JEL-KÉP

KOMMUNIKÁCIÓ, KÖZVÉLEMÉNY, MÉDIA

2022/3. szám

A DIGITÁLIS BIZTONSÁG TÉMÁJÁNAK MEGJELENÍTÉSE A MAGYAR ONLINE MÉDIÁBAN: EGY ÉVET FELÖLELŐ SZENTIMENTANALÍZIS

Kapornaky Mihály – Ujhelyi Adrienn

misi.kapornaky@gmail.com – ujhelyi.adrienn@ppk.elte.hu

DOI: 10.20520/JEL-KEP.2022.2.55

Absztrakt

Jelen írás a digitális biztonság tágabb értelemben vett témakörének elterjedtségét vizsgálja a magyarnyelvű interneten. A *social listening* technikával végzett kutatás alapját válogatott kulcsszavak keresése és nagyméretű korpuszon végzett automatikus szöveganalitika jelentette. Az adatok forrásául a különféle típusú médiumok nyilvános tartalmai (cikkek, fórumbejegyzések, hozzászólások) szolgáltak. Az egyéves időtartamot felölelő, 27132 főképpen semleges érzelmi tónusú szöveges említést detektáló elemzés a téma jól mérhető jelenlétét mutatta ki az adatvédelmi irányelvek és szabályozások (pl. GDPR) jogi-bürokratikus nyelvezetű említéseinek egyértelmű mennyiségi dominanciájával. Emellett viszont gyakoriságukon túlmutató befolyással, jelentős eléréssel jelentek meg a felhasználók számára átélhetőbb, a fenyegetést, kockázatokat hangsúlyozó szövegek, legmarkánsabban a kibertámadások témaköre kapcsán.

Kulcsszavak

digitális biztonság, kiberbiztonság, privacy, online hírek, szentimentelemzés

THE PREVALENCE OF THE TOPIC OF CYBER-SECURITY IN THE HUNGARIAN ONLINE MEDIA: SENTIMENT ANALYSIS OF ONE YEAR

Mihály Kapornaky – Adrienn Ujhelyi

Abstract

Background and objectives: This paper examines the prevalence of the topic of digital security on online Hungarian sources.

Method: The research carried out using the social listening technique was based on a search for selected keywords and automatic text analytics on a large corpus. The source of the data was public content from various types of media (articles, forum posts, comments).

Results and conclusions: The analysis covering a period of one year and detecting 27,132 textual mentions of mainly neutral emotional tones, showed a measurable presence of the topic with a clear quantitative dominance of legal-bureaucratic language mentions of data protection guidelines and regulations (e.g., GDPR). In addition, texts emphasizing threats and risks were published with a significant reach and influence beyond their frequency, most notably in relation to the topic of cyber-attacks.

Keywords

digital safety, cybersecurity, privacy, sentiment analysis, SentiOne, social listening

JEL-KÉP

KOMMUNIKÁCIÓ, KÖZVÉLEMÉNY, MÉDIA

2022/3. szám

A DIGITÁLIS BIZTONSÁG TÉMÁJÁNAK MEGJELENÍTÉSE A MAGYAR ONLINE MÉDIÁBAN: EGY ÉVET FELÖLELŐ SZENTIMENTANALÍZIS[1]

Kapornaky Mihály – Ujhelyi Adrienn

Az online világ és vele együtt a közösségi média az elmúlt években vitathatatlanul életünk meghatározó részeivé váltak. 2022-ben a magyar lakosság 95%-a használt valamilyen Social Networking Site-ot vagyis közösségi média felületet (a későbbiekben SNS) (Globalstat 2022). Az online aktivitás térnyerésével párhuzamosan eddig nem ismert veszélyek jelentek meg, például a magánélet védelmével és az adatbiztonsággal kapcsolatban. Egyre égetőbbé váló kérdések tehát, hogy pontosan milyen nyomokat, információkat hagyunk magunk után egy-egy internetes aktivitás után, és hogy azokat egyes vállalatok, kormányok, egyéb szervezetek vagy magánemberek mire használják fel (Bergström 2015, Preibusch 2013, Turow – Hennessy 2007).

A téma kutatásának egyik alapvetése, hogy az online biztonságérzet szubjektív és objektív aspektusa eltérő lehet, a felhasználó saját online aktivitásával kapcsolatos véleményét, hiedelmeit és végső soron a viselkedését számtalan kognitív torzítás befolyásolja (Baruh és mtsai. 2017, Cho és mtsai. 2010, Maskall 2017). Az egyik legfontosabb ilyen tényező a hozzáférhetőségi heurisztika, vagyis az az emberi tulajdonság, hogy az esélyeket, kockázatokat a leghamarabb eszünkbe jutó példák alapján ítéljük meg (Tversky – Kahneman 1973). Kognitív reprezentációink tartalmának egyik legmeghatározóbb ágense a média, vagyis azt, hogy mit gondolunk bizonyos – főként bonyolult és újszerű – jelenségekről, a médiában megjelent hírek alapvetően befolyásolják. Ezért választottuk jelen kutatás témájául a digitális biztonság témájának megjelenésének elemzését: egy egyéves időszakot felölelve statisztikai mutatókat és példákat is felvonultatva betekintést adunk abba, hogy mennyire volt elterjedt ez a témakör a magyarnyelvű online nyilvánosságban.

