Sorbán Kinga

Hacktivizmus a demokráciában – bűncselekmény vagy politikai véleménynyilvánítás?

A hacktivizmus a „hackelés” és az „aktivizmus” szavak összevonásából keletkezett neologizmus, amelynek társadalmi megítélése napjainkban igen szélsőséges skálán mozog. Az elmúlt időszakról kifejezetten elmondható, hogy össztársadalmi szinten növekedett a hackerek támogatottsága, amihez több esemény együttese járult hozzá, köztük a radikális információszabadság iránti igény és az orosz–ukrán háború kibertérben megvalósuló cselekményei. Tanulmányom arra kíván választ adni, hogy a jogtudomány szempontjából nézve mi a hacktivizmus: a politikai véleménynyilvánítás egyik formája vagy elítélendő, pönalizálandó cselekmény? Ennek érdekében igyekszem csoportosítani azokat a magatartásokat, amelyek e körbe tartozhatnak, kitérve az online aktivizmus szerepére a politikai véleményformálásban és a kiberterrorizmus szerepére.

Bevezetés

Az internet lehetőségek garmadáját kínálja az emberek számára, hogy kifejezhessék véleményüket. A véleménynyilvánítás az online térben többnyire teljesen ártalmatlan, vannak azonban olyan megnyilvánulások, amelyek nemcsak a közösség morális alapon nyugvó ellenszenvét, hanem akár büntetőjogi szankciót vonhatnak maguk után. Ha a büntetőjog által szankcionált véleménynyilvánításokra gondolunk, akkor többnyire olyan deliktumok sejlenek fel előttünk, mint a gyűlöletbeszéd vagy a becsületsértés. Van azonban az online véleménynyilvánításnak egy olyan formája, amellyel idáig keveset foglalkozott a jogtudomány, az orosz–ukrán háború nyomán azonban – ahogy sok egyéb magatartás – előtérbe került. Ez a magatartás a *hacktivizmus,* amely a „hackelés” és az „aktivizmus” szavak összevonásából keletkezett neologizmus. Sokak szerint ez az első olyan háború, amelynek az egyik jelentős frontja a virtuális térben húzódik, nap mint nap hallunk híreket meghackelt orosz kémműholdakról,[1] vagy olyan oroszországi éttermekről, amelyek Google Maps-profilján az értékelők ukrán városokról készült fényképekkel igyekeznek felhívni a lakosok figyelmét az Ukrajnában zajló eseményekre.[2] Noha mindkét esetben a hacktivizmus kifejezést használjuk, érezzük, hogy egy másik állam tulajdonában

[1] Az Anonymous azt állítja, meghackelték az orosz kémműholdakat. *HVG.hu,* 2022. március 3.
[2] Takács Petra: A Google Mapsen több ezer „értékeléssel” figyelmeztetik az orosz népet. *Liner.hu,* 2022. március 4.

https://doi.org/10.36250/01164_16

lévő katonai műhold feltörése nem ugyanolyan súlyú magatartás, mint fényképeket közzétenni egy étterem internetes profilján.

Tanulmányom arra kíván választ adni, hogy a jogtudomány szempontjából nézve mi a hacktivizmus: a politikai véleménynyilvánítás egyik formája vagy elítélendő, pönalizálandó cselekmény? Ennek érdekében igyekszem csoportosítani azokat a magatartásokat, amelyek e körbe tartozhatnak, illetve kitérek az online aktivizmus szerepére a politikai véleményformálásban.

A hacktivizmus társadalmi megítélése és megjelenési formái

A hacktivizmus társadalmi megítélését nem annyira az e csoportba tartozó magatartások szabályozottsága befolyásolja, hanem inkább az állami intézményrendszerbe és a jogrendszerbe vetett állampolgári bizalom.[3] Giovanni A. Travaglino egyik tanulmányában kifejti, hogy azok az egyének, akik igazságtalannak tartják a rendszer működését, ám politikailag kevésbé hatékonyak, a dühüket gyakran úgy fejezik ki, hogy olyan személyeket vagy szervezeteket támogatnak, akiknek a magatartása megzavarja a rendszert.[4] Szemben a politikailag hatékony csoportok szereplőivel, akik közvetlenül és a fizikai térben nyilvánulnak meg – a szerző ilyennek tartja az Arab Tavasz vagy az Occupy Wall Street résztvevőit –, a politikailag nem hatékony egyének alternatív módját választják az ellenállásnak, például az olyan hackercsoportok, mint az Anonymous támogatását.[5]

Az elmúlt időszakról kifejezetten elmondható, hogy össztársadalmi szinten növekedett a hackerek támogatottsága, amihez több esemény együttese járult hozzá. Jessica L. Beyer a hacktivizmus erősödő támogatottsága egyik okaként a radikális információszabadság iránti igényt nevesíti.[6] Az olyan platformok, mint a kiszivárogtatott, gyakran érzékeny állami információkat közzétevő WikiLeaks, éppen azért váltak népszerűvé, mert az állami működés hagyományosan átláthatatlan, az információszabadság hagyományos értelmezésében elzárt területeire engedtek betekintést.

A hackerek támogatottsága növekedésének kedvezett az Oroszország és Ukrajna között kitört háború is, amihez nagyban hozzájárult Ukrajna háborús kommunikációja. Az ukrán digitális fejlesztési miniszter már a háború elején bejelentette, hogy önkéntes kiberhadsereget toboroznak, amelynek bárki a részese lehet, akár

[3] Leanna Ireland: We Are All (Not) Anonymous: Individual- and Country-Level Correlates of Support for and Opposition to Hacktivism. *New Media & Society,* (2022). 1.

