Médiakutató, 2023. tavasz
XXIV. évf. 1. szám, 21-37. o.
https://doi.org/10.55395/MK.2023.1.2

Bátorfy Attila – Bárdos Kata Kincső

Magyar újságírók digitális biztonsággal és zaklatással kapcsolatos tájékozottsága és eszközhasználata – kutatási eredmények[1]

Kérdőíves és fókuszcsoportos kutatásunkban azt vizsgáltuk, hogy a magyar újságírók és szerkesztőségek milyen ismeretekkel rendelkeznek a digitális biztonságról, valamint milyen tapasztalataik vannak az online zaklatással kapcsolatban. Kutatásunkból az derül ki, hogy a magyar újságírók kevésbé tájékozottak a digitális biztonság kérdésében, a legjellemzőbb az online zaklatás valamilyen formája, a válaszadók 43 százaléka nem használ semmiféle digitális védelmi eszközt, és az újságírók nem is magukat, hanem inkább a forrásaikat, a nyomozásaikat és a családjukat féltik, miközben többségük munkája természetes velejárójának véli az online zaklatásokat és támadásokat.

Kulcsszavak: digitális biztonság, megfigyelés, újságírás, védelem, zaklatás

Digital security awareness and device use among Hungarian journalists – research findings

Our online questionnaire and focus group research looked into the knowledge of Hungarian journalists and of newsrooms about digital security and digital safety. Our findings suggest that Hungarian journalists are little informed about digital security; some form of online harassment is the most frequent; 43 per cent of respondents do not use any tools for digital protection; and journalists are mainly not concerned about their own safety, but that of their sources, investigations and family; and most of them consider online harassment and attacks natural parts of their work.

Key words: digital safety, harassment, journalism, security, surveillance

1 A szerzők szeretnének köszönetet mondani Vajda Évának a kutatás előkészítésében és a szöveg végleges formájának létrehozásában betöltött nélkülözhetetlen szerepéért. A kutatást és a tanulmány megírását a Független Médiaközpont támogatta.

1. Bevezetés: az újságírók digitális biztonsága

Az újságírók biztonságát sokáig csak a fizikai erőszak (gyilkosság, verés, bebörtönzés), az egzisztenciális fenyegetettség (a politikai, a hirdetői, a tulajdonosi cenzúrák fajtái), továbbá a női újságírók elleni munkahelyi, szakmai vagy szexuális zaklatás felől kutatták. Az újságírók digitális biztonsága nemzetközi szinten is viszonylag friss kutatási terület, amelynek kiindulópontjaként az Edward Snowden által nyilvánosságra hozott amerikai digitális titkosszolgálati megfigyelési botrányt szokták megadni (Henrichsen et al. 2015, Angwin 2017, di Salvo 2021). A poszt-Snowden-időszak digitálisbiztonság-kutatása többnyire a jelenségek problematizálására, az újságírói gyakorlatok változására, továbbá az online zaklatások genderkülönbségeire helyezi a hangsúlyt (Henrichsen 2019, 2021, Tsui 2019, Tsui & Lee 2021, Watkins & Anderson 2019). A lokális kutatások nem példa nélküliek, de még mindig ritkák (Suraj & Olaleye 2017, Çalışkan 2019, Jamil 2020). Ezek a kutatások rendre azonos következtetésekre jutottak: az egyes országok megkérdezett újságírói kevés tudással rendelkeztek a digitális biztonságról, és – noha kifejezetten igényelték az erről való párbeszédet és tanulási lehetőségeket – nem értékelték különösen fontos területként.

A magyar újságírók digitális biztonságáról eddig nem született kutatás. A korábbi hazai újságíró-kutatások az általános demográfiai jellemzők, az értékpreferenciák és a karrierutak mellett a politikai és az üzleti nyomásgyakorlás, továbbá az egzisztenciális biztonságérzet mértékére kérdeztek rá (Vásárhelyi 1999, 2007, Mérték 2012, 2014), valamint az újságírónők helyzetére és a szerkesztőségen belüli diszkriminációjára (Végh 2020). A magyar újságírók online zaklatásáról interjúk alapján készült már rövidebb összefoglaló (Bajomi-Lázár 2021: 792), valamint átfogó jelentés is (Tófalvy 2017/2022).* Különösen a Tófalvy Tamás által készített jelentés következtetései közül mi is számos jelenséget tapasztaltunk. Ilyen például az online zaklatások „érzéketlenítő hatása", amelyet mi normalizációként fogalmaztunk meg, illetve az öncenzúra. Ezeken kívül néhány rövidebb hazai cikkben szólaltak meg magyar újságírónők az őket ért online zaklatás formáiról (Botás 2021, Rutai 2021). Korábban újságírók és civilek megfigyeléséről és azok törvényi hátteréről összeállított nemzetközi tanulmányban szerepeltek magyar újságírók is (Mills & Sarikakis 2016).

A trendszerű kutatói érdeklődés nem véletlen. Egyfelől a Pegasus-kémszoftver nemzetközi megfigyelési ügyében nem csupán politikusok, civilek, hanem újságírók, köztük magyar újságírók, többek között a Direkt36 két újságírója, Panyi Szabolcs és Szabó András tényfeltárók, illetve az akkor még az Átlátszónál dolgozó Csikász Brigitta bűnügyi újságíró és Németh Dániel fotóriporter is érintettek voltak (Panyi & Pethő 2021). A 2022-es választások előtt kikerülő, a Black Cube-ügyhöz nagyon hasonló módszerrel készített lejárató videók egyikét Kálmán Mátyás videós újságíróval készítették (Horn 2022). Másfelől azonban az újságírók egyre több digitális eszközt használnak a kommunikációra, az információgyűjtésre, a nyomozásra, a tárolásra, így ezeknek az eszközöknek a védelme, biztosítása kulcsfontosságú a munkavégzés szempontjából. Ebből fakad, hogy az újságírók digitális biztonsága olyan társterületeket is érint, mint a forrásvédelem és a szivárogtatás.

A szakmaspecifikus megfélemlítésnek az újságírók körében számos szakmai és pszichológiai-egészségügyi következménye lehet. A szakmaiságot és a munkát érintő káros következmények közé tartozik az öncenzúra, a kényesebb témák, források kerülése és a források elvesztése is, míg a pszichológiai-egészségügyi következmények között említendők a félelemérzet, az álmatlanság, a megalázottság-érzés, az önhibáztatás, a szorongás, a depresszió, az üldözési mánia, a szociális izoláció, a stressz, a gyakori fejfájás, az émelygés, a szédülés, a súlyvesztés/-gyarapodás és a gyomorbántalmak (Parker 2015: 2–3, Parker et al. 2017).

Természetesen az újságírók digitális biztonsága egy jóval nagyobb társadalmi-politikai jelenségcsoportba illeszkedik, úgy is, mint az állampolgárok személyes digitális adatainak profitérdekelt, sokszor összefonódó vállalati és politikai abúzusa, továbbá a főként, de nem kizárólag tekintélyelvű hatalmi berendezkedések az ellenőrzésre, megfigyelésre és követésre épülő digitális rezsimje (O'Neil 2016, Zuboff 2019).

* Tófalvy Tamás eredeti, 2017-es jelentésének kissé rövidített és szerkesztett verziója megjelent a Médiakutató 2022-es téli számában – A szerk.

A mi kutatásunk nem érinti az újságírók digitális biztonságának nagyobb társadalmi és politikai összefüggéseit. Ugyanakkor a kérdőívre kapott válaszok és még inkább a fókuszcsoportos beszélgetések során ezek az összefüggések rendre előkerültek. Nyilvánvaló, hogy az újságírók egy adott politikai és társadalmi környezetben végzik a munkájukat, így nem mellékes, hogy adott esetben milyen társadalmi, politikai, esetleg törvényalkotói jóindulatra vagy segítségre számíthatnak a digitális biztonság terén.[2] Ez a kérdés egyelőre nyitott, ám fontos megjegyezni, hogy Magyarországon az újságírók elleni online zaklatások, szervertámadások és megfigyelések fő megrendelője az eddigi ismereteink szerint nem a magánszektor, nem is a szervezett bűnözés, hanem – különféle proxyszereplőkön keresztül – a kormány.

2. A kutatás fókusza

Korábbi hazai kutatások hiányában kutatásunk során arra törekedtünk, hogy feltérképezzük az újságírókat ért online zaklatások kiterjedtségét, típusait, továbbá a digitális biztonságra vonatkozó újságírói és szerkesztőségi ismereteket, gyakorlatokat és protokollokat. A kutatás így az alábbi három részterületet érintette:

- az újságírókat ért online zaklatások gyakorisága, súlyossága és típusai,
- az újságírók digitális biztonsággal kapcsolatos ismeretei, gyakorlatai és eszközei, valamint
- a szerkesztőségek gyakorlatai, protokolljai és eszközei.

