Mezei Kitti – Szentgáli-Tóth Boldizsár

Az online platformok használatában rejlő veszélyek: a dezinformáció és a kibertámadások jogi kockázatai

A modern technológiák rosszindulatú használata mögött meghúzódó motiváció gyakran irányulhat közvetlenül a közbeszéd befolyásolására: manipulált álláspontok generálására, vagy a vitában már egyébként is jelen lévő álláspontok felnagyítására, vagy éppen relativizálására. Például az automatizált eszközök („botok") segítségével létrehozott közlések, illetve hozzászólások hamis képet alakíthatnak ki az olvasóban az adott témában a társadalomban jelen lévő álláspontokról, illetve azok tényleges súlyáról, támogatottságáról. Ezenkívül új kihívást jelent a mesterségesintelligencia-alapú deepfake-technológia térnyerése. Az így létrehozott tartalmak súlyos károkat okozhatnak mind az egyénnek, mind a közösségnek: a magánszemélynek okozott károkon túl a deepfake hozzájárulhat a demokratikus döntéshozatali eljárások torzításához és a választási eljárás manipulációjához, ezzel erodálva a közbizalmat és súlyosbítva a társadalom megosztottságát. Mindemellett büntetőjogi kérdéseket is felvethet.

A kiberbűnözés egyre jelentősebb társadalmi és gazdasági károkat okoz, ami sérti az egyének alapvető jogait, illetve veszélyt jelent a jogállamiságra és a demokratikus társadalmak stabilitására egyaránt. A visszaélések számára új színteret biztosítanak az online platformok. A felhasználók sokszor nincsenek tisztában a virtuális jelenléttel járó veszélyekkel, a megosztott információk következményeivel. Ezért az internetes platformokat és felhasználóikat érő kibertámadások gyakran irányulnak a személyes adatok vagy egyéb érzékeny adatok megszerzésére, amelyek akár további bűncselekmények elkövetéséhez is felhasználhatók (például csalás és zsarolás stb.). Ezenkívül főleg a közösségi oldalak alkalmasak a különböző rosszindulatú programok, illetve jogellenes tartalmak terjesztésére. Különösen nagy veszélyt jelentenek mindezek a jelenségek a járványhelyzetben, amikor szinte mindannyian a korábban megszokottnál jóval több időt töltünk az online térben.

Tanulmányunkban a jogi szabályozás főbb lehetséges továbblépési irányait keressük e komplex problémakör kezelésére. Milyen eszközökkel lehet hatékonyan fellépni a vélemények szabad áramlása érdekében az új fenyegetésekkel szemben, hogy megvédjük a plurális társadalmi és politikai rendszernek ezt a nélkülözhetetlen előfeltételét? És a közösségi szintű fellépés megalapozásaként hogyan oltalmazhatjuk meg az internetes platformokon közérdekű kérdésekben tájékozódó felhasználókat a kibertérből érkező dezinformációs támadásoktól?

Az egyes alapvető jogokat hátrányosan befolyásoló kibertámadásokkal szembeni eredményes fellépéshez kombinált eszközrendszerre van szükség, meg kell teremteni az érdemi ellenintézkedések technológiai, gazdasági, személyi és jogi feltételeit egyaránt. Jogi tekintetben rögzíteni kell, hogy milyen garanciákat kell nyújtania a platformszolgáltatóknak a kibertámadások és jogellenes tartalmak kivédése érdekében minden egyes felhasználónak, ezek rendelkezésre állásának folyamatos

https://doi.org/10.36250/01065_17

ellenőrzéséről pedig jogi eszközökkel is szükséges lenne gondoskodni. Ezenfelül a platformon megosztott tartalmakkal, illetve az üzemeltető részére rendelkezésre bocsátott személyes adatokkal kapcsolatos visszaélés esetén világos felelősségi viszonyokat kell teremteni, rendezni kell, hogy a védekezés milyen körben a platform üzemeltetőjének, illetve felhasználójának a felelőssége. Tanulmányunkban ezeknek a kihívásoknak a kezelésére vázolunk fel szabályozási alternatívákat.

Bevezetés

Az elmúlt években a közösségi média a digitális kommunikációnk fő csatornájává vált, és ma már számos olyan platformot tartalmaz, amelyeket a „kiberbűnözők" is előszeretettel kihasználnak. [1] Már megjelentek többek között a Facebookon kívül az Instagramon, a Twitteren, a Snapchaten, a WhatsAppon és legutóbb a Telegramon, utóbbi egy *bot* funkcióval rendelkező üzenetküldő alkalmazás. Az online platformok körében tehát a közösségi média egyes platformjai kétségtelen, hogy a kiberbűnözés új színtereivé váltak. Az alábbi eseteket mutatjuk be részletesen e témakörön belül: a kibertámadások (hacking és malware), adathalászat és adatszivárgás, online csalások és zsarolások, valamint a deepfake-technológia használatában rejlő veszélyek.

A tanulmány második felében arra keressük a választ, hogy milyen eszközökkel lehet hatékonyan fellépni a vélemények szabad áramlása érdekében a közösségi médiában megjelenő új fenyegetésekkel szemben, hogy megvédjük a plurális társadalmi és politikai rendszernek ezt a nélkülözhetetlen előfeltételét. Továbbá a közösségi szintű fellépés megalapozásaként hogyan oltalmazhatjuk meg az említett internetes platformokon közérdekű kérdésekben tájékozódó felhasználókat a kibertérből érkező dezinformációs támadásoktól.

A kiberbűnözés számos fontos indítékát részletesen elemezte már a vonatkozó hazai és nemzetközi szakirodalom,[2] magunk is röviden kitérünk több ilyenre tanulmányunkban. A közvélemény alakítása, a döntéshozatal befolyásolása és a politikai

[1] Jelen tanulmány a Nemzeti Közszolgálati Egyetemen 2021. május 27-én tartott *Internetes platformok kora – társadalmi hatások és szabályozási kihívások* című konferencián elhangzott előadás írásos változata. A 128976; a 138965; valamint a 2019-2.1.11-TÉT-2020-00243 számú NKFIH pályázat és a Mesterséges Intelligencia Nemzeti Laboratórium keretében az Innovációs és Technológiai Minisztérium, valamint a Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal támogatásával valósul meg.

[2] Lásd ehhez bővebben David S. Wall: Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime. *International Review of Law, Computers and Technology,* 22. (2008), 1–2. 45–63.; Alisdair A. Gillespie: *Cybercrime: Key Issues and Debates*. New York, Routledge, 2019; Marija T. Britz: *Computer Forensics and Cyber Crime: An Introduction.* London, Pearson, 2013; Nagy Zoltán András: *Bűncselekmények számítógépes környezetben.* Budapest, Ad Librum, 2009; Szathmáry Zoltán: *Bűnözés az információs társadalomban. Alkotmányos büntetőjogi dilemmák az információs társadalomban*. PhD-értekezés. Budapest, PTE ÁJK, 2012; Mezei Kitti: *A kiberbűnözés aktuális kihívásai a büntetőjogban.* Budapest, L'Harmattan – TK JTI, 2020.

haszonszerzés azonban olyan motivációk, amelyekről kevesebb szó esett eddig az online térben végrehajtott támadások hátterének kutatásakor. Talán ez az oka annak is, hogy a kérdéskör jelentőségéhez képest csak kevés tanulmány foglalkozott eddig az új technológiáknak a szólásszabadság érvényesülésére, a politikai vélemények piacára gyakorolt hatásaival.[3] Azonban egyre többször merül fel ezen összefüggések alaposabb megismerésének igénye, és egyre világosabb az is, hogy a következő időszakban tovább növekedhet az új technológiák hatása a közéleti vitákban. Ezért is tartjuk különösen fontosnak, hogy a szólásszabadság aktuális kérdéseivel, illetve a kiberbűnözéssel foglalkozó szakemberek egymással összefogva törekedjenek e komplex terület törvényszerűségeinek feltárására és a vonatkozó szabályozás alapelveire, valamint konkrét tartalmára vonatkozóan közös javaslatok megfogalmazására.

A kiberbűnözés fogalma

Mindenekelőtt fontos egy rövid fogalmi áttekintést nyújtanunk a kiberbűnözés kapcsán. A kibertér *(cyberspace)* kifejezést – a kibernetika és a tér szavak összevonásából – William Gibson amerikai író alkotta meg az 1982-ben megjelent *Izzó króm (Burning Chrome)* című novellájában, amely később a *Neurománc (Neuromancer)* című regénye által vált ismertté. Gibson a kibertér elnevezést használta a globális számítógépes hálózatra, amely összeköti az embereket, a számítógépeket és az információforrásokat. Az ebből képzett angolszász *cybercrime* nyomán honosodott meg az általunk használt kiberbűnözés szó. A cybercrime elnevezés használata napjainkban széles körben elterjedt, különösen a nemzetközi szakirodalomban, de például a Budapesti Egyezmény[4] (Convention on Cybercrime) is ezt alkalmazza.

A nemzetközi szakirodalomban több szerző is, így Jonathan Clough,[5] Peter Grabosky[6] és Susan W. Brenner[7] is a kiberbűnözésre mintegy gyűjtőfogalomként tekint, amelynek két fő kategóriája különböztethető meg: az egyik azon deliktumok

[3] Példaként lásd Bartóki-Gönczi Balázs: A keresőmotorok és a szólásszabadság kapcsolata. Megközelítés és szabályozási javaslatok az Európai Unióban és az Egyesült Államokban. *Iustum Aequum Salutare,* 14. (2018), 1. 157–194.; Klein Tamás: Keresőmotor-szolgáltatók és az internetes szólásszabadság. In Koltay András – Nyakas Levente (szerk.): *Tanulmányok a technológia- és cyberjog néhány aktuális kérdéséről.* Budapest, Médiatudományi Intézet, 2018. 26–29.; valamint Koltay András: *Az új média és a szólásszabadság. A nyilvánosság alkotmányos alapjainak újragondolása.* Budapest, Wolters Kluwer, 2019; Bernát Török: Platforms and Fundamental Rights: The Case of Social Media and Freedom of Speech. *Hungarian Conservative,* 1. (2021), 2. 42–47.