E kutatás egy kutatássorozat része, mely további kvalitatív (fókuszcsoportos interjúk) és kvantitatív (7000 fős reprezentatív kutatás) részekből állt, és mely a (Jel-Kép által anonimizált) XXX pályázat keretében jött létre.

Módszer: social listening

Az elemzéshez a SentiOne elnevezésű webes szöveganalitikai szoftvert vettük igénybe (https://sentione.com), amely a nyilvános online platformokon közzétett szöveges tartalmakat gyűjti és elemzi (cikkek, posztok, kommentek stb.), amelyek a rendszerben létrehozott projekt

[1] A kutatást a (Jel-Kép által anonimizált) XXX intézmény támogatta.

beállítása után azonnal elérhetővé válnak. A SentiOne közösségi média adatokat és a hagyományos weboldalakról származó tartalmakat is gyűjt. Minden összegyűjtött adat egy adattárházba kerül, amelyben a megfelelő kulcsszavak megadásával lehet keresni (több mint 30 nyelven). A SentiOne jelenlegi adattárházában több mint 20 milliárd említés érhető el, és ez folyamatosan bővül. A nyelvfelismeréshez a SentiOne saját fejlesztésű algoritmust használ, amely a lingvisztikai tulajdonságokat és az elérhető metaadatokat is figyelembe veszi, így 99,93 százalékos pontossággal tudja detektálni az adott nyelvet.

A SentiOne nap mint nap új címeket ad hozzá a rendszerhez: automatizált folyamatok mentén, valamint kézi beállítások nyomán, online keresőmotor API-ok használatával. A domain címeket azon jelszavak alapján szűri és bővíti, amelyekre a felhasználók rákerestek a rendszerben. A website-adatok begyűjtésekor az algoritmusok igyekeznek annyi tartalmat összegyűjteni, amennyit csak tudnak, későbbi elemzésekhez. A rendszer azokat a domaineket figyeli, amelyeken felhasználói tartalom jelenik meg (blogok, fórumok, hírportálok, review-oldalak). A SentiOne saját tulajdonú és fejlesztésű algoritmusokat használ a strukturálatlan HTML tartalmak kinyeréséhez. Az adatgyűjtés folyamata manuálisan írt XPath profilokon keresztül történik, ahol az automatikus algoritmusok nem működnek, vagy az oldal dinamikus tartalommal operál.

A SentiOne a különböző közösségimédia-oldalakról a hivatalos és nyilvános API-hozzáféréseken keresztül gyűjti be az adatokat. A figyelni kívánt Facebook oldalakat a felhasználó adja meg. Mi olyan, a vizsgált időszakban aktív magyarnyelvű oldalakat választottunk, amelyek profiljában vagy bejegyzéseiben szerepeltek a kutatás témájának főbb szavai (ld. később). A Facebook esetében a SentiOne a publikus oldalakon közzétett tartalmakat figyeli. A privát Facebook oldalakon publikált bejegyzéseket nem látja, még akkor sem, ha azok nyilvánosként lettek közzétéve (mert a Facebook API szabályzatával ez nem összeegyeztethető). A Twitter nyilvános API kódot használ, azaz lehetőség van a tweetek monitorozására, így azonnal láthatók a legfrissebb bejegyzések is. Az Instagramról professzionális fiók (business account) hiányában nem gyűjtöttünk adatot, illetve a végső elemzésbe a YouTube sem került bele, mivel a SentiOne korlátozottan tárolja, analitikai modulja pedig nem aggregálja az onnan származó adatokat, ezeken felül pedig a rendszer bizonyos algoritmusai sem használhatóak a platformon.

A bejegyzések érzelmi hátterének megállapításánál Watson, Clark és Tellegen (1988) Positive and Negative Affect Schedule (PANAS) elnevezésű mérőeszközét vették alapul a szoftver fejlesztői (ld. még Crawford – Henry 2004). E mentén olyan algoritmusokat fejlesztettek, amelyek segítenek beazonosítani az adott bejegyzés szerzőjének témához kötődő érzelmi viszonyát (pozitív, negatív, semleges).