3. Definíciók

A digitális biztonságnak vannak személyes és szerkesztőségi dimenziói. Itt érdemes tehát tisztázni, hogy noha a magyar fordítás nem tesz különbséget a *digital security* és a *digital/online safety* között, a két fogalom még újságírói összefüggésben sem azonos (Geybullayeva 2022: 3). Míg a digital security az újságírók által használt eszközök, szoftverek digitális védelmét, megbízhatóságát jelenti, addig a digital safety az ezeket az eszközöket használók biztonságát, tájékozottságát, ismereteit. Mivel kutatásunk során mind a személyes, mind pedig a szerkesztőségi dimenzióra kíváncsiak voltunk, mindkét fogalom megjelenik az eredményekben, noha magyarul mi is csak a digitális biztonságot használjuk. A digitális biztonsággal kapcsolatban gyakran előkerülő fogalom továbbá az online zaklatás *(online harassment/abuse),* amelynek módja lehet az újságírók és/vagy környezetük jelszavainak, profiljainak, digitális eszközeinek feltörése, megfigyelése, követése is. Noha kutatásunk során az online zaklatásra vonatkozóan is fogalmaztunk meg kérdéseket, fókusza a digitális biztonság volt. Értelemszerűen vannak olyan jelenségek, amelyek egyszerre zaklatási és biztonsági kérdések is, így ezek a kérdések nem csupán az újságírók fejében kapcsolódnak össze, hanem a szakirodalomban is van átfedés.

Az általános digitális biztonsághoz szorosan kapcsolódnak kétirányú gyakorlatok, módszerek és eszközök. A visszaélés felőli gyakorlatok közé tartozik az adat- és a jelszólopás *(breaching)*, az adathalászat *(phishing)*, a profilok feltörése, a zsarolóvírusok használata, a *social engineering* (álprofilok általi megtévesztés), az online megfigyelés, a szerkesztőségi szerverek elleni támadás, továbbá újabban a mesterségesintelligencia-alapú megtévesztés, a személyazonosság-lopás is. Fontos, hogy ezek mindegyike bűncselekménynek számít (Mezei 2019) ha magánszemélyek vagy szervezett bűnözői körök követik el. Ugyanakkor a kormányoknak és rajtuk keresztül a rendvédelmi szerveknek, a titkosszolgálatoknak szigorú protokollok mentén felhatalmazásuk van ugyanezekkel a módszerekkel élni, ha nemzetbiztonsági kockázat merül fel, vagy a szervezett bűnözés elleni akció kívánja meg. A probléma akkor merül fel, ha a kormányok önkényesen definiálhatják, mi számít nemzetbiztonsági

2 Az egyelőre csak tervezet formában létező Európai Médiaszabadság Törvény (European Media Freedom Act, EMFA) 4. cikkének b és c pontjai megtiltják, hogy a kormányok lehallgassák az újságírókat, és hogy eszközeikre kémszoftvereket telepítsenek (EMFA 2022).

kockázatnak, a döntéshozatali struktúra és eljárásrend pedig szándékosan átláthatatlan és elszámoltathatatlan. Ezekben az esetekben a kormányok bármikor nemzetbiztonsági kockázatnak tekinthetnek újságírókat.

Az eddig említettek elleni védekezési gyakorlatok közé soroljuk a különféle jelszóvédelmeket, a többfaktoros azonosítást *(multi-factor authentification)*, a titkosított *(encrypted)* kommunikációt, a személyes adatokat nem rögzítő és továbbító keresőmotorok használatát, a szerkesztőségi szervervédelmet, a közösségimédia-protokollokat, és egyre gyakoribb a digitális eszközök, továbbá a közösségi média tudatos kerülése vagy használatuk radikális csökkentése is.

Ezeknek a támadó és védelmi módszereknek, eszközöknek a keverése és bonyolultsága egymásra hat. Ez azt jelenti, hogy jellemzően azokat az újságírókat támadják a legfejlettebb digitális módszerekkel, akiknek digitális biztonsági eszközhasználata is tudatosabb és fejlettebb. Minél értékesebb tehát a megszerezhető információ, az újságíró annál magasabbra emeli a belépési küszöböt, a támadó pedig annál magasabbra a befektetett erőforrásokat, mindaddig, ameddig még megéri neki.

4. Módszer és korlátok

Az általunk választott kutatási módszer két pillérre épült: egy kérdőívre és két fókuszcsoportos beszélgetésre. A kérdőív összeállítása során részben támaszkodtunk az Internews globális újságírást támogató szervezet korábbi nemzetközi kutatásának kérdőívére. A kérdőív 29, a digitális biztonságra, továbbá a demográfiára vonatkozó kérdést tett fel, amelyet 36 online és offline, közéleti témával foglalkozó szerkesztőségnek küldtünk el. A szerkesztőségek között független és kormánypárti, fővárosi és vidéki, online és nyomtatott lapok, nagy és kis létszámú szerkesztőségek egyaránt szerepeltek. Nem szerepeltek ugyanakkor televíziós és rádiós szerkesztőségek, ahogyan magazinok, egyéb időszaki kiadványok sem. Az előzetes, az impresszumok összeszámolása utáni becslésünk szerint ezekben a szerkesztőségekben összesen 650 belsős újságíró dolgozott a kérdőív kiküldésének idején. A kérdőív 2022. július 1. és július 31. között egy hónapig volt élő. A kérdőívezés során több *follow-up* is volt, továbbá számos főszerkesztőt kértünk meg arra, hogy segítsen a szerkesztőségben növelni a kitöltések számát. A kérdőívet végül 84 újságíró töltötte ki, ami közel 13 százalékos kitöltési aránynak felel meg. Ez a nemzetközi, online kérdőívek területén végzett metaelemzések alapján viszonylag alacsony kitöltési aránynak számít (Wu z et al. 2022), ám a hazai online kérdőíves felmérésekhez képest az átlagosnál magasabbnak.[3] Konkrétan az újságírók körében végzett online felmérések kitöltési hajlandóságáról nincs adatunk, mivel a megadott válaszadók száma mellett nem közölték a minta nagyságát.[4] Így azt sem tudjuk eldönteni, hogy ez a kitöltési hajlandóság szakmaspecifikus-e. Az alacsony kitöltési hajlandóság mindenesetre jelezheti azt is, hogy a témára a hazai újságírók eleve kevésbé fogékonyak, mint más, a szakmájukat érintő problémákra. A kitöltési hajlandóságot ugyanakkor nem torzította a szerkesztőségek mérete: minden szerkesztőségből nagyjából hasonló arányban töltötték ki a kérdőívet. A demográfiai összetevőknél a nemek, a területi elhelyezkedés és a szerkesztőségek tényleges arányainak megfelelően alakult a kitöltési hajlandóság. Néhány, különösen a több opciót is felkínáló vagy szabadszavas kérdésre adott válasznál a jobb érthetőség és az egyszerűsítés kedvéért néhány kategóriát összevontunk.

A két fókuszcsoportos beszélgetésre 2022. július 5-én és 11-én került sor. Mindkét beszélgetésen négy-négy újságíró vett részt különböző szerkesztőségekből. A második beszélgetésen csak női újságírók vettek részt. A fókuszcsoportos beszélgetések félig strukturált módon zajlottak. A személyes beszélgetést azért tartottuk fontosnak, hogy személyesebb történetekhez, mintázatokhoz jussunk hozzá. A beszélgetések előtt megegyeztünk,

3 Mivel erről nincsen hazai specifikus kutatás, ezt az állítást több, online kérdőívekkel kutató szakember megkérdezése után tesszük.

4 A Mérték a Publicus-szal közösen készített, már említett két Sajtószabadság-index kutatásának online kérdőívét (2012, 2014) 88 és 188 újságíró töltötte ki, de nem tudni, mekkora volt a konkrét vagy a becsült minta.

hogy azok a téma érzékenysége miatt anonim módon történnek, és a felhasznált válaszokat semmiképpen nem lehet majd sem személyhez, sem konkrét szerkesztőséghez kötni.

A kutatás feltáró jellege miatt – noha egyes kérdésekre adott jellemző válaszokkal kapcsolatban voltak előfeltevéseink – konkrét hipotéziseket nem fogalmaztunk meg.

