávání jednání orgánů profesních na příkladu advokátní	65
---	----

## Recenze

<i>Zdeněk Koudelka,</i> Recenze knihy: Pavel Kučera, Martin Švehla: V taláru napříč dobou	69
--	----

<i>Zdeněk Koudelka</i> Recenze knihy: Ivan Halász: Republika so Svätou korunou?	73
--	----

## Cizojazyčné texty

<i>Jana Müllerová</i> New challenges of Crisis Management in Public Administration	75
---	----

# DEZINFORMÁCIE AKO BEZPEČNOSTNÁ HROZBA PRE DEMOKRATICKÚ SPOLOČNOSŤ\*

*Radoslav Ivančík*

## 1. ÚVOD

Jedným z moderných výdobytkov, ktoré priniesol dynamický vývoj ľudskej civilizácie v posledných desaťročiach a ktorý charakterizuje náš súčasný životný štýl, je mobilný telefón. Inteligentné zariadenie, bez ktorého si už náš bežný život ani nevieme predstaviť. Pravdepodobne si narýchlo ani nedokážeme spomenúť na osobu, ktorá by ho nevlastnila. Ide totiž o produkt z oblasti moderných informačných a komunikačných technológií, ktorý nám umožňuje byť v kontakte s kýmkoľvek chceme, takmer kedykoľvek a kdekoľvek na svete, a ktorý nám ponúka množstvo rôznych možností a funkcií. Prirodzene, oveľa viac vnímame pozitíva spojené s jeho využívaním. Menej si už uvedomujeme, aký naozaj chytrý, náš mobilný telefón vlastne je, čo všetko o nás vie a čo všetko sa s informáciami,<sup>1</sup> ktoré ním prejdú, deje, ako sa využívajú, či ako sa v niektorých prípadoch doslova zneužívajú. Navyše, v posledných rokoch, ako uvádza Kuchtová, prichádza na trh okrem mobilných telefónov neuveriteľné množstvo ďalších technických a technologických novinek a inteligentných zariadení, ktoré je možné vzájomne prepájať a využívať ich plné rozhranie aplikovateľné vo verejnej, pracovnej i súkromnej sfére.<sup>2</sup>

Ďalším symbolom súčasnej modernej doby sú sociálne siete, ktoré nás prepájajú s rodinami, priateľmi i blízkymi, ale v podstate môžu s akoukoľvek inou osobou na svete. Množstvo informácií, ktoré o nás pri neopatrnom nastavení sociálne siete získavajú, zbierajú a postupujú ďalej, je obrovské.

---

\* Príspevok bol spracovaný v rámci riešenia projektu APVV-20-0334 „Nie je to pravda, ale mohla by byť.“ Konšpiračné teórie a hoaxy v modernom vývoji Slovenska v európskom kontexte.

<sup>1</sup> V tejto súvislosti možno bez akéhokoľvek zveličovania uviesť, že v dnešnej modernej spoločnosti zohrávajú informácie úlohu najhodnotnejšieho a najziskovejšieho tovaru (Baričičová, 2018, s. 8), čo bezprostredne súvisí s rýchlym rozvojom informačných a komunikačných technológií, systémov a prostriedkov. Výmena informácií a dát sa odohráva prakticky v reálne možnom čase bez ohľadu na miesto pobytu účastníkov vzájomnej interpersonálnej komunikácie. Vzdialenosť, ako obmedzujúci faktor, stráca na dôležitosti a význame (Baričičová, 2011, s. 67).

<sup>2</sup> 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.

Najčastejšie sa stretávame s ich využívaním vo forme komerčného online marketingu, ktorý cestou pokročilej analýzy získaných informácií čo najpresnejšie cieľi na potenciálnych spotrebiteľov a zvyšuje prostredníctvom cielenej reklamy príjmy zainteresovaných firiem. Žiaľ, ukazuje sa, že existujú aj podvodné, zlomyseľné a kriminálne spôsoby využitia / zneužitia sociálnych sietí a na nich dostupných informácií o ich užívateľoch. Krádeže identity<sup>3</sup>, šírenie počítačových vírusov<sup>4</sup>, napádanie bankových účtov<sup>5</sup> alebo kyberšikana<sup>6</sup> a ďalšie kybernetické hrozby<sup>7</sup> predstavujú len niektoré príklady z viacerých negatívnych javov, s ktorými sa môžeme stretnúť na internete a sociálnych sieťach. Práve kybernetické hrozby sú v súčasnosti vnímané veľmi citlivo, pretože sa veľakrát týkajú obrovského počtu ľudí. Nedostupnosť internetbankingu, výpadok internetu, e-mailu či telekomunikačnej siete sú pritom bežnými občanmi vnímané oveľa osobnejšie a citlivejšie ako ozbrojené konflikty vo svete.<sup>8</sup>

Spomínané negatívne javy sa väčšinou určitým spôsobom prejavia a my ako užívatelia vieme, že sme boli zneužití, či dokonca napadnutí. Existujú však aj situácie, kedy sa môžeme stať obeťou bez toho, aby sme o tom vedeli. Rovnako ako v prípade marketingu, kedy na nás cieľi reklama, ktorá je šitá na mieru tak, aby nás presvedčila k nákupu určitého tovaru či k objednaníu určitej služby, môžu na nás cieľiť správy a informácie, ktoré nie sú pravdivé, aby zmenili náš názor.

---

<sup>3</sup> ZACHAR, Š. 2018. Anonymizácia komunikácie zmenou IP adresy ako metóda bezpečného prehliadania internetu. In *Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2018, s. 217-224. ISBN 978-80-8054-773-8.

<sup>4</sup> KOSTREC, M. 2020. Nebezpečné hrozby v digitálnom priestore. In *Aktuálne výzvy kybernetickej bezpečnosti (Special Edition 2020) : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2020, s. 78-87. ISBN 978-80-8040-819-3.

<sup>5</sup> KORAUŠ, A. – KELEMEN P. 2018. Protection of persons and property in terms of cybersecurity. In *Ekonomické, politické a právne otázky medzinárodných vzťahov 2018 – zborník príspevkov z medzinárodnej vedeckej konferencie*. Bratislava : Vydavateľstvo Ekonóm, 2018. ISBN 978-80-225-4506-8.

<sup>6</sup> RÉVESZOVÁ, L. 2018. Počítačová kriminalita a dynamika jej vývoja v rokoch 2014 - 2017. In *Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2018, s. 161-173. ISBN 978-80-8054-773-8.

<sup>7</sup> TOMÁŠEK, R. – TOMÁŠEKOVÁ, L. 2020. Kybernetické hrozby a kybernetický terorizmus. In *Aktuálne výzvy kybernetickej bezpečnosti (Special Edition 2020) : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2020, s. 146-152. ISBN 978-80-8040-819-3.