[4] Az Európa Tanács Budapesten, 2001. november 23-án kelt *Számítástechnikai bűnözésről szóló egyezménye,* amelyet a 2004. évi LXXIX. törvénnyel hirdettek ki Magyarországon.

[5] Jonathan Clough: *Principles of cybercrime.* Cambridge, Cambridge University Press, 2015. 10–11.

[6] Peter Grabosky: *Cybercrime*. London, Oxford University Press, 2016. 8–9.

[7] Susan W. Brenner: *Cybercrime: Criminal Threats From Cyberspace.* Santa Barbara (CA), Praeger, 2010. 39–47.

csoportja, amelyek kizárólag információs rendszerekkel (például számítógépekkel, azok hálózatával vagy egyéb információs és kommunikációs technológiák használatával) követhetők el. Jellemzően az ilyen bűncselekmény tárgya az információs rendszer. Ez a tisztán informatikai bűncselekmény vagy kiberbűncselekmény az úgynevezett *cyber-dependent crime* (például számítógépes vírusok használata, hacking stb.).

A második, tágabb kategóriába tartoznak azok a hagyományos bűncselekmények, amelyeket az információs rendszerek felhasználásával követnek el (például a csalás, a zsarolás, a gyermekpornográfia, a szerzői jogi jogsértések, a zaklatás stb.). Ez az úgynevezett *cyber-enabled crime* esetköre, amikor az információs rendszer a bűncselekmény elkövetésének az eszköze.[8]

Mindezekre tekintettel megállapítható, hogy a kiberbűnözés esetén egyrészt olyan új típusú bűncselekményekről beszélhetünk, amelyek kizárólag az információs rendszerek segítségével követhetők el, és olyan speciális védett jogi tárggyal rendelkeznek, mint amilyen az információs rendszer vagy adat. Másrészt idetartoznak azok a hagyományos bűncselekmények is, amelyek sokkal könnyebben elkövethetők az új eszközök segítségével.

Az informatikai környezetben elkövetett bűncselekmények motívumai, céljai általánosságban nem térnek el a valós térben elkövetett bűncselekményekétől, mert ugyanúgy elkövethetők haszonszerzés vagy károkozás céljából, valamint az adatok, titkok kifürkészése végett vagy akár szexuális indíttatásból. A manipuláció útján, dezinformációk terjesztésével elérhető politikai haszonszerzés azonban olyan motívumokat is bevonhat ebbe a gondolkodásba, amelyek a hagyományos bűncselekmények kapcsán nem relevánsak. Talán ez is az egyik oka annak, hogy ezek a vonatkozások eddig kevesebb figyelmet kaptak, holott súlyuk a virtuális világ bűnelkövetői számára egyre jelentősebb.

A kiberbűnözésbe tartozó bűncselekmények szabályozása a büntetőjog körében alapvetően nemzeti hatáskör, mivel a büntetőjog tipikusan – de nem kizárólagosan – egy állam belső joghatósági körébe tartozik, tehát a nemzeti büntetőjogok tudják a leginkább kezelni a kérdést. Ezért jelen tanulmányban a hazai büntetőjogi rendelkezésekre tekintettel vizsgáljuk a kiberbűnözés egyes eseteit. Fontos azonban megjegyezni, hogy a hazai jogra jelentős hatással van e téren az említett Budapesti Egyezmény és ennek kiegészítő jegyzőkönyve,[9] valamint a vonatkozó uniós szabá-

[8] Clough (2015): i. m. 10–11. A *cyber-related crime* elnevezést használja az Egyesült Államok Igazságügyi Minisztériuma, amikor a hagyományos bűncselekmény elkövetésének eszköze a számítógép, míg a *Budapesti Egyezmény* is utal arra, hogy azon bűncselekményeket foglalja magában, amelyeket a számítógép használatával követnek el. Lásd ehhez U.S. Department of Justice: *The National Information Infrastructure Protection Act of 1996, Legislative Analysis.* 1996; Council of Europe: Explanatory Report to the Convention on Cybercrime. *European Treaty Series,* 185. (2001). 79. cikk.

[9] 2003-ban a Budapesti Egyezményt kiegészítették a számítástechnikai rendszerek útján megvalósított rasszista és idegengyűlölő cselekmények büntetendővé nyilvánításáról szóló jegyzőkönyvvel. 2017 szeptemberében pedig az Európa Tanács úgy döntött, hogy elkészíti az egyezmény második ki-

lyozás (például az információs rendszerek elleni támadásokról szóló 2013/40/EU irányelv).

A kiberbűnözés egyes esetei az online platformokon

Írásunkban az online platform alatt a vélemények és információk széles körben való terjesztésére, illetve kommentálására alkalmas online kommunikációs felületeket tekintjük át. Az üzleti élet is egyre inkább e platformoktól függ, valamint a magánszemélyek is nagy számban vannak jelen ezeken az online felületeken. A koronavírus-járvány pedig fokozta az online jelenlétet. A felhasználók sokszor nincsenek tisztában az online jelenléttel járó veszélyekkel, a megosztott információk következményeivel. Ennek eredményeképpen a szenzitív adatokat az illetéktelen személyek egyre könnyebben tudják megszerezni (például az erre a célra kifejlesztett rosszindulatú programokkal, adathalász és egyéb módszerekkel). A közösségimédia-platformok tehát a hackerek számára könnyű utat kínálnak, hogy elérjék vagy feltérképezzék a kiválasztott célpontjaikat. A közösségimédia-felhasználók növekvő száma vonzóvá tette az online platformokat a kiberbűnözők számára, ami azt jelenti, hogy például a rosszindulatú programok, avagy *malware*-fertőzések[10] fő forrásává váltak, amelyek mind a magánszemélyeket, mind a vállalkozásokat egyaránt érintik. A probléma egyre jelentősebb, e platformok különösen alkalmasak a rosszindulatú programok terjesztésére, mert általában több képet, videót, hirdetést és úgynevezett *plugin*eket jelenítenek meg. Ezenkívül a közösségi hálózatokon keresztüli interakció jellege elősegíti a fertőzés gyors és zökkenőmentes terjedését, ezt a problémát bonyolítja az a tendencia, hogy a közösségi média lehetővé teszi a felhasználói profilok több platformon történő megosztását. Az egyik tipikus példa erre a Facebook Messengeren található adathalász linkek voltak, amelyeket arra használtak, hogy az áldozatokat egy YouTube-ra hasonlító oldalra átirányítsák. Egy frissítés letöltése

egészítő jegyzőkönyvét, amely egy hatékonyabb és egyszerűbb kölcsönös jogsegélyrendszerre irányuló rendelkezéseket tartalmazna. E rendszer lehetővé tenné a közvetlen együttműködést az egyezmény egy másik részes államában székhellyel rendelkező szolgáltatókkal, a kereséseket pedig határokon átnyúlóan is lehetne végezni. A jegyzőkönyv erőteljes biztosítékokat és adatvédelmi követelményeket fog tartalmazni. Egy ilyen megállapodás előnye, hogy akár világszerte alkalmazhatóvá válhat. Lásd erről Jennifer Daskal – Debrae Kennedy-Mayo: Budapest Convention: What is it and How is it Being Updated? *Cross-Border Data Forum,* 2020. július 2.

[10] A malware a malicious software, vagyis a rosszindulatú szoftver rövidítése, ami arra utal, hogy általában ezeket a kártevő programokat használják arra, hogy jogosulatlanul behatoljanak az információs rendszerekbe, vagy módosításokat végezzenek a felhasználó tudta és hozzájárulása nélkül, és kárt okozzanak az adatokban. Egyre gyakrabban használják fel ezeket arra, hogy bizalmas adatokhoz férjenek hozzá, amelyek elősegítik a további csalásokat vagy egyéb jogsértéseket (például zsarolás, személyazonosság-lopás stb.). A kártékony programok különböző fajtáiról bővebben lásd Sorbán Kinga: Vírusok és zombik a büntetőjogban. Az információs rendszer és adatok megsértésének büntető anyagi és eljárásjogi kérdései. *In Medias Res,* 7. (2018), 2. 376–377.

után a felhasználókat rosszindulatú programmal fertőzték meg, amely képes volt a jelszavakat és egyéb szenzitív információkat megszerezni.[11]

A rosszindulatú programok terjesztése jellemzően posztok vagy üzenetek formájában történik, például a fertőzött hirdetésekre kattintásokkal, illetve ismerősök által megosztott tartalmakkal (például vicces videókkal, képekkel, hírekkel és hirdetésekkel), továbbá a telepített pluginek és alkalmazások (például játékok és tesztek) révén. Gyakran üzenetként küldenek rosszindulatú programokat, vagy egy weboldalra irányítanak át, de megjelent már a *drive-by downloads* is, ami azért különösen veszélyes, mert ekkor a malware magától letöltődik, kihasználva a rendszer sebezhetőségét, a weboldalba vagy alkalmazásba illesztve. A közösségi oldalakon gyakran találkozhatunk úgynevezett *bot*okkal, amelyek alkalmasak az automatikus üzenetek generálására és a rosszindulatú programok terjesztésére. Például a Facebook Messenger programban található *chatbot* alkalmas lehet arra, hogy automatikusan szétküldje az akár bűncselekményt is magában hordozó üzeneteket.[12] A rosszindulatú programokon kívül pedig gyakori a személyes vagy üzleti céllal használt felhasználói fiókok feltörése (ez az úgynevezett *hacking,* avagy jogosulatlan belépés esete), amelynek következtében átveszik az irányítást a fiók felett, és hozzáférnek minden a fiókhoz kötődő adathoz (például bankkártya- és egyéb személyes adatokhoz). Gyakran olyan fiókokat céloznak, amelyek „ellenőrzöttek". Az ilyen támadások elkerülése érdekében különösen fontos a kétlépcsős azonosítás beállítása a felhasználói fiókoknál. Ezek a vizsgált esetek mind az információs rendszer elleni bűncselekményekhez kapcsolódnak: az elkövetők az információs rendszer vagy adat megsértését követik el (Btk. 423. §), ha jogosulatlanul, a technikai intézkedés kijátszásával belépnek a felhasználói fiókba, vagy jogosulatlanul adatmanipulációt hajtanak végre a rosszindulatú programmal, illetve az információs rendszer felhasználásával elkövetett csalás valósul meg (Btk. 375. §), ha például a jogosulatlanul megszerzett bankkártyaadatokkal tranzakciókat hajtanak végre.