[4] Giovanni A Travaglino: Support for Anonymous as Vicarious Dissent: Testing the Social Banditry Framework. *Group Processes & Intergroup Relations,* 22. (2019), 2. 163–181.

[5] Travaglino (2019): i. m.

[6] Jessica L. Beyer: The Emergence of a Freedom of Information Movement: Anonymous, WikiLeaks, the Pirate Party, and Iceland. *Journal of Computer-Mediated Communication,* 19. (2014), 2. 141–154.

hackerként, akár olyan „civilként", akinek a számítógépét a DDoS-támadásokban botként felhasználhatják.[7] A kezdeményezéshez sokan csatlakoztak, mivel úgy érezték, hogy ezzel is tudnak tenni valamit Ukrajna megsegítése érdekében.

A közvéleménnyel szemben biztonsági szakértők kimondottan óva intenek a hackercsoportok támogatásától, érveik között gyakran elhangzik, hogy a legtöbb ország büntetni rendeli a hacktivisták eszköztárába tartozó tevékenységeket.

Mivel a hacktivizmus kifejezést főleg a köznyelvben használjuk, vagyis nem egy egzakt jogtudományi fogalom, jogi megítélése nagyon sokféle lehet. Az alábbiakban a hacktivizmus legjellemzőbb megjelenési formáit csoportosítom, elsősorban három fogalom elhatárolásával. A hacktivizmustól el kell választanunk az ahhoz nagyon hasonlító, de megítélésükben sokszor erőteljesen különböző egyéb cselekményeket, az online aktivizmust, vagy más néven kiberaktivizmust, valamint a kiberterrorizmust. Az elhatárolás, mint látjuk, nem mindig mentes a nehézségektől, hiszen sokszor ezek a tevékenységek összeérnek, nem lehet élesen megkülönböztetni őket egymástól.

A kiberaktivizmus

2015. február 19-én az Európai Gazdasági és Szociális Bizottság (EGSZB) úgy határozott, hogy saját kezdeményezésű véleményt dolgoz ki a kiberaktivistákról és civil társadalmi szervezetekről. A kiberaktivizmust a dokumentum az aktivizmus egyik formájaként definiálja, mégpedig olyan formájaként, amely „ösztönzi a politikai, környezeti, társadalmi, állampolgári, kulturális stb. ügyek militáns felvállalását, és ehhez nincs szüksége meghatározott ideológiákban, hierarchiákban vagy programokban megtestesülő előzményekre, és amely olyan technológiai eszközöket használ, amelyek lehetővé teszik az információ gyors terjedését és a részvétel »járványszerű« bővülését".[8] A kiberaktivizmus, vagy más néven online aktivizmus kizárólag jogszerű, a véleménynyilvánítás normális rendjébe illeszkedő cselekményeket takar, amelyek az új technológiákat kommunikációs csatornaként alkalmazva törekszenek a közvélemény befolyásolására. A fentebb hivatkozott EGSZB-vélemény az online aktivizmus eszközei között elsősorban nem destruktív internetes eszközöket sorol fel, úgymint:

- információkeresés;
- információt és dokumentumokat kínáló webhelyek építése;
- elektronikus kiadványok közreadása;

[7] Matt Burgess: Ukraine's Volunteer 'IT Army' Is Hacking in Uncharted Territory. *Wired,* 2022. február 27.

[8] Európai Gazdasági és Szociális Bizottság: Az Európai Gazdasági és Szociális Bizottság véleménye – Kiberaktivisták és civil társadalmi szervezetek (saját kezdeményezésű vélemény). C 13/116 (2016. január 15.). 1.1.

– virtuális közösségek létesítése;
– vitafórumok létrehozása;
– közösségi akciók tervezése, hirdetése, cselekvések összehangolása.[9]

A kiberterrorizmus

A kiberterrorizmus fogalmának meghatározásakor az egyik nehézség, amellyel szembe kell néznünk, hogy mind a „kibertér", mint a „terrorizmus" fogalmának többféle meghatározása létezik. Jelen tanulmányban a kiberterrorizmuson azokat az információs rendszerek és hálózatok felhasználásával elkövetett erőszakos cselekményeket értem, amelyek valamely állam ellen irányulnak, és halálhoz, sérüléshez, vagyontárgy súlyos károsodásához vagy a társadalmi rend megzavarásához vezetnek. Tipikusan ilyennek minősülnek a kritikus infrastruktúrák, például erőművek elleni támadások. Dornfeld László a kiberbűnözés egyik fajtájaként tekint a kiberterrorizmusra, ugyanakkor elválasztja azt a kiberhadviseléstől.[10] Kifejti, hogy a kiberhadviselés hadtudományi fogalom, végrehajtói államok, kiberterrorizmust ellenben bármilyen államtól független szervezet elkövethet.[11]

A hacktivizmus

A hacktivizmus valahol a kiberaktivizmus és a kiberterrorizmus között helyezkedik el. A hacktivisták alapvető jellemzője, hogy a hackerek eszköztárát használják annak érdekében, hogy valamilyen társadalmi, politikai célt érjenek el. Gyakori motivációjuk az internetes szólás- és információszabadság biztosítása, valamint az internetes polgári engedetlenség. A hacktivista csoportok kommunikációit és kiáltványait megfigyelve látható, hogy e szerveződések üzeneteinek egyik kulcspontja a moralitás és az igazság keresése. Fehér Katalin rámutat, hogy ez a morál a jogi szabályozással gyakran szembemenő, olyan univerzális morál, amely globálisan is érvényesíthető.[12] Ennek az univerzális morálfelfogásnak köszönhető, hogy az egyes hacktivista csoportok működése nem korlátozódik egy-egy országon belülre, az igazságtalanság és a „hatalmasoknak" visszavágás narratíváján keresztül könnyedén megszólíthatók azok a támogatók is, akik az egyes konkrét ügyekben viszonylag kevésbé érdekeltek,