<sup>8</sup> BREZULA, J. 2017. Koncepcia kybernetickej bezpečnosti na Slovensku a pripravované legislatívne zmeny v tejto oblasti. In *Národná a medzinárodná bezpečnosť – zborník príspevkov z 8. ročníka medzinárodnej vedeckej konferencie*. Liptovský Mikuláš : Akadémia ozbrojených síl gen. M. R. Štefánika, 2017, s. 26-31, ISBN 978-80-8040-551-9.

Používanie lží alebo prekrúcanie faktov k ovplyvneniu jednotlivcov alebo celej verejnosti nie je síce žiadnou novinkou, ak sa však spojí so sofistikovanými prostriedkami, aké predstavujú dnešné moderné, tzv. „smart“ prostriedky a technológie, s prostredím sociálnych sietí a internetu, prípadne aktivitou hackerov, objavuje sa tu nová a veľmi silná hrozba šírenia dezinformácií, ktoré môžu predstavovať nebezpečenstvo nielen pre jednotlivcov a organizácie, ale v niektorých prípadoch bezpečnostnú hrozbu pre národnú i medzinárodnú bezpečnosť.

## 2. TEORETICKÉ A TERMINOLOGICKÉ VYMEDZENIE POJMU DEZINFORMÁCIE

Dezinformácie sú, podobne ako mnohé iné pojmy, definované rôzne. V súčasnosti neexistuje žiadne ich jednotné, unifikované a všeobecne akceptované definíčné vymedzenie a tak sa v literatúre môžeme stretnúť s pomerne veľkým množstvom definícií líšiacich sa predovšetkým tým, 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 ide o úmyselnú modifikáciu poskytovaných informácií so zámerom ovplyvniť, oklamať či uviesť adresátov týchto informácií do omylu.

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*“.<sup>9</sup> V Slovníku súčasného slovenského jazyka je už dezinformácia definovaná obširnejšie ako „*nepravdivá, vedome skreslená informácia, ktorej cieľom je ovplyvniť určitú skupinu ľudí, prípadne celú populáciu*“.<sup>10</sup> 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*“.<sup>11</sup>

<sup>9</sup> Slovník cudzích slov. 2015. *Dezinformácia*. [online] [cit. 16.6.2021] Dostupné na: <[<sup>10</sup> Slovník súčasného slovenského jazyka. 2015. \*Dezinformácia\*. \[online\] \[cit. 16.6.2021\] Dostupné na: <\[<sup>11</sup> Slovník pojmov z mediálnej výchovy. 2020. \\*Dezinformácia\\*. \\[online\\] \\[cit. 16.6.2021\\] Dostupné na: <\\[18\\]\\(https://medialnavychova.sk/dezinformacia/></a>></p></div><div data-bbox=\\)\]\(https://slovník.juls.savba.sk/?w=dezinformácia&s=exact&c=a861&cs=&d=kssj4&d=psp&d=sssj&d=orter&d=scs&d=sss&d=peciar&d=ssn&d=hssj&d=ber nolak&d=noun db&d=orient&d=locutio&d=obce&d=priezv iska&d=un&d=pskcs&d=psken#></a>></p></div><div data-bbox=\)](https://slovník.juls.savba.sk/?w=dezinformácia&s=exact&c=a861&cs=&d=kssj4&d=psp&d=sssj&d=orter&d=scs&d=sss&d=peciar&d=ssn&d=hssj&d=ber nolak&d=noun db&d=orient&d=locutio&d=obce&d=priezv iska&d=un&d=pskcs&d=psken#></a>></p></div><div data-bbox=)

Národný bezpečnostný úrad na margo definovania dezinformácií uvádza, že tento pojem zatiaľ nebol v Slovenskej republike kodifikovaný, a preto sú v literatúre a príslušných dokumentoch väčšinou uvedené definície prevzaté z odborných publikácií či oficiálnych európskych dokumentov, ktoré sú si podobné a vystihujú podstatu pojmu. Zároveň dodáva, že „*dezinformácie môžu byť súčasťou širšieho procesu informačného ovplyvňovania, ktorý sa označuje pojmom informačné operácie*“.<sup>12</sup>

V českom prostredí, v Sociologickej encyklopédii je dezinformácia definovaná ako „*akákoľvek skreslená, falošná informácia, používaná s cieľom ovplyvniť jednotlivca aj určitú skupinu ľudí určitým žiaducim spôsobom. Väčšinou ide predovšetkým o vyvolanie dobrého či zlého dojmu o nejakej osobe, udalosti, diele, jave, rokovaní a pod. v záujme politickom, ideologickom alebo aj rýdzo súkromnom. Často je zameraná na ovplyvnenie verejnej mienky, pričom môže byť s takým zámerom už vytvorená, ale môže vzniknúť aj náhodne alebo za iným účelom, ktorý nemusí byť vyslovene dezinformačný (napr. keď je spôsobená vytrhnutím určitého oznámenia z pôvodného kontextu, resp. jeho zasadením do iného kontextu)*“.<sup>13</sup> Ministerstvo vnútra Českej republiky na svojich webových stránkach označuje dezinformáciu za „*šírenie zámerne nepravdivých informácií, obzvlášť štátnymi aktérmi alebo ich odnožami voči cudziemu štátu alebo voči médiám, s cieľom ovplyvniť rozhodovanie alebo názory tých, ktorí ich prijímajú*“.<sup>14</sup> Mleziva v tejto súvislosti dodáva, že „*dezinformácia, ak má byť účinná, tak by mala obsahovať aj časť pravdivých informácií*“.<sup>15</sup>

Na doplnenie vyššie uvedených definícií možno uviesť, že v anglofónnom jazykovom prostredí sa môžeme stretnúť tiež s viacerými vymedzeniami pojmu dezinformácia.

---

<sup>12</sup> NBÚ. 2021. *Dezinformácie a informačné operácie*. [online] [cit. 16.6.2021] Dostupné na: <<https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/dezinformacie/index.html>>

<sup>13</sup> Sociologická encyklopedie. 2017. *Dezinformace*. [online] [cit. 16.6.2021] Dostupné na: <<https://encyklopedie.soc.cas.cz/w/Dezinformace>>

<sup>14</sup> MV ČR. 2020. *Definice dezinformací a propagandy*. [online] [cit. 16.6.2021] Dostupné na: <<https://www.mvcr.cz/cthh/clanek/definice-dezinformaci-a-propagandy.aspx>>

<sup>15</sup> MLEZIVA, E. 2000. *Encyklopedie lži, podvádění a klamání s příklady a obrana proti nim*. Praha : Vyšehrad. 240 s. ISBN 80-702-1391-4.