5. A kutatás eredményei

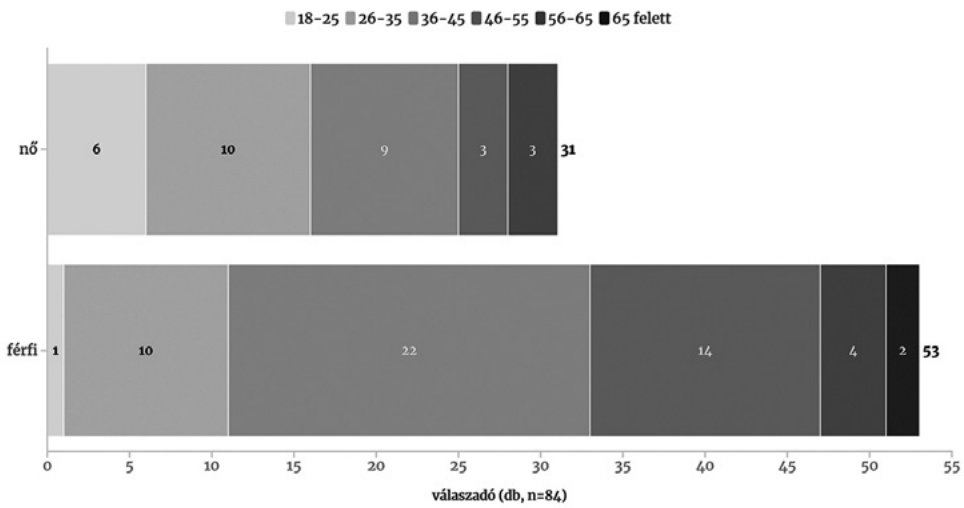
Az alábbi fejezetben azokat az eredményeket osztjuk meg, amelyek az olvasók, az újságírók és a szerkesztőségek számára relevánsak, tanulságosak és érdekesek lehetnek. A kutatás legfontosabb, az alfejezetekben részletezendő megállapításai a következők:

- a válaszadók 82 százalékát érte már az online zaklatás valamilyen formája
- a válaszadók legtöbbször jelszólopással találkoztak
- a válaszadók negyedének törték már fel az emailfiókját, és szintén negyedük telefonját hallgatták már le
- a válaszadók 43 százaléka semmilyen digitális védelmi eszközt nem használ
- a válaszadók leginkább használt eszköze a Signal titkosított kommunikációs eszköz
- az eszközhasználat hiányának indokaként megadott leggyakoribb válasz az ismeretek hiánya
- a tapasztalatok, az érintettség és az ismeretek terén nincs szignifikáns különbség a nem, a kor, az újságírói tapasztalat és a szerkesztőség nagysága szerint.

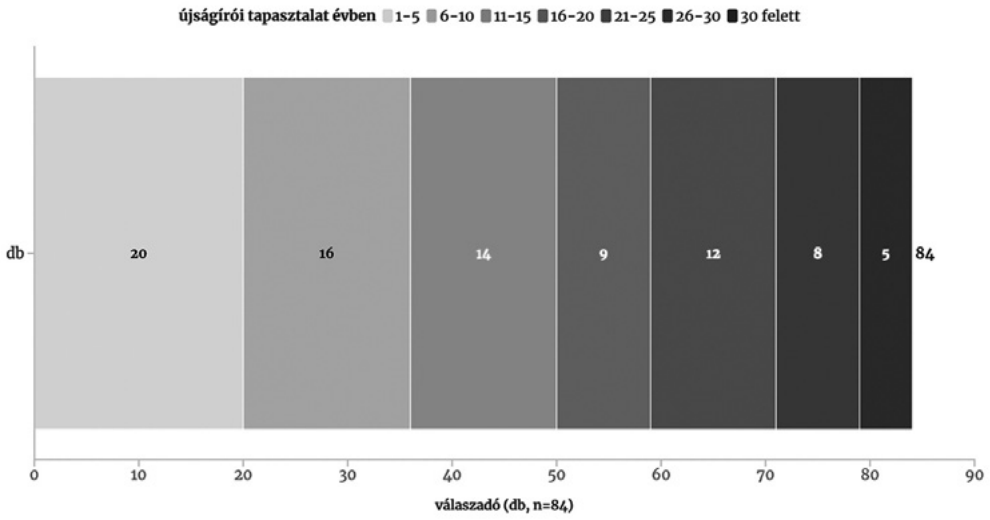
5.1. Általános demográfiai és karrierjellemzők

A kutatást összesen 84 újságíró töltötte ki, közülük 31 nő és 53 férfi (37 és 63 %). A korosztályok közül a legjellemzőbb a 36 és 45 év közötti (31 válasz, 37 %) (lásd az 1. ábrát). A születésük helyére nem kérdeztünk rá. Noha a szerkesztőségek között több vidéki szerkesztőség is szerepelt, mivel a munkahelyet nem volt kötelező megadni, nem tudjuk a fővárosi és a vidéki válaszadási arányt. A kérdőívben rákérdeztünk azonban arra, hogy mióta dolgoznak újságíróként. Itt a legtöbben, összesen 20 válaszadó (24 %) egy és öt év közötti időtartamot jelölt meg (lásd a 2. ábrát). A válaszadók megadhatták továbbá azt is, hogy a szerkesztőségen belül milyen területeken dolgoznak. Itt több opciót is választhattak. Ezek közül a politikai-közéleti terület volt a legjellemzőbb (47 válasz), utána a kultúra (30 válasz), gazdaság (24 válasz) és oknyomozás (17 válasz) (lásd a 3. ábrát).

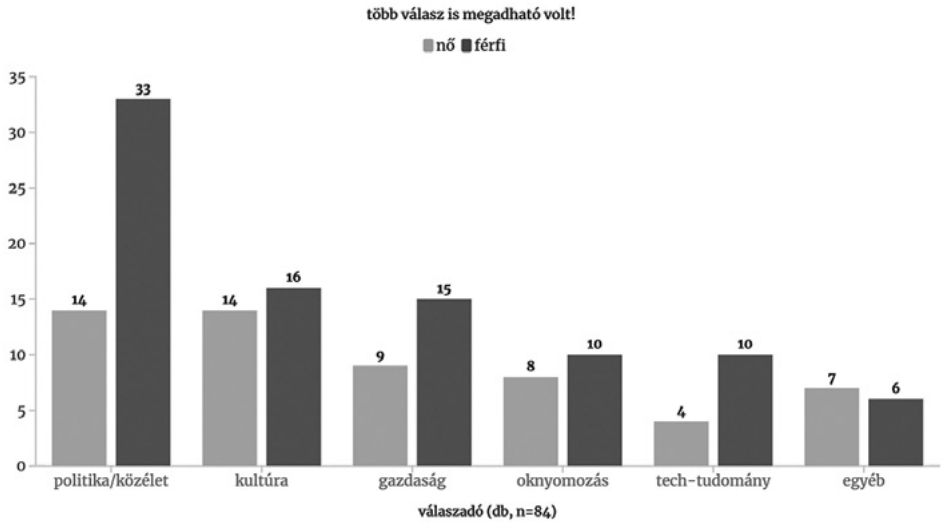
1. ábra
A válaszadók összetétele nem és kor szerint



2. ábra
A válaszadók összetétele az újságírásban eltöltött évek szerint



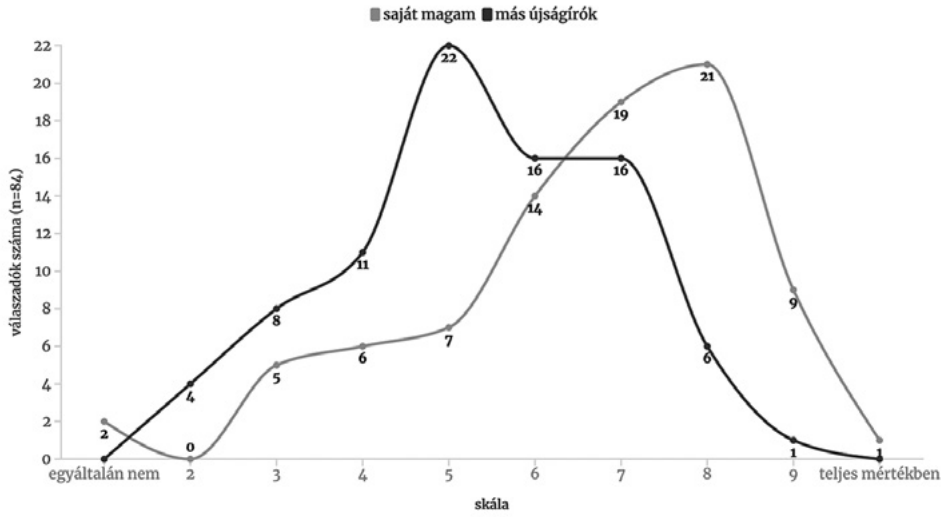
3. ábra
A válaszadók összetétele szakterületek és nemek szerint



5.2. Az újságírók saját tudásának és mások tudásának megítélése

Az ilyen jellegű kutatásoknál is általános tapasztalat, hogy a válaszadók a saját tudásukat, ismereteiket hajlamosak túlbecsülni, míg a munkatársaik, a szakmai környezetük tudását előzetesen jóval alacsonyabbra értékelik. A kérdőívben így arra kértük a válaszadókat, hogy egy 1 ponttól 10 pontig terjedő skálán értékeljék a saját és az újságírószakma digitális biztonsággal kapcsolatos előzetes tájékozottságát. Az alábbi eloszlásgörbe (lásd a 4.ábrát) jól szemlélteti, hogy a válaszadók a saját tájékozottságukat magasabbra értékelik, mint a többi újságíróét.