[9] Európai Gazdasági és Szociális Bizottság (2016): i. m. 3.4.
[10] Dornfeld László: Kiberterrorizmus – a jövő terrorizmusa? In Mezei Kitti (szerk.): *A bűnügyi tudományok és az informatika*. Pécs–Budapest, Pécsi Tudományegyetem Állam- és Jogtudományi Kar – MTA Társadalomtudományi Kutatóközpont, 2019. 18.
[11] Dorothy E. Denning: Activism, Hacktivism, and Cyberterrorism: The Internet As a Tool for Influencing Foreign Policy. In John Arquilla – David Ronfeldt (szerk.): *Networks and Netwars. The Future of Terror, Crime, and Militancy.* Santa Monica, RAND Corporation, 2001. 239–288.
[12] Fehér Katalin: *Digitalizáció és új média.* Budapest, Akadémiai Kiadó, 2017.

ám hajlandóak szolidaritást vállalni akár más országok polgáraival is. A kiberaktivizmustól elsősorban az különbözteti meg, hogy míg az előbbi legális eszközökre épít a figyelemfelhívás érdekében, a hacktivisták által alkalmazott megoldások a legtöbb jogrendszerben jogsértőnek, de legalábbis jogilag aggályosnak minősülnek. A hacktivizmus körébe tartozó magatartások ugyanakkor jellemzően nem eredményeznek súlyos kárt, vagyis a kiberterrorizmus súlyosságát nem érik el. Illig szerint a hacktivizmus művelői kifejezetten elkötelezettek az erőszakmentesség mellett,[13] tevékenységükben tehát sokkal inkább a figyelemfelhívás dominál, köszönhetően annak, hogy akcióik általában nagy médiafigyelmet kapnak. Denning úgy látja, hogy a hacktivizmus leggyakoribb megjelenési formái az alábbiak:

- virtuális tüntetések *(virtual sit-in);*
- weboldalak megrongálása *(defacing);*
- weboldalak tükrözése *(website mirroring);*
- érzékeny, jogosulatlanul megszerzett információk nyilvánosságra hozatala *(doxing);*
- DDoS támadások;
- spamek.

Virtuális tüntetések esetében több ezer hacktivista látogat meg egy weboldalt, olyan forgalmat generálva, amelyet nem tud kezelni a rendszer, és összeomlik. Legelőször 1995-ben került rá sor, amikor a magát Strano Networknek nevező csoport úgy demonstrált a francia kormányzat nukleáris politikája ellen, hogy támogatóikat arra kérték, hogy egy meghatározott egyórás időtartamban keressenek fel francia kormányzati weboldalakat.[14]

A weboldalak megrongálása *(defacing)* során az oldal valamely sérülékenységét kihasználva a hacktivisták hozzáférnek annak forráskódjához, és különböző változtatásokat eszközölnek az eredeti portálon. Weboldalrongálásra hazai példa is van, az Anonymous hackercsoport magyarországi csoportja 2012-ben átírta az Alkotmánybíróság honlapján az Alaptörvény szövegét.[15] A weboldalak tükrözése szintén az eredeti oldal valamely sérülékenységének kihasználásával történik, ahelyett azonban, hogy az oldalt megváltoztatnák, a domaint átirányítják egy másik címre, amely gyakran az eredeti oldal módosított változata.

A *doxing* motivációja jellemzően az, hogy a hacktivisták az állami működés átláthatatlan rétegeibe engedjenek bepillantást. A kiszivárogtatott információk érinthetnek egy-egy társadalmilag érzékeny témakört vagy konkrét személyeket, de célja lehet általánosságban a minősített adatok körébe tartozó információk közzététele is.

[13] Andrew T. Illig: Computer Age Protesting: Why Hacktivism is a Viable Option for Modern Social Activists. *Dickinson Law Review,* 119. (2015), 4. 1035–1036.

[14] Denning (2001): i. m. 264.

[15] Az Anonymous átírta az alaptörvényt. *Index,* 2012. március 4.

Hiába az a célja ezeknek a magatartásoknak, hogy közérdekű ügyekkel kapcsolatos véleményt fejezzenek ki, radikális módszereik olyan érdekeket sértenek, amelyek miatt a demokratikus társadalmakban korlátozás alá vonhatók. Az Emberi jogok európai egyezményének 10. cikke a szólásszabadság legitim korlátai között említi a nemzetbiztonságot, a közbiztonságot, a bűnüldözési érdeket, valamint az egyének jogainak sérelmét; egy-egy információs rendszerbe való jogszerűtlen belépés és az abban végrehajtott adatmanipuláció, még ha csak figyelemfelkeltésre irányul is, egészen biztosan kockázatot jelent ezek valamelyikére. A hacktivizmussal azonosított magatartásokra a magyar büntetőtörvény, a Büntető Törvénykönyvről szóló 2012. évi C. törvény (Btk.) rendelkezései egytől egyig kiterjednek. A következőkben a magyar büntetőjogi rendelkezéseket mutatom be, amelyek az információs rendszer és adatok elleni bűncselekményeket szabályozzák.

