Iustum Aequum Salutare
XVI. 2020. 3. • 179–192.

A TÁRSADALMI TUDATOSSÁG ÉS AZ ONLINE KÖZVETÍTŐ SZOLGÁLTATÓK SZEREPE AZ INFORMATIKAI BŰNÖZÉS ELLENI FELLÉPÉSBEN

Sorbán Kinga
tudományos segédmunkatárs (NKE ITKI)

2004-ben – még a cselekményt kriminalizáló büntető törvénykönyvi paragrafus híján – felmentették azokat a fiatalokat, akik betörtek az Elender Rt. szerverére, majd 1900 ügyfél nevét és jelszavait tették közzé.[1] 2016-ban zsarolóvírussal fertőződött meg egy veszprémi kórház informatikai rendszere és az egészségügyi intézmény nem tudta biztosítani az ellátásokat.[2] 2018-ban Chrissy Chambers részére nagy összegű kártérítést ítélt meg egy brit bíróság.[3] A hölgy korábbi párja Chambers tudta nélkül készített szexuális együttléteikről felvételeket és ezeket a szakításukat követően feltette az internetre, ahol több százezer alkalommal tekintették meg őket. Az elkövetés időpontjában a bosszúból közzétett szexuális felvétel még nem volt büntetendő az Egyesült Királyságban, ezért csak polgári eljárás jöhetett szóba. 2020 márciusában a holland rendőrség letartóztatta a Darkscandals nevű weboldal adminisztrátorát.[4] Az oldal tárhelyet biztosított olyan szexuális felvételeknek, amelyek a szereplők beleegyezése nélkül készültek, illetve erőszakos szexuális tevékenységet ábrázoltak.

Az előbbiekben ismertetett cselekmények sokfélék ugyan, de van bennük egy fontos közös elem: a számítógépek és az internet mindegyikben hangsúlyos szerepet játszottak. Az online térben előforduló jogsértések, és egyéb (magatartási vagy erkölcsi) normát sértő magatartások számtalan formát ölthetnek, így az informatikai bűnözésre sem adható uniformizált, minden cselekményre egységesen alkalmazható

[1] https://index.hu/tech/jog/lendrhck0505/

[2] https://index.hu/tech/2016/04/08/itt_az_elso_magyar_korhazi_zsarolovirus/

[3] Jenny Kleeman: YouTube star wins damages in landmark UK ‚revenge porn' case. *The Guardian,* 2018. január 17. https://www.theguardian.com/technology/2018/jan/17/youtube-star-chrissy-chambers-wins-damages-in-landmark-uk-revenge-porn-case

[4] https://www.europol.europa.eu/newsroom/news/dark-web-child-abuse-administrator-of-darkscandals-arrested-in-netherlands

válasz, ami nagy kihívás elé állítja napjaink jogalkotóit és bűnüldöző szerveit. A büntető törvénykönyvekben található tényállások jelentős része – de azok biztosan, amelyek közlésekkel kapcsolatosak (például a rágalmazás) – elkövethető az online térben is, egyes cselekmények pedig specifikusan információtechnológiai eszközökhöz kötöttek (például az információs rendszerbe való jogosulatlan behatolás, köznyelvi megfogalmazásban hekkelés). Az online tér jogellenes cselekedetei nem kezelhetőek a fizikai tér cselekményeivel azonos módon, mivel több olyan jellegzetességük van, amely eltérő, sajátos megközelítést indokol, mind a jogalkotó, mind a jogalkalmazó részéről. Szász Antónia szerint „a kiberbűnözést módszerei, eszközhasználata, környezete, gyors terjedése, globális, folyamatosan változó mivolta, a károkozások rövid időn belül is számottevő mértéke, illetve társadalmi megítélésének jellegzetességei megkülönböztetik más devianciaformáktól."[5]

Jelen tanulmány három problémára szeretné felhívni a figyelmet. Az egyik, hogy alacsony a rendelkezésre álló megbízható statisztikai adatok száma, mind globális, mind nemzeti szinten. A statisztikák rendelkezésre állása különösen fontos az informatikai bűnözés elemzése szempontjából, hiszen ezek a kvantitatív adatok adnak tájékoztatást az előttünk álló probléma nagyságáról, a potenciális elkövetőkről, valamint a cselekmények demográfiai megoszlásáról. A pontos adatok informálják a jogalkotót arról, hogy mely területen érdemes új szabályokat megalkotni vagy már létezőket felülvizsgálni, a fellépésben érintett hatóságokat és egyéb szerveket pedig arról, hogy milyen régiókra, illetve személyekre érdemes összpontosítani, hol lehet *soft-law* eszközöket alkalmazni. Anna Alvazzi del Frate rávilágít, hogy a bűnözésről és büntető igazságszolgáltatásról szóló információk gyűjtése, elemzése és terjesztése kulcsfontosságú lenne a bűncselekmények megelőzése szempontjából is.[6]

A második problémakör a felhasználói tudatosság alacsony szintje. A Nemzeti Közszolgálati Egyetem által végzett 2019-es felmérés azt mutatja, hogy a magyar emberek jogtudatossága az online térben meglehetősen alacsony. A kutatás eredményei azt mutatják, hogy a magyar emberek nincsenek tisztában azzal, hogy milyen tevékenységek minősülnek jogsértőnek az online térben, és nem is törekednek arra, hogy képezzék magukat annak érdekében, hogy teljesebb képet kapjanak az online világ működéséről.

A tanulmány által érintett harmadik problémakör, hogy az online térnek vannak olyan szolgáltatói, amelyek tevékenységükkel maguk is hatást gyakorolnak az online kommunikációs folyamatokra, működésük mégis sokszor átláthatatlan, jogállami garanciákat nélkülöző. Az internetes közvetítő szolgáltatók,[7] amelyek harmadik személyek tartalmainak biztosítanak tárhelyet (például a videómegosztóplatform-

---

[5] Szász Antónia: A kiberbűnözés társadalmi kontextusa. In: Kovács Janka – Kökényessy Zsófia – Lászlófi Viola (szerk.): *A normán innen és túl*. Budapest, ELTE BTK Történeti Kollégium, 2017. 95.