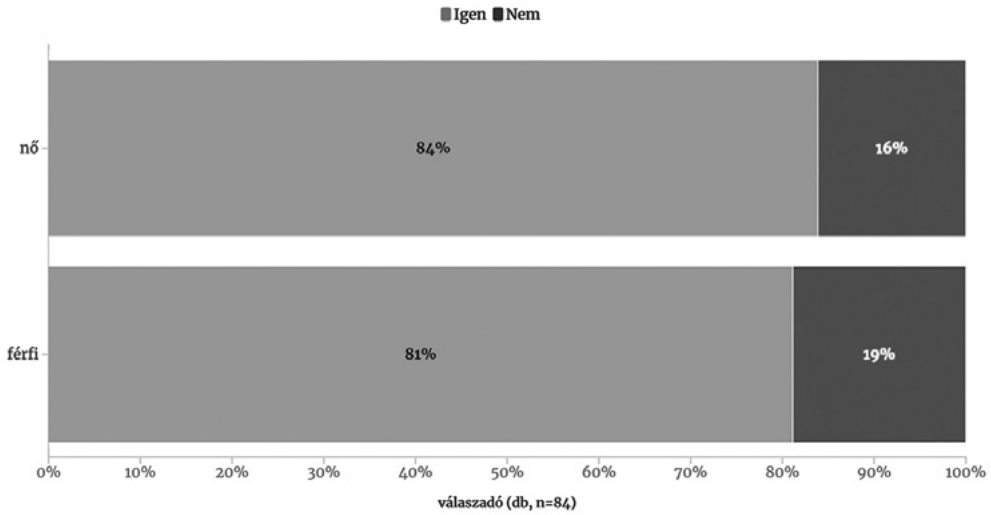
4. ábra
Mennyire érzed saját magad és más újságírókat tájékozottnak a digitális biztonság témakörében?



5.3. Az újságírók online zaklatással kapcsolatos tapasztalatai

Az alábbiakban a kérdőíves kutatásból nyert adatokat és magyarázatokat a felhozott tematikák mentén együttesen tárgyaljuk a fókuszcsoportos beszélgetések eredményeivel. A válaszadók 82 százaléka találkozott már az online zaklatás valamilyen formájával. Noha a különféle nemzetközi kutatások és a hazai cikkek azt sugallják, hogy a női újságírók gyakoribb áldozatai az online zaklatásnak, a kérdőívünkre adott válaszok alapján nincs lényeges különbség a nemek között (lásd az 5. ábrát). Elképzelhető, hogy ez az arány csak a kis elemszám miatt alakult így.

5. ábra
Tapasztaltad-e már az online zaklatás valamilyen formáját?



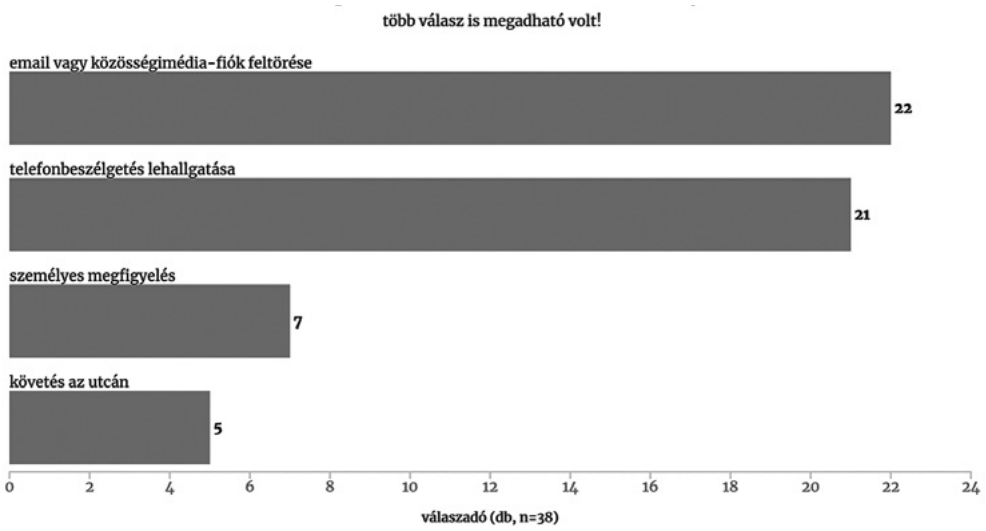
Nincsen egy jellegzetes zaklatási forma. Szinte minden válaszadó (n=69) kapott fenyegető üzeneteket kommentekben, emailben vagy chaten, továbbá találkozott trollkodással (a cikkhez fűzött rossz szándékú, cinikus, vagy az értelmes vitát szándékosan blokkoló, elterelő kommenttel). Volt olyan válaszadó, akit telefonon fenyegettek meg, egy másik válaszadó pedig azt a gyakorlatot említette, amikor egy újságíró fotóját uszító felhívással teszik ki szélsőséges Facebook-csoportok, blogok.

A fókuszcsoportos beszélgetésekben résztvevő újságírók mindegyike volt személyesen is alanya az online zaklatás valamelyik formájának. Mindegyikük kapott már fenyegető üzeneteket vagy a kinézetét gyalázó kommenteket. A női újságírók kiemelték, hogy ezek száma és intenzitása különösen a nyilvános szerepléseik után nő meg. Az újságírók a személyeskedő megjegyzések miatt öncenzúrát alkalmaznak védekezésképpen: bizonyos szerepeket vagy munkaköröket azért nem töltenek be, vagy eseményeken azért nem jelennek meg, hogy ne kapjanak támadásokat. Többüknek a családtagjaik is kaptak hasonló üzeneteket, és az is általánosan elterjedt gyakorlat, hogy a fotóikkal is visszaélnek. Politikai szereplők részéről is tapasztaltak retorikai abúzust, amikor olyan témákkal foglalkoztak, amelyeket az illetők sérelmeztek, de belenyugvóan úgy vélték, hogy az átpolitizált vagy nagyon érzékeny témákkal való foglalkozásnak az a következménye, hogy ezek a támadások elszaporodnak. Az online zaklatásra az egyik szerkesztőségnek protokollja is létezik, amin keresztül jogi eljárást is kezdeményeznek az ilyen esetek után, mivel nagyon gyakoriak az ilyen típusú támadások.

5.4. Az újságírók digitális biztonsággal kapcsolatos tapasztalatai

Sokkal kevesebben voltak azok a válaszadók, akik valamilyen digitális biztonsági károkozás áldozatának vallották magukat: mindössze a válaszadók 45 százaléka (n=38). A legjellemzőbb kár az email- és a közösségimédia-fiók feltörése, valamint a telefonbeszélgetések lehallgatása (lásd a 6. ábrát). Ez azt jelenti, hogy a válaszadók negyede volt már áldozata ennek a kettőnek.

6. ábra
Tapasztaltad-e már a következők valamelyikét?

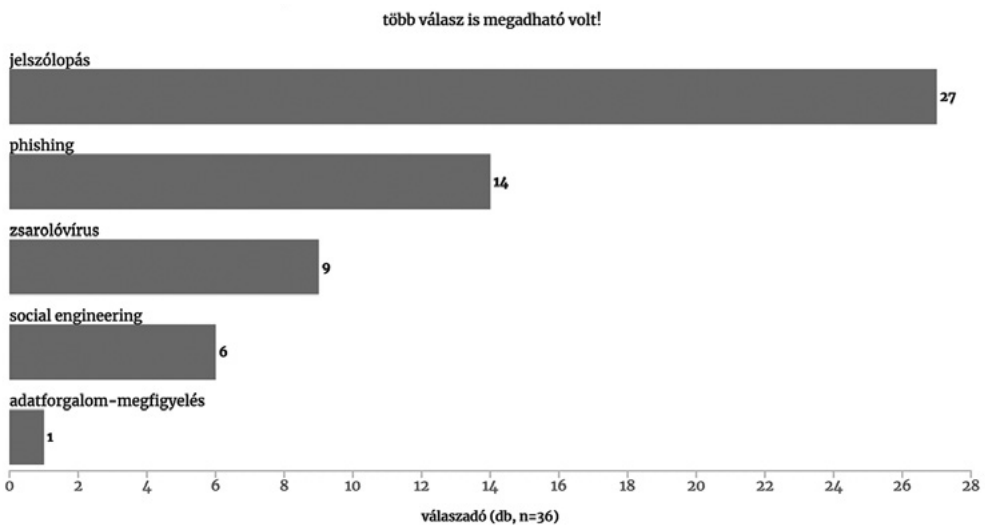


A károkozás típusai között a leggyakoribbnak a jelszólopást jelölték meg, a második legjellemzőbb károkozás pedig a phishing (adathalászat) (lásd a 7. ábrát).

A fókuszcsoportos beszélgetések az eredményeket annyiban kiegészítették, hogy igazolták azt az elméleti részben idézett, ám a kérdőívben nem vizsgált megállapítást, hogy a kémszoftveres, komolyabb erőforrás-

befektetést kívánó támadásoknak inkább azok az újságírók vannak kitéve, akikről a támadó eleve feltételezi, hogy alternatív módszereket és összetettebb digitális védelmet használnak.