A bejegyzések vizsgálatánál szintén fontos paraméter az elérés (reach), hogy valamiféle képet kaphassunk az adott bejegyzés befolyásosságának (influence) mértékéről. A SentiOne különböző becsült elérést számító algoritmust használ a generikus weboldalak, a fórumok és a közösségi média felületek ilyen típusú vizsgálatához. Weboldalak esetén az adott weboldal forgalmának teljesítményét külső adatszolgáltató cég közreműködésével elemzi. Figyelembe vesz olyan változókat, mint például a domain forgalma, a látogatószám, a tartalom kora, a weboldal vitalitása (például, milyen gyakran frissül), a tartalom típusa (hozzászólás, cikk). Ahhoz, hogy egy egyedi említés elérése megbecsülhető legyen, a domain statisztikákon kívül a saját adatbázisba elmentett adatokat is figyelembe veszi a rendszer. Ha nincsen a külső adatszolgáltató partnertől elérhető adat az adott website-ra nézve, akkor a domain Page Authority értékét veszi figyelembe az algoritmus, amely minden domainhez elérhető, és az oldal nézettségével (page view) arányos. A fórumok esetében neurális hálózati algoritmusokat használ a szolgáltatás, amely fórumonként és témánként különbözik (áttekintésért ld. Schmidhuber 2015, van Gerven – Bohte 2017). A közösségi média felületek esetében vagy az adott oldalra vo-

natkozó API által biztosított értékeket veszi alapul, vagy a posztokra érkezett interakciókat súlyozza az algoritmus a követőszám nagyságával.

A kulcsszavas keresés alapját a „kiberbiztonság”, a „privacy” és az „adatvédelem” szavak, valamint a „digitális/online biztonság” szókapcsolatok jelentették. A keresési paraméterek konfigurálásakor figyelembe vettük a magyar nyelv sajátosságait, hogy a kulcsszavak ragozott, toldalékolt, némileg módosult formáit (pl. „privacy-*val*”, „adatvédel*mi*”) tartalmazó szövegeket is detektáljuk.

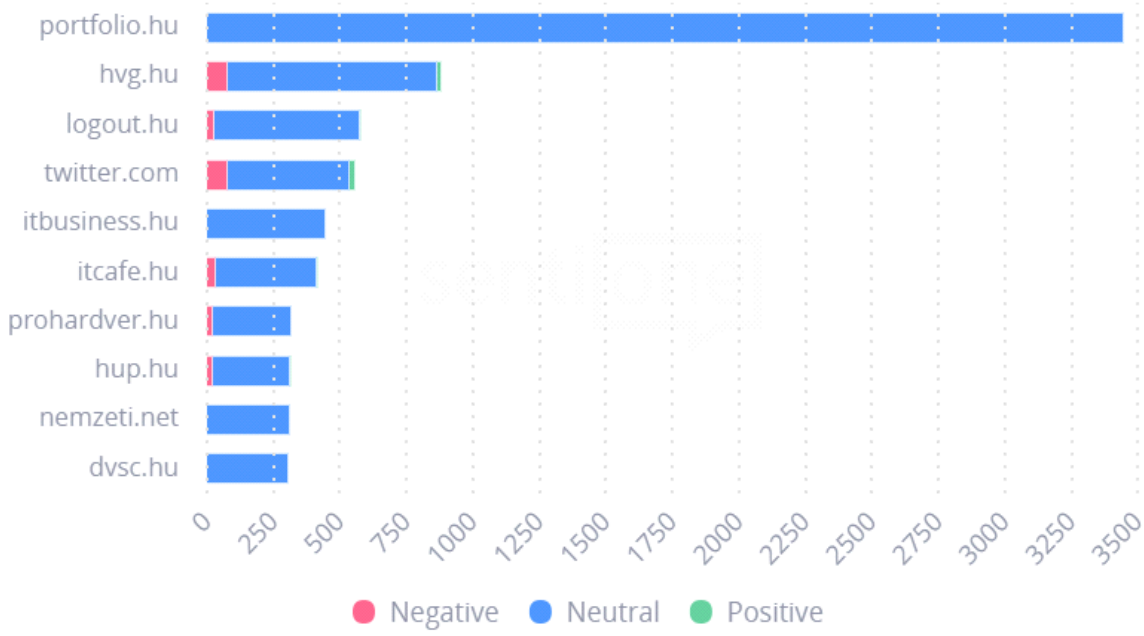
A vizsgált időszakot a teljes 2021-es év jelentette, a célzott Facebook oldalakon kívül a keresés válogatás nélkül terjedt ki a magyarnyelvű online tartalmakra (híroldalak, blogok, fórumok, digitális tájékoztató felületek, bejegyzések és hozzászólások egyaránt).