A kiberbiztonságban a leggyengébb láncszem az ember. Az esetek döntő többségében ugyanis minden sikeres támadás mögött a sértetti közrehatás áll,[13] és éppen ezért az elkövetők gyakran előnyben részesítik a *social engineering* támadásokat (a célszemély megtévesztésével megvalósított támadások tartoznak ebbe a körbe, például az elkövető adathalász levélben megbízható személynek vagy szervezetnek adja ki magát annak érdekében, hogy bizalmas információkat csaljon ki az áldozattól)[14] a technikai jellegű megoldások alkalmazása helyett. Kevin D. Mitnick

[11] Michael McGuire: *Into the Web of Profit: Social Media Platforms and the Cybercrime Economy.* Cupertino (CA), Bromium, 2019. 7–8.

[12] Ambrus István: *Digitalizáció és büntetőjog.* Budapest, Wolters Kluwer, 2021. 46.

[13] Parti Katalin – Kiss Tibor: Az informatikai bűnözés. In Borbíró Andrea et al. (szerk.): *Kriminológia*. Budapest, Wolters Kluwer, 2017. 506.

[14] Abdullah Algarni – Yue Xu – Taizan Chan: An Empirical Study on the Susceptibility to Social Engineering in Social networking sites: the Case of Facebook. *European Journal of Information Systems,* 26. (2017), 6. 661–687.

szerint a pszichológiai manipuláció könnyedén megkerüli a technológiai akadályokat (például tűzfalat vagy egyéb védelmet) a befolyásolás és megtévesztés segítségével.

Az egyik oka annak, hogy a közösségi média különösen kedvelt az elkövetők körében, hogy jelenleg meglehetősen könnyű álprofilt létrehozni. A Facebooknak nemrég több mint 5 milliárd álfiókot kellett törölnie az egész platformjáról. Az álprofilokat jellemzően arra használják, hogy megtévesszenek más felhasználókat, például az említett social engineering módszerekkel rávegyék őket arra, hogy a fertőzött linkekre kattintsanak, vagy akár szenzitív információkat osszanak meg.

A Nemzeti Adatvédelmi és Információszabadság Hatóság kapcsolódó gyakorlata alapján különösen bűncselekmény gyanúját keltő ügyeknek tekinthetők az olyan esetek, ha ismeretlen személyek a felhasználó nevében és fényképei felhasználásával a közösségi oldalon álprofilt hoznak létre. Ezen az álprofilon keresztül a megszemélyesített felhasználó valódi ismerőseit jelöli be az elkövető, és a felhasználó nevében üzeneteket küld, bejegyzéseket tesz közzé. A cél gyakran az érintett lejáratása, hírnevének rontása mások előtt, és ez jelentős érdeksérelemmel járhat.[15] Előfordul az is, hogy mások személyes adatait használják fel bűncselekmények elkövetéséhez (például az álprofilon keresztül pénzt vagy bankkártyaadatot csalnak ki más gyanútlan felhasználóktól). Az álprofilmódszer során gyakran más felhasználó személyes adatait (például nevét és fotóit) használják fel, amit akár további csalás vagy zsarolás követhet (például ilyen az úgynevezett romantikus csalás esete, amikor az illető a közösségi oldalakon a társkeresési szándék látszatával a másik fél bizalmába férkőzik, és tévedésbe ejti, vagy a megszerzett kompromittáló képekkel zsarolja az illetőt).[16] Az álprofilok esetében leggyakrabban tehát a személyes adattal visszaélés bűncselekménye merülhet fel (Btk. 219. §), ha az elkövető más személyes adatait jogosulatlanul kezeli az adatvédelmi rendelkezések megszegésével, haszonszerzési célból vagy jelentős érdeksérelmet okozva. Ezenkívül kihívást jelentenek az adatszivárgások, amikor nyilvánosságra hozzák a közösségimédia-platformok felhasználóinak tömeges személyes adatait, aminek adatvédelmi jogi következményei is vannak (lásd Cambridge Analytica-botrány).[17]

Az online csalások gyakran úgy valósulnak meg, hogy közszereplők nevében tesznek közzé tartalmakat. Például a Twitteren egy üzenet volt elérhető Elon Musktól, „Dojo 4 Doge" címmel, és erre az üzenetre válaszoltak a csalók, és megosztottak egy linket is. A csábító üzenet egy profi weboldalra vezetett, ahol arra próbálták rávenni a látogatókat, hogy küldjenek bitcoint állítólag Elon Musknak,

[15] Péterfalvi Attila – Eszteri Dániel: A személyes adatok büntetőjogi védelme Magyarországon és a Nemzeti Adatvédelmi és Információszabadság Hatóság kapcsolódó gyakorlata. In Görög Márta – Menyhárd Attila – Koltay András (szerk.): *A személyiség és védelme. Az Alaptörvény VI. cikkelyének érvényesülése a magyar jogrendszeren belül.* Budapest, ELTE ÁJK, 2017. 411.

[16] Gyaraki Réka: A közösségi média hatása a kiberbűncselekmények elkövetésére. *Magyar Rendészet*, 21. (2021), 2. 77.

[17] Margaret Hu: Cambridge Analytica's black box. *Big Data & Society,* 7. (2020), 2.; valamint lásd erről Chris Hoofnagle: Facebook in the Spotlight: Dataism vs. Privacy. *JURIST,* 2018. április 20.

mert ha ezt teljesítik, akkor rövid időn belül Musk befektetéseinek köszönhetően a dupláját fogják visszakapni, sőt a honlapon olvasható volt, hogy a bizonyos összeg feletti küldők megkaphatják a fődíjat is, amely egy Tesla Model S lesz.[18] A közösségi média platformjain egyre több befektetési és kriptovaluta-csalás jelenik meg (gyorsan megtérülő befektetéssel kecsegtető ajánlatok formájában), amelyek kihasználják e virtuális fizetőeszközök és az új típusú befektetések népszerűségét (például a Twitteren több mint 15 ezer botot azonosítottak a kriptovaluta-csalások kapcsán). Büntetőjogi aspektusból vizsgálva ezek az esetek jellemzően hagyományos csalásnak (Btk. 374. §) minősülnek, amelyek során természetes személyeket haszonszerzési célzattal tévedésbe ejtenek, és ezzel kárt okoznak.

A másik téma, amellyel érdemes külön foglalkoznunk, az az online szexuális zsarolás *(sextortion),* amely mind a felnőtteket, mind a gyermekeket érinti, azonban utóbbiak különösen veszélyeztetettek.[19] Utóbbi esetben az elkövető a gyermek bizalmába férkőzik (például a felnőtt fiatalkorúnak adja ki magát, és barátkozik a gyermekkel, kifejezetten szexuális tartalmú anyagot mutat neki, hogy csökkentse a szexualitáshoz kapcsolódó gátlásait), és kihasználja a sebezhetőségét. Ezt annak érdekében teszi, hogy a gyermeket ábrázoló szexuális jellegű képekhez vagy videókhoz jusson hozzá,[20] amit végül a zsarolás fázisa követ. Az elkövető kényszeríti, zsarolja az áldozatát, hogy szexuális szívességet teljesítsen a részére, vagy további kompromittáló képeket vagy videókat küldjön magáról. Amennyiben a kérésnek nem tesz eleget, akkor a már birtokában lévő felvételnek a megosztásával fenyeget (például a közösségi médián keresztül), és ezzel már irányítása alá vonja az illetőt.[21]

Végül érdemes a deepfake-technológia térnyeréséről említést tenni, amely viszonylag új, és egyre súlyosabb kihívást jelent a társadalom egésze számára. A deepfake esetében algoritmus segítségével képesek az adott személyről készült videófelvételben az arckép kicserélésére egy másik személy arcképére, amely bárki számára megtévesztő lehet. Az így létrehozott tartalmak súlyos károkat okozhatnak mind az egyénnek, mind a közösségnek: a magánszemélynek okozott károkon túl (lásd *revenge porn,* avagy „bosszúpornó" esete)[22] a deepfake hozzájárulhat a dezin-

[18] Mia Jankowicz: A Man in Germany Said He Fell for a Fake Elon Musk Crypto Scam that Cost Him $560,000. *Business Insider Australia,* 2021. március. 16.

[19] Anastasia Powell – Nicola Henry: *Sexual Violence in a Digital Age.* London, Palgrave Macmillan, 2017. 122–124.

[20] Például a fiatalok körében különösen népszerű a Snapchat videómegosztó portál és alkalmazás, ahol a felhasználók saját maguk által meghatározott időre oszthatnak meg egymással szöveges üzeneten kívül képet vagy videót.