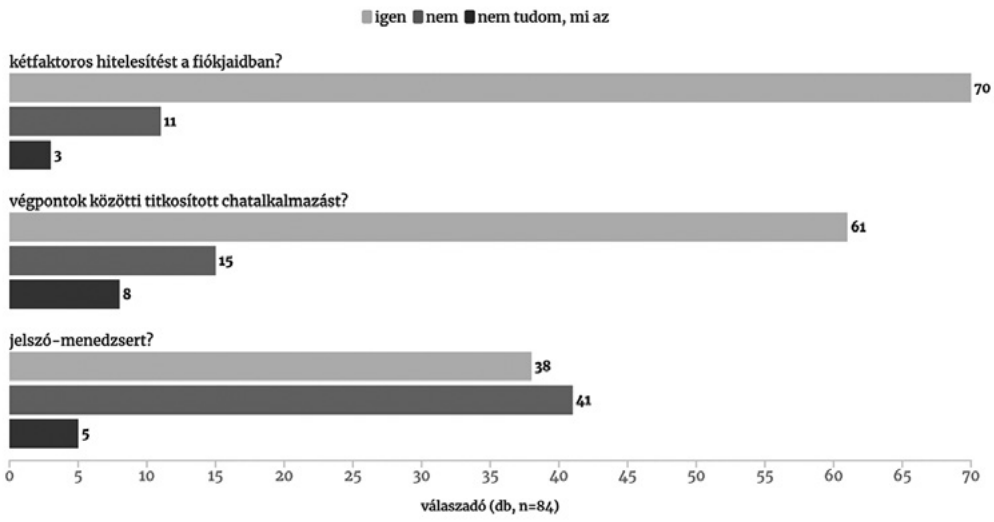
7. ábra
Voltál-e már áldozata a következőknek?



5.5. Az újságírók digitális biztonsági eszközhasználata

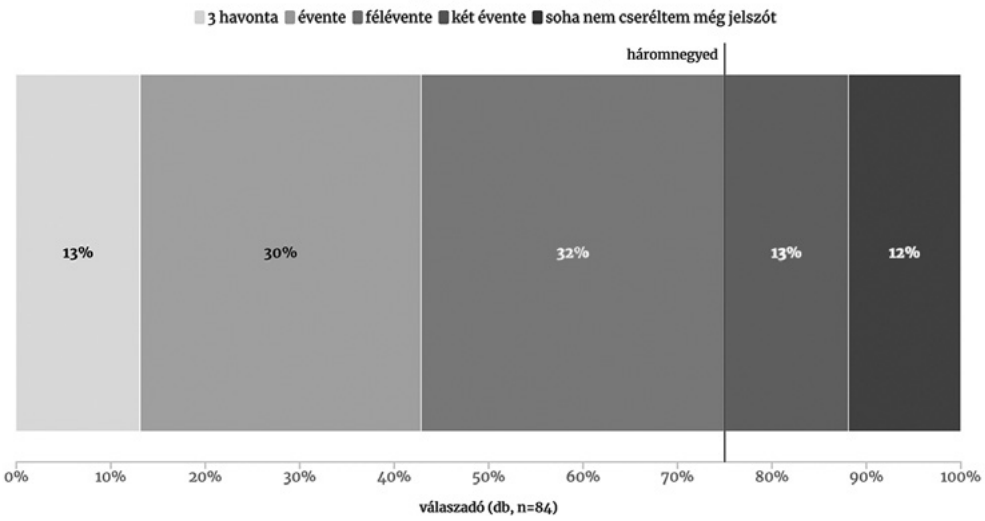
A válaszokból az derült ki, hogy a legtöbben használnak valamilyen digitális módszert vagy eszközt a kommunikációjuk védelmére. A többség (83 %) használ kétfaktoros azonosítást a különféle fiókjaiban, továbbá használ (73 %) végpontok közötti titkosított chatalkalmazást. Még a sokak által nem kedvelt jelszómenedzser-alkalmazást is a válaszadók 45 százaléka használja (ez olyan szoftver, amely egy bonyolult mesterjelszóval védi az összes jelszót, de elég csak a mesterjelszót megjegyezni) (lásd a 8. ábrát).

8. ábra
Használsz-e...

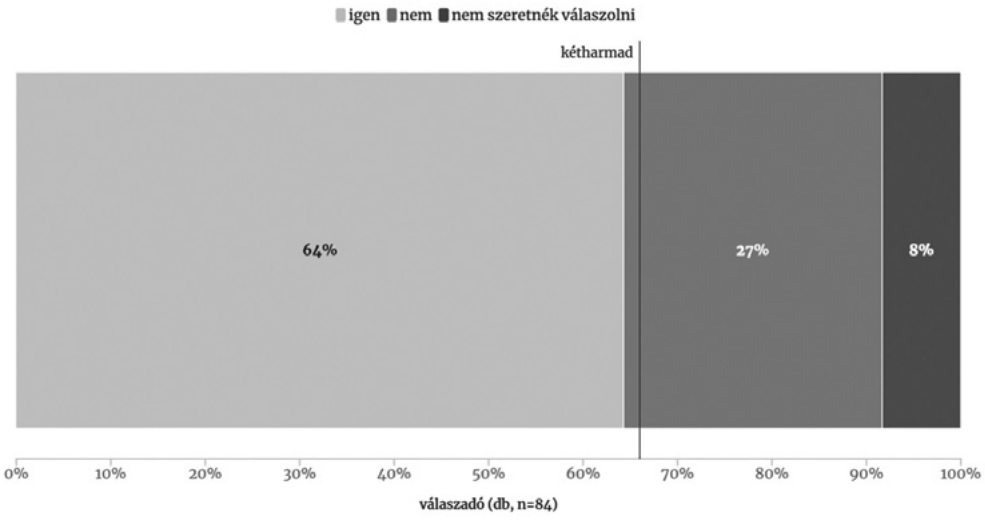


Mivel az újságírók eszközeihez, kommunikációjához és profiljaihoz a jelszavukon keresztül vezet az egyik legkönnyebb út, kíváncsiak voltunk arra, hogy egyfelől milyen gyakran cserélnek jelszavakat, másfelől használják-e ugyanazt a jelszót több helyen is. Mindenképpen a tudatosság magas indikátora, hogy a válaszadók háromnegyede legalább évente cserél jelszót (lásd a 9. ábrát), ugyanakkor közel kétharmaduk ugyanazt a jelszót egyszerre több emailhez, profilhoz is használja (lásd a 10. ábrát).

9. ábra
Milyen gyakran cserélsz jelszót?

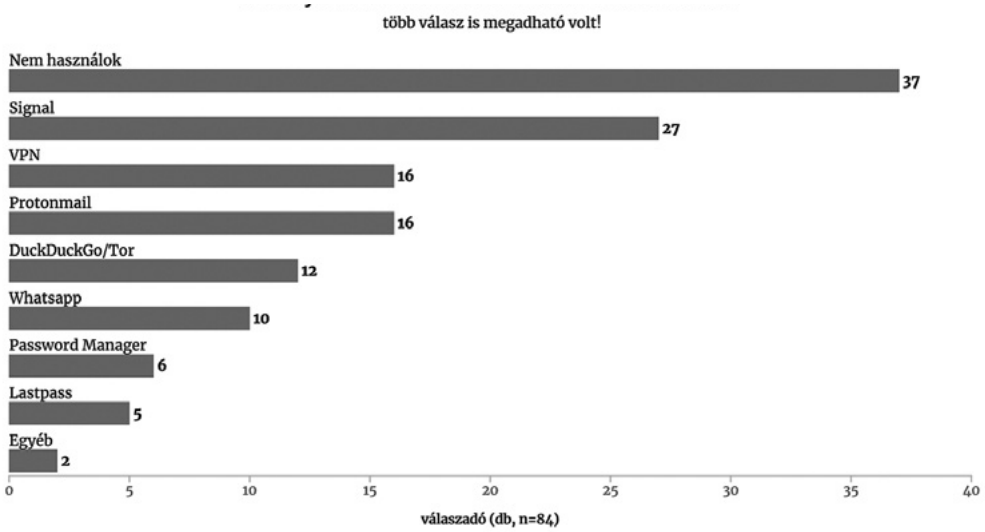


10. ábra
Használod-e ugyanazt a jelszót egyszerre több fiókhoz is?

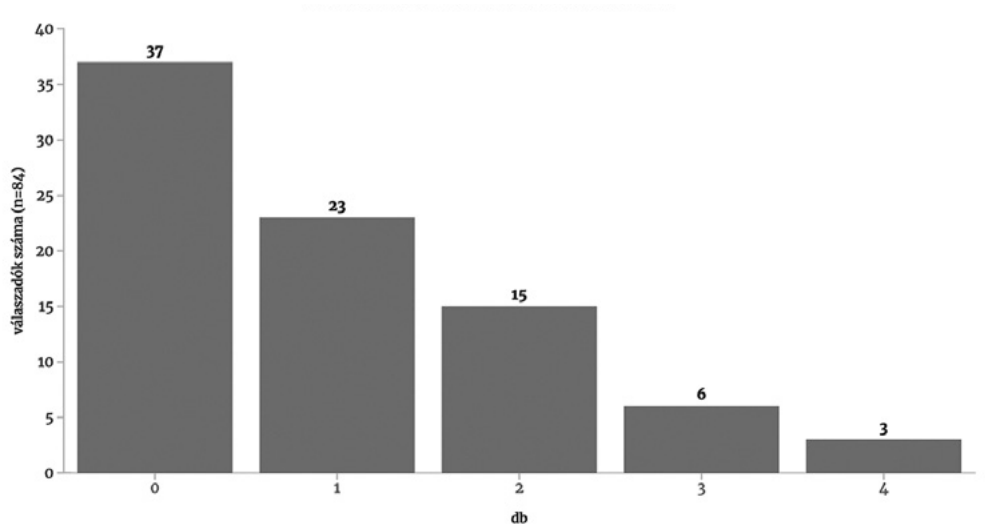


A konkrét eszközök közül a közelmúltban számos biztonsági problémát felvető, két végpont között titkosított üzenetváltást és telefonálást lehetővé tévő Signal a leginkább használt alkalmazás (27 válaszadó), ám 16–16 válaszadó jelölte meg a VPN-klienst (Virtual Private Network) és a titkosított emailklienst, a Protonmailt. Ugyanakkor 37 válaszadó semmilyen dedikált szoftvert, alkalmazást sem használ tevékenysége digitális védelmére (lásd a 11. ábrát). Az összes válaszadó 27 százaléka legalább egy alkalmazást használ (lásd a 12. ábrát).