Eredmények

A lefuttatott keresés 27 132 úgynevezett említést (mentions) talált, amelyek összesen 628 287 383 megjelenítést (impression) generáltak. Ez nem egyszerű szógyakoriságot, hanem olyan szöveges tartalmak számosságát takarja, amelyekben a keresőkifejezések tetszőleges halmaza legalább egyszer előfordult. Többségük különböző weboldalakról (23 803), elsősorban a portfolio.hu-ról (3 449), illetve fórumokról (1 786), kisebb részük pedig blogokról (735) vagy a Twitterről (574) származott (1. ábra).

1. ábra

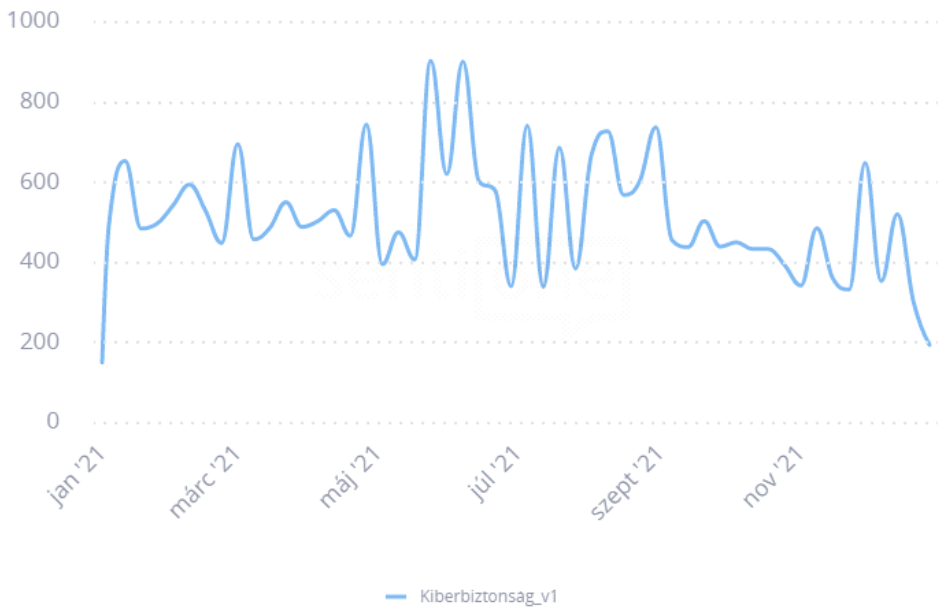
Top források



A vizsgált időszakban az említések száma némileg oszcilláló tendenciát mutatott, az időszakos kiugrásokon túl nyári csúcsidőszak és őszi „pangás” volt megfigyelhető, míg az abszolút mélypontokat az év eleje és legvége jelentették: a május 24-i és a június 7-i héten 904, illetve 902 említés született, az év első hetén 151, míg az utolsón 195 (2. ábra).

2. ábra

Említések időbeli eloszlása



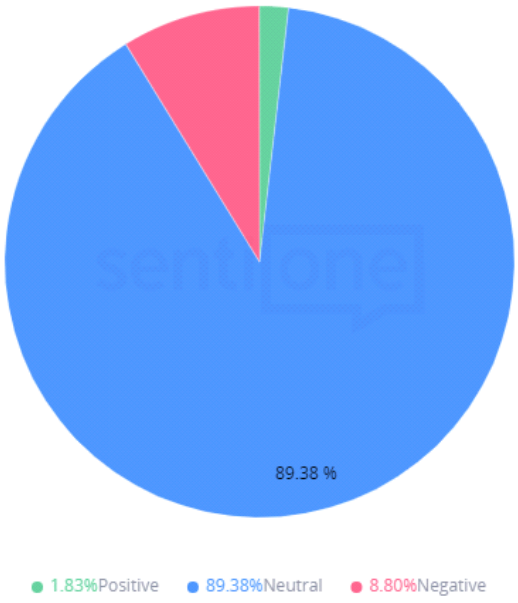
Az első nyári csúcshét aktivitásának többek között olyan virális, sok médium által feldolgozott hírek voltak felelősek, amelyek jellegükben elsősorban inkább politikai jellegűek voltak, de hangsúlyos adatvédelmi vonatkozással (is) bírtak, vagy ilyen területen dolgozó szakemberek szólaltak meg velük kapcsolatban. Ide sorolhatók például a belarusz választások kapcsán kirobbant tömeges tiltakozások bizonyos témái, mint az ellenzéki szereplők által széleskörűen használt Telegram csevegőprogram titkosítása és sokak által túl engedékenynek tartott adatvédelmi szabályai vagy éppen Raman Prataszevics újságíró gépének eltérítéshez vezető e-mail hitelességének elemzése. Sokszor hivatkozott belföldi téma volt ebben az időszakban az úgynevezett „pedofilellenes törvényjavaslat" egyik eleme is, amely nyilvánosan, név szerint kereshető szexuális bűnelkövetői adatbázis létrehozását szorgalmazta, amely utat nyitott egyebek mellett a magyar és uniós adatvédelmi gyakorlatok és azokat felülíró kivételes feltételekről szóló nem csupán jogalkotói, de társadalmi vitára is, hasonlóan ahhoz, ahogyan korábban a COVID-19 kapcsán hirtelen sokakat érdeklő, intenzív, érzelmekkel is fűtött kérdéssé vált, hogy kinek és mikor van joga különösen szenzitív (pl. egészségügyi) személyes adatokhoz való hozzáférésre, amely kérdés kissé más formában, de később újra aktuálissá vált az uniós Covid-igazolványok bevezetése kapcsán. Ezeken kívül a Kaspersky Lab nagy figyelmet kiváltó vizsgálatának köszönhetően a populáris média ingerküszöbét is átütve nagyobb figyelmet váltott ki a zsarolóvírusok jelentette fenyegetettség és a magyar felhasználók kitettségének mértéke.