[21] Europol: *Internet Organised Crime Threat Assesment (IOCTA).* 2014. 30.

[22] Általában féltékenységből, a párkapcsolat megszakítása miatti bosszúból a volt partner által a sértettről készült pornográf felvételek nyilvánosságra hozatalát jelenti. Az ilyen kép vagy videó készülhet csak magáról a (tipikusan meztelen) sértettről, az elkövető és a sértett közös szexuális cselekményéről, illetve az is elképzelhető, hogy nem valódi, hanem manipulált felvételről van szó, amikor tehát a bosszúpornográfia a deepfake-kel kombinálva jelenik meg. A hazai szakirodalomban Ambrus (2021): i. m. 223., valamint tanulmányában e témával foglalkozik Sorbán Kinga: A bosz-

formációhoz,[23] a demokratikus döntéshozatali eljárások eltorzításához és a választási eljárás manipulációjához, ezzel erodálva a közbizalmat és súlyosbítva a társadalom megosztottságát.[24] Sőt, a koronavírus elleni védekezést is akadályozhatják az álhírek (például a közösségi oldalakon megosztott tartalmak, bejegyzések a vírus és a vakcinák kapcsán), ezért a rémhírterjesztés tényállása (Btk. 337. §) kiegészült új elkövetési magatartással és a (2) bekezdés szerint, aki különleges jogrend idején nagy nyilvánosság előtt olyan valótlan tényt vagy való tényt oly módon elferdítve állít vagy híresztel, amely alkalmas arra, hogy a védekezés eredményességét akadályozza vagy meghiúsítsa, e deliktum miatt felelősségre vonható.[25]

Eddig a kibertámadások főbb sajátosságainak, mechanizmusainak bemutatására törekedtünk, a következőkben rátérünk a véleménynyilvánítás szabadsága ezzel közvetlen kapcsolatba hozható aspektusaira. Az összefüggések megvilágítását követően tanulmányunkat a szabályozás alapelveire, illetve egyes részelemeire vonatkozó *de lege ferenda* javaslatainkkal zárjuk.

Szólásszabadság az online platformokon

Az online platformok mint a szólásszabadság terepei

Az elmúlt évtizedekben, különösen az elmúlt években a politikai vélemények ütköztetésének elsődleges terepévé a virtuális térben található platformok váltak. Mivel egyre több választópolgár egyre intenzívebben használja az online felületeket, illetve ezeken a csatornákon keresztül a terjeszteni kívánt tartalmak sokkal gyorsabban és hatékonyabban érik el célközönségüket, egyre népszerűbbé váltak a politikai kommunikáció lebonyolítására. A pártok, jelöltek elsősorban a virtuális térben közelítik meg választóikat, akik ugyancsak az online térben reflektálnak a feléjük artikulált álláspontokra.[26] A magánvélemények is jórészt az internetes platformokon

szúpornó és a deepfake pornográfia büntetőjogi fenyegetettségének szükségességéről. *Belügyi Szemle,* 68. (2020), 10. 81–104. Az angolszász szakirodalom pedig részletesen foglalkozik ezzel a kérdéskörrel: Karolina Mania: The Legal Implications and Remedies Concerning Revenge Porn and Fake Porn: A Common Law Perspective. *Sexuality & Culture,* 24. (2020), 6. 2079–2097.; és Catherine D. Marcum et al.: Exploration of Prosecutor Experiences with Non-consensual Pornography. *Deviant Behavior,* 42. (2021), 5. 646–658.

[23] Christopher Whyte: Deepfake News: AI-enabled Disinformation as a Multi-Level Public Policy Challenge. *Journal of Cyber Policy* 5. (2020), 2. 1–19.

[24] Tyrone Kirchengast: Deepfakes and Image Manipulation: Criminalisation and Control. *Information & Communications Technology Law,* 29. (2020), 3. 308–323.

[25] Lásd a rémhírterjesztésről Bencze Mátyás – Ficsor Krisztina: A koronavírus kihívásai és a jogtudomány: a rémhírterjesztés tényállásának jogalkalmazási kérdései. *jtiblog,* 2020. április 2.

[26] Török Bernát: A szólásszabadság védelmének dinamikája. *Magyar Jog,* 64. (2017), 12. 721–733.

kerülnek szembe egymással, ahol ezek is korábban sosem tapasztalt gyorsasággal terjeszthetők és könnyen, sokszor akár névtelenül is észrevételezhetők.[27]

Különösen felgyorsultak ezek a folyamatok a pandémia időszakában, amikor a kijárási és kapcsolattartási korlátozások következtében gyakorlatilag mindenki rákényszerült online jelenlétének fokozására.[28] Ráadásul a járványügyi intézkedések egy része kifejezetten érintette a véleménynyilvánítás gyakorlásának egyes formáit, például a gyülekezéseket sok helyen megtiltották, vagy legfeljebb szigorú korlátok között és csekély számú résztvevővel engedélyezték. Ilyen körülmények között kellett választási kampányokat megszervezni, illetve egyáltalán fenntartani a politikai diskurzust az ebben történő részvétel iránt érdeklődő állampolgárok számára. Ez kizárólag, vagy legalábbis túlnyomórészt az online platformokon volt csak lehetséges, amelyek szerepe így még inkább felértékelődött.

A politikai kommunikáció virtualizálódása számos politológiai, szociológiai kérdést is felvet, jelen tanulmányban ezen probléma politikai aspektusaival foglalkozunk. A felhasználóknak csak kisebb része kezeli tudatosan ezeket a felületeket, és számol azokkal a kockázati tényezőkkel, amelyek együtt járnak az online platformok igénybevételével elsősorban a fentebb már vázolt rosszindulatú kibertevékenységek következtében.[29] Továbbá legtöbbször nem jelenik meg a véleményt nyilvánító személyek tudatában az sem, hogy álláspontjuk nyilvánosságra hozatalával egy legalább három résztvevős jogviszony szereplőivé válnak.[30] A platform üzemeltetője felületet biztosít a magánszemélyek számára álláspontjuk kifejtésére és megosztására más felhasználókkal, illetve ehhez kapcsolódóan a vélemények ütköztetésére. Az üzemeltető elsősorban a platform megfelelő működtetéséért és folyamatos rendelkezésre állásáért felel, korlátozott körben azonban helyt kell állnia az általa fenntartott felületeken megosztott tartalmakért is. A szolgáltatást igénybe vevő magánszemély ezzel szemben elsősorban az általa folytatott kommunikációval valósíthat meg esetleges jogsértéseket, például gyűlöletbeszéd közzétételével.[31] Ezenfelül pedig figyelembe kell vennünk harmadik személyek bekapcsolódásának lehetőségét is az online véleménycserével összefüggő jogviszonyokba, ilyenként me-

[27] *The Right to Freedom of Expression and the Use of Encryption and Anonymity in Digital Communications.* Submission to the United Nations Special Rapporteur on the Right to Freedom of Opinion and Expression by the Association for Progressive Communication (APC). Association for Progressive Communications (APC), 2015.

[28] Andrea M. Matwyshyn: Cyber Harder. *Boston University Journal of Science and Technology Law,* 24. (2018), 450.

[29] Joe Burton: Cyber-Attacks and Freedom of Expression: Coercion, Intimidation and Virtual Occupation. *Baltic Journal of European Studies,* 9. (2019), 3. 116–133.

[30] Pavlina Pavlova: Human Rights-based Approach to Cybersecurity: Addressing the Security Risks of Targeted Groups. *Peace Human Rights Governance,* 4. (2020), 3. 391–418.

[31] Török Bernát: A gyűlöletbeszéd tartalmának médiajogi mércéi. *Jogtudományi Közlöny*, 68. (2013), 2. 59–72.

rülhetnek fel az adathalász célzattal vagy a demokratikus diskurzus eltorzításának szándékával fellépő szereplők.

Dezinformáció

A kibertámadások két irányban gyakorolnak hatást a demokratikus diskurzus alakulására a platformokon:[32] egyrészt rendszerszinten torzítják a vélemények piacát, másrészt pedig visszatartó erőként jelenhetnek meg az egyének számára a nyilvános vitákba történő bekapcsolódást illetően.[33] Ebben az alfejezetben először a legfontosabb rendszerszintű kockázatra, a dezinformáció létrehozatalára és terjesztésére térünk ki.

Az Európai Bizottság megfogalmazása szerint a dezinformáció „olyan igazolhatóan hamis vagy félrevezető információ, amelyet gazdasági haszonszerzés vagy szándékos megtévesztés céljából hoznak létre, hoznak nyilvánosságra és terjesztenek, és amely kárt okozhat a közérdeknek".[34] Az Európai Bizottság 2018-ban szakértői csoportot is felállított az álhírek terjesztésével és az online dezinformáció jelenségeivel összefüggő mechanizmusok feltérképezésére.[35] A dezinformáció jelenségének négy fő iránya létezhet, az új technológiák hozzájárulhatnak valamennyi alakzat előidézéséhez. Egyrészt fiktív felhasználói profilok generálásával és azokon keresztül bizonyos álláspontok artikulálásával a kibertevékenység olyan szempontokat helyezhet előtérbe a diskurzusban, amelyek megvitatására nincs valós társadalmi igény.[36] Ezt elősegíti az is, hogy gyakran a valós személyek is álnéven, esetleg név nélkül fejtik ki nézeteiket az online platformokon, így a felhasználó számára nem elkülöníthetők a valós személyt megtestesítő és a fiktív hozzászólások, állásfoglalások.[37]

Egy másik létező alternatíva az egyébként is jelen lévő álláspontok jelentőségének felnagyítása, vagy éppen relativizálása, ami azért képes a közvélemény

[32] Gregory T. Nojeim: Cybersecurity and Freedom on the Internet. *Journal of National Security Law & Policy,* 2010. augusztus 13.