Napríklad v Oxfordskom anglickom výkladovom slovníku je dezinformácia definovaná stručne ako „*úmyselne poskytovaná falošná informácia*“,<sup>16</sup> v Cambridgeskom slovníku anglického jazyka ako „*nepravdivá informácia šírená s cieľom oklamať ľudí*“,<sup>17</sup> a v MacMillanovom výkladovom slovníku ako „*nepravdivá informácia, ktorá má presvedčiť ľudí, aby verili niečomu, čo v skutočnosti nie je pravda*“.<sup>18</sup>

Dezinformácie je možné rozlíšiť z niekoľkých hľadísk. Z pohľadu ich tvorby a prejavu ich možno rozdeliť na a) pasívne a b) aktívne. Pasívne dezinformácie spočívajú v zatajení, zadržaní alebo oneskorení informácie s cieľom navodenia mylného dojmu. Aktívne dezinformácie reprezentujú, ako vyplýva z ich označenia, aktívnu tvorbu nepravdivých informácií alebo modifikáciu pôvodných informácií či ich kontextu. Ide o ich priamu aktívnu falzifikáciu. Z hľadiska cieľov je možné dezinformácie rozdeliť na a) strategické, ktorých použitím sa sleduje určitý dlhodobý strategický cieľ, napríklad nastolenie nejakého nového usporiadania, poriadku a pod., a b) taktické, ktorých využitie má operatívny charakter a slúži k postupnému napĺňaniu vytýčených dlhodobých cieľov.<sup>19</sup>

Z vyššie uvedených informácií jednoznačne vyplýva, že za hlavný znak dezinformácie možno považovať to, že ide o úmyselné konanie, a to tak v prípade pasívnej formy, kedy dochádza k úmyselnému zatajovaniu správ či ich pozdržaniu, ako aj v prípade aktívnej formy, kedy sa informácie aktívne vytvárajú alebo upravujú podľa stanoveného zámeru.

Pre lepšie pochopenie pojmu dezinformácia, pre jeho správne používanie a vyhnutie sa zamieňaniu s inými podobnými pojmami, predovšetkým s pojmom misinformácia, je potrebné vysvetliť aspoň základný rozdiel medzi týmito dvomi pojmami. Kým v prípade dezinformácie, ako už je uvedené vyššie, ide o úmyselné konanie s cieľom zaviesť, pomýliť, oklamať ľudí alebo presvedčiť ich, aby verili niečomu, čo nie je pravda, tak v prípade misinformácie tento úmysel chýba. Je to síce nesprávna alebo zavádzajúca informácia, avšak nie je šírená ani systematicky, ani úmyselne, ani s cieľom ovplyvniť rozhodovanie alebo názory tých, ktorí ju prijímajú.

---

<sup>16</sup> Oxford Learner's Dictionary. 2021. *Disinformation*. [online] [cit. 16.6.2021] Dostupné na: <<https://www.oxfordlearnersdictionaries.com/definition/english/disinformation?q=disinformation>>

<sup>17</sup> Cambridge Dictionary. 2021. *Disinformation*. [online] [cit. 16.6.2021] Dostupné na: <<https://dictionary.cambridge.org/dictionary/english/disinformation>>

<sup>18</sup> MacMillan Dictionary. 2021. *Disinformation*. [online] [cit. 16.6.2021] Dostupné na: <<https://www.macmillandictionary.com/dictionary/british/disinformation>>

<sup>19</sup> Neumannová, Š. 2017. *Dezinformace*. [online] [cit. 16.6.2021] Dostupné na: <<https://encyklopedie.soc.cas.cz/w/Dezinformace>>

Napriek tomu, hoci ide o neúmyselný akt, môže mať misinformácia v konečnom dôsledku rovnaký vplyv na obyvateľov ako dezinformácia, a teda ovplyvniť názory cieľovej skupiny na základe nepravdivej správy.

Druhým, veľmi blízkym pojmom, úzko súvisiacim s dezinformáciami, je propaganda, ktorá predstavuje „*cielené šírenie neobjektívnych, zavádzajúcich informácií a myšlienok na presadenie či podporu určitého názoru*“.<sup>20</sup> Možno ju charakterizovať aj ako „*šírenie informácií, faktov, argumentov, klebiet, poloprávď alebo lží za účelom ovplyvňovania verejnej mienky*“.<sup>21</sup> Pomerne obsírnú definíciu propagandy a vysvetlenie pojmu uvádza na svojom webovom sídle Encyklopédia Britannica. Podľa nej propaganda predstavuje „*viac či menej systematické úsilie o manipuláciu s vierou, postojmi alebo činmi iných ľudí pomocou symbolov (slov, gest, plagátov, bannerov, monumentov, hudby, odevov, insígnií, účesov, vzorov na minciach, poštových známkach a pod.)*“.<sup>22</sup> Práve úmyselnosť a pomerne veľký dôraz na manipuláciu odlišujú propagandu od bežného rozhovoru alebo od voľnej a ľahkej výmeny myšlienok. Propagandisti majú stanovený cieľ alebo súbor cieľov a aby ich dosiahli, zámerné vyberajú fakty, argumenty alebo zobrazenia symbolov a prezentujú ich spôsobmi, o ktorých si myslia, že budú mať čo najväčší efekt. Pre maximalizáciu účinku môžu vynechať či skresliť niektoré skutočnosti alebo jednoducho klamať a pokúšať sa odvrátiť pozornosť reaktorov (t. j. ľudí, ktorých sa pokúšajú ovládať) od všetkého iného, okrem vlastnej propagandy.“<sup>23</sup>

V oblasti politiky si propaganda kladie rôzne ciele, využíva rôzne prostriedky, ktoré sa nestále vyvíjajú, a spájajú s účelmi od politického presvedčania až k verejnej diplomacii. Súčasťou propagandy môžu byť tiež niektoré médiá. Ak ide o vládou financované alebo dokonca priamo riadené médiá, možno silne pochybovať o ich objektivite. Typickým príkladom krajiny s veľkým podielom štátom financovaných médií je Ruská federácia. Niektoré ruské médiá, ako napríklad Sputnik a RT, sú často vyhodnocované ako dezinformačné a ich spravodajská produkcia býva označovaná ako fake news.

Pojem fake news sa dá vysvetliť veľmi jednoducho prostým prekladom z angličtiny ako sfalšovaná, podvodná či nepravdivá správa.

---

<sup>20</sup> MV ČR. 2020. *Definice dezinformací a propagandy*. [online] [cit. 16.6.2021] Dostupné na: <<https://www.mvcr.cz/cthh/clanek/definice-dezinformaci-a-propagandy.aspx>>

<sup>21</sup> KAČMÁR, R. 2017. Informačná vojna a propaganda. In *Zabezpeč si vedomosti*. Bratislava : SSPI, 2017, s. 41-47. ISBN 978-80-972228-3-3, s. 41

<sup>22</sup> Encyclopædia Britannica. 2021. *Propaganda*. [online] [cit. 16.6.2021] Dostupné na: <<https://www.britannica.com/topic/propaganda>>

<sup>23</sup> Tamtiež.