A második kiugrás mögött inkább tágabb értelemben vett kiberfenyegetettségekről szóló említések álltak. Egyfelől a világpolitikai szintéren, többek között Joe Biden és Vlagyimir Putyin tervezett genfi csúcstalálkozójának apropóján, amely a kiberbiztonságot az egyik legfontosabb megtárgyalandó kérdésként aposztrofálta, az Európai Parlament pedig fokozott fellépést sürgetett az olyan kérdésekben, mint a hibrid hadviseléssel (másképpen információs háború) szembeni EU-s ellenállóképesség. Másfelől pedig nagy sajtónyilvánosságot kapó hírek láttak napvilágot, amelyek adatlopásokról, hackertámadásokról, vagy éppen zaklató és kémprogramokról szóltak.

Az elemzett időszak szentimentelemzése betekintést enged az említések érzelmi polaritásába, nyelvi karakterébe. A rendszer által érzelmi töltetet hordozóként azonosított említések túlnyomó többsége, több mint 89%-a „semleges"-ként lett kategorizálva (3. ábra).

3. ábra

Érzelmi megoszlás



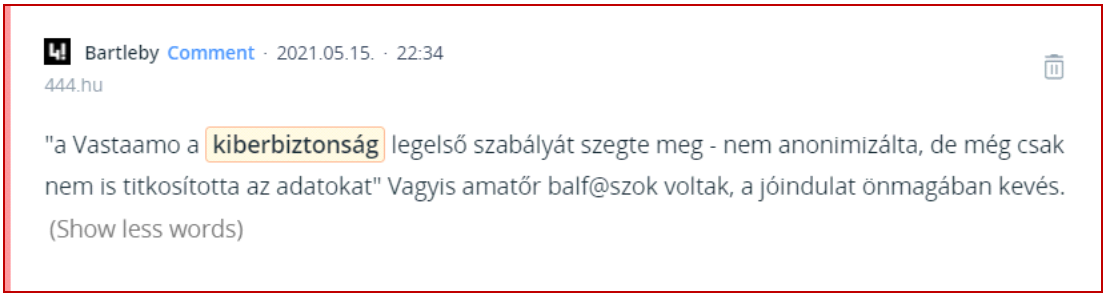
Ez az eloszlás tükrözi a detektált szövegek jellemző tónusát, amely részben a tágabban vett téma „technicizált”, műszaki, protokollokat, irányelveket és szakkifejezésekkel telített szókészletéből fakad. A befolyásos, népszerű hírek közül számos fogalmazódott meg figyelemfelhívó stílusban, olyan kifejezéseket használva, amelyek alkalmasak lehetnek érzelmi reakció kiváltására: gondoljunk csak egyebek mellett a „kockázat”, „veszély”, „támadás”, „csalás”, „zsarolás”, „kémkedés”, „kiszolgáltatottság” altémáinak felbukkanására. Azonban a szövegtestek egészében mégiscsak túlsúlyba kerülnek az eljárásokra, szabályozásokra, technológiákra vonatkozó szakkifejezések. Röviden: egy hacker/hekkertámadás (424 említés) vagy adatlopás (283 említés) leírása tartalmazhat nyelvileg felfokozott elemeket, de összességében mennyiségileg elmaradnak az olyan témákra, mint a GDPR-ra (5 152 említés) vagy általánosságban az adatvédelemre (17 395 említés) való hivatkozásoktól. Mindezt jól szemlélteti az időszak leggyakrabban használt kifejezései alapján generált szófelhő is, amelyben csupa semleges kifejezés szerepel (4. ábra).