[33] Noha Fathy: Freedom of Expression in the Digital Age: Enhanced or Undermined? The Case of Egypt. *Journal of Cyber Policy,* 3. (2018), 1. 96–115.

[34] Az Európai Bizottság és az Unió külügyi és biztonságpolitikai főképviselőjének közös jelentése a dezinformációval szembeni közös cselekvési terv végrehajtásáról: Európai Bizottság: *Közös közlemény az Európai Parlamentnek, az Európai Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – Jelentés a dezinformációval szembeni közös cselekvési terv végrehajtásáról.* JOIN(2019)12 végleges (2019. június 14.).

[35] European Commission: *Final Report of the High Level Expert Group on Fake News and Online Disinformation.* Shaping Europe's Digital Future, 2018. március 12.

[36] Holly A. Garnett – Toby S. James: Cyber Elections in the Digital Age: Threats and Opportunities of Technology for Electoral Integrity. *Election Law Journal: Rules, Politics, and Policy,* 19. (2020), 2.

[37] European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs: *The Fight Against Disinformation and the Right to Freedom of Expression.* 2021. 24–26.

befolyásolására, mert egyre inkább az online platformokon észlelhető kommunikációk alapján vonunk le következtetéseket a közvélemény aktuális állására vonatkozóan.[38] Ha tehát azt érzékeljük adott esetben a részben vagy egészben kibereszközökkel generált megnyilvánulások következtében, hogy a résztvevők többsége egy bizonyos álláspontot támogat, azt fogjuk feltételezni, hogy a közhangulat is ennek megfelelő. Az pedig már szociológiai kérdés, ugyanakkor a választói akarat befolyásolásán keresztül alkotmányjogi vonatkozása is van, hogy ennek a szubjektív érzetnek a keltése számottevően befolyásolhatja a közbeszédet és akár az egyes választások kimenetelét is.[39] A közvélemény említett manipulásának legszervezettebb formáit a trollfarmok jelentik, amelyek kifejezetten azzal a céllal létesülnek, hogy valótlan információk megosztásával befolyásolják a politikai folyamatokat és a döntéshozatalt.[40]

A harmadik idekapcsolódó tendencia olyan tények hangoztatása az online platformokon jelen lévő fiktív profilok segítségével, amelyeknek semmilyen valóságalapja nincsen. Az ilyen tájékoztatások rendkívül nagy kockázata a modern nyilvánosság szerkezetét figyelembe véve különösen szembetűnő.[41] A legmeghökkentőbb álhírek is nagyon gyorsan eljutnak a felhasználók széles köreihez, sőt éppen ezek terjednek a leggyorsabban, ugyanakkor az azok valótlanságát leleplező tartalmak iránt már jóval kevesebben érdeklődnek. Egy vaskos álhír tehát akár egyes közszereplők megítélését is számottevően kedvezőtlenül érintheti, vagy éppen egyes, az aktuális politikai diskurzusban napirenden lévő témák értékelését befolyásolhatja.

Végezetül számolnunk kell a dezinformáció azon formájával is, amikor tényszerűen igaz állítások jelennek meg kontextusukból kiragadva, olyan módon elferdítve, hogy az alkalmas a tartalmat fogyasztók félrevezetésére, a valóságtól ténylegesen eltérő látszat keltésére tényszerűen hamis tényállítás hangoztatása nélkül.[42]

A továbbiakban arra térünk ki, a rendszerszintű kedvezőtlen következmények mellett az egyének szintjére lebontva, hogy melyek azok a veszélyforrások, amelyek elrettentőek lehetnek egyesek számára a közérdekű online vitákba történő

[38] Bartóki-Gönczy Balázs: A keresőmotorok és a szólásszabadság kapcsolata. Megközelítés és szabályozási javaslatok az Európai Unióban és az Egyesült Államokban. *Iustum Aequum Salutare,* 14. (2018), 1. 157–194.

[39] Kevin M. Caramancion: An Exploration of Disinformation as a Cybersecurity Threat. *2020 3rd International Conference on Information and Computer Technologies (ICICT),* (2020). 440–444.; valamint Kovács László – Krasznay Csaba: „Mert övék a hatalom". Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során. *Nemzet és Biztonság: Biztonságpolitikai Szemle,* 10. (2017), 3. 3–15.

[40] Lásd a trollfarmokról bővebben Kathleen Hall Jamieson: *Cyberwar: How Russian Hackers and Trolls Helped Elect a President: What We Don't, Can't, and Do Know.* Oxford, Oxford University Press, 2018.

[41] Allison O. Larsen: Constitutional Law in an Age of Alternative Facts. *New York University Law Review,* 93. (2018), 2. 178.

[42] Ari E. Waldman: The Marketplace of Fake News. *Journal of Constitutional Law,* 20. (2018), 4. 101–105.

bekapcsolódás tekintetében, vagy amelyeknek áldozatul eshetnek a virtuális térben gyanútlanul véleményt nyilvánító személyek.

A szólásszabadságot érintő kiberfenyegetések az online platformokon

Adatvédelmi aggályok

Az egyéni szinten érzékelhető egyik fő motiváció a platformokra irányuló kibertevékenység kapcsán az adatok megszerzése.[43] Ennek célja kettős lehet: egyrészt az érintett személyek profilozása akár álláspontjuk alapján is, másrészt mindenféle politikai célzat nélkül történő visszaélés a megszerzett személyes adatokkal (például vagyoni haszonszerzés céljából). A platformokon kommentelők személyes adatai sorsával összefüggő adatvédelmi kihívások négy fő csoportba sorolhatók.

Egyrészt a kibertámadások mögött ténylegesen jelen lévő természetes személyek gyakran nem, vagy csak igen nehezen visszakövethetők, így pedig nem átlátható az sem, hogy kinek a kezébe kerülnek nem kellően védett személyes adataink.[44] Ennek az átláthatósági deficitnek az az eredménye, hogy teljesen elveszíthetjük az ellenőrzést személyes adataink sorsa felett, és gyakran akár egy személyiségprofil felépítéséhez is elegendő információ kerülhet rólunk olyan kezekbe, amelyeket még csak nem is ismerünk.

Másrészt az a tény, hogy átláthatatlan hátterű személyek juthatnak a felhasználók személyes adatainak birtokába, nem önmagában jelent igazán nagy problémát, hanem azért, mert kiszámíthatatlan, hogy az adathalászok milyen szándékkal kívánják felhasználni az általuk jogellenesen kezelt személyes adatokat.[45] Különösen fontos ez annak tudatában, hogy az online platformokon véleménynyilvánításunk során gyakran igen érzékeny témákban foglalunk állást, amikor a névtelenség bár kockázati tényező, de garancia is lehet egyben.[46] A kibereszközök segítségével harmadrészt akár a névtelenül kommentelők is beazonosíthatóvá válnak, vagy a nevüket felvállaló kommentelőkről is olyan személyes adatok kerülhetnek ki, amelyeket ők nem kívántak megosztani. Nagyon sok esetben pedig nem egyszerűen személyes adatokról, hanem különösen érzékeny személyes adatokról beszélünk, emiatt pedig sokan inkább távol maradnak az online diskurzusoktól egy olyan időszakban,

[43] Elizabeth F. Judge – Michael Pal: Voter Privacy in the Age of Big-Data Elections. *Osgoode Hall Law Journal,* 58. (2021), 1. 2.

[44] Lyria B. Moses: Recurring Dilemmas: The Law's Race to Keep Up with Technological Change. *University of Illinois Journal of Law, Technology & Policy,* (2007). 274–275.

[45] Ira S. Rubinstein: Voter Privacy in the Age of Big Data. *Wisconsin Law Review,* (2014), 5. 861–936.

[46] Koltay András – Nyakas Levente: *Tanulmányok a technológia- és cyberjog néhány aktuális kérdéséről.* Budapest, Médiatudományi Intézet, 2018. 18–19.

amikor a közérdekű témákról zajló párbeszéd egyre nagyobb része terelődik ezekre a felületekre.

A negyedik, a platformok integritását fenyegető kiberjelenség az ilyen felületeket igénybe vevők megszerzett adatainak adatbázisokba történő rendezése, így pedig nem csupán az egyénről magáról, hanem a szélesebb társadalmi környezetben elfoglalt helyéről is kialakulhat egy kép a kiberbűnözők számára.

A demokratikus diskurzus akadályozása

Az adatvédelmi kérdéseknél talán még messzebbre vezet, ha az egyén helyzetét vizsgáljuk az egyre inkább virtualizálódó demokratikus térben, ugyanis azt tapasztaljuk, hogy egyre nehezebb az egyes állampolgároknak navigálniuk a vélemények egyre bonyolultabb és átláthatatlanabb piacán.[47] Ezzel a platformokat használók jelentős része tisztában van, érzékelhető az információforrások egyre alacsonyabb megbízhatósági foka, valamint a politikai kommunikációban egyre hangsúlyosabbá váló manipuláció.[48] Ez felerősíti az apolitikus tendenciákat a társadalomban, ami tovább nehezíti az inkluzív demokratikus diskurzus kibontakozását.