[6] Anna Alvazzi del Frate: Crime and criminal justice statistics challenges. In: Stefan Harrendorf – Markku Heiskanen – Steven Malby (eds.): *International Statistics on Crime and Justice*. Helsinki, 2010. 67.

[7] Az internetes közvetítő szolgáltatók fogalmát sem az uniós, sem a magyar jog nem határozza meg. Mind az Eker. irányelv, mind az Eker. törvény csak felsorolja, hogy mely szolgáltatók minősülnek közvetítő szolgáltatóknak. Az Eker. irányelv szerinti közvetítő szolgáltató az egyszerű továbbítást végző szolgáltató, a gyorsítótárolás szolgáltatást nyújtó szolgáltató, valamint a tárhelyszolgáltató.

szolgáltatók vagy a közösségi média platformok) több szempontból is kulcsszerepet töltenek be az informatikai bűncselekmények elleni fellépésben.[8] Egyrészt moderálják a szolgáltatásukba feltöltött tartalmakat, amelynek révén ők azok a szereplők, akik az online tartalomközlések formájában megjelenő jogsértések jelentős részét képesek kiszűrni. Másrészt közvetlen kapcsolatban állnak a felhasználókkal, és e kapcsolatnak köszönhetően hatást gyakorolhatnak azokra, akár tájékoztatás révén, akár magatartási szabályok megfogalmazásával.

1. Informatikai bűncselekmények számszerűsítve

Az informatikai bűncselekmények tényleges volumenét a rendelkezésre álló adatokból lehetetlen megállapítani. Collier és Spaul a számítógépes bűncselekmények esetében úgy tartják, hogy nagy kihívást jelent a megbízható statisztikai adatok hiánya.[9] Az adatok hiányát részben arra vezetik vissza, hogy nincsenek globálisan egységes fogalmak, amelyek alapján a különálló statisztikák összevethetők lennének. Az ITU jelentése[10] szintén problémaként emeli ki, hogy a statisztikák nemzeti szinten készülnek, holott a kiberbűnözés többnyire nemzetközi jelenség, az egyes országok számai tehát nem összehasonlíthatók. A jelentés szerint gondot okoz az is, hogy egyes bűncselekménytípusok esetében nincsenek kifejezetten az online elkövetésre koncentráló statisztikák. Pergel Józsefné szerint ez a magyar statisztikákra is jellemző, ami szinte lehetetlenné teszi a nyomon követést.[11] A bűnügyi statisztikák – köztük a magyar Bűnügyi Statisztikai Rendszer[12] – azoknál a cselekményeknél, amelyeknek nem szükségszerű eleme az információs rendszer, nem tesznek különbséget az egyes magatartások között aszerint, hogy azok az online térben vagy máshol történtek. Így a rágalmazás, becsületsértés, uzsítás, zaklatás esetében nincs információ arról, hogy az esetek hány százalékának volt információtechnológiai vonzata, illetve hány valósult meg online. Kabay az informatikai bűncselekményekről szóló statisztikák elkészítésében két nagy nehézséget lát: a cselekmények azonosítását és azok bejelentését.[13] Az azonosítással kapcsolatban Kabay szerint a fő probléma, hogy az elkövetett cselekmények jelentős részére nem derül fény, az informatika biztonsági szektor úgy számol, hogy az információs rendszerek elleni

---

8 A témáról ld. bővebben: Sorbán Kinga: Az internetes közvetítő szolgáltatók kettős szerepe a kiberbűncselekmények nyomozásában: Felelősség és kötelezettségek. *In Medias Res: Folyóirat a sajtószabadságról és a médiaszabályozásról,* VIII. évf., 2019/1. 84–101.

9 P. A. Collier – B. J. Spaul: Problems in Policing Computer Crime. *Policing and Society*, Vol. 2., 1992. 308.

10 Marco Gercke: *Understanding Cybercrime: A Guide for Developing Countries*. ICT Applications and Cybersecurity Division, Policies and Strategies Department, ITU Telecommunication Development Sector. Geneva, 2011. 37.

11 Pergel Józsefné: A számítógépes csalás és egyéb számítógépes bűncselekmények. *Statisztikai Szemle*, 79. évf., 2001/9. 765.

12 https://bsr.bm.hu/

13 M. E. Kabay: *Understanding Studies and Surveys of Computer Crime*. 2013., www.mekabay.com/methodology/crime_stats_methods.pdf 3.

támadásoknak nagyjából a tizede derül ki.[14] A bejelentéssel kapcsolatos fő gond, hogy az észlelt cselekményeket gyakran maguk a sértettek vonakodnak jelenteni.

A rendelkezésre álló statisztikákból is nehéz pontos következtetéseket levonni az informatikai bűncselekményekkel kapcsolatban. Ennek az egyik oka az, hogy mind a hazai, mind a nemzetközi színtéren többféle statisztika létezik, amelyek eltérő módszertannal próbálják felmérni a cselekménycsoport egy-egy részét, átfogó szupranacionális adatgyűjtés pedig ezen a területen nem létezik. A másik nehézséget az okozza, hogy amit például egy vírusirtó cég már számítógépes vírusként érzékel, vagy az a tartalom, amit egy videómegosztó károssága miatt töröl, a bűnüldöző szervek látóterébe már nem feltétlenül kerül be, ezért a bűnügyi statisztikákban sem jelenik meg. A rendelkezésre álló egymástól független statisztikai adatok azonban alkalmasak arra, hogy érzékeltessék a probléma nagyságrendjét.