Toto zjednodušené vysvetlenie môže viesť k rôznym debatám, pretože z pohľadu žurnalistiky by správa mala byť vždy pravdivá a nemala by sa dostať na verejnosť, pokiaľ nie je overená z niekoľkých dôveryhodných zdrojov.<sup>24</sup> V tejto súvislosti je potrebné upozorniť na fakt, že samotná identifikácia fake news môže byť veľmi obtiažna. Zvyčajne sa totiž podvodné, falošné oznámenie komunikuje v kombinácii so skutočnými a overiteľnými faktami, aby pôsobilo dôveryhodne. Allcott a Gentzkow definujú fake news ako „*spravodajské príspevky, ktoré sú zámerne a overiteľne klamlivé a môžu čitateľa zavádzať*“.<sup>25</sup>

Fake news nepredstavujú nijako prevratný objav v oblasti komunikácie či žurnalistiky, vyskytujú sa už veľmi dlho, avšak do hlbokého podvedomia verejnosti sa dostali hlavne až v súvislosti s americkými prezidentskými voľbami v roku 2016 a konkrétne s osobou Donalda Trumpa. Podľa Gregora a kol. ide o „*chytľavé súšlovie, ktoré označuje úmyselne nepravdivé alebo zavádzajúce informácie, ktoré sa objavujú v médiách alebo na sociálnych sieťach*“.<sup>26</sup> Aktuálne síce pôsobí tento pojem sprofanovane, ide však o súčasť zásadnej problematiky šírenia dezinformácií a ovplyvňovania verejnej mienky.

Hoci môžu pojmy fake news a dezinformácie pôsobiť totožne, z vyššie uvedených definícií je zrejmé, že sú odlišné. Kým fake news sú chápané ako forma, tak dezinformácie sú chápané ako obsah. Kým fake news je označenie správy, mediálneho či spravodajského príspevku alebo postu na sociálnej sieti, tak dezinformácie tvoria obsahovú časť takejto správy alebo príspevku, ktorá je nepravdivá, zavádzajúca alebo klamlivá. V praxi používajú označenie fake news niektoré politické osobnosti ako argument proti nepriaznivým správam na ich osobu alebo aj nadradene proti celému spravodajskému médiu, s ktorého výstupmi nesúhlasia.

---

<sup>24</sup> DRAGOMIROVÁ, A. M. 2017. The Fake News Phenomenon in the Social Media Era. In *Strategic Impact*; 2017, č. 64/65, s. 54–65. ISSN 18415784, s. 55

<sup>25</sup> 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 0895-3309, s. 213

<sup>26</sup> GREGOR, M. a kol. 2018. *Nejlepší kniha o Fake News, dezinformacích a manipulacích!!!* Brno: CPress, 2018. 143 s. ISBN 978-80-264-1805-4, s. 7

### 3. BOJ PROTI ŠÍRENÍ DEZINFORMÁCIÍ AKO BEZPEČNOST- NEJ HROZBE PRE DEMOKRATICKÚ SPOLOČNOSŤ

Základným cieľom všetkých dezinformácií je pokúsiť sa ovplyvniť skutočných ľudí. Pre naplnenie tohto cieľa je potrebná stratégia, ktorá zahŕňa široké spektrum jednotlivých krokov, ktoré je potrebné naplánovať pre dosiahnutie požadovaného úspechu. Pre šíriteľa je veľmi dôležité konkrétne stanovenie cieľovej skupiny, ktorú má dezinformácia zasiahnuť, a vybrať vhodný obsah korešpondujúci s vytýčeným cieľom. Jedným z hlavných elementov je voľba vhodných prostriedkov, ktoré majú byť využité pre dezinformačné účely. Primárnou platformou pre dezinformácie je dnes internet, v ktorého sieti ich šírenie sprostredkovávajú najmä rôzne dezinformačné weby a sociálne siete.

Významnosť tohto problému ilustruje fakt, že napr. v Spojených štátoch amerických skoro dve tretiny dospelých ľudí čerpá správy takmer výhradne zo sociálnych sietí.<sup>27</sup> Navyše, v porovnaní s minulosťou sa toto percento každým rokom neustále zvyšuje. A hoci chýbajú presné dáta, je vysoko pravdepodobné a nie je dôvod nijako spochybňovať, že tento trend je prítomný aj na Slovensku. Na sociálnej sieti Facebook má vytvorený profil vyše dvoch miliónov Slovákov a Sloveniek.<sup>28</sup> Tieto čísla za posledné roky taktiež vykazujú rastúci trend, a tým pádom čoraz väčšie množstvo interakcií prebieha v online prostredí internetu.

Internet sa stal obrovským míľnikom v oblasti komunikácie a prenosu informácií. Burkhard ho označuje 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.<sup>29</sup> Ktokoľvek s prístupom k internetu a chuťou zdieľať svoje myšlienky či nápady má dnes možnosť tak robiť. Spočiatku to síce vyžadovalo odbornú znalosť programovania a písania kódov, ale trh neskôr priniesol mnohé softvérové nástroje na to, aby aj jednotlivci bez špeciálnych znalostí boli schopní vytvoriť webovú stránku a zverejňovať či prenášať informácie.

---

<sup>27</sup> GOTTFRIED, J. - SHEARER, E. 2020. *News Use Across Social Media Platforms*. PEW Research Center, 2020 [online] [cit. 16.6.2021] Dostupné na: <<http://www.journalism.org/2020/05/26/news-use-across-social-media-platforms-2020/>>

<sup>28</sup> STATISTA. 2017. *Forecast of Facebook user numbers in Slovakia from 2015 to 2021 (in million users)*. [online]. [cit. 16.6.2021]. Dostupné na: <<https://www.statista.com/statistics/568836/forecast-of-facebook-user-numbers-in-the-slovakia/>>

<sup>29</sup> BURKHARDT, J. M. 2017. How Fake News Spreads. In *Library Technology Reports*, 2017, roč. 53, č. 8, s. 10-13. ISSN 0024-2586, s. 11

V súčasnosti existujú milióny aktérov šíriacich informácie, ktorých objem sa stáva ohromným a vyčerpávajúcim. Demokratická v oblasti informácií dáva priestor bez výnimky všetkým vrátane pochybných aktérov so zaujatým názorom alebo odlišným uhlom pohľadu či s nevzdelanými a limitovanými názormi. Keďže pravdivé správy môžu vyzeráť úplne rovnako ako tie nepravdivé, zaujaté, zmenené alebo satira, informačné presýtenie je potom podobné tomu stavu, keď nemáme informácie v podstate žiadne, pretože človek vtedy nevie, akým informáciám má venovať svoju pozornosť.

S nespočetným množstvom informácií, ktorými sme dnes zahlcovaní, sa spája fakt, že ľudia dnes nie sú schopní rozumieť veciam okolo seba. Príkladom môžu byť technológie a ich fungovanie (ako funguje mobilný telefón, čo sa deje s dátami po nahraní "na cloud", ako pracuje hybridný motor atď.), ale aj otázky zdravia (vhodnosť očkovania, vedľajšie účinky vakcín alebo konkrétnych liekov) alebo historické fakty. Efekt fake news v najrôznejších oblastiach má za následok, že ľudia sú viac náchylní nechať sa zasiahnuť a ovplyvniť dezinformáciami a nie sú schopní rozlišovať medzi faktami a fikciou.