Információs rendszer és adatok elleni bűncselekmények a magyar büntetőjogban

A Btk. XLIII. fejezete szól a tiltott adatszerzésről, valamint az információs rendszer elleni bűncselekményekről, így az információs rendszer vagy adat megsértéséről, valamint az információs rendszer védelmét biztosító technikai intézkedés kijátszásáról. E rendelkezések 2004 óta képezik a magyar jog részét – Magyarország ekkor ratifikálta az Európa Tanács 2001. november 23-án Budapesten elfogadott, a számítástechnikai bűnözésről szóló egyezményét,[16] aminek alapján kötelezettséget vállalt arra, hogy megalkotja a megfelelő jogszabályokat az egyezményben meghatározott cselekmények kriminalizálása érdekében. A Btk. e szabályainak beiktatásával a magyar jogalkotó az uniós aktusok átültetésére vonatkozó kötelezettségének is eleget tett.

Az Európai Parlament és a Tanács 2013/40/EU irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról lényegében a Cybercrime-egyezménnyel azonos szabályokat fektet le. Az irányelv, sok egyéb európai uniós normához hasonlóan, a *minimumharmonizáció* elvét követi, vagyis a tagállamok annak szabályainál részletesebb, illetve szigorúbb szabályokat szabadon megállapíthatnak.

Az információs rendszer vagy adat megsértése tényállásáról a Btk. 423. §-a rendelkezik. Az e szakasz által kriminalizált elkövetési magatartások köznyelvi elnevezése általában sokkal beszédesebb – ezek a bekezdések szabályozzák a hackelést, a kártékony szoftverek, például vírusok terjesztését, a botnethálózatok kiépítését és a túlterheléses támadásokat.

[16] Az egyezményt Magyarországon az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről szóló 2004. évi LXXIX. törvény hirdette ki.

423. § (1) Aki információs rendszerbe az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve vagy azt megsértve bent marad, vétség miatt két évig terjedő szabadságvesztéssel büntetendő.

(2) Aki

a) az információs rendszer működését jogosulatlanul vagy jogosultsága kereteit megsértve akadályozza, vagy

b) információs rendszerben lévő adatot jogosulatlanul vagy jogosultsága kereteit megsértve megváltoztat, töröl vagy hozzáférhetetlenné tesz,

bűntett miatt három évig terjedő szabadságvesztéssel büntetendő.

(3) A büntetés bűntett miatt egy évtől öt évig terjedő szabadságvesztés, ha a (2) bekezdésben meghatározott bűncselekmény jelentős számú információs rendszert érint.

(4) A büntetés két évtől nyolc évig terjedő szabadságvesztés, ha a bűncselekményt közérdekű üzem ellen követik el.

(5) E § alkalmazásában adat: információs rendszerben tárolt, kezelt, feldolgozott vagy továbbított tények, információk vagy fogalmak minden olyan formában való megjelenése, amely információs rendszer általi feldolgozásra alkalmas, ideértve azon programot is, amely valamely funkciónak az információs rendszer által való végrehajtását biztosítja.

A Btk. 423. §-a által szabályozott tényállás valójában háromféle elkövetési magatartással is megvalósítható, ezek:

- az információs rendszerbe történő jogosulatlan belépés [(1) bekezdés];
- a rendszer működésének akadályozása [(2) bekezdés a) pontja]; valamint
- az információs rendszerben tárolt adatokkal végzett jogosulatlan műveletek [(2) bekezdés b) pontja].

E bekezdés szövegén látszik, hogy a technológiasemlegesség jegyében fogalmazták meg, így az alkalmazott technológiától és az elkövetés módszerétől függetlenül büntetendő minden olyan magatartás, amely a meghatározott eredményre vezet.

A 9/2012. számú büntető elvi döntés szerint „a védett jogi tárgy a számítástechnikai rendszerek működéséhez, a bennük tárolt, feldolgozott, továbbított adatok megbízhatóságához, valamint titokban maradásához fűződő érdek, és nem magának a számítógépnek vagy gépeknek a mechanikus védelme, erre ugyanis a rongálás törvényi tényállása nyújt büntetőjogi védelmet". A védett jogi tárgy jogosulatlan belépés és az információs rendszer működésének akadályozása esetén az elektronikus adatfeldolgozó és adatátviteli rendszer integritása, biztonsága, míg az adatokkal való visszaélés esetében az adatok által megtestesített érték, érdek. A bűncselekmény elkövetési tárgya az információs rendszer, amelynek fogalmát a Btk. 459. szakasz (1) bekezdésének 15. pontja pontosan meghatározza. Eszerint „információs rendszer:

az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezés, vagy az egymással kapcsolatban lévő ilyen berendezések összessége".