11. ábra
Mely alkalmazásokat használod az alábbiak közül?



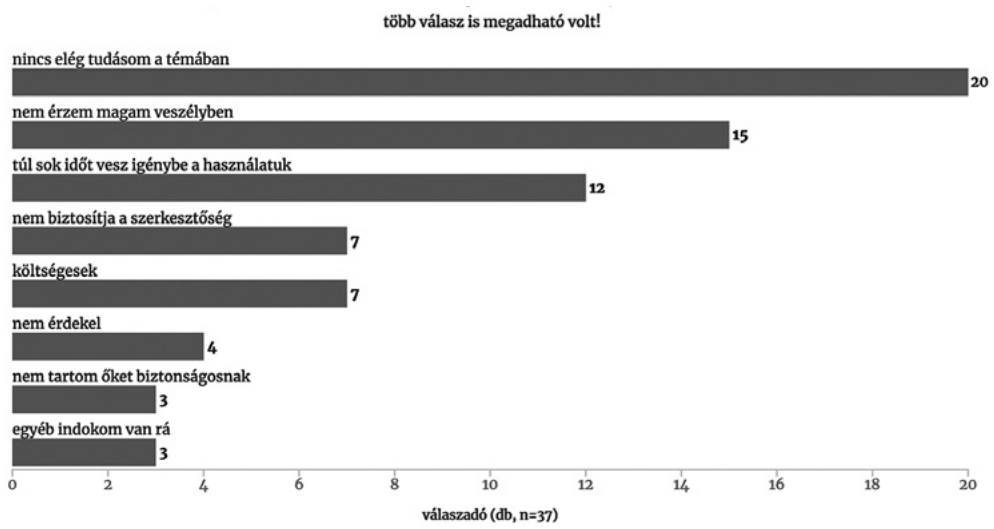
12. ábra
Használt alkalmazások száma



Arra is kíváncsiak voltunk, hogy mik az indokaik azoknak, akik semmilyen alkalmazást, eszközt nem használnak. Noha a leggyakoribb indok a tudáshiány volt, a második helyre az az indok került, hogy nem érzik magukat veszélyben. Érdekes továbbá, hogy heten azt is megjelölték indokként, hogy ezek az alkalmazások költségesek, miközben ezek az alkalmazások ingyenesek, vagy bizonyos használati szint (tárhely, együttes használat) alatt ingyenesek (lásd a 13. ábrát).

A fókuszcsoport résztvevői a biztonsági módszerek közül egyértelműen a többfaktoros hitelesítést tartották a legkörülményesebbnek, és ezzel magyarázták azt is, hogy számos kollégájuk nem is használja azt. Ugyanakkor a kérdőívben említetteken kívül egyéb biztonsági módszereket is alkalmaznak. Az egyikük például elmondta, hogy a szerkesztőségen belül a Signal-kommunikációnál eleve megtévesztő neveket adnak a chatszobáknak. Többen említették továbbá, hogy kényes témáknál, fontos oknyomozásoknál eleve a személyes megbeszélést alkalmazzák, ilyenkor a telefonokat is vagy kikapcsolják, vagy nem is viszik be őket a tárgyalószobába. Mások az eddig említett megoldásokon kívül említették még az álnevek és az álprofilok használatát a közösségi médiában, illetve a külön munkacélú telefon használatát.

13. ábra
Ha nem használsz ilyen eszközöket, akkor miért nem?



Arra is próbálnak figyelni néhányan, hogy a szerkesztőségi rendszerekben mindenkinek csak ahhoz legyen hozzáférése, amihez feltétlenül szükséges, mivel úgy tapasztalták, hogy egy emberen keresztül már könnyen feltörhetik egy teljes szerkesztőség rendszerét. Az érzékenyebb anyagokat úgy védik, hogy nem kerülnek fel a szerkesztőségi rendszerbe idő előtt, illetve papíron kinyomtatva kezelik azt a szerkesztők.

5.6. A szerkesztőségek közös ismeretei, gyakorlatai

Az újságírók többsége még mindig szerkesztőségi környezetben végzi a munkáját, és a károkozás számos esetben nem is egyenként érinti az újságírókat, hanem szerkesztőségek ellen követik el. Több interjúalanyunk is kiemelte, hogy a szerkesztőség tagjainak gondatlansága és nemtörődömsége, valamint a szerkesztőségi gépek nem megfelelő biztonsága is védelmi rést jelenthet. Ezért arra is rákérdeztünk, hogy a szerkesztőségben beszélnek-e ezekről a veszélyekről, aggályokról. A válaszadók közel kétharmada (53 válaszadó) azt válaszolta, hogy ezek a témák napirenden vannak. Ez természetesen nem jelenti azt, hogy a magyar szerkesztőségek kétharmadában ez folyamatosan tárgyalt probléma volna. Ráadásul ha a megadott munkahelyekre bontjuk a válaszokat, akkor ellentmondásos lesz ez az arány. Négy olyan szerkesztőség is van a válaszokban, amelynek munkatársai vegyesen válaszoltak erre a kérdésre igennel vagy nemmel.

Hasonló ellentmondást találtunk az arra a kérdésünkre adott válaszokban is, hogy a szerkesztőségen belül létezik-e valamilyen kötelezően betartandó biztonsági protokoll. A válaszadók 51 százaléka válaszolt igennel, 49 százaléka nemmel. Viszont ha ismét lebontjuk a szerkesztőségekre a válaszokat, akkor három olyan szerkesztőséget is találunk, amelynek munkatársai vegyesen válaszoltak igennel vagy nemmel. Ennek a két ellentmondásnak az oka lehet a szerkesztőségen belüli rossz minőségű vagy aszimmetrikus kommunikáció, az információhiány (valaki rosszul tud valamit), az elvárás és a kötelezővé tétel közötti vékony határvonal, és lehet a válaszadó újságírók különféle munkahelyi státusa (belsős, állandó külsős), pozíciója (junior, senior, rovatvezető, szerkesztő), szakterülete (politika vs. sport) is.

Alighanem inkább az információhiányra vezethető vissza az, hogy amikor azt kérdeztük, a szerkesztőségben van-e olyan dedikált munkatárs, szakember, akihez a digitális biztonsággal kapcsolatos problémákkal, kérdésekkel lehet fordulni, akkor számos szerkesztőségnél arányaiban sokkal több munkatárs válaszolt igennel, mint nemmel. Feltételezhető, hogy a nemmel válaszoló munkatárs inkább csak nem tudja, hogy a szerkesztőségen belül van ilyen munkatárs.

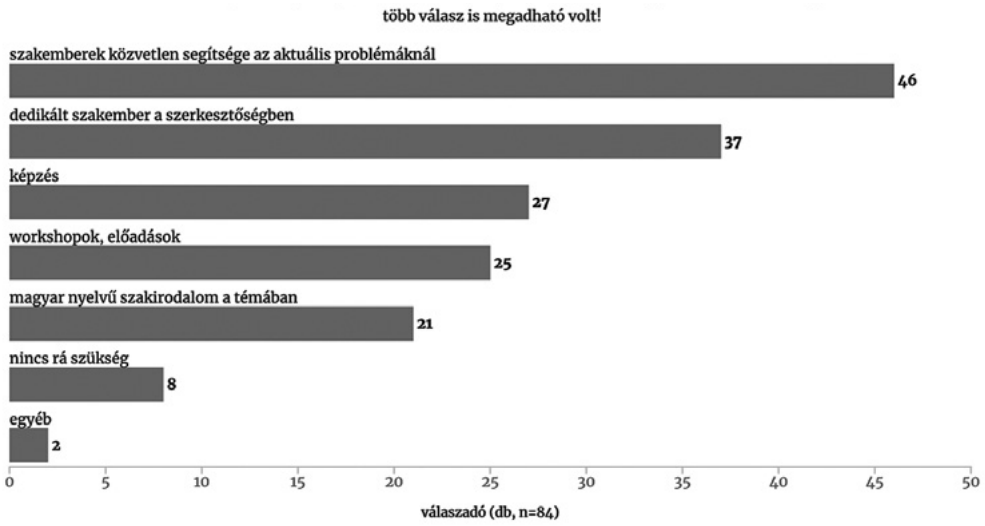
A fókuszcsoportos beszélgetések során felmerült továbbá a szerkesztőség közös fellépésének hiánya is. A résztvevők úgy látták, hogy még egy nagyobb szerkesztőségben sincsen kapacitás, illetve erőforrás arra, hogy utánajárjanak, kik állnak a digitális biztonsági fenyegetések és támadások mögött, a kisebb szerkesztőségekben pedig ez fel sem merül. Minél nagyobb egy szerkesztőség, annál inkább téma a digitális biztonság, és annál nagyobb fokú a védelem is.