Boj proti dezinformáciám sa tak čoraz viac dostáva do centra verejného diskurzu, a to na medzinárodnej aj národnej úrovni. Medzinárodné organizácie ako Severoatlantická aliancia (ďalej len „NATO“) a Európska únia (ďalej len „EÚ“) považujú šírenie dezinformácií za jednu zo súčasných najväznejších nevojenských bezpečnostných hrozieb a boj proti ich šíreniu sa stal neoddeliteľnou agendou ich aktivít. Obe organizácie ako celky, ale aj ich členské štáty individuálne reagujú na túto hrozbu. Príkladom je vytvorenie Centra výnimočnosti pre spoluprácu v oblasti kybernetickej obrany (NATO Cooperative Cyber Defense Center of Excellence<sup>30</sup>) na úrovni NATO alebo Centra výnimočnosti pre boj proti hybridným hrozbám (European Centre of Excellence for Countering Hybrid Threats<sup>31</sup>) na úrovni EÚ. Na úrovni technologických firiem prebiehajú najmä diskusie o zodpovednosti sociálnych sietí za šírenie dezinformácií na ich platformách. Akceptovanie určitej zodpovednosti za šírenie dezinformácií naznačuje rozhodnutie Facebooku prijať opatrenia, ktoré budú označovať zavádzajúce a falošné správy ako dezinformácie, v prípade že budú šírené na tejto platforme.<sup>32</sup>

---

<sup>30</sup> Bližšie pozri: NATO. 2021. *Cooperative Cyber Defense Center of Excellence*. [online] [cit. 16.6.2021] Dostupné na: <<https://ccdcoe.org>>

<sup>31</sup> Bližšie pozri: EU. 2021. *The European Centre of Excellence for Countering Hybrid Threats*. [online] [cit. 16.6.2021] Dostupné na: <<https://www.hybridcoe.fi>>

<sup>32</sup> JAMIESON, A. - SOLON, O. 2016. Facebook to begin flagging fake news in response to mounting criticism. In *The Guardian*. [online] [cit. 16.6.2021]. Dostupné na: <<https://www.theguardian.com/technology/2016/dec/15/facebook-flag-fake-news-fact-check>>

Dezinformácie predstavujú bezpečnostnú hrozbu, ktorá presahuje individuálny vplyv na jednotlivca konzumujúceho klamlivé, zavádzajúce informácie. Dá sa identifikovať aj na úrovni spoločnosti. K najvýznamnejším hrozbám patrí negatívny vplyv na demokratické procesy a ich deformácia v jednotlivých krajinách, v rámci ktorých sú dezinformácie rozšírené. Tento vplyv je možné ilustrovať na niekoľkých oblastiach.

Jedným z prvých negatívnych efektov je zvyšujúca sa polarizácia spoločnosti. Tento efekt je úzko spojený s už spomínaným čoraz väčším využívaním sociálnych sietí, ktoré sa stávajú primárnym zdrojom informácií a správ v kombinácii s nastavením fungovania týchto platforiem. Sociálne siete sú nastavené tak, aby svojim užívateľom zobrazovali pre nich čo najrelevantnejšie informácie a správy, ktoré zdieľajú ich najbližšie kontakty, a z toho dôvodu vedú k vytváraniu informačných bublín. Práve takéto uzatváranie sa v informačných bublinách vedie k zvýšenej polarizácii politických názorov v rámci spoločnosti.<sup>33</sup> Prílišné uzatváranie sa v informačných bublinách, ktorého následkom je čerpanie správ z ideologicky homogénnych zdrojov vedie v niektorých prípadoch dokonca k adoptovaniu extrémistických názorov.<sup>34</sup>

Ďalším problémom spojeným s dezinformáciami v online prostredí je predstieranie online podpory bežných občanov – tzv. politický astroturfing. Analýza amerických priebežných volieb a politickej podpory kandidátov v roku 2010 v prostredí sociálnej siete Twitter a jeho používateľov ukázala, že niektoré politické kampane, ktoré boli prezentované ako spontánne a vychádzajúce od obyčajných občanov, boli organizované centrálnou pomocou sociálnych botov, t. j. falošných účtov riadených softvérom, ktoré vyzerajú ako skutoční ľudia.<sup>35</sup> Zdanie masovej podpory vytvára dojem legitimity pre politické kampane a politických kandidátov, ktorí by v opačnom prípade pravdepodobne ostali marginálni. Tisíce sociálnych botov na Twitteri bolo identifikovaných aj v prípade podpory Brexitu v rámci kampane pred referendumom o zotrvaní Spojeného kráľovstva v EÚ.<sup>36</sup>

Iným druhom politického astroturfingu je využívanie koordinovaných diskutérov, ktorí v digitálnom prostredí komentujú a zdieľajú politicky motivované články.

---

<sup>33</sup> MITCHELL, A. 2017. *Political Polarization & Media Habits*. PEW Research Centre [online] [cit. 16.6.2021] Dostupné na: <<http://www.journalism.org/2014/10/21/political-polarization-media-habits/>>

<sup>34</sup> WARNER, B. R. 2010. Segmenting the Electorate: The Effects of Exposure to Political Extremism Online. In *Communication Studies*, 2010, roč. 61, č. 4, s. 430-444. ISSN 1051-0974.

<sup>35</sup> RATKIEWICZ, J. 2011. *Detecting and Tracking Political Abuse in Social Media*. [online] [cit. 16.6.2021] Dostupné na: <<http://www.aai.org/ocs/index.php/ICWSM/ICWSM11/paper/view/2850/3274>>

<sup>36</sup> HOWARD, P. - KOLLANYI, B. 2016. *Bots, #StrongerIn, and #Brexit: Computational Propaganda during the UK-EU Referendum*. [online] [cit. 16.6.2021] Dostupné na: <<https://arxiv.org/ftp/arxiv/papers/1606/1606.06356.pdf>>

Toto je problematika, ktorú je akademicky veľmi komplikované skúmať a ktorá je do veľkej miery neprebádaná. V prostredí Slovenskej republiky bolo zmapovaných niekoľko prípadov falošných diskutérov podporujúcich politické strany ako napríklad SMER-SD, Siet' a TIP.<sup>37</sup>

V neposlednom rade majú dezinformácie vplyv na politické rozhodovanie jednotlivcov. Procesy rozhodovania sa vždy dejú na základe dostupných informácií, ktoré má ten, ktorý sa rozhoduje, k dispozícii. Ak súčasťou balíka týchto informácií sú aj dezinformácie, tak bude prijaté rozhodnutie ovplyvnené. V tomto prípade sa dá spraviť analógia s klesajúcim počtom zaočkovaných detí proti osýpkam a nárastom vplyvu antivakcinačného hnutia.<sup>38</sup>