„Az információs rendszer fogalma nemcsak az egyes berendezésekre terjed ki, hanem felöleli az azok összekapcsolása révén létrejött hálózatot, valamint az adattovábbítást, a kapcsolatfelvételt biztosító műszaki berendezéseket is. A berendezések közötti kapcsolat nem jelent feltétlenül fizikai összekapcsoltságot. Az információs rendszerek közötti összeköttetés létrejöhet elektronikus vagy optikai jeleket továbbító kábelek, vagy vezetékek útján, valamint rádióhullámok, infravörös, illetőleg rövidhullámok segítségével, vagy műholdas sugárzás igénybevételével is."[17]

Jogosulatlan belépés, bent maradás és a belépési jogosultság túllépése vagy kijátszása

Az I. alapeset, amely az (1) bekezdésben jelenik meg, a valamely hálózatba vagy számítógépbe történő jogosulatlan belépés, illetve jogosulatlan bent maradás. Nagy Zoltán András részletesen foglalkozik azzal, hogy mikor jogellenes a hálózatba való belépés vagy bent maradás.[18]

Ha a számítógépbe az elkövető nem jogosult belépni, és a számítógép olyan biztonsági mechanizmusokkal védett, amelyek csak meghatározott személyek számára engedélyeznek belépést, valamint ezek a mechanizmusok aktiválva is vannak az elkövetés idején, a belépés vagy bent maradás jogellenes. Jogosultság nélkül lép be a felhasználó abban az esetben is, ha nem a számára engedélyezett belépési ponton lép be (például a munkahelye helyett az otthonában), a számítógép vagy hálózat biztonsági rendszere megoldásait kihasználva lép be, illetőleg más felhasználó nevével, jelszavával lép be. A magatartás csak abban az esetben tényállásszerű, ha arra az információs rendszer védelmét szolgáló intézkedések megsértésével, kijátszásával kerül sor. A jogszabály nem követeli meg, hogy a védelmet megvalósító biztonsági intézkedések műszaki-technikai jellegűek legyenek, azok elvileg lehetnek testi, személyi jellegűek is, ez esetben, ha az elkövető az előbbi adatokat erőszak vagy fenyegetés alkalmazásával szerzi meg, más bűncselekmény (kényszerítés, zsarolás) is megvalósulhat. A belépéshez szükséges adatok megszerzésének egyik elterjedt módszere, ahogyan arra Mezei Kitti is rámutat, a pszichológiai manipuláció, az úgynevezett *social engineering*.[19]

[17] Görgényi Ilona et al.: *Magyar büntetőjog különös rész.* Budapest, Wolters Kluwer, 2020. XLIII. fejezet. Tiltott adatszerzés és az információs rendszer elleni bűncselekmények.

[18] Nagy Zoltán András: A számítógépes bűnözés története. In Dobák Imre – Hautzinger Zoltán (szerk.): *Szakmaiság, szerénység, szorgalom. Ünnepi kötet a 65 éves Boda József tiszteletére.* Budapest, Dialóg Campus Kiadó, 2018. 473–474.

[19] Mezei Kitti: A jogosulatlan belépés, avagy a hacking szabályozása a büntetőjogban. *Rendőrségi Tanulmányok,* 3. (2020), 2. 32.

A jogosulatlan belépést valósítja meg a hackerek tevékenysége is, akik informatikai ismeretek, módszerek segítségével lépnek be különféle rendszerekbe. Az összes ilyen módszert nyilvánvalóan célszerűtlen lenne felsorolni, az információs rendszerek sokfélesége és összetettsége miatt pedig vélhetően lehetetlen volna mindenre teljes körű listát állítani, ezért az alábbiakban csak néhány fontosabb módszert emelünk ki. Népszerű módszerek a puffertúlterhelés *(buffer overflow)* vagy a „nyers erő" *(brute force)* módszer. Előbbi „alapját programozási hiányosságok képezik, konkrétan a bevitt adatokat tároló pufferek mérete nem megfelelően meghatározott. Ha nincs rendesen kezelve az adatbevitel, a támadó túlírhatja a puffert, és a program adatterületén továbbírva a program visszatérési értékét egy tetszőleges helyre irányíthatja. Jellemzően olyanra, mely részére rendszergazdai jogosultságaival való élést tesz lehetővé, amennyiben a támadott program is ilyen jogokkal futott."[20] A *brute force* módszer működésének lényege, hogy a rejtjelező rendszer ismeretében az összes lehetséges kulcsot kipróbálva határozza meg az alkalmazott jelszót, adatot. Mezei Kitti említést tesz az alap felhasználói műveletekkel, illetve a rendszergazdáéhoz hasonló jogosultságokkal rendelkező „*root level* access" vagy „*god level* access" hozzáférésekről is.[21] Az információs rendszer feletti irányítás megszerzése gyakran úgy történik, hogy az elkövető rosszindulatú szoftvert juttat a célzott számítógépes rendszerbe, ezek azonban már olyan módszerek, amelyek a számítógép működését is akadályozzák, így a következő alapesetnek megfelelően ítélendőek meg. A jogosulatlan belépés után végzett további műveletek esetében általánosságban elmondható, hogy ezek már a következő bekezdés valamelyik fordulatát valósítják meg.

Kritikája lehet a jogosulatlan belépést szabályozó szakasznak, hogy gyakorlatilag egy olyan cselekedetet rendel büntetni, amelynek társadalomra veszélyessége sok esetben igen csekélynek mondható. Főképp a fiatalok körében figyelhető meg az a tendencia, hogy azért törnek be rendszerekbe, hogy megmutassák, ők képesek rá, vagyis vannak annyira képzettek technikailag, hogy ki tudják játszani a rendszert védő mechanizmusokat mindenféle ártó szándék nélkül.