Végezetül fontos kiemelni, hogy a digitális biztonság kérdése a szerkesztőségi gyakorlatokon is túlmutat. Mint arra a fókuszcsoportban résztvevők rámutattak, egy újságíró számára nem csupán a saját digitális védelmi tudása fontos, hanem az ismerősei, a családtagjai és a forrásai ismeretei is. Hiszen ők hiába védekeznek a támadások ellen, ha a kapcsolataik ezt nem teszik meg, akkor a támadók bizalmas üzenetekhez, információkhoz ezeken a kapcsolatokon keresztül ugyanúgy hozzáférhetnek.

5.7. Lehetséges segítségek

Végül azt is szerettük volna megtudni, hogy az újságíróknak milyen segítségre lenne szükségük a digitális biztonság terén. A legtöbben a személyes, dedikált segítséget jelölték meg, akár szerkesztőségen belüli ez a szakember, akár külsős szakemberről van szó (lásd a 14. ábrát).

14. ábra
Milyen segítségre lenne szükséged, vagy szüksége a szerkesztőségnek?



A fókuszcsoportos beszélgetések alapján különösen az online zaklatásnak kitett újságírók mentális egészségével kellene többet foglalkozni az esetek után, és szakemberek segítségét, pszichológiai tanácsadást javasolnának és igényelnének. Az egyik fontos, bár nem örömteli konklúziója a beszélgetéseknek az volt, hogy noha a zaklatások és a digitális fenyegetések normalizálását és relativizálását veszélyesnek tartják, ezeket a fenyegetéseket a mindennapi valóság részeként kell elfogadni, miközben a védelemre egyre nagyobb hangsúlyt kell fektetni. A jelenleg hatályos törvények szigorítását vagy speciális törvények meghozatalát[5] ugyanakkor nem tartják sem szükségesnek, sem segítségnek, mivel elméletben a hatályos törvényeknek is meg kellene tudniuk védeni őket. A résztvevők azt tartanák átfogó és hosszú távú megoldásnak a törvénykezés helyett és előtt, ha a laptulajdonosok és a szerkesztőség vezetése lenne kiképezve a digitális biztonság témakörében, az újságírókat pedig tanáccsal és oktatással segítenék a mindennapi munkájukban.

5 Itt csak lábjegyzetben térünk ki arra, hogy noha speciálisan az újságírók megfigyelésére vonatkozó törvény nincs Magyarországon, a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény szabályozza az állampolgárok megfigyelésének lehetőségeit és körülményeit. A megfigyelésnek, illetve titkos információszerzésnek szigorú kritériumai vannak, és rendészeti vagy nemzetbiztonsági okból rendelheti el az Igazságügyi miniszter. A Pegasus-ügyben sem a Nemzeti Adatvédelmi és Információszabadság Hivatal (NAIH), sem a Központi Nyomozó Főügyészség (KNYF) nem tárt fel jogsértést, vagyis álláspontjuk szerint nem történt jogosulatlan megfigyelés. A Társaság a Szabadságjogokért szervezet szerint azonban jogsértő volt a Pegasus-ügy (TASZ 2022).

Megjegyzendő, hogy ilyen képzések, oktatási segédanyagok amúgy több nemzetközi szervezet oldaláról is elérhetők, akár magyar nyelven is. Tudomásunk szerint több szerkesztőségben is indultak időközben belső képzések. Különösen pedig a Pegasus-ügy után az újságírók körében elindult valamiféle párbeszéd is a digitális biztonság kérdésköréről.

6. Összegzés és következtetések

Mivel a kutatás során csak kevés újságírót tudtunk megszólítani, érdemes a kutatás megállapításait eszerint értékelni. Ugyanakkor mind a kérdőívben, mind a fókuszcsoportban feltettünk kifejezetten a szerkesztőségi gyakorlatokra vonatkozó kérdéseket is, így a válaszokból mégis kirajzolódik az egyéni tapasztalatokon túlmutató gyakorlat is. Kutatásunk rámutatott a válaszadó újságírók digitális biztonság terén szerzett tapasztalataira, továbbá ismeretbeli hiányosságaikra. A legtöbb válaszadó volt már alanya valamiféle online zaklatásnak, ahogy volt már elszenvedője valamilyen digitális bűncselekménynek is. Ez természetesen nem meglepő, és nem csupán az újságírókat érintő probléma. Ugyanakkor a kérdőívekre adott válaszokból, továbbá a fókuszcsoportos beszélgetésekből világosan kiderül, hogy az újságírók leginkább a magyar kormány és szervei aktív szerepét emelték ki. Jellemző és visszatérő fordulat volt a kormány által finanszírozott online zaklatás, a trollfarmok működtetése, továbbá a kormány különféle megfigyelési és kémszoftverbotrányokban való, oknyomozó cikkekkel bizonyított érintettsége. A fókuszcsoportos beszélgetések alapján megállapítható, hogy az újságírók hajlamosak normalizálni az online zaklatást, mivel ez része az újságírói munkának, amivel együtt kell tudniuk élni.

Érdekes továbbá, hogy az újságírók leginkább nem a saját fizikai és mentális egészségüket, továbbá egzisztenciájukat féltik, hanem a családi és a baráti környezetükét, például abban a formában, hogy egy családtagjuk, barátjuk azért veszíti el a munkáját, mert ők maguk újságírók. Ezek a kapcsolatok digitális megfigyeléssel, adatalapú profilozással ma már sokkal könnyebben feltárhatók, mint korábban. Ez akár már rövid távon is öncenzúrához vagy a kényesebb témák elhagyásához vezethet. Emellett általános volt az attól való félelem is, hogy egyre kevesebb ember mer majd szívárogtatni, a háttérben információkat, dokumentumokat megosztani vagy forrásként név nélkül nyilatkozni egy-egy cikkhez. Noha a pályaelhagyás gondolata senkiben nem merült fel, a tanulmány szerzői ismernek olyan újságírókat, akiknek a karrierváltásában a fentebbi okok ha nem is kizárólagos, de jelentős szerepet játszottak. Az újságírók digitális biztonsága tehát egyre fontosabb kérdés lesz a demokratikus nyilvánosság szemszögéből is.

Ennek minden aspektusát és mélységét kutatásunk nem tárta fel. Egy jövőbeli, megismételt és kibővített kutatáshoz a televíziós és a rádiós újságírókat is be kell majd vonni, továbbá érdemes lenne a médiafogyasztók körében is rákérdezni a digitális biztonsággal kapcsolatos tapasztalataikra. Annál is inkább, mert a magyar társadalom jellemzően és egyre nagyobb mértékben etatista (Szabó 2009, Bíró-Nagy et al. 2016: 10–12, Szabó & Gerő 2020), ami nem csupán a szociális és gazdasági kérdésekben mutatkozik meg, hanem abban is, hogy a társadalom újabb és újabb csendes felhatalmazásokat ad a kormánynak arra, hogy a befolyását, a preferenciáit, az ideológiáját az élet egyre több területére kiterjessze. Ebből is fakadhat, hogy a magyar kormány folyamatos határátlépései nemhogy semmilyen ellenreakciót nem váltanak ki a magyar társadalomból, hanem a társadalom nagyobbik része helyesli és támogatja a kormány ilyen akcióit, ezek között is az újságírók digitális megfigyelését, titkosszolgálati profilozását.

A magyar kormány 2022. júniusában az évi 60 milliárd forintos keret mellé további 30 milliárd forinttal növelte a Miniszterelnöki Kabinetiroda, azon belül is a Rogán Antal irányítása alá tartozó titkosszolgálatok büdzséjét, arra hivatkozva, hogy a többletfeladatokhoz többletkeret is jár. Orbán Viktor miniszterelnök azzal indokolta a törvényt, hogy „az ország függetlenségét és szuverenitását számos támadás éri majd a következő időszakban".[6] Alighanem az újságírók elleni megfigyelések, digitális támadások száma növekedni fog,[7] éspedig elsősorban nem az ország függetlenségét érő támadások miatt, hanem a magyar kormány újságírók digitális megfigyelését, titkosszolgálati profilozását végző gyakorlata miatt.