A szövegek szentimentelemzése alapján megbecsülhetjük, hogy egy-egy kifejezés vagy téma milyen érzelmi színezettel kerül tálalásra, sőt, a felhasználók által generált szövegek (bizonyos posztok, hozzászólások, fórumbejegyzések) esetén a megítélésre, viszonyulásra is lehet következtetni. A mintánknak azonban csak egy kisméretű halmazában (454 említés) jelent meg egyértelmű értékelő viszonyulás a fogalmak kontextusában, például egy alkalmazás/szolgáltatás adatvédelmi szabályozása kapcsán megfogalmazott felhasználói élményekként vagy egy hírre adott hevesebb reakcióként (5. ábra).

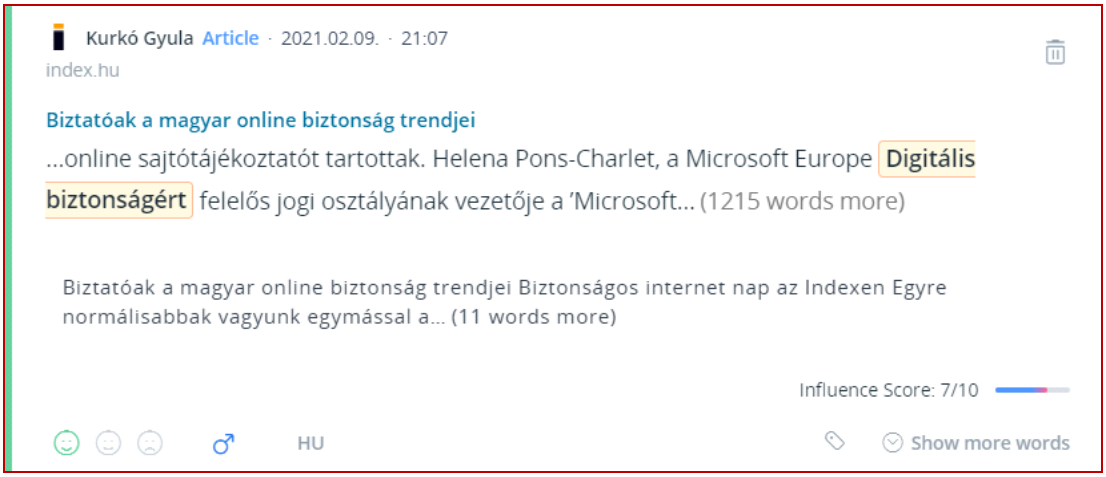
A gyakoriságok indikátorai lehetnek egy téma elterjedtségének, de nem feleltethetők meg egy az egyben a téma fontosságának vagy hatásosságának. A nagyobb forgalmat, aktivitást generáló, több embert elérő szövegeket (ezekre a rendszer magasabb ún. Influence Score-t ad) vizsgálva azt láttuk, hogy az altémák jobban kiegyenlítődnek és hangsúlyosabbak az olyan szövegek esetében, amelyek a köznapi értelemben nagyobb hírértékkel bírnak (jelentős anyagi kár, érzékeny adatok kiszivárgása, stb.), illetve felhasználói oldalról jobban azonosulhatóak, figyelemfelkeltőbbek. Így például a szervezetek, személyek ellen elkövetett kibertámadások, vagy az interneten megosztott személyes adatokban rejlő kockázatok felülreprezentálttá váltak összevetve például a különböző szabályozásokra, „policy-kra” való technikai vagy jogi hivatkozásokkal, amelyek a teljes mintában domináns gyakorisággal bírtak (6. ábra).