Itt kell szólni azokról az esetekről is, amikor a rendszerbe való belépés nem károkozásra irányul, de még csak nem is öncélú fitogtatása az informatikai ismereteknek, hanem valójában segítségnyújtási céllal történik. Az úgynevezett etikus hacking olyan tevékenység, amelynek során a hacker azért tör be bizonyos rendszerekbe, hogy azok sebezhető pontjait feltárja, az információkat pedig megossza a rendszer üzemeltetőjével a hibák kijavítása és a komolyabb, rosszindulatú támadások megelőzése végett. Az etikus hackerek gyakran egy-egy cég alkalmazottjaiként működnek, ez esetben a büntetőjogi felelősségük értelemszerűen fel sem merül, más esetekben azonban kívülállóként avatkoznak be a rendszer

[20] Varga Balázs: Informatikai bűncselekmények. *Jogi Fórum,* 2003. december 19. 36.
[21] Mezei Kitti (2020): i. m. 24.

működésébe, ezt Szathmáry Zoltán kéretlen sérülékenységvizsgálatnak nevezi.[22] Noha e cselekmény önmagában véve tényállásszerűnek minősül, a társadalomra veszélyesség gyakorta hiányzik, sőt a sérülékenységek feltárása inkább a társadalom hasznára válik, amennyiben komolyabb károsodástól óvja meg az érintett cégeket és azok ügyfeleit. Mivel vékony a határmezsgye a bűncselekmény és a jó szándékú, de kéretlen sérülékenységvizsgálat között, a jelenség semmiképpen nem maradhat szabályozási anomáliaként, a jelenlegi Btk.-beli szabályozás azonban túl szigorú, és nem feltétlenül szolgál társadalmi érdeket. A rosszindulatú hackerek számára szolgálhat a kódex e passzusa elrettentésül, azonban a fiatal informatikusok jövőjének derékba törése már nyilvánvalóan túlmutat a jogalkotó eredeti szándékán. Meglátásom szerint a probléma kezelhető jogalkotás révén, valamint a joggyakorlat finomhangolásával is a már létező jogszabályi kereteken belül. A bírói gyakorlat azzal tudná elősegíteni a helyzet megoldását, ha a bűncselekmény tárgyi oldali elemeinek megvalósulásán túl nagy hangsúlyt helyezne a motívumra és a célzatra, továbbá ha azonos elbánásban részesítené az azonos tőről fakadó cselekményeket. Figyelemre méltó Ambrus István meglátása is, aki a panaszokról és a közérdekű bejelentésekről szóló 2013. évi CLXV. törvényre hivatkozva közérdekű bejelentésként kategorizálja az egyes, kéretlen sérülékenységvizsgálattal összefüggő magatartásokat.[23] Álláspontja szerint az etikus hackerek bejelentése a feltárt problémáról a társadalom érdekét szolgáló, jogellenességet kizáró közérdekű bejelentésnek minősülhet. E minősítésnek azonban meg kell felelnie azoknak a feltételeknek, amelyek kimunkálása jelenleg is a joggyakorlatra vár, így például a hackerrel szembeni követelmény, hogy dokumentálja a cselekménye egyes lépéseit, haladéktalanul jelezze a feltárt sérülékenységet, és tevékenysége ne irányuljon haszonszerzésre.

A másik lehetőség az etikus hackerek tevékenységével kapcsolatos feszültségek feloldására a szabályozási út, vagyis az etikus hackerek tevékenységének *expressis verbis* dekriminalizálása. Mivel a kibertérben számtalan jogellenes belépés fordul elő, én a szabályozási választ tartom követendőnek, amely a joggyakorlat számára vezérfonalként szolgálva egységesen meghatározhatja a büntetőjogi felelősségre vonás alóli mentesülés szükséges feltételrendszerét is.

Belépési jogosultsága kereteinek túllépésével, illetőleg annak megsértésével marad benn az elkövető, ha van ugyan valamilyen szintű jogosultsága a rendszer használatára, azonban e jogosultságát meghaladó műveleteket folytat, vagy a számára engedélyezett idő lejártával nem lép ki a rendszerből. A bűncselekmény befejezett, amint a tettes az első hozzáférési korlátot átlépte, és számára az adatok vagy az adatfeldolgozó rendszer további lépései nyitva állnak.[24] A Kúria az egyik

[22] Szathmáry Zoltán: Etikus és nem etikus hacking – a kéretlen sérülékenységvizsgálat büntetőjogi kérdései. *Magyar Jog,* 67. (2020), 6. 340–346.

[23] Ambrus István: *Digitalizáció és büntetőjog.* Budapest, Wolters Kluwer, 2021. 87.

[24] Gelányi Anikó – Csepely-Knorr Tamás: A jogosulatlan wifi használat minősítése, avagy ha nyitva van az ajtó, akkor bemehetek? *Infokommunikáció és Jog,* 6. (2009), 34. 201–207.

ítéletében felhívta a figyelmet arra, hogy ahhoz, hogy a jogosultság keretein való túllépés bűncselekménynek minősüljön, szintén szükséges a rendszer védelmét biztosító technikai intézkedés megsértése vagy kijátszása, önmagában a jogosultság kereteinek túllépése „nem éri el azt a veszélyességi szintet, mint amit az első fordulat megkíván" (BH2017. 392.).

Az információs rendszer működésének akadályozása

Az információs rendszer működésének megzavarása történhet akár hardvereszközök (például különböző jelzavarók), akár szoftvereszközök révén.