6 Harmincmilliárddal növelné a titkosszolgálatok kiadásait a kormány. *Telex.hu,* 2022. VII. 5.

7 A miniszteri engedéllyel végzett megfigyelések száma a 2015-ös évi 1038 esetről 2021-re 1469-re nőtt (Lengyel 2022).

Adatok

A nyers adat erről a linkről tölthető le: https://docs.google.com/spreadsheets/d/1KErF2o_FPA3vInslnMGa-EuC29WFnD-6e-3apyA6zh0/edit?usp=sharing

Irodalom

Angwin, Julia (2017): Digital Security for Journalists. In: Emily Bell, Taylor Owen, Smitha Khorana & Jennifer R. Henrichsen (eds.): *Journalism after Snowden. The Future of the Free Press in the Surveillance State,* pp. 114–129. New York: Columbia University Press, https://doi.org/10.7312/bell17612-010

Bajomi-Lázár, Péter (2021): Hungary. In Marlis Prinzig & Roger Blum (eds.): *Handbuch Politischer Journalismus,* pp. 789–793. Köln: Herbert von Halem Verlag.

Bíró-Nagy András, Dobszai Dalma, Kadlót Tibor & König Annamária (2016): *Rendszerváltás, demokrácia és a magyar társadalom.* Budapest: Friedrich-Ebert-Stiftung.

Botás Enikő (2021): „Bárcsak belehaltál volna a szülésbe" – női újságíróként a szexista támadásokkal is meg kell küzdeni. *Marie Claire*, 2021. II. 11., https://marieclaire.hu/riporter/2021/02/11/noi-ujsagirok-szexista-zaklatas/.

Çalışkan, Behlül (2019): Digital Security Awareness and Practices of Journalists in Turkey: A Descriptive Study. *Conflict & Communication,* vol. 18, no. 1.

Di Salvo, Philip (2021): "We Have to Act Like Our Devices are Already Infected": Investigative Journalists and Internet Surveillance. *Journalism Practice*, vol. 16, no. 9, pp. 1849–1866, https://doi.org/10.1080/17512786.2021.2014346

EMFA (2022): *European Media Freedom Act. Proposal,* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0457.

Geybullayeva, Arzu (2022): *Online Safety and Digital Security for all Journalists. A Prerequisite for Media Freedom.* Vienna: OSCE.

Henrichsen, Jennifer, Michelle Betz & Joanne M. Lisosky (2015): *Building Digital Safety for Journalism. A Survey For Selected Issues.* Paris: UNESCO.

Henrichsen, Jennifer (2019): Breaking Through the Ambivalence: Journalistic Responses to Information Security Technologies. *Digital Journalism,* vol. 8, no. 3, pp. 328–346, https://doi.org/10.1080/21670811.2019.1653207

Henrichsen, Jennifer (2021): Understanding Nascent Newsroom Security and Safety Cultures: The Emergence of the "Security Champion." *Journalism Practice,* vol. 16, no. 9. pp. 1829–1848, https://doi.org/10.1080/17512786.2021.1927802

Horn Gabriella (2022): Mutatjuk, kik és hogyan csinálták az újságírókat lejárató interjúkat a Fidesz-kampányhoz. *Átlátszó,* 2022. II. 6.

Jamil, Sadia (2020): Red Lines Of Journalism: Digital Surveillance, Safety Risks and Journalists' Self-Censorship in Pakistan. In: Anna Grøndahl Larsen, Ingrid Fadnes & Roy Krøvel (eds.): *Journalist Safety and Self Censorship,* pp. 29–46. London: Routledge, https://doi.org/10.4324/9780367810139-3

Lengyel Tibor (2022): Titkosították, ki írja alá Varga Judit tárcájánál a titkosszolgálati megfigyeléseket. *Hvg.hu,* 2022. V. 24.

Mezei Kitti (2019): A kiberbűncselekmények hazai szabályozásának aktuális kérdései. *Magyar Jog,* 5. sz. 305–314. o.

Mérték (2012): *Sajtószabadság-index 2012*. Budapest: Mérték Médiaelemző Műhely.

Mérték (2014): *Sajtószabadság-index 2013*. Budapest: Mérték Médiaelemző Műhely.

Mills, Anthony & Katherine Sarikakis (2016): Reluctant Activists? The Impact of Legislative and Structural

Attempts of Surveillance on Investigative Journalism. *Big Data & Society,* vol. 3, no. 2, pp. 1–11, https://doi.org/10.1177/2053951716669381

O'Neil, Cathy (2016): *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy.* New York: Crown.

Panyi Szabolcs & Pethő András (2021): Lelepleződött egy durva izraeli kémfegyver, az Orbán-kormány kritikusait és magyar újságírókat is célba vettek vele. *Direkt36*, 2021. VII. 19.

Parker, Kelsey (2015): *Aggression Against Journalists. Understanding Occupational Intimidation of Journalists Using Comparisons With Sexual Harassment.* Phd Dissertation. Tulsa: University Of Tulsa.

Parker, Kelsey, Susan Drevo, Nigel Cook, Autumn Slaughter & Elana Newman (2017): *Journalists and Harassment.* New York: Columbia Journalism School, Dart Center For Journalism And Trauma.

Rutai Lili (2021): „Menstruálsz vagy régen dugtál?" – szexizmus és zaklatás nehezíti az újságírónők munkáját. *Átlátszó,* 2021. III. 12.

Suraj, Olunifesi Adekunle & Olawale Olaleye (2017): Digital Safety Among Nigerian Journalists. Knowledge, Attitudes and Practice. In: Ulla Carlsson & Reeta Pöythäri (eds.): *The Assault on Journalism. Building Knowledge to Protect Freedom of Expression*, pp. 329–333. Göteborg: NORDICOM.

Szabó Andrea & Gerő Márton (2020): A magyar társadalom politikai integrációja. In: Kovách Imre (szerk.): *Mobilitás és integráció a magyar társadalomban,* 89–128. o. Budapest: Argumentum & MTA Társadalomtudományi Kutatóközpont.

Szabó Máté (2009): Autonómia és etatizmus a civil társadalomban. *Politikatudományi Szemle*, 18. évf. 3. sz. 157–163. o.

TASZ (2022): Mindent megtesz a kormány, hogy eltusolja a Pegasus-ügyet. A botrány kirobbanása óta eltelt egy év mérlege. *ataszjelenti.444.hu,* 2022. VII. 18.

Tófalvy, Tamás (2017/2022): Újságírók online zaklatása Magyarországon. *Médiakutató,* 23. évf. 3–4. sz. 79–88. o.

Tsui, Lokman (2019): The Importance of Digital Security to Securing Press Freedom. *Journalism,* vol. 20, no. 1, pp. 80–82. https://doi.org/10.1177/1464884918809276

Tsui, Lokman & Francis Lee (2021): How Journalists Understand the Threats and Opportunities of New Technologies: A Study of Security Mindsets and its Implications for Press Freedom. *Journalism,* vol. 22, no. 6, pp. 1317–1339, https://doi.org/10.1177/1464884919849418

Végh Veronika (2020): *Az újságírónők helyzete a mai magyar médiában.* MA-szakdolgozat. ELTE BTK Kommunikáció- és Médiatudomány.

Watkins, Elizabeth Anne & Chris W., Anderson (2019): Managing Journalistic Innovation and Source Security in the Age of the Weaponized Internet. In: Arne L. Bygdås, Stewart Clegg, Aina Landsverk Hagen (eds.): *Media Management And Digital Transformation*, pp. 119–131. New York: Routledge, https://doi.org/10.4324/9780429490187-10

Wu, Meng-Jia, Kelly Zhao, Francisca Fils-Aime (2022): Response Rates of Online Surveys in Published Research: A Meta-Analysis. *Computers In Human Behavior Reports,* vol. 7, https://doi.org/10.1016/j.chbr.2022.100206

Vásárhelyi Mária (1999): *Újságírók, sajtómunkások, napszámosok.* Budapest: Új Mandátum.

Vásárhelyi Mária (2007): *Foglalkozása újságíró.* Budapest: MÚOSZ & MTA-ELTE Kommunikációelméleti Kutatócsoport.

Zuboff, Shoshana (2019): *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* New York: Public Affairs.

Bátorfy Attila médiakutató, az ELTE BTK kommunikáció és médiatudomány tanszékének mesteroktatója és doktori hallgatója, a *Médiakutató* szerkesztője. Korábban a *Kreatív* médiaipari szaklap szerkesztője és az *Átlátszó.hu* oknyomozó központ újságírója volt. Újságírói munkájáért számos díjat kapott. Médiakutatói érdeklődési területe a médiarendszer-elméletek és a politika és a média viszonyrendszere, valamint a vizuális újságírás. A *Médiakutató*ban legutóbb megjelent írása: „Egy autoriter médiarendszer felé tartó ország: Magyarország" (2022. ősz–tél). Email: batorfy.attila@btk.elte.hu

Bárdos Kata Kincső az Internews szervezet Journalist Security Fellowship regionális médiafejlesztési programjának tagja. A Budapesti Műszaki és Gazdaságtudományi Egyetemen és az ELTE BTK kommunikáció és médiatudomány szakán szerezte a diplomáit. Korábban újságíróként dolgozott a *WMN.hu*-nál, a *168 Óra*nál és a *Pesti Hírlap*nál. Email: katabardos97@gmail.com