4. ábra

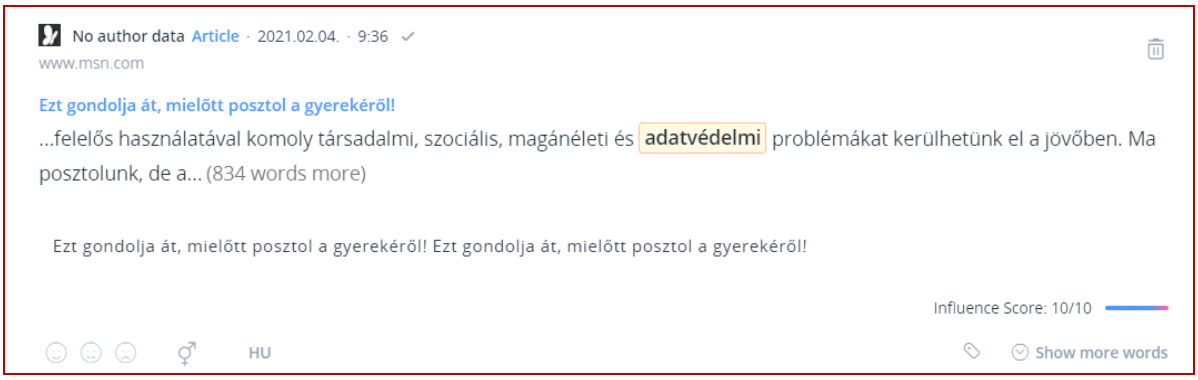
Szófelhő



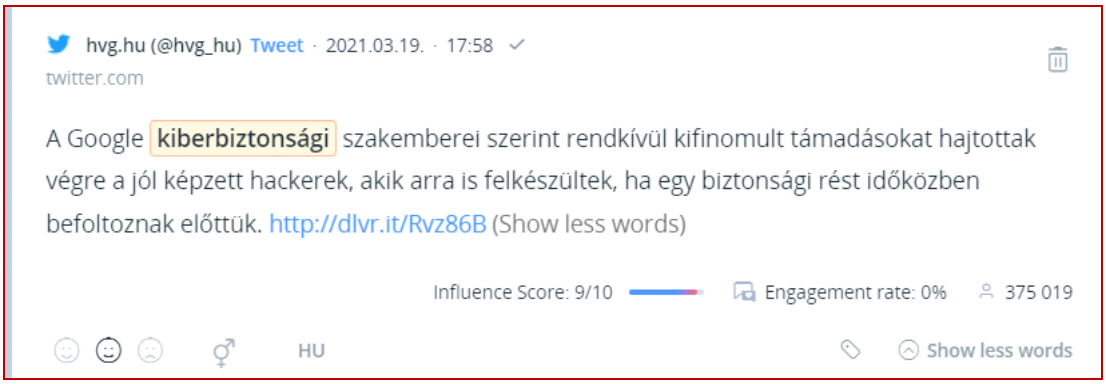
5. ábra



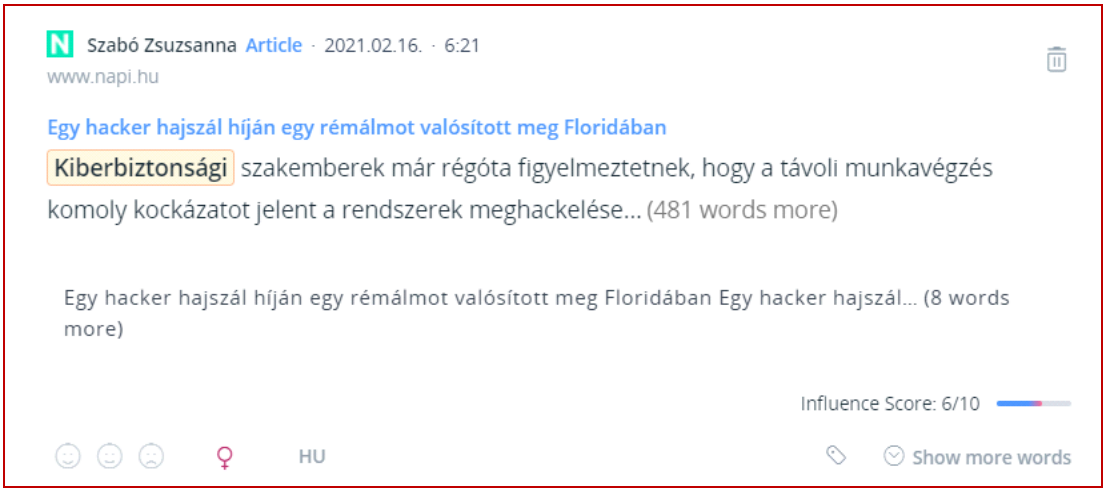
5. ábra
(folytatás)



6. ábra



6. ábra
(folytatás)



Összefoglalás, kitekintés

Az adatok alapján digitális biztonság témaköre egyértelműen, nap mint nap mérhető mennyiségben van jelen a magyar interneten, még ha hagyományos értelemben virálisnak vagy populárisnak semmiképpen nem is nevezhető. A témakörön belül mennyiségileg főként a szabályozások, irányelvek kontextusában megjelenő adatvédelmi szövegek (leglátványosabban a GDPR-ra való hivatkozás) domináltak.

A tény, hogy a médiában nem elég hangsúlyosan, illetve nem elég közérthetően jelenik meg a téma, erősen hozzájárulhat, hogy a magyarok mind a kiberbiztonsággal kapcsolatos attitűdjükben, mind viselkedésükben elmaradnak az Európai Unió átlagától (Eurobarometer, 2019). Egy magyar kutatás úgy fogalmaz, hogy az általuk vizsgált magyar egyetemi hallgatók a kiberbiztonsággal kapcsolatos elemi tudásnak sincsenek birtokában, és ami még aggasztóbb, nem is érzik magukat motiváltnak a további ismeretek elsajátítására (Mai – Tick 2021).