Jedným z najvýraznejších a najmedializovanejších príkladov šírenia dezinformácií v rámci predvolebného boja je príklad prezidentských volieb v USA z roku 2016, v ktorých zvíťazil Donald Trump. Webový portál BuzzFeed<sup>39</sup> analyzoval všetky správy, ktoré v období siedmich pracovných dní tesne pred voľbami zdieľali tri najväčšie pravicové a tri najväčšie ľavicové stránke stránky na sociálnej sieti Facebook. Zistil, že kým pravicové stránky zdieľali až 38 % správ, ktoré obsahovali dezinformácie alebo kombináciu pravdivých a zavádzajúcich správ, u ľavicových portálov to bolo 19 %.<sup>40</sup>

Mapovanie šíriteľov dezinformácií v spojení s americkými prezidentskými voľbami v roku 2016 však ukázalo, že dezinformácie nie sú šírené len za účelom propagandy. Častým motívom ich šírenia bol aj zisk z predaja reklamy. Portál BuzzFeed identifikoval viac ako stovku pro-Trumpovských webových stránok so sídlom v Macedónsku, ktoré produkovali a šírili rôzne dezinformácie. Cieľom prevádzkovateľov týchto stránok bolo maximalizovanie návštev týchto portálov za účelom čo najväčšieho zisku z predaja reklamy. Vysokú návštevnosť im zabezpečovali práve vymyslené, klamlivé a zavádzajúce správy týkajúce sa prezidentských kandidátov (v prospech Donalda Trumpa a v neprospech Hillary Clintonovej), ktoré dosiahli najväčšiu sledovanosť na sociálnych sieťach.<sup>41</sup>

---

<sup>37</sup> STRUHÁRIK, F. 2016. Prochádzkovi v kampani na webe pomáhajú falošní diskutéri. Nie je to prvý raz. In *Denník N* [online] [cit. 16.6.2021]. Dostupné na: <<https://dennikn.sk/346480/prochazkovi-kampani-webe-pomahaju-falosni-diskuteri-nie-prvy/>>

<sup>38</sup> HOTEZ, P. 2018. *Texas and Its Measles Epidemics*. [online] [cit. 16. 6. 2021] Dostupné na: <<http://journals.plos.org/plosmedicine/article?id=10.1371/journal.pmed.1002153>>

<sup>39</sup> Bližšie pozri: BuzzFeed. 2021. [online] [cit. 16.6.2021] Dostupné na: <<https://www.buzzfeed.com>>

<sup>40</sup> SILVERMAN, C. 2016. Hyperpartisan Facebook Pages Are Publishing False And Misleading Information At An Alarming Rate. In *BuzzFeed News* [online] [cit. 16.6.2021] Dostupné na: <<https://www.buzzfeed.com/craig-silverman/partisan-fb-pages-analysis>>

<sup>41</sup> SILVERMAN, C. – ALEXANDER, L. 2016. *How Teens In The Balkans Are Duping Trump Supporters With Fake News*. *BuzzFeed News* [online] [cit. 16.6.2021] Dostupné na: <<https://www.buzzfeed.com/craig-silverman/how-macedonia-became-a-global-hub-for-pro-trump-misinfo>>

Výroba a šírenie dezinformácií v prospech vtedy ešte kandidáta Trumpa za účelom produkcie ekonomického zisku, ale samozrejme aj za cieľom politického zisku, to v prvom rade, bolo identifikované aj v domácom prostredí v rámci USA.<sup>42</sup>

Spoločná správa amerických spravodajských služieb – Ústrednej spravodajskej služby (CIA), Federálneho úradu pre vyšetrovanie (FBI) a Národnej bezpečnostnej agentúry (NSA) – z januára 2017 konštatovala, že v priebehu prezidentskej kampane sa objavilo na sociálnych sieťach obrovské množstvo dezinformácií s cieľom diskreditácie demokratickej prezidentskej kandidátky Hillary Clintonovej. V správe sa konštatuje, že viaceré z týchto aktivít boli s veľkou pravdepodobnosťou (nie so stopercentnou istotou) sponzorované ruskou vládou.<sup>43</sup> Obsah zverejnených emailových správ vedenia americkej demokratickej strany na portáli Wikileaks však upriamil pozornosť aj na viacero ďalších problémov spojených so šírením zavádzajúcich a klamlivých informácií v rámci demokratických primárnych volieb. Medzi najväčšie patrilo šírenie dezinformácií tentokrát podporujúcich Hillary Clintonovú a, naopak, podkopávajúcich kandidatúru Bernieho Sandersa zo strany vedenia Demokratickej strany.<sup>44</sup>

#### 4. ZÁVER

O prítomnosti najrôznejších klamlivých a zavádzajúcich informácií – dezinformácií – v digitálnom verejnom i súkromnom priestore, a to aj v rámci Slovenska a iných vyspelých demokratických krajín, neexistujú žiadne pochybnosti. Relatívne dobre je zmapovaných viacero mechanizmov a nástrojov s akými pracujú domáca, resp. ruská, čínska alebo iná zahraničná propaganda či už pri ovplyvňovaní demokratických procesov alebo pri šírení dezinformácií. Problematika dezinformácií a ich šírenia predstavuje veľmi komplikovanú oblasť, v ktorej sa prelína veľmi veľa rôznych tém. Aktuálne šírenie dezinformácií prostredníctvom internetu a sociálnych sietí je extrémne nebezpečnou hrozbou, ktorá môže mať pre jednotlivcov, organizácie i celú spoločnosť veľmi nepriaznivé dôsledky.

---

<sup>42</sup> DEWEY, C. 2016. Facebook fake-news writer: 'I think Donald Trump is in the White House because of me.' In *The Washington Post* [online] [cit. 16.6.2021]. Dostupné na: <<https://www.washingtonpost.com/news/the-intersect/wp/2016/11/17/facebook-fake-news-writer-i-think-donald-trump-is-in-the-white-house-because-of-me/>>

<sup>43</sup> NIC. 2017. *National Intelligence Council. Assessing Russian Activities and Intentions in Recent US Elections. Intelligence Community Assessment.* [online] [cit. 16.6.2021] Dostupné na: <[https://www.dni.gov/files/documents/ICA\\_2017\\_01.pdf](https://www.dni.gov/files/documents/ICA_2017_01.pdf)>

<sup>44</sup> SHEAR, M. – ROSENBERG, M. 2016. Released Emails Suggest the D.N.C. Derided the Sanders Campaign. In *New York Times*, 2016. [online] [cit. 16.6.2021]. Dostupné na: <<http://www.nytimes.com/2016/07/23/us/politics/dnc-emails-sanders-clinton.html>>

Sociálne siete nás prepájajú s celým svetom, poskytujú nám množstvo informácií, ale zároveň nás robia zraniteľnými. Je preto veľmi dôležité zo strany demokratických štátov a ich kompetentných inštitúcií, vrátane bezpečnostných zložiek, podporovať prevenciu 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 akékoľvek ovplyvňovanie alebo rozdeľovanie spoločnosti práve na základe posúvania klamlivých a zavádzajúcich informácií. Angažovanie relevantných inštitúcií demokratických štátov v tejto problematike je z toho dôvodu nielen žiaduce, ale dokonca nevyhnutné. Na druhej strane si všetci musíme uvedomiť, že ich možnosti nie sú nekonečné, nie všetko za nás vyrieši štát, a tak je nutné, aby sme aj my sami prispeli k potláčaniu množstva, sily a vplyvu dezinformácií a ich šíriteľov na naše konanie.