A Symantec 2018-as kiberfenyegetésekről szóló jelentése szerint[15] Magyarországon minden 213 e-mailből egy kéretlen üzenetet tartalmaz, azaz spam. Az Egyesült Királyságban minden 255-ből 1 spam, az Egyesült Államokban pedig csak minden 674. emailre jut 1 spam. Ugyanez a jelentés szól arról, hogy minden 36 mobileszközből 1 olyan van, amelyen található kockázatosnak minősített applikáció. A kártékony internetes hivatkozások (URL-ek) száma is folyamatosan emelkedik: amíg 2017-ben 16 URL-re jutott egy olyan, amely kártékony programkódot (*malware*-t) tartalmazó oldalra mutatott, 2018-ban már minden tizedik URL ilyen volt. A vírusirtó szoftvereket gyártó cégek többnyire a szoftvereik által gyűjtött adatokkal dolgoznak, ezek viszont az online térben megvalósuló bűncselekmények jelentős részének mérésére nem alkalmasak. A közlésekkel megvalósított jogsértések (például a gyermekpornográfia, az online zaklatás, a becsületsértés, vagy a gyűlöletbűncselekmények) számára azoknak a szolgáltatóknak az adataiból következtethetünk, amelyek átláthatósági jelentéseikben megosztják az általuk moderált tartalmak számát és a moderálás indokait. Az átláthatósági jelentésekben található adatok segítenek felmérni az online tartalomközzététellel megvalósuló jogsértések számát, két ponton azonban torzítanak. Egyrészt csak az adott jelentést közzétevő szolgáltató által moderált tartalmak számába nyújtanak betekintést, arról azonban nem informálnak, hogy a bíróság ténylegesen hány tartalmat minősít jogsértőnek, illetve hány tartalom eltávolítására került sor bírósági határozat alapján. Másrészt a moderált tartalmak számához hozzászámítják azokat a tartalmakat, amelyek ténylegesen jogi normát sértenek és azokat is, amelyek csupán a platform belső szabályzatával ellentétesek és ezért kerültek eltávolításra. Az adatok mindenesetre jelentős számú lehetséges jogsértésről tanúskodnak. A YouTube 2019 októbere és decembere között – tehát egy mindössze három hónapos időszakban – 5 887 021 darab videót távolított el a közösségi iránymutatások megsértése miatt.[16] Az eltávolítás oka leggyakrabban a videó spam, vagy félrevezető jellege volt (52%), ezt követte a kiskorúak biztonsága miatt (15,8%), a meztelenség és szexualitás megjelenítése miatt

[14] Uo.

[15] Symantec Internet Security Threat Report Volume 24 | February 2019 https://www-west.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf

[16] https://transparencyreport.google.com/youtube-policy/removals

(14,1%), valamint az erőszakos jelleg miatt (9,8%) történő eltávolítás volt. A Facebook átláthatósági jelentésében nem találhatunk kumulált adatot az eltávolított tartalmakról, az egyes kategóriák számait azonban közzéteszi a cég. 2019 júliusa és szeptembere között 30,3 millió meztelenséggel és szexualitással, 3,2 millió bullyinggal és zaklatással, 11,6 millió gyermekek szexuális kizsákmányolásával, 7 millió gyűlöletbeszéddel, 1,9 milliárd spammel, 5,2 millió terrorista propagandával kapcsolatos döntést hozott.[17] A Facebookon és a YouTube-on kívül természetesen még számos szolgáltató megtalálható az online térben. Egyes szolgáltatóknak nemhogy átláthatósági jelentésük nincs, de kifejezetten azért jöttek létre, hogy megkönnyítsék a jogsértő tartalmak feltöltését.

A magyar Bűnügyi Statisztikai Rendszer[18] számai sokkal visszafogottabbak, mint a vírusirtó cégek által, illetve a közösségi média platformok és videómegosztók által nyilvántartott adatok. A rendszerben rögzített tartalombűncselekmények csak kevés átfedést mutatnak a közösségi média platformok és a videómegosztó-platformok által moderált tartalmakkal, hiszen ahogy arról korábban esett szó platformok sok olyan tartalmat is moderálnak, ami nem minősül tartalombűncselekménynek, mert csak a platform felhasználási feltételeivel ellentétes. Magyarországon 2018 és 2020 áprilisa között mindössze 928 alkalommal regisztráltak információs rendszer megsértésével járó cselekményt és 46 alkalommal regisztrálták az információs rendszer védelmét biztosító technikai rendszer kijátszását. Simon Béla felhívja arra a figyelmet, hogy hazánkban a gyermekpornográfia esetében a statisztikai rendszer nem a sértettek számát, hanem a felvételek számát rögzíti, ami helytelen gyakorlat.[19] A tartalomközléssel megvalósuló bűncselekmények esetében a magyar statisztikai rendszer sem rögzíti, hogy hány cselekménynek volt online vonzata, noha Simon Béla rámutat, hogy 2017 óta a statisztikai rendszerben megjelölhető, ha egy cselekményt online követtek el.[20]

2. Az elkövetői kör heterogenitása

A heterogenitás nem csak a cselekményekre, hanem azok elkövetőire is jellemző. Az elkövetői kör sokszínűségét az eredményes és célzott fellépés érdekében mindenképpen számításba kell venni.

Az információs rendszerek és adatok elleni bűncselekményeket gyakran tulajdonítjuk hekkereknek, de ez a kifejezés túlságosan általánosító és inkább köznyelvi értelemben használatos. Azok a személyek, akik információs rendszerekbe törnek be, több csoportra oszthatók, a csoportképzés alapjai az életkor, a szakképzettség és a motiváció.

---

17 https://transparency.facebook.com/community-standards-enforcement

18 https://bsr.bm.hu/

19 Simon Béla: A kiberbűncselekmények statisztikai rögzítettsége. In: Kiss Tibor (szerk.): *Kibervédelem a bűnügyi tudományokban*. Budapest, Dialóg Campus, 2020. 93.