Az információs rendszer rendeltetésszerű működésének akadályozására a modern technológia állása szerint különösen alkalmasak a különféle kártékony programok, ezért a 423. §-ban szabályozott cselekmény két legtipikusabb elkövetési magatartása a *malware*-, illetve a botnettámadás. Az 1978. évi Btk.[25] *Kommentár*ja a számítástechnikai rendszer megsértésének egyik eszközeként a számítógépes vírusokat említi.[26] A számítógépes vírus azonban csak egyike azoknak a kártékony programoknak *(malware),* amelyek alkalmasak a számítógép működésének kedvezőtlen befolyásolására. A kártékony programok közös jellemzője, hogy olyan szoftverek, amelyek akadályozzák a számítógép működését, illetve korlátozzák a rendeltetésszerű használatát. A legismertebb *malware*-fajták az alábbiak:[27]

- Vírus *(virus):* vírusnak nevezzük azokat a szoftvereket, amelyek képesek a felhasználó tudta nélkül egyik számítógépről a másikra, vagy akár ugyanazon a gépen belül több helyre észrevétlenül reprodukálódni. Általában fertőzött program segítségével terjednek. A programvírusok *(file-infector virus)* bináris futtatható (például exe) fájlokba ágyazódnak. Gyakran találhozhatunk mostanában az úgynevezett zsarolóvírusokkal *(ransomware),* amelyek a rendszert megfertőzve állományokat titkosítanak, és csak akkor adják meg a feloldáshoz szükséges kódot, ha a felhasználó egy megadott számlaszámra váltságdíjat utalt. A zsarolóvírusok egyre gyakrabban jelennek meg Magyarországon is, ahol magánszemélyek mellett főként cégek, illetve kritikus infrastruktúrák (például kórházi rendszerek) válnak áldozatul. Adatfájlokban lévő vírusok például a makrovírusok, valamint az érvénytelen fájlformátumot kihasználó vírusok.
- Féreg *(worm):* a féreg olyan önmagában működő szoftver, amely képes önmagát reprodukálva egyik számítógépről a másikra terjedni. Abban

[25] 1978. évi IV. törvény a Büntető Törvénykönyvről.

[26] Varga Zoltán (szerk.): *Nagykommentár a Büntető törvénykönyvről szóló 1978. évi IV. törvényhez.* Budapest, KJK-Kerszöv, 2004.

[27] A csoportosítás és a fogalommagyarázat a https://nki.gov.hu/it-biztonsag/kiadvanyok/szorolapok/ felhasználásával készült.

különbözik a vírustól, hogy önmagában is működik és életképes, nem kapcsolódik egyéb szoftverekhez. Az önsokszorosításon kívül a féreg számtalan dologra programozható – ezeknek a másodlagos funkcióknak a neve *payload*.
- Trójai faló *(trojan horse):* trójai szoftvereknek nevezzük azokat a kártékony szoftvereket, amelyek magukat általában ártalmatlan vagy segítő célú szoftvernek álcázva települnek fel a számítógépre. Hasonlóan a számítógépes férgekhez, a rendszerbe kerülésüket követően számtalan dologra programozhatók, például a számítógépen található állományok titkosítására, zombiszámítógép létrehozására, személyes adatok összegyűjtésére és elküldésére, a felhasználó webkamerájának használatára, az operációs rendszer távoli használatára stb.
- *Rootkit:* olyan szoftvereszközök, amelyek elrejtenek egyes folyamatokat vagy adatokat az operációs rendszerben, vagy hozzáférést tesznek lehetővé bizonyos alrendszerekhez vagy programokhoz.
- Hátsó ajtó *(backdoor):* olyan program, amely a felhasználó tudta nélkül távoli hozzáférést tesz lehetővé. Ezek a programok általában egy előre meghatározott TCP- vagy UDP-portot nyitnak, amelyre az elkövető rácsatlakozhat.
- Kémprogram *(spyware):* célja a számítógépről információ megszerzése. Lehet webalapú, mint egy káros weboldal, települhet is webről, de megeshet, hogy maga az ártani kívánó fél telepíti fel a gépre (például billentyűleütés-naplózó program *[keylogger],* amely megjegyzi az összes leütött billentyűt).
- Kéretlen reklám *(adware):* olyan szoftver, amely automatikusan reklámokat jelenít meg.

Az előbbiekben felsorolt kártékony programok általában nem egymástól elhatárolhatóan működnek, az előbbi kategóriák a mai környezetben inkább az egyes programfunkciók leírására szolgálnak. Egy-egy kártevő több funkció ellátására is programozható, így valójában a modern *malware*-ek a fentiek valamilyen csomagba szerkesztett változatát jelentik. Kártékony szoftverek egyre gyakrabban jelennek meg Magyarországon is, az Országos Bírósági Hivatal adatbázisában rendelkezésre álló nyilvános információk azonban arra engednek következtetni, hogy ezek terjesztőivel szemben jogerős ítéletek ritkán születnek. Ennek hátterében számos ok állhat, részben az, hogy az elkövetők felett nem Magyarország rendelkezik joghatósággal, az eljárások bonyolultak és elhúzódnak, valamint az is, hogy kevés sértett tesz feljelentést, tartva az üzleti jó hírnevük csorbulásától. A 2017-ben futótűzként elterjedt WannaCry zsarolóvírus miatt az ORFK tájékoztatása szerint csak ketten tettek feljelentést.[28]

A hacktivisták eszköztárában kiemelt helyen szerepelnek az úgynevezett botnethálózatok, amelyeken keresztül a hackerek összehangolt támadásokat tudnak indítani különböző célpontok ellen. A botnet a *robot* és a *network* szavak

[28] ORFK: ketten tettek feljelentést a WannaCry vírus támadása miatt. *HVG,* 2017. június 16.