#### **Literatúra:**

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 0895-3309.

BARIČIČOVÁ, Ľ. 2011. *Kompetencie policajných manažérov*. Bratislava: Akadémia Policajného zboru, 2011. 160 s. ISBN 978-80-8054-514-7.

BARIČIČOVÁ, Ľ. 2018. Informačná kompetentnosť v kontexte aktuálnych potrieb informačnej spoločnosti. In *Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2018, s. 8-15. ISBN 978-80-8054-773-8.

BELAN, L. – UCHAL, M. 2018. Narušenie bezpečnosti. In *Národná a medzinárodná bezpečnosť – zborník príspevkov z 9. ročníka medzinárodnej vedeckej konferencie*. Liptovský Mikuláš : Akadémia ozbrojených síl gen. M. R. Štefánika, 2018, s. 29-38. ISBN 978-80-8040-568-7.

BREZULA, J. 2017. Koncepcia kybernetickej bezpečnosti na Slovensku a pripravované legislatívne zmeny v tejto oblasti. In *Národná a medzinárodná bezpečnosť – zborník príspevkov z 8. ročníka medzinárodnej vedeckej konferencie*. Liptovský Mikuláš : Akadémia ozbrojených síl generála M. R. Štefánika, 2017, s. 26-31. ISBN 978-80-8040-551-9.

BURKHARDT, J. M. 2017. How Fake News Spreads. In *Library Technology Reports*, 2017, roč. 53, č. 8, s. 10-13. ISSN 0024-2586.

Cambridge Dictionary. 2021. *Disinformation*. [online] [cit. 16. 6. 2021] Dostupné na: <<https://dictionary.cambridge.org/dictionary/english/disinformation>>

DEWEY, C. 2016. Facebook fake-news writer: 'I think Donald Trump is in the White House because of me.' In *The Washington Post* [online] [cit. 16. 6. 2021]. Dostupné na: <<https://www.washingtonpost.com/news/the-intersect/wp/2016/11/17/facebook-fake-news-writer-i-think-donald-trump-is-in-the-white-house-because-of-me/>>

DRAGOMIROVÁ, A. M. 2017. The Fake News Phenomenon in the Social Media Era. In *Strategic Impact*, 2017, č. 64/65, s. 54-65. ISSN 18415784.

Encyclopedia Britannica. 2021. *Propaganda*. [online] [cit. 16. 6. 2021] Dostupné na: <<https://www.britannica.com/topic/propaganda>>

EU. 2021. *The European Centre of Excellence for Countering Hybrid Threats*. [online] [cit. 16. 6. 2021] Dostupné na: <<https://www.hybridcoe.fi>>

GOTTFRIED, J. – SHEARER, E. 2020. *News Use Across Social Media Platforms*. PEW Research Center, 2020 [online] [cit. 16.6.2021] Dostupné na: <<http://www.journalism.org/2020/05/26/news-use-across-social-media-platforms-2020/>>

GREGOR, M. a kol. 2018. *Nejlepší kniha o Fake News, dezinformacích a manipulacích!!!* Brno: CPress, 2018. 143 s. ISBN 978-80-264-1805-4.

HOTEZ, P. 2018. *Texas and Its Measles Epidemics*. [online] [cit. 16. 6. 2021] Dostupné na: <<http://journals.plos.org/plosmedicine/article?id=10.1371/journal.pmed.1002153>>

HOWARD, P. – KOLLANYI, B. 2016. *Bots, #StrongerIn, and #Brexit: Computational Propaganda during the UK-EU Referendum*. [online] [cit. 16. 6. 2021] Dostupné na: <<https://arxiv.org/ftp/arxiv/papers/1606/1606.06356.pdf>>

JAMIESON, A. – SOLON, O. 2016. Facebook to begin flagging fake news in response to mounting criticism. In *The Guardian*. [online] [cit. 16. 6. 2021]. Dostupné na: <<https://www.theguardian.com/technology/2016/dec/15/facebook-flag-fake-news-fact-check>>

KAČMÁR, R. 2017. Informačná vojna a propaganda. In *Zabezpeč si vedomosti*. Bratislava: SSPI, 2017, s. 41-47. ISBN 978-80-972228-3-3.



KAZANSKÝ, R. 2018. *Nové prístupy k výskumu transformácie bezpečnostného sektora*. České Budejovice : Vysoká škola evropských a regionálnych štúdií, 2018. 133 s. ISBN 978-80-7556-040-7.

Korauš, A. – Kelemen P. 2018. Protection of persons and property in terms of cybersecurity. In *Ekonomické, politické a právne otázky medzinárodných vzťahov 2018 – zborník príspevkov z medzinárodnej vedeckej konferencie*. Bratislava : Vydavateľstvo Ekonóm, 2018. ISBN 978-80-225-4506-8.

KOSTREC, M. 2020. Nebezpečné hrozby v digitálnom priestore. In *Aktuálne výzvy kybernetickej bezpečnosti (Special Edition 2020) : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2020, s. 78-87. ISBN 978-80-8040-819-3.

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.

MITCHELL, A. 2017. *Political Polarization & Media Habits*. PEW Research Centre [online] [cit. 16. 6. 2021]. Dostupné na: <<http://www.journalism.org/2014/10/21/political-polarization-media-habits/>>

MLEZIVA, E. 2000. *Encyklopedie lži, podvádění a klamání s příklady a obrana proti nim*. Praha : Vyšehrad. 240 s. ISBN 80-702-1391-4.

MV ČR. 2020. *Definice dezinformací a propagandy*. [online] [cit. 16. 6. 2021] Dostupné na: <<https://www.mvcr.cz/cthh/clanek/definice-dezinformaci-a-propagandy.aspx>>

NATO. 2021. *Cooperative Cyber Defense Center of Excellence*. [online] [cit. 16. 6. 2021] Dostupné na: <<https://ccdcoe.org>>

NBÚ. 2021. *Dezinformácie a informačné operácie*. [online] [cit. 16. 6. 2021] Dostupné na: <<https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/dezinformacie/index.html>>

NEUMANNOVÁ, Š. 2017. *Dezinformace*. [online] [cit. 16. 6. 2021] Dostupné na: <<https://encyklopedie.soc.cas.cz/w/Dezinformace>>

NIC. 2017. *National Intelligence Council. Assessing Russian Activities and Intentions in Recent US Elections. Intelligence Community Assessment.* [online] [cit. 16. 6. 2021] Dostupné na: <[https://www.dni.gov/files/documents/ICA\\_2017\\_01.pdf](https://www.dni.gov/files/documents/ICA_2017_01.pdf)>

Oxford Learner's Dictionary. 2021. *Disinformation.* [online] [cit. 16.6.2021] Dostupné na: <<https://www.oxfordlearnersdictionaries.com/definition/english/disinformation?q=disinformation>>

RATKIEWICZ, J. 2011. *Detecting and Tracking Political Abuse in Social Media.* [online] [cit. 16. 6. 2021] Dostupné na: <<http://www.aaai.org/ocs/index.php/ICWSM/ICWSM11/paper/view/2850/3274>>

RÉVESZOVÁ, L. 2018. Počítačová kriminalita a dynamika jej vývoja v rokoch 2014 - 2017. In *Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou.* Bratislava : Akadémia Policajného zboru, 2018, s. 161-173. ISBN 978-80-8054-773-8.