Súlyos probléma a platformokkal összefüggésben, hogy gyakran azok üzemeltetői maguk is moderálják a közbeszédben jelen lévő tartalmakat azzal, hogy eltávolítják a legfeljebb belső szabályzatukban rögzítettek alapján nemkívánatos tartalmakat.[49] Az ilyen beavatkozás rendszerint mindig valamely konszenzuálisnak tekinthető célt szolgál, például a gyűlöletbeszéd visszaszorítását, az emberi méltóság, vagy egyes személyek vagy jól körülhatárolható társadalmi csoportok méltóságának védelmét.[50] Ezen fogalmak értelmezésében azonban már jelentős különbségek mutatkoznak, és sokan érzik úgy, hogy megnyilvánulásaikat a platformok üzemeltetői alaptalanul távolították el a vélemények piacáról. Ráadásul a platformok működése jogilag alig szabályozott, üzemeltetői háttere pedig gyakran kevéssé átlátható, így a politikai diskurzus kereteiről és nemritkán az egyes egyén kommunikációs szabadságának határairól is a platformok üzemeltetői, vagyis semmilyen közhatalommal nem fel-

[47] Rebecca Green: Counterfeit Campaign Speech. *Hastings Law Journal,* 70. (2019), 1445.

[48] Elizabeth F. Judge – Amir M. Korhani: A Moderate Proposal for a Digital Right of Reply for Election-Related Digital Replicas: Deepfakes, Disinformation, and Elections. In Holly A. Garnett – Michael Pal (szerk.): *Cyber-Threats to Canadian Democracy.* McGill-Queen's University Press, 2021.

[49] Parti Katalin: Harc az online illegális tartalom ellen. In *Kriminológiai tanulmányok 49.* Budapest, Országos Kriminológiai Intézet, 2012.

[50] Lásd ehhez Nagy Krisztina: Facebook files – gyűlöletbeszéd törölve? A közösségimédia-platformok tartalom-ellenőrzési tevékenységének alapjogi vonatkozásai. In Polyák Gábor (szerk.): *Algoritmusok, keresők, közösségi oldalak és a jog – A forgalomirányító szolgáltatások szabályozása.* Budapest, HVG-ORAC, 2020. 148–170.

ruházott magánszereplők határoznak,[51] ráadásul úgy, hogy gyakran maguk a moderálók, illetve a mögöttük álló érdekcsoportok sem beazonosíthatók.

Javaslatok: szabályozási megoldások

A kibertámadások azért is lehetségesek az online platformokon, mert e felületek jogilag rendkívül alulszabályozottnak számítanak, nem léteznek olyan jogi kódexek, amelyek rendeznék a kapcsolódó felelősségi viszonyokat.[52] Nem világos, hogy milyen jogi kötelezettségei vannak a platform üzemeltetőjének, igénybe vevőjének, így az sem, hogy mely magatartásokra kötelezhetők a kibertámadások megelőzése érdekében. Ennek a globálisan is érzékelhető bizonytalanságnak egy jó példája volt a francia alkotmánytanács 2020. júniusi döntése, amelyben egy olyan törvényt semmisített meg, amelynek értelmében a platformot üzemeltető jelentős összegű pénzbírsággal volt sújtható, amennyiben 36 órával a jogsértő tartalom közzétételét követően nem távolította el azt felületéről.[53] E döntésből is az tűnt ki, hogy egyáltalán nem tisztázott, mi várható el jogi értelemben az online platformokon történő eszmecsere különböző résztvevőitől.[54] Hasonló kihívásokra törekszik választ adni a modellértékűnek tekinthető német szabályozás is, amelynek jelenlegi formája széles körű konzultációt követően alakult ki, és amely szintén a digitális platformokon megosztott jogellenes tartalmak minél gyorsabb eltávolítását célozza.[55]

A jogi szabályozásnak tehát lépnie kell ezen a területen, ebben lényegében egyetértés mutatkozik, kérdéses azonban, hogy milyen irányú elmozdulásra lenne szükség a helyzet javítása érdekében. Az újonnan felmerülő olyan digitális kihívások kezelése érdekében, mint például a hamisított áruk terjedése, a gyűlöletbeszéd, a kiberfenyegetések, a dezinformáció, a korlátozott verseny és a digitális piacok lezárása, az Európai Bizottság 2020 decemberében digitális szolgáltatásokkal kapcsolatos csomagot terjesztett elő. Jelenleg is zajlik e jogalkotási csomag keretében[56] a digitális szolgáltatásokra vonatkozó külön rendelet tervezetének vitája,[57]

[51] Elizabeth F. Judge – Amir M. Korhani: Digital Information Equality, Disinformation, and Elections. *Election Law Journal,* 19. (2020), 2. 240.

[52] Philip N. Howard: *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*. New York, Oxford University Press, 2018.

[53] Décision n° 2020-801 dc du 18 juin 2020.

[54] Szentgáli-Tóth Boldizsár: Vigyázó szemetek Párizsra vessétek – avagy pénzbírsággal, vagy anélkül a gyűlöletbeszéd ellen? *Jogi Fórum – Sajtó és Média Blog,* 2021. június 30.

[55] Jacob Mchangama – Natalie Alkiviadou: *The Digital Berlin Wall: How Germany (accidentally) Created a Prototype for Global Censorship – Act Two.* Copenhagen, Justitia, 2020.

[56] European Commission: The Digital Services Act package (é. n.).

[57] Európai Bizottság: *Az Európai Parlament és a Tanács rendelete a digitális szolgáltatások egységes piacáról (digitális szolgáltatásokról szóló jogszabály) és a 2000/31/EK irányelv módosításáról.* COM(2020)825 végleges (2020. december 15.).

ez a javaslat több újdonságot hozna a platformok üzemeltetőire nézve is. Lényegében általánosságban véve nem szankcionálná a platformszolgáltatókat a felületeiken megosztott jogellenes tartalom eltávolításának hiányáért, ugyanakkor kötelezné őket arra, hogy amennyiben a jogellenesség tudomásukra jut, azonnal távolítsák el a kérdéses tartalmat. Ez még nem jelent alapvető újdonságot, hiszen mindez megfelel az eddig is alkalmazott jogi előírásoknak, illetve joggyakorlatnak, ugyanakkor újabb kötelezettségek is megjelennek a legnagyobb platformszolgáltatókkal szemben: nyilvánosságra kell hozniuk a közléseket vizsgáló mesterségesintelligencia-alapú algoritmusaik működési elveit, továbbá azt, hogy milyen formában döntenek egyes tartalmak eltávolításáról felületeikről. Ez tehát némileg átláthatóbbá teszi a felhasználók számára véleménynyilvánításuk elbírálásának folyamatát, és ezzel mérsékelhetik az egyik olyan tényezőt, amely sokakat visszatarthat az online platformokon történő kommenteléstől. Sem a digitális tartalom szolgáltatásáról szóló irányelv, sem bármilyen más jelenleg ismert jogszabálytervezet nem foglalkozik viszont azzal a kérdéssel, hogy hogyan kellene a platformokra nehezedő nyomást enyhíteni, ezzel az e felületeken véleményt nyilvánítók biztonságát elősegíteni.

Álláspontunk szerint a szólásszabadsággal összefüggő kihívások kezelésekor abból szükséges kiindulni, hogy csak integrált szemlélettel és kombinált eszközrendszerrel lehet érdemi eredményt elérni ezen a téren.[58] Technológiai, gazdasági, személyi és jogi feltételei is vannak a platformokon zajló diskurzus megtisztításának a manipulált tartalmaktól, illetve a kibertámadásoktól. Technológiai feltételekről azért kell beszélnünk, mert folyamatosan fejleszteni kell azokat az informatikai megoldásokat, amelyek képesek megakadályozni a rosszindulatú kibertérből érkező beavatkozásokat a platformok működésébe. Gazdasági tekintetben is szükséges folytatni ezt a gondolkodást, mert a platformokat érintő kiberbűnözés elsődlegesen ilyen motivációkból ered, ezeket kell tehát kiismernünk és ellensúlyoznunk. Személyi vonatkozásban a platformok védelmének fontos előfeltétele az, hogy legyenek olyan szakemberek, akik egyrészt képesek beazonosítani a főbb kihívásokat és kimunkálni azokkal szemben a fellépés legmegfelelőbb módjait, másrészt napi szinten is részt tudnak venni a rendelkezésükre álló technológiák segítségével a védekezésben.

A jogi szabályozásnak az iménti szempontokat figyelembe véve kell reflektálnia a platformokra nehezedő nyomásra, ennek egyik iránya nézetünk szerint a védekezés felelősségének megosztása lehet a platform üzemeltetője és felhasználója között. Az üzemeltetőkre nézve olyan előírásokat kellene rögzíteni, hogy milyen biztonsági intézkedések eszközlésére kötelesek, illetve milyen technológiai megoldásokat kellene igénybe venniük a kibertámadások kivédése érdekében. Amennyiben a platformszolgáltatók nem teljesítik e kötelezettségüket egy számukra kellő felkészülési időt jelentő határidőn belül, pénzbírsággal lennének sújthatók, végső esetben pedig a platform működésének befejezésére lehetne kötelezni őket. Ezzel párhuzamosan a felhasználók felelősségi körét is körvonalazni kellene: mely esetben várható el

[58] Jamie Lund: Correcting Digital Speech. *UCLA Entertainment Law Review,* 19. (2012), 1. 186.

a körültekintő eljárás a platformok igénybe vevőitől, és mi az a virtuális térben megvalósítható, prudenciát nélkülöző magatartás, amelynek megvalósításakor a felhasználónak magának kell viselnie óvatlansága következményeit? Ilyen lehet például, hogy ha a felhasználó indokolatlanul széles kör számára olyan személyes adatait teszi önkéntesen hozzáférhetővé, amelyek semmilyen módon nem kapcsolódnak sem a platform igénybevételéhez, sem pedig a platformon keresztül másokkal megosztott véleményéhez.