összekapcsolásából ered, és vírussal fertőzött számítógépek hálózatára utal, amelyeket az elkövető(k) távolról küldött utasítások sorozatán keresztül képes(ek) irányítani, ezáltal tömegesen felhasználni bűncselekmények elkövetéséhez. A botnet kifejezést európai uniós dokumentumban először 2006-ban említik. A spamekről szóló közleményében az Európai Bizottság a kéretlen üzenetek küldésére szolgáló eszközként jellemezte a botnethálózatokat. A 2007 májusában kiadott, a kiberbűncselekmények elleni fellépés általános megközelítéséről szóló közlemény már jóval nagyobb szerepet tulajdonított a botneteknek, és ezeket az infrastruktúrákat tette felelőssé az olyan átfogó, információs rendszerek elleni támadásokért, mint amilyen az észtországi kritikus infrastruktúrák elleni támadás volt 2007-ben.[29]

Az információs rendszerek elleni támadásokról szóló irányelv kiemelten foglalkozott a botnethálózatok elleni fellépés kérdésével.[30] Ez az uniós norma már a célját is abban határozza meg, hogy „[büntetőjogi] szankciókat állapítson meg a botnetek létrehozására, vagyis azon cselekményre vonatkozóan, amellyel célzott informatikai támadások révén jelentős számú számítógép felett veszik át a távvezérelt irányítást oly módon, hogy rosszindulatú számítástechnikai programokkal fertőzik meg őket".[31] Az irányelv arról is rendelkezik, hogy az olyan támadások esetében, amelyek célja botnet létrehozása, vagy amelyeket botnet révén hajtanak végre, a tagállamok megállapíthatnak súlyosabb szankciót.[32] Ezt a szabályt a Btk. akképp ültette át, hogy az információs rendszer vagy adat megsértése bűntettének minősített esete valósul meg, ha a cselekmény jelentős számú információs rendszert érint.[33] A botnet számos funkciót elláthat, Nagy Zoltán és Mezei Kitti a következő botnetfunkciókat különbözteti meg: DDoS-támadások indítása, spamküldés, adathalászat, hálózatfigyelés, billentyűzetfigyelés, internetes reklámokhoz kapcsolódóan klikkelések begyűjtése.[34] Újabban a botnethálózatokat gyakran használják kriptovaluták (például bitcoin) bányászására.

[29] Hancu [Hanula Zsolt]: Az oroszok visszabombázzák Észtországot az online kőkorszakba. *Index,* 2007. május 31.

[30] Az Európai Parlament és a Tanács 2013/40/EU irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról. L 218/8 (2013. augusztus 4.).

[31] Az Európai Parlament és a Tanács 2013/40/EU irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról. L 218/8 (2013. augusztus 4.). (1) preambulumbekezdés.

[32] Az Európai Parlament és a Tanács 2013/40/EU irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról. L 218/8 (2013. augusztus 4.). (13) preambulumbekezdés.

[33] Btk. 423. § (3) bekezdés.

[34] Nagy Zoltán András – Mezei Kitti: A zsarolóvírus és a botnet vírus mint napjaink két legveszélyesebb számítógépes vírusa. In Gaál Gyula – Hautzinger Zoltán (szerk.): *Szent Lászlótól a modernkori magyar rendészettudományig.* Pécs, Magyar Hadtudományi Társaság, Határőr Szakosztály, Pécsi Szakcsoport, 2017. 163–168.

A botnethálózatok funkciói közül talán az egyik leghírhedtebb a túlterheléses támadás *(denial of service attack – DOS).* A túlterheléses támadások esetében az elkövető azzal akadályozza a rendszer működését, hogy olyan adatmennyiséget zúdít a célrendszerre, amelyet az képtelen kezelni. A túlterheléses támadások manapság leggyakrabban úgynevezett elosztott túlterheléses támadással *(distributed denial of service attack – DDoS)* történnek, ami annyit jelent, hogy a megfertőzött zombiszámítógépek a megcélzott szervereknek folyamatosan kéréseket – adatcsomagokat – küldenek, és ha több ezer csomag érkezik egyszerre, a forgalmazás mértékét a támadott rendszer nem bírja el, és ez a rendszer teljes összeomlását eredményezheti. Ugyanakkor az információs rendszer működésének akadályozásához nem feltétel a célrendszer teljes megbénulása, ahogy Nagy és Mezei is kiemelik: a „funkcionális működésképtelenséghez elegendő a nagymértékű lelassulás is, ami a válaszidő megnövekedett mértékéből adódik".[35] A cselekmény különösen súlyos lehet, hiszen a Btk. szerint a cselekmény minősített esetét követi el, aki a 423. §-ban szabályozott magatartásokat közérdekű üzem ellen követi el. Mivel bizonyos infrastruktúrák megbénításának a hátterében gazdasági érdek, de akár politikai figyelemfelhívás is állhat, a szervezett bűnözői körök ma már gazdasági szolgáltatásként kínálják a DDoS-támadások lefolytatását, illetve az ilyen támadások lefolytatásához használható infrastruktúra bérbeadását. Mezei Kitti tanulmányában kifejti, hogy napjainkban „napi vagy havi díjjal átlagosan 5 $ és 1000 $ közötti áron lehet szert tenni hasonló eszközökre".[36]

Az elosztott túlterheléses támadások esetében érdemes röviden foglalkozni a tettesség kérdésével. Témánk szempontjából különösen fontos, kit tekinthetünk tettesnek, hiszen a hacktivistákat támogató egyének gyakran maguk telepítik fel a számítógépeikre azokat a programokat, amelyekkel hackercsoportok kezébe adják annak irányítását. A Btk. *Kommentár*ja alapján a Btk. 423. § (2) bekezdése szerinti cselekmények elkövetője bárki lehet, azonban azok csak szándékosan valósíthatók meg.[37] A botnetek esetében a támadásban zombiként, távoli vezérléssel