SHEAR, M. – ROSENBERG, M. 2016. Released Emails Suggest the D.N.C. Derided the Sanders Campaign. In *New York Times*, 2016. [online] [cit. 16. 6. 2021]. Dostupné na: <<http://www.nytimes.com/2016/07/23/us/politics/dnc-emails-sanders-clinton.html>>

SILVERMAN, C. 2016. Hyperpartisan Facebook Pages Are Publishing False And Misleading Information At An Alarming Rate. In *BuzzFeed News* [online] [cit. 16. 6. 2021] Dostupné na: <<https://www.buzzfeed.com/craigsilverman/partisan-fb-pages-analysis>>

SILVERMAN, C. – ALEXANDER, L. 2016. *How Teens In The Balkans Are Duping Trump Supporters With Fake News.* *BuzzFeed News* [online] [cit. 16. 6. 2021]. Dostupné na: <<https://www.buzzfeed.com/craigsilverman/how-macedonia-became-a-global-hub-for-pro-trump-misinfo>>

Slovník cudzích slov. 2015. *Dezinformácia.* [online] [cit. 16. 6. 2021] Dostupné na: <<https://slovník.juls.savba.sk/?w=dezinformácia&s=exact&c=a861&cs=&d=kssj4&d=psp&d=sss&d=orter&d=scs&d=sss&d=peciar&d=ssn&d=hssj&d=ber nolak&d=noun db&d=orient&d=locutio&d=obce&d=priezviska&d=un&d=pskcs&d=psken#>>>

Slovník pojmov z mediálnej výchovy. 2020. *Dezinformácia.* [online] [cit. 16. 6. 2021] Dostupné na: <<https://medialnavychova.sk/dezinformacia/>>

- Slovník súčasného slovenského jazyka. 2015. *Dezinformácia*. [online] [cit. 16. 6. 2021] Dostupné na: <[https://slovník.juls.savba.sk/?w=dezinformácia&s=exact&c=a861&cs=&d=kssj4&d=psp&d=sssj&d=orter&d=scs&d=sss&d=peciar&d=ssn&d=hssj&d=ber nolak&d=noundb&d=orient&d=locutio&d=obce&d=priezviska&d=un&d=pskcs&d=psken#](https://slovník.juls.savba.sk/?w=dezinformácia&s=exact&c=a861&cs=&d=kssj4&d=psp&d=sssj&d=orter&d=scs&d=sss&d=peciar&d=ssn&d=hssj&d=ber nolak&d=noundb&d=orient&d=locutio&d=obce&d=priezviska&d=un&d=pskcs&d=psken#>)>
- SOCIOLOGICKÁ ENCYKLOPEDIA. 2017. *Dezinformace*. [online] [cit. 16. 6. 2021] Dostupné na: <<https://encyklopedie.soc.cas.cz/w/Dezinformace>>
- STATISTA. 2017. *Forecast of Facebook user numbers in Slovakia from 2015 to 2021 (in million users)*. [online] [cit. 16. 6. 2021]. Dostupné na: <<https://www.statista.com/statistics/568836/forecast-of-facebook-user-numbers-in-the-slovakia/>>
- STRUHÁRIK, F. 2016. Prochádzkovi v kampani na webe pomáhajú falošní diskutéri. Nie je to prvý raz. In *Denník N* [online] [cit. 16.6.2021]. Dostupné na: <<https://dennikn.sk/346480/prochazkovi-kampani-webe-pomahaju-falosni-diskuteri-nie-prvy/>>
- TOMÁŠEK, R. – TOMÁŠEKOVÁ, L. 2020. Kybernetické hrozby a kybernetický terorizmus. In *Aktuálne výzvy kybernetickej bezpečnosti (Special Edition 2020) : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2020, s. 146-152. ISBN 978-80-8040-819-3.
- WARNER, B. R. 2010. Segmenting the Electorate: The Effects of Exposure to Political Extremism Online. In *Communication Studies*, 2010, roč. 61, č. 4, s. 430-444. ISSN 1051-0974.
- ZACHAR, Š. 2018. Anonymizácia komunikácie zmenou IP adresy ako metóda bezpečného prehliadania internetu. In *Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2018, s. 217-224. ISBN 978-80-8054-773-8.

**Abstract:**

***Disinformation as a Security Threat for Democratic Society***

*Today's modern human civilization is significantly influenced by deepening globalization processes, which are reflected to a greater or lesser extent in all spheres of society. With one of the characteristic manifestations of the present, with the dynamic onset of new media, the rapid development and massive use of information and communication technologies, systems and means, another new range of possibilities has emerged, such as disseminating, sharing, but also searching for information and news. At the same time, however, a new range of options has emerged for disseminating misleading and information – disinformation – in order to influence people's actions. The spread of disinformation thus represents an extremely dangerous threat today, which can have very adverse consequences for individuals, organizations, and society as a whole. Therefore, the aim of the author of the article is to point out the danger of dissemination of disinformation, the need to look at them as a security threat for democratic society and the need to take adequate measures to prevent their dissemination.*

**Key words:** *Security, disinformation, information, security threats, social networks.*

**JEL:** Z00

Ing. **Radoslav Ivančík**, PhD. et PhD. – Akadémia Policajného zboru v Bratislave, Katedra informatiky a manažmentu, Sklabinská 1, 835 17 Bratislava, Slovenská republika, radoslav.ivancik@akademiapz.sk.

**Adresa redakce**

AMBIS vysoká škola, a.s.

Časopis Právo a bezpečnost

Šujanovo nám. 1, 602 00 Brno

[zdenek.koudelka@mail.ambis.cz](mailto:zdenek.koudelka@mail.ambis.cz)

Webové stránky časopisu:

[pravoabezpecnost.cz](http://pravoabezpecnost.cz)

**Vydává:**

AMBIS vysoká škola, a.s.

Lindnerova 575/1

180 00 Praha 8 - Libeň

**Tisk:**

NOVPRESS s.r.o.,

Nám. Republiky 15,

614 00 Brno-Židenice

*Registrováno Ministerstvem kultury pod číslem E 21228.*

**ISSN 2336–5323**

***Datum vydání: 15.12.2021***

*Objednávky předplatného přijímá vydavatel, cena předplatného je 600 Kč ročně, jednotlivé číslo stojí 200 Kč a lze jej zakoupit na adrese redakce. Vychází 3x ročně.*