Mint ahogyan általában sincs kidolgozva a platform üzemeltetőjének és igénybe vevőjének jogi státusza az online kommenteléssel összefüggésben, nincs ez másként a kibertámadásokkal szembeni védekezés kapcsán sem. E nehezen azonosítható veszélyforrással szembeni tudatosabb és hatékonyabb fellépés csak akkor remélhető, ha az egyes szereplők világosan látják a feladataikat ezen a téren. Szankció alkalmazására pedig a fokozatosság szem előtt tartásával és csak végső esetben lenne szükség, amennyiben más módon nem kényszeríthető ki a kockázatok mérséklésére alkalmas magatartás.

Az európai térben emellett felmerülhetnek további jogi eszközök is a tagállamok közötti együttműködés erősítésére a határon átnyúló kiberbűnözés visszaszorítása érdekében. Mivel ezen elkövetési magatartások alapvető sajátossága azok határon átnyúló jellege, ezért az európai szintű együttműködés alapvető bűnmegelőzési érdek. Szükség lenne egyrészt az elektronikus bizonyítékok megszerzése érdekében a jelenleginél szélesebb körű együttműködésre, továbbá az ilyen irányú bűnözéssel összefüggő adatokat elérhetővé kellene tenni valamennyi érdekelt hatóság, illetve a kapcsolódó témákkal foglalkozó kutatók számára is.

Összegzés

Számos szerző foglalkozott már a kiberbűnözés aktuális tendenciáival, és a szólásszabadság kapcsán megfigyelhető változásokat is gyakran elemzi a szakirodalom. Mégis kevés kísérlet történt eddig arra, hogy e két, egymástól látszólag távol eső szakterület metszéspontjára fókuszálva felvázolja a szólásszabadsággal összefüggő, a kibertérben fellelhető kihívások jogi vonatkozásait. Ezt komoly hiányosságnak tartjuk különösen annak fényében, hogy a közügyekről zajló diskurzus egyre nagyobb része terelődik az online platformokra, köszönhetően a járványhelyzetből következő fizikai elszigeteltségnek is.

További problémának érezzük azt, hogy a jogi szabályozás hézagos volta általában a platformszolgáltatók, illetve igénybe vevők kapcsán merül fel, kevés azonban a külső szereplőkkel szembeni közös védekezés esetleges jogi kereteit előtérbe helyező tanulmány. Ennek a kimunkálásra váró jogi keretrendszernek néhány alapelvére, illetve intézményére tettünk javaslatot a felelősség megosztásának hangsúlyozásával a platformok üzemeltetői és igénybe vevői között. Úgy véljük, a kibertámadásokban rejlő kockázatok demokratikus diskurzusra gyakorolt hatása valódi jelentőségének

felismerése, illetve a jogszabályi környezet ennek megfelelő továbbfejlesztése hozzájárulhat a platformokon zajló politikai kommunikáció manipulatív jellegének visszaszorításához, ezzel pedig kihatással lehet a demokratikus participáció valamennyi formájára és minden egyes, vagy legalábbis számos állampolgár mindennapjaira.

Írásunkban e távlati célkitűzésekkel összefüggésben nem végleges válaszokat kívántunk megfogalmazni, hanem a szakirodalomban már eddig is tárgyalt dilemmák néhány újabb aspektusára hívtuk fel a figyelmet. További kiterjedt szakmai diskurzusra lesz még szükség a szólásszabadsággal összefüggő kihívások hosszú távú kezelésének kimunkálásához, bízunk abban, hogy felvetéseinkkel hozzá tudtunk járulni e párbeszéd további irányainak kijelöléséhez.

The Dangers of Online Platforms: The Legal Risks of Disinformation and Cyberattacks

Abstract

The motivations behind the malware use of modern technologies could often target the influence of public discourse: to generate manipulated opinions; fictive arguments; or relativise the weight of a certain viewpoint. For instance, communications created with the help of automatised instruments (bots) could result in a distortive image of the public opinion from a particular matter. Apart from this, a further new challenge is the spread of deep fake technologies based on artificial intelligence. The contents established with these methods could cause severe harm also for the individuals and the community. In addition to the harms caused to individuals, deep fake could distort the democratic decision-making processes and manipulate democratic elections, which would erode public trust and increase the borderlines within society. Moreover, criminal law issues may also arise.

Cybercrimes always entail more significant social and economic losses, which may infringe the fundamental rights of individuals, and may also threaten the rule of law and the stability of democratic societies. Online platforms serve as new venues for malware practices: online users are not aware of the threats that come from the virtual sphere and the not sufficiently careful share of personal data. For this reason, the cyberattacks against internet platforms and their users usually target obtaining personal or other sensitive data, which might be used to commit further crimes (for instance, fraud, blackmail, etc.). Apart from this, the social media platforms are proper grounds for spreading malware programs and unlawful content: these constitute a great danger, especially during the pandemic, when the online presence of people increased significantly.

In our study, we look for different perspectives of the regulatory framework to treat this complex issue properly. With which instruments could we protect the free marketplace of ideas as a main pillar of democracy from these new challenges? And as part of these collective efforts, how could the users of online platforms be protected from undue cyberattacks? The combined set of tools would be necessary to protect fundamental rights efficiently from cyberattacks with establishing legal, personal, technological and economic background of effective countermeasures. Regarding the legal aspect, the platform-holders' safeguards against unlawful contents and attacks should be determined. At the same time, monitoring of the compliance with this requirement should be monitored continuously. Furthermore, in case of misusing contents and especially personal data shared in the platforms and provided to the platform operator, the responsibility shall be allocated. It should also be distinguished

which protective measures are expected from the operator and the platform users. Our study outlines regulatory alternatives to treat these issues.

Felhasznált irodalom

2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről.

Algarni, Abdullah – Yue Xu – Taizan Chan: An Empirical Study on the Susceptibility to Social Engineering in Social Networking Sites: the Case of Facebook. *European Journal of Information Systems,* 26. (2017), 6. 661–687. Online: https://doi.org/10.1057/s41303-017-0057-y

Ambrus István: *Digitalizáció és büntetőjog.* Budapest, Wolters Kluwer, 2021.

Bartóki-Gönczi Balázs: A keresőmotorok és a szólásszabadság kapcsolata. Megközelítés és szabályozási javaslatok az Európai Unióban és az Egyesült Államokban. *Iustum Aequum Salutare,* 14. (2018), 1. 157–194.

Bencze Mátyás – Ficsor Krisztina: A koronavírus kihívásai és a jogtudomány: a rémhírterjesztés tényállásának jogalkalmazási kérdései. *jtiblog,* 2020. április 2. Online: https://bit.ly/3zdtqmg

Brenner, Susan W.: *Cybercrime: Criminal Threats From Cyberspace.* Santa Barbara (CA), Praeger, 2010.

Britz, Marija T.: *Computer Forensics and Cyber Crime: An Introduction.* London, Pearson, 2013.

Burton, Joe: Cyber-Attacks and Freedom of Expression: Coercion, Intimidation and Virtual Occupation. *Baltic Journal of European Studies,* 9. (2019), 3. 116–133. Online: https://doi.org/10.1515/bjes-2019-0025

Caramancion, Kevin M.: An Exploration of Disinformation as a Cybersecurity Threat. *2020 3rd International Conference on Information and Computer Technologies (ICICT),* (2020). 440–444. Online: https://doi.org/10.1109/ICICT50521.2020.00076

Clough, Jonathan: *Principles of Cybercrime.* Cambridge, Cambridge University Press, 2015. Online: https://doi.org/10.1017/CBO9781139540803

Council of Europe: Explanatory Report to the Convention on Cybercrime. *European Treaty Series,* 185. (2001). 79. cikk.

Daskal, Jennifer – Debrae Kennedy-Mayo: Budapest Convention: What is it and How is it Being Updated? *Cross-Border Data Forum,* 2020. július 2. Online: https://bit.ly/3flRrfx

Décision n° 2020-801 DC du 18 juin 2020. Online: https://bit.ly/3PD0xp0

Európai Bizottság: *Közös közlemény az Európai Parlamentnek, az Európai Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – Jelentés a dezinformációval szembeni közös cselekvési terv végrehajtásáról.* JOIN(2019)12 végleges (2019. június 14.). Online: https://bit.ly/3Pg9Dbn

Európai Bizottság: *Az Európai Parlament és a Tanács rendelete a digitális szolgáltatások egységes piacáról (digitális szolgáltatásokról szóló jogszabály) és a 2000/31/EK irányelv módosításáról.* COM(2020)825 végleges (2020. december 15.). Online: https://bit.ly/3PhwF1r

European Commission: *Final Report of the High Level Expert Group on Fake News and Online Disinformation.* Shaping Europe's Digital Future, 2018. március 12. Online: https://bit.ly/3aMIyxw

European Commission: *The Digital Services Act Package* (é. n.). Online: https://bit.ly/3aIQKyC

European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs: *The Fight Against Disinformation and the Right to Freedom of Expression.* 2021. Online: https://bit.ly/3B56t5M

Europol: *Internet Organised Crime Threat Assesment (IOCTA).* 2014.

Fathy, Noha: Freedom of Expression in the Digital Age: Enhanced or Undermined? The Case of Egypt. *Journal of Cyber Policy,* 3. (2018), 1. 96–115. Online: https://doi.org/10.1080/23738871.2018.1455884

Garnett, Holly A. – Toby S. James: Cyber Elections in the Digital Age: Threats and Opportunities of Technology for Electoral Integrity. *Election Law Journal: Rules, Politics, and Policy,* 19. (2020), 2. Online: https://doi.org/10.1089/elj.2020.0633

Gillespie, Alisdair A.: *Cybercrime: Key Issues and Debates.* New York, Routledge, 2019. Online: https://doi.org/10.4324/9781351010283

Grabosky, Peter: *Cybercrime.* London, Oxford University Press, 2016.