20 Simon i. m. 94.

Az információs rendszerek elleni bűncselekményeket elkövető személyek kategorizálását végezte el az UNCRI, amely kérdőíves felmérés alapján alkotott kilenc elkövetői profilt:[21]

1. *Wannabe lamer*: a fiatal lelkes kezdő, aki példaképeit követi és iránymutatások, leírások alapján próbálkozik rendszerekbe való bejutással.
2. *Script kiddie*: a fiatal és informatikai tudással nem rendelkező elkövető, akinek nem célja az önfejlesztés, motivációja pusztán a károkozás.
3. *Cracker*: anyagi haszonszerzés céljával tör fel rendszereket, technikailag közepesen képzett.
4. *Csendes-paranoid képzett hekker*: aki komoly programozói háttértudással rendelkezik, de csak a rendszerekbe való bejutás motiválja, amint felfedezik tevékenységét, eltűnik.
5. *Etikus hekker*: az, aki a rendszer sérülékenységeit igyekszik feltérképezni, és a szerzett információt átadja a rendszer fejlesztőinek. Nem feltétlen bűnelkövetői kategória, hiszen cégek gyakran alkalmaznak hekkereket rendszereik sérülékenységeinek feltárására.
6. *Kiberharcos*: aki ideológiai megfontolásból intéz támadásokat rendszerek ellen. Ilyenek a „hacktivisták," akik politikai aktivizmusként törnek be rendszerekbe, honlapokba. Magyarországon is ismert hacktivista csoport az Anonymous. Tevékenységük hasonló a kiberterroristákéhoz, akik összehangolt támadásokat folytatnak bizonyos rendszerek, gyakran kritikus infrastruktúrák ellen.
7. *Ipari kém*: az a professzionális elkövető, aki foglalkozás-szerűen fürkészik ki védett információkat.
8. *Kormányügynök*: aki kormányzati megbízásból hajt végre információs rendszerek elleni támadásokat.
9. *Katonai hekker*: aki kiberhadviselésben vesz részt.

Fel kell hívni a figyelmet arra, hogy sem a felosztás, sem az egyes elkövetői típusok meghatározása nem általánosan elfogadott. A cracker kifejezést Morris és Blackburn a nem bűnelkövető hekkerrel hozzák összefüggésbe, aki károkozási szándék nélkül csak kíváncsiságból tör be rendszerekbe.[22] Varga Árpád is rámutat arra, hogy a hekker kifejezés értelmezése és tartalma nem egyértelmű a szakirodalomban.[23] A meglehetősen szerteágazó hekker kifejezés használata helyett Varga az informatikai bűnelkövetők fogalom alkalmazását javasolja, arra, aki „számítástechnikai tudásának felhasználásával úgy követ el IKT-kal kapcsolatos bűncselekményeket, hogy abban információ-

---

[21] Raoul Chiesa – Stefania Ducci – Silvio Ciappi: *Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking*. Boca Raton, Auerbach Publications, CRC Press, Taylor & Francis Group, 2008. 57.

[22] Robert G. Morris – Ashley G. Blackburn: Cracking the Code: an Empirical Exploration of Social Learning Theory and Computer Crime. *Journal of Crime and Justice,* vol. 32., N. 1., 2009. 1–34.

[23] Varga Árpád: Az informatikai bűnözés fogalmi meghatározása, csoportosítása és helye a hazai jogfejlődésben. *In Medias Res: Folyóirat a sajtószabadságról és a médiaszabályozásról,* VIII. évf., 2019/1. 147.

és vagyonszerzési vagy károkozási motívum is megjelenik."[24] A tisztán informatikai bűncselekmények mellett vannak azok a cselekmények, amelyek az online és fizikai térben egyaránt elkövethetők. Mivel az információs rendszerrel kapcsolatos bűncselekmények csoportja heterogén természetű és egymástól igen különböző karakterű cselekményekből áll, nem célszerű és valószínűleg nem is lehetséges elkövetői profilok alapján csoportosítani az elkövetőket. A szerzői jogsértést megvalósító bűncselekmények esetében az elkövetők teljesen átlagos emberek is lehetnek, akik nem tekintenek bűncselekményként arra, amit tesznek. Teljesen más elkövetői körrel lehet számolni a becsületsértés vagy a rágalmazás esetében, amelyet elkövethet egy irigy ismerős vagy sértett ügyfél. Megint más típusba tartoznak a gyűlöletbűncselekmények ideológiai túlfűtöttségből kommunikáló elkövetői, a bosszúpornó esetében pedig a tipikus elkövető egy féltékeny expartner. Seigfried-Spellar és Treadway a személyazonosság-tolvajok, az online zaklatók és a vírusírók egyéni különbségeiről írnak.[25] Az információs rendszerrel kapcsolatos cselekmények esetében célszerűbb a cselekmény motivációja alapján csoportosítani. Kiss, Parti és Prazsák[26] az informatikai bűncselekményeknél tágabb magatartási kör, a cyberdevianciák motivációit térképezték fel. Az online térben megvalósuló devianciák mögött háromféle motivációt azonosítottak: az agresszióra épülő, a szexuális, valamint a haszonszerzési motivációt. Az agressziónál szűkebb fogalom a kibertérben megnyilvánuló erőszak, amely nem fizikai formában megvalósított kényszerítést, fenyegetést foglal magában, amely „pszichikai erőszak előidézésére alkalmas, társadalmi elítélés övezi, minden esetben normasértő és jogi normasértést idéz elő."[27] Az agresszív cselekmények maguk is széles skálán mozognak, ide tartozik a negatív érzelmeken alapuló párbeszéd *(flaming)*, az online rágalmazás és becsületsértés, de az egyén és a közösség ellen irányuló szándékos károkozó magatartások is (például az információs rendszer megsértése). Erőszakra épülő normasértés a zsarolás, a zaklatás, extrémista csoportok, terrorszervezetek működése az online térben. A motivációk második nagy csoportját a szexuális szükségletekre épülő motivációk alkotják. A kibertérben történő normasértő szexuális viselkedések „olyan szexuális ösztönkésztetéseken alapuló magatartások, amelyek a felek egységes akaratának hiánya miatt olykor agresszióval vagy pszichés erőszak elemeivel karöltve közvetlen kommunikációban, szexuális tartalmak küldésével, fogadásával, közzétételével, vagy rendszerintegritás elleni támadással manifesztálódnak."[28] A harmadik csoportba a haszonszerzési motiváció miatt elkövetett cselekmények tartoznak. A haszonszerzésre irányuló normasértések további három alcsoportra bonthatók. Ezek: a) haszonszerzés információs rendszer elleni támadásokkal (pl. zsarolóvírusok); b) az illegális kereskedelmi tevékenységek (pl. illegális szolgáltatások adásvétele, tiltott áruk, köztük fegy-

[24] Varga i. m. 148.

[25] Katheryn C. Seigfried-Spellar – Kellyn N. Treadway: Differentiating Hackers, Identity Thieves, Cyber - bullies, and Virus Writers by College Major and Individual Differences. *Deviant Behavior,* vol. 35., 2014/10. 782–803.

[26] Kiss Tibor – Parti Katalin – Prazsák Gergő: *Cyberdeviancia*. Budapest, Dialóg Campus, 2019.

[27] Kiss–Parti–Prazsák i. m. 69.

[28] Kiss–Parti–Prazsák i. m. 71.

ver vagy kábítószer adásvétele, online aukciós csalások); c) információközléssel vagy kommunikációval megvalósított haszonszerzés, például a zsarolás, csalás (például a nigériai levelek).[29]

3. A felhasználói tudatosság szerepe az informatikai bűnözés megfékezésében

A fentebb ismertetett, szerteágazó és tömegeket érintő cselekménycsoport esetén az elkövetők felelősségre vonásában nem csak a bűnüldöző szerveknek és a közvetítő szolgáltatóknak van szerepük, hanem maguknak a felhasználóknak is. A felhasználói tudatosság a kibertérben elősegíti a megelőzést, a jogsértő cselekmények felismerését és a felelősségre vonást. A felhasználók szerepe a jogellenes online cselekmények felismerésében azért számottevő, mert sok esetben a felhasználók jelzik, ha olyat érzékelnek az online térben, amit jogellenesnek találnak, például panasszal élnek a szolgáltató felé, vagy büntetőfeljelentést tesznek. A nagyobb videómegosztóplatform-szolgáltatók és közösségi média szolgáltatók ugyan alkalmaznak automatizált eszközöket a tartalomszűrésre, de a felhasználók észlelése és hozzáállása bizonyos tartalomfajtákhoz fontos a platformszolgáltatók számára. A felhasználói tudatosság azt is segítheti, hogy az informatikai bűncselekmények a nyomozó hatóságok látóterébe kerüljenek. Sok esetben egy-egy cselekmény éppen azért nem jut a bűnüldöző szervek tudomására, mert a felhasználó szkeptikus a jogérvényesítési lehetőséggel szemben,[30] és tartanak az elhúzódó eljárásoktól, így csak a nagy anyagi kárral járó cselekményeket jelentik.[31] Van, hogy egyes cselekmények jogellenességével a felhasználók nincsenek tisztában, így fel sem merül bennük, hogy jelentsék azokat, más esetekben pedig tudják ugyan a felhasználók, hogy az adott tevékenység jogellenes, mégsem tartják elítélendőnek (tipikus példája ennek a torrentezés).

Magyarországon az online térrel kapcsolatos jogtudatosság kimondottan alacsony. A Nemzeti Közszolgálati Egyetem Információs Társadalom Kutatóintézete 2019-ben reprezentatív országos felmérést készített „Bizalom, tudatosság, veszélyérzet az interneten" címmel.[32] Az adatfelvétel a Nemzeti Közszolgálati Egyetem Eötvös József Kutatóintézete Információs Társadalom Kutatóintézetének megrendelésére készült 2019 augusztusában. Telefonos adatfelvétel során országos adatfelvételre került sor, az adatok reprezentatívak nem, kor, iskolai végzettség, településtípus és régiók szerint a teljes magyar lakosságra.

A kérdőívben a magyar emberek jogtudatosságának felmérésére irányuló kérdések is szerepeltek. A kérdőívre adott válaszok azt mutatják, hogy a magyar emberek tudatosságának szintje nem túl magas, ha az online tér jogellenes cselekedeteiről van szó.

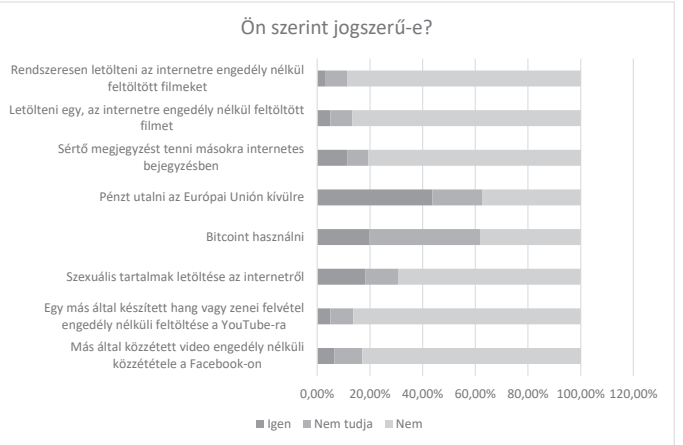
---

29 Kiss–Parti–Prazsák i. m. 72–73.

30 Collier–Spaul i. m. 310.

31 Gercke i. m. 37.

32 Rab Áprád – Török Bernát: *Bizalom, tudatosság, veszélyérzet az interneten. Az NKE Információs Társadalom Kutatóintézet reprezentatív, országos felmérésének eredményei.*2020. 06. 17. https://itki.uni-nke.hu/hirek/2020/06/17/bizalom-tudatossag-veszelyerzet-az-interneten

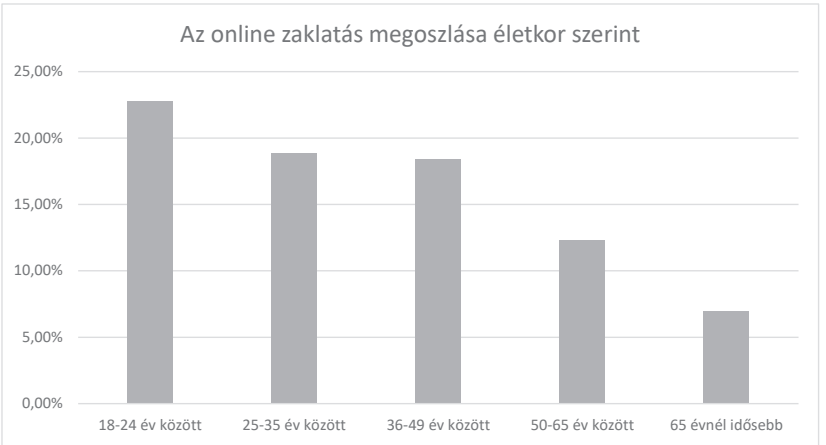


1. sz. ábra: Az online tér egyes cselekményei jogszerűségének megítélése Magyarországon (Forrás: saját szerkesztés)

A válaszadók a kérdőívben szereplő legtöbb online tevékenységfajtát jogszerűtlennek ítélték. A válaszadók 86,7%-a tudja, hogy jogszerűtlen letölteni egy az internetre engedély nélkül feltöltött filmet, 86,3%-uk pedig jogszerűtlennek tartja a másokat sértő megjegyzések közzétételét. A tudatosság alacsony szintjét legjobban az mutatja, hogy az emberek nagy számban ítéltek jogellenesnek olyan magatartásokat, amelyek nem, vagy többnyire nem azok. A válaszadók 37,4%-a gondolja úgy, hogy jogszerűtlen pénzt utalni az Európai Unión kívülre, 18,9% pedig nem tudott felelni erre a kérdésre. A szexuális tartalmak letöltését a válaszadók 69,1%-a tartja jogszerűtlen cselekedetnek, amely azt mutatja, hogy a tartalmak letöltését a felhasználók általában, függetlenül annak forrásától ítélik jogsértőnek. Az új technológiákban a válaszadók többsége járatlannak mondható. A bitcoin nevű kriptovaluta használatának jogszerűségével kapcsolat kérdésre az emberek 41,9 %-a nem tudott felelni, míg 19,9% tartotta jogszerűnek és 38,2% jogszerűtlennek annak használatát. A magyarok igen jelentős része, 83% jogszerűtlennek ítéli a más által már közzétett videók linkjének engedély nélküli közzétételét a Facebookon, holott a tartalom megosztása, vagy beágyazása nem engedélyköteles tevékenység, legfeljebb akkor lehet jogellenes, ha maga a tartalom is jogsértést valósít meg.

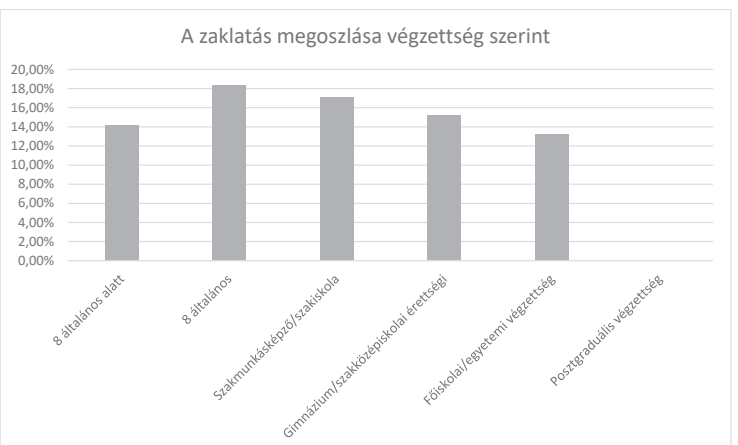
Önbevallás alapján a magyar internetezők csupán 4%-a töltött le vagy osztott meg olyan cikket vagy videót, amiről tudta, hogy jogsértő módon került fel az internetre, 1,5% pedig le is töltött és meg is osztott, annak ellenére, hogy 75%-uk tudta, hogy magatartása jogellenes volt.

Az internethasználók egy részét érte már sérelem online, ugyanis 15,6%-uk jelezte, hogy zaklatták már online. A zaklatás elszenvedői nagyobb arányban fiatalok. A zaklatottak 22,8%-a 18-24 év közötti, 18,9%-a 25-35 év közötti és 18,4%-a 36-49 év közötti.



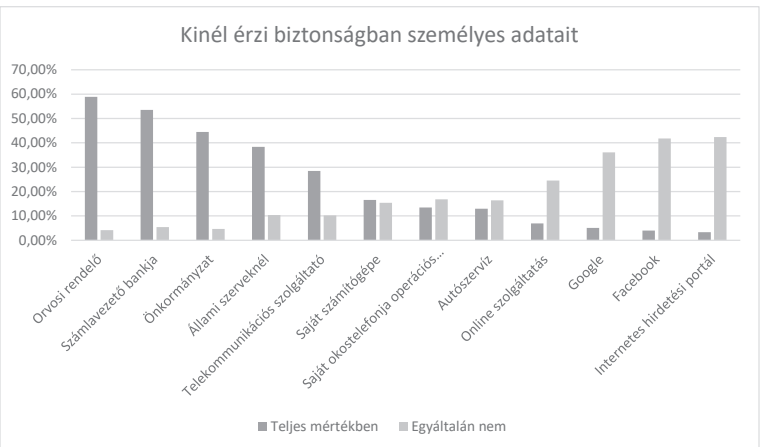
2. sz. ábra: Az online zaklatás megoszlása életkor szerint (Forrás: saját szerkesztés)

Végzettség szerinti megoszlásnál azt figyelhetjük meg, hogy a végzettség csökkenésével valamivel többen számolnak be online zaklatásról, ám az eltérés nem mondható jelentősnek. A zaklatottak 18,4%-a 8 általános iskolát végzett, míg 17,1%-uk szakiskolai, 15,24%-uk gimnáziumi vagy szakközépiskolai, 13,2%-uk egyetemi végzettséggel rendelkezik. A férfiak és a nők közel azonos arányban számoltak be arról, hogy éltek át online zaklatást. A kérdőívre adott válaszokból nem derül ki, hogy az emberek pontosan mit értettek zaklatás alatt, ezért az általuk érzékelt sérelmet nem lehet pontosan megfeleltetni egyetlen büntetőjogi tényállásnak sem, ez takarhat becsületsértést, rágalmazást, tényleges zaklatást, de akár olyan közléseket is, amelyek büntetőjogi szankcióval nem sújtható enyhébb cselekménynek minősülnek.



3. sz. ábra: Az online zaklatás megoszlása végzettség szerint (Forrás: saját szerkesztés)

Noha a tanulmány előző részében esett szó a spamnek minősülő levelek arányának a növekedéséről és a kártékony programkódokra mutató hivatkozások számáról, az emberek megítélése a számítógépek biztonságáról változó. Közel ugyanannyian gondolják úgy, hogy személyes adataik teljes biztonságban vannak a számítógépükön (16,6%), mint ahányan úgy gondolják, hogy adataik egyáltalán nincsenek biztonságban (15,40%). Hasonló tendenciát figyelhetünk meg az emberek mobileszközök biztonságával kapcsolatos felfogásában, azzal, hogy mobileszközök biztonságában kevésbé bíznak az emberek. Az emberek 13,5%-a bízik csak meg teljes mértékben a mobileszköze biztonságában, 16,8%-uk pedig egyáltalán nem érzi biztonságban személyes adatait mobil eszközén. Az emberek az online közvetítő szolgálatókkal szemben túlnyomórészt bizalmatlanok, a magyarok 36,1%-a ugyanis egyáltalán nem érzi biztonságban a személyes adatait a Google-nél, 41,8%-uk pedig a Facebook-nál.

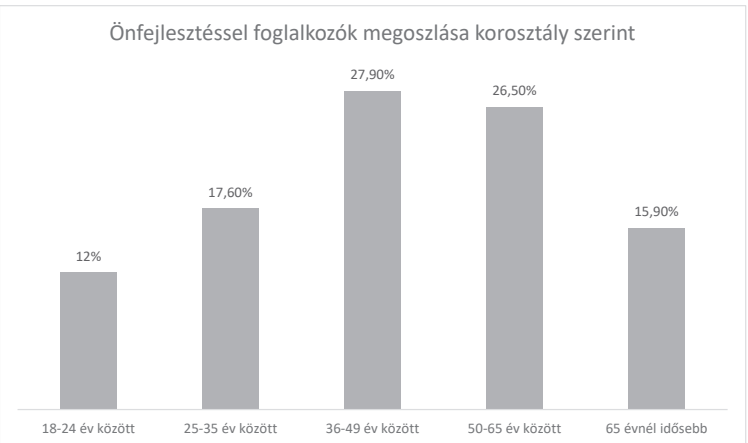


4. sz. ábra: Személyes adatok biztonsága az online tér egyes szereplőinél. (Forrás: saját szerkesztés)

A csökkent biztonságérzet ellenére a magyarok továbbra is rendszeresen használják a nevesített szolgáltatásokat. Korábban már esett arról szó, hogy viszonylag kevesen jelezték azt, hogy töltöttek le vagy osztottak meg jogellenes forrásból származó tartalmat, ezzel összhangban áll az, hogy arra a kérdésre, hogy előfordult-e már, hogy a Facebook törölte a válaszadó posztját vagy letiltotta a szolgáltatásból, kevesen feleltek igennel. Mindössze 10,1% jelezte, hogy előfordult vele az, hogy a Facebook moderálta az általa feltöltött vagy megosztott tartalmat. A platform moderációjával való találkozás az iskolai végzettség csökkenésével nő. Míg a legfeljebb 8 általános iskolai osztályt végzettek 14,7%-ának törölték már tartalmát vagy fiókját, az érettségivel rendelkezők 5,8%-ának a tevékenysége nem felelt meg a platform szabályzatának. Érdekes kiugrás tapasztalható a diplomásoknál, akik szintén valamivel magasabb arányban (10,9%) tettek olyat, amelyet a platformszolgáltató a felhasználási feltételekbe ütközőnek minősített. A platformok moderációs tevékenységének átláthatatlanságát mutatja, hogy az eltávolítással vagy törléssel érintett felhasználóknak csak a 36,5%-a kapott megfelelő tájékoztatást a törlés okáról. 30,2% kapott ugyan tájékoztatást, de nem ítélte megfelelő-

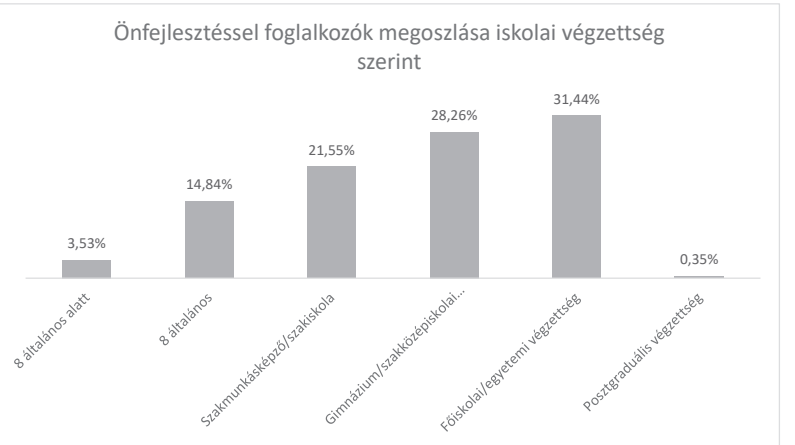
nek azt, 33,3% pedig nem kapott semmilyen visszajelzést a törlés okáról. Elmondható az is, hogy az emberek többnyire beletörődnek a platform döntésébe. 65% ugyanis nem tett lépéseket annak érdekében, hogy megváltoztassa a döntést és visszaállíttassa a szóban forgó tartalmat. Ez jelentheti azt, hogy a felhasználó már a megosztás pillanatában tisztában volt a cselekménye kifogásolható természetével, de jelentheti azt is, hogy nem tudja, hová fordulhat igényével, vagy nem bízik a platform eljárásában, ahogyan azt is, hogy nem tulajdonít akkora jelentőséget a megosztott közlésnek, hogy vitába szálljon a platformmal. Azok közül, akik kérvényezték a döntés megváltoztatását, 43,5% még választ sem kapott a platformszolgáltatótól, az esetek 30,4%-ában a szolgáltató azonban megváltoztatta a döntését.

A tudatossági deficit ellenére a felhasználók kevéssé figyelnek oda az önfejlesztésre. A felhasználóknak csak a 28,2%-a képezi magát, hogy felkészült legyen az online világ kihívásaival szemben. Az önfejlesztésre gondot fordító felhasználók jelentős része (27,9%) 36-49 év közötti. A legkevesebb időt a legfiatalabbak és a legidősebbek fordítják saját maguk képzésére. Az önfejlesztésre gondot fordító felhasználóknak mindössze 12%-a 18-24 év közötti, és 15,9%-a 65 év feletti.



5. sz. ábra: A önfejlesztéssel foglalkozók megoszlása korosztály szerint (Forrás: saját szerkesztés)

Az is elmondható, hogy a magasabb iskolai végzettséggel rendelkező felhasználók nagyobb arányban fordítanak időt arra, hogy fejlesszék készségeiket az online térben. Az önmagukat fejlesztő felhasználók aránya a végzettséggel párhuzamosan növekszik, a főiskolai/egyetemi végzettséggel rendelkező felhasználók aránya a legmagasabb (31,44%), míg a 8 általános iskolai osztályt végzettek aránya már csak 14,8%.



6.sz. ábra: Az önfejlesztéssel foglalkozók megoszlása iskolai végzettség szerint (Forrás: saját szerkesztés)

4. Összegzés

Ahogy a tanulmány első részéből kiderült, az informatikai bűnözésről rendelkezésre álló statisztikák nagy részét alapvetően profitorientált piaci szereplők szolgáltatják. Ez két szempontból sem szerencsés. Az egyik a közös módszertan hiánya, ami híján a kapott adatok nehezen összevethetők, a módszertani különbségekből adódóan pedig félrevezető eltéréseket is mutathatnak. A cégek által rögzített cselekmények közül nem biztos, hogy mindegyik bűncselekményt valósít meg. Különösen igaz ez a tartalomközlések moderálása esetén, ahol a platformszolgáltatók moderálási szabályzatai gyakran szigorúbbak, mint a jogszabályok. Javasolt lenne tehát olyan módszerek kidolgozása, amelyek segítségével jól mérhető az emberek kitettsége az informatikai bűncselekményeknek. A tartalomközléssel megvalósuló normasértő magatartások jelentős részét az olyan internetes közvetítő szolgáltatók regisztrálják, mint a közösségi média platform szolgáltatók, illetve a videómegosztóplatform-szolgáltatók, ezért statisztikai adatgyűjtés szempontjából kulcsfontosságú szereplőknek számítanak. Noha a nagyobb szolgáltatók rendszeresen tesznek közzé átláthatósági jelentést, ezekben nem választható külön, hogy mely tartalom került törlésre jogsértő volta miatt és melyik azért, mert a platform magatartási szabályaiba ütközött, így nem ad pontos képet a tartalomközléssel megvalósuló bűncselekményekről.

Szükség volna a felhasználói tudatosság fejlesztését célzó intézkedések megerősítésére. Mivel az emberek viszonylag csekély része fordít figyelmet az önfejlesztésre, meg kell találni azokat az alternatívákat, amelyekkel eredményesen felhívható a figyelem az online tér veszélyeire. A felhasználói tudatosság növekedése nem csak a védekezésnek és a prevenciónak lehet eszköze, hanem elősegíti, hogy a felhasználók jogkövető magatartást tanúsítsanak, valamint a jogsértések jobb észlelését és bejelentését. Mivel a harmadik személyek tartalmai számára tárhelyet biztosító szolgáltatók közvetlen kapcsolatban vannak a felhasználókkal és képesek arra, hogy azok online térben folytatott

tevékenységét befolyásolják, ezeknek a szolgáltatóknak nagy szerepe lehet az online tudatosság fejlesztésében.

Az informatikai bűncselekmények esetében a látencia jellemzően magas. Nagy különbségek vannak a vírusirtó cégek és a bemutatott platformok által rögzített incidensek száma, valamint a Bűnügyi Statisztikai rendszerben rögzített cselekmények száma között. Még abban az esetben is, ha figyelmen kívül hagyjuk azokat a tartalmakat, ahol az eltávolítás alapját nem jogsértés, hanem a szolgáltató belső szabályzatával való ütközés képezte, feltételezhető, hogy a platformok igen nagy számú olyan tartalmat is moderálnak, amelyek esetében büntető vagy polgári eljárásnak lehetne helye, de mégsem jutnak el az igazságszolgáltatás szerveihez. Az online tartalomáramlás nagysága miatt a platformoknak ez az elsődleges szűrő funkciója kimondottan fontos, ám össztársadalmi érdek, hogy az általuk végzett tartalomszűrés átlátható legyen, a felhasználók számára pedig rendelkezésre álljanak megfelelő jogorvoslati lehetőségek. A bemutatott adatok jelenleg még azt tükrözik, hogy a moderálás hátterében álló döntések átláthatósága nem éri el az ideális szintet, és a szolgáltatók által kidolgozott panaszkezelési eljárások is fejlesztésre szorulnak.