Mindez pedig rávilágít a téma pszichológiai-viselkedéstudományi aspektusának, valamint a pszichoedukációnak a fontosságára. Az olyan praktikus cikkeken túl, melyek tanáccsal szolgálnak például a biztonságos online vásárláshoz vagy egy adott típusú zsaroló email felismeréséhez, szükség lenne olyan kampányok indítására, melyek az információátadáson túl képesek a felhasználók atttitűdjének és viselkedésének valódi megváltoztatására. Ehhez szükségesek olyan pszichológiai ismeretek, mint a kognitív torzítások, heurisztikák működésmódjai, a társadalmi intervenciók jó gyakorlatai, vagy azon elmélete számbavétele, melyek az attitűd és a viselkedés diszkrepanciáját (lásd például privacy paradox, Kokolakis 2017) próbálják megmagyarázni.

Irodalom

Baruh, Lemi – Secinti, Ekin – Cemalcilar, Zeynep (2017). Online Privacy Concerns and Privacy Management: A Meta-Analytical Review: Privacy Concerns Meta-Analysis. *Journal of Communication*, *67*(1). 26–53. https://doi.org/10.1111/jcom.12276

Bergström, Annika (2015). Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses. *Computers in Human Behavior*, *53*. 419–426. https://doi.org/10.1016/j.chb.2015.07.025

Cho, Hichang – Lee, Jae-Shin – Chung, Siyoung (2010). Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior*, *26*(5). 987–995. https://doi.org/10.1016/j.chb.2010.02.012

Crawford, John R. – Henry, Julie D. (2004) The Positive and Negative Affect Schedule (PANAS): Construct validity, measurement properties and normative data in a large non-clinical sample. *British Journal of Clinical Psychology*, 43(3). 245–265. https://doi.org/10.1348/0144665031752934

Digital security – OECD. Oecd.Org. https://www.oecd.org/sti/ieconomy/digital-security/

Eurobarometer (2019) https://europa.eu/eurobarometer/surveys/detail/2249

Globalstat (2022) https://globalstat.eu/

Gottlob, Georg – Koch, Christoph – Pichler, Reinhard (2005) Efficient algorithms for processing XPath queries. *ACM Transactions on Database Systems (TODS)*, *30*(2). 444–491. https://doi.org/10.1145/1071610.1071614

Kokolakis, Spiros (2017) Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 64. 122134. https://doi.org/10.1016/j.cose.2015.07.002

Mai, Phuong Thao – Tick, Andrea (2021) Cyber Security Awareness and behavior of youth in smartphone usage: A comparative study between university students in Hungary and Vietnam. *Acta Polytech. Hung*, 18. 67–89. https://doi.org/10.12700/APH.18.8.2021.8.4

Maskall, Paul (2017) Risk and Digital Security: the perception versus reality and the cognitive biases of online protection. International Conference on Economic Sciences and Business Administration. Spiru Haret University, Vol. 4, No. 1. 280–287. http://icesba.eu/ocs/index.php/ICESBA2017/icesba2017/index https://doi.org/10.26458/v4.i1.33

Powell, Gregory E. – Seifert, Harry A. – Reblin, Tjark – Burstein, Phil J. – Blowers, James – Menius, J. Alan – Dasgupta, Nabarun (2016) Social Media Listening for Routine Post-Marketing Safety Surveillance. *Drug Safety*, *39*(5). 443–454. https://doi.org/10.1007/s40264-015-0385-6

Preibusch, Sören (2013) Guide to measuring privacy concern: Review of survey and observational instruments. *International Journal of Human-Computer Studies*, *71*(12). 1133–1143. https://doi.org/10.1016/j.ijhcs.2013.09.002

Schneier, Bruce (2015) *Secrets and lies: digital security in a networked world*. John Wiley & Sons. https://doi.org/10.1002/9781119183631

Schmidhuber, Jürgen (2015) Deep Learning in neural networks: An overview. *Neural Networks* 61 (2015). 86–104. https://doi.org/10.1016/j.neunet.2014.09.003

Turow, Joseph – Hennessy, Michael (2007). Internet privacy and institutional trust: Insights from a national survey. *New Media & Society*, *9*(2). 300–318. https://doi.org/10.1177/1461444807072219

Tversky, Amos – Kahneman, Daniel (1973) Availability: A heuristic for judging frequency and probability. *Cognitive psychology*, 5(2). 207–232. https://doi.org/10.1016/0010-0285(73)90033-9

van Gerven, Marcel – Bohte, Sander (2017). Editorial: Artificial Neural Networks as Models of Neural Information Processing. *Frontiers in Computational Neuroscience*, (Vol. 11). https://doi.org/10.3389/fncom.2017.00114

Watson, David – Clark, Lee Anna – Tellegen, Auke (1988) Development and Validation of Brief Measures of Positive and Negative Affect. The PANAS Scales. *Journal of Personality and Social Psychology*. 54(6). 1063–1070. https://doi.org/10.1037/0022-3514.54.6.1063