Green, Rebecca: Counterfeit Campaign Speech. *Hastings Law Journal,* 70. (2019), 1445.

Gyaraki Réka: A közösségi média hatása a kiberbűncselekmények elkövetésére. *Magyar Rendészet,* 21. (2021), 2. 67–82. Online: https://doi.org/10.32577/mr.2021.2.4

Hoofnagle, Chris: Facebook in the Spotlight: Dataism vs. Privacy. *JURIST,* 2018. április 20. Online: https://bit.ly/3AXyVXx

Howard, Philip N.: *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media.* New York, Oxford University Press, 2018.

Hu, Margaret: Cambridge Analytica's Black Box. *Big Data & Society,* 7. (2020), 2. Online: https://doi.org/10.1177/2053951720938091

Jamieson, Kathleen Hall: *Cyberwar: How Russian Hackers and Trolls Helped Elect a President: What We Don't, Can't, and Do Know.* Oxford, Oxford University Press, 2018.

Jankowicz, Mia: A Man in Germany Said He Fell for a Fake Elon Musk Crypto Scam that Cost Him $560,000. *Business Insider Australia,* 2021. március. 16. Online: www.businessinsider.com.au/man-lost-560000-worth-of-bitcoin-elon-musk-scam-bbc-2021-3

Judge, Elizabeth F. – Amir M. Korhani: Disinformation, Digital Information Equality, and Electoral Integrity. *Election Law Journal,* 19. (2020), 2. 240–261. Online: https://doi.org/10.1089/elj.2019.0566

Judge, Elizabeth F. – Amir M. Korhani: A Moderate Proposal for a Digital Right of Reply for Election-Related Digital Replicas: Deepfakes, Disinformation, and Elections. In Holly A. Garnett – Michael Pal (szerk.): *Cyber-Threats to Canadian Democracy.* McGill-Queen's University Press, 2021. Online: https://doi.org/10.2139/ssrn.3827249

Judge, Elizabeth F. – Michael Pal: Voter Privacy in the Age of Big-Data Elections. *Osgoode Hall Law Journal,* 58. (2021), 1. 1–55.

Kirchengast, Tyrone: Deepfakes and Image Manipulation: Criminalisation and Control. *Information & Communications Technology Law,* 29. (2020), 3. 308–323. Online: https://doi.org/10.1080/13600834.2020.1794615

Klein Tamás: Keresőmotor-szolgáltatók és az internetes szólásszabadság. In Koltay András – Nyakas Levente (szerk.): *Tanulmányok a technológia- és cyberjog néhány aktuális kérdéséről.* Budapest, Médiatudományi Intézet, 2018. 26–29.

Koltay András: *Az új média és a szólásszabadság. A nyilvánosság alkotmányos alapjainak újragondolása.* Budapest, Wolters Kluwer, 2019.

Koltay András – Nyakas Levente (szerk.): *Tanulmányok a technológia- és cyberjog néhány aktuális kérdéséről.* Budapest, Médiatudományi Intézet, 2018.

Kovács László – Krasznay Csaba: „Mert övék a hatalom": Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során. *Nemzet és Biztonság: Biztonságpolitikai Szemle,* 10. (2017), 3. 3–15.

Larsen, Allison O.: Constitutional Law in an Age of Alternative Facts. *New York University Law Review,* 93. (2018), 2. 175–248.

Lund, Jamie: Correcting Digital Speech. *UCLA Entertainment Law Review,* 19. (2012), 1. 170–188. Online: https://doi.org/10.5070/LR8191027152

Mania, Karolina: The Legal Implications and Remedies Concerning Revenge Porn and Fake Porn: A Common Law Perspective. *Sexuality & Culture,* 24. (2020), 6. 2079–2097. Online: https://doi.org/10.1007/s12119-020-09738-0

Marcum, Catherine D. – George E. Higgins – Tsung Martin Tsai – Jeffrey Sedlacek: Exploration of Prosecutor Experiences with Non-consensual Pornography. *Deviant Behavior,* 42. (2021), 5. 646–658. Online: https://doi.org/10.1080/01639625.2020.1821410

Matwyshyn, Andrea M.: Cyber Harder. *Boston University Journal of Science and Technology Law,* 24. (2018). 450.

McGuire, Michael: *Into the Web of Profit: Social Media Platforms and the Cybercrime Economy.* Cupertino (CA), Bromium, 2019.

Mchangama, Jacob – Natalie Alkiviadou: *The Digital Berlin Wall: How Germany (accidentally) Created a Prototype for Global Censorship – Act Two.* Justita, 2020. szeptember. Online: https://bit.ly/3uU52mO

Mezei Kitti: *A kiberbűnözés aktuális kihívásai a büntetőjogban.* Budapest, L'Harmattan – TK JTI, 2020.

Moses, Lyria B.: Recurring Dilemmas: The Law's Race to Keep Up with Technological Change. *University of Illinois Journal of Law, Technology & Policy,* (2007). 239–285.

Nagy Krisztina: Facebook files – gyűlöletbeszéd törölve? A közösségimédia-platformok tartalom-ellenőrzési tevékenységének alapjogi vonatkozásai. In Polyák Gábor (szerk.): *Algoritmusok, keresők, közösségi oldalak és a jog – A forgalomirányító szolgáltatások szabályozása. ProFutoro,* 8. (2020), 2. 115–136. Online: https://doi.org/10.26521/Profuturo/2018/2/4722

Nagy Zoltán András: *Bűncselekmények számítógépes környezetben.* Budapest, Ad Librum, 2009.

Nojeim, Gregory T.: Cybersecurity and Freedom on the Internet. *Journal of National Security Law & Policy,* 2010. augusztus 13. Online: https://jnslp.com/wp-content/uploads/2010/08/09_Nojeim.pdf

Parti Katalin: Harc az online illegális tartalom ellen. In *Kriminológiai tanulmányok 49.* Budapest, Országos Kriminológiai Intézet, 2012. Online: https://bit.ly/3AWGBZP

Parti Katalin – Kiss Tibor: Az informatikai bűnözés. In Borbíró Andrea – Gönczöl Katalin – Kerezsi Klára – Lévay Miklós (szerk.): *Kriminológia.* Budapest, Wolters Kluwer, 2017.

Pavlova, Pavlina: Human Rights-based Approach to Cybersecurity: Addressing the Security Risks of Targeted Groups. *Peace Human Rights Governance,* 4. (2020), 3. 391–418. Online: https://doi.org/10.14658/pupj-phrg-2020-3-4

Péterfalvi Attila – Eszteri Dániel: A személyes adatok büntetőjogi védelme Magyarországon és a Nemzeti Adatvédelmi és Információszabadság Hatóság kapcsolódó gyakorlata. In Görög Márta – Menyhárd Attila – Koltay András (szerk.): *A személyiség és védelme. Az Alaptörvény VI. cikkelyének érvényesülése a magyar jogrendszeren belül.* Budapest, ELTE-ÁJK, 2017.

Powell, Anastasia – Nicola Henry: *Sexual Violence in a Digital Age.* London, Palgrave Macmillan, 2017. Online: https://doi.org/10.1057/978-1-137-58047-4

Rubinstein, Ira S.: Voter Privacy in the Age of Big Data. *Wisconsin Law Review,* (2014), 5. 861–936. Online: https://doi.org/10.2139/ssrn.2447956

Sorbán Kinga: Vírusok és zombik a büntetőjogban. Az információs rendszer és adatok megsértésének büntető anyagi és eljárásjogi kérdései. *In Medias Res,* 7. (2018), 2. 369–386.

Sorbán Kinga: A bosszúpornó és a deepfake pornográfia büntetőjogi fenyegetettségének szükségességéről. *Belügyi Szemle,* 68. (2020), 10. 81–104. Online: https://doi.org/10.38146/BSZ.2020.10.4

Szathmáry Zoltán: *Bűnözés az információs társadalomban. Alkotmányos büntetőjogi dilemmák az információs társadalomban.* PhD-értekezés. Budapest, PTE ÁJK, 2012.

Szentgáli-Tóth Boldizsár: Vigyázó szemetek Párizsra vessétek – avagy pénzbírsággal, vagy anélkül a gyűlöletbeszéd ellen? *Jogi Fórum – Sajtó és Média Blog,* 2021. június 30. Online: https://bit.ly/3zctliq

The Right to Freedom of Expression and the Use of Encryption and Anonymity in Digital Communications. Submission to the United Nations Special Rapporteur on the Right to Freedom of Opinion and Expression by the Association for Progressive Communication (APC). Association for Progressive Communications (APC), 2015. Online: https://bit.ly/3Pe4rov

Török Bernát: A gyűlöletbeszéd tartalmának médiajogi mércéi. *Jogtudományi Közlöny,* 68. (2013), 2. 59–72.

Török Bernát: A szólásszabadság védelmének dinamikája. *Magyar Jog,* 64. (2017), 12. 721–733.

Török, Bernát: Platforms and Fundamental Rights: The Case of Social Media and Freedom of Speech. *Hungarian Conservative,* 1. (2021), 2. 42–47.

U.S. Department of Justice: *The National Information Infrastructure Protection Act of 1996.* Legislative Analysis, 1996.

Waldman, Ari E.: The Marketplace of Fake News. *Journal of Constitutional Law,* 20. (2018), 4. 101–105.

Wall, David S.: Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime. *International Review of Law, Computers and Technology,* 22. (2008), 1–2. 45–63. Online: https://doi.org/10.1080/13600860801924907

Whyte, Christopher: Deepfake News: AI-Enabled Disinformation as a Multi-Level Public Policy Challenge. *Journal of Cyber Policy,* 5. (2020), 2. 1–19. Online: https://doi.org/10.1080/23738871.2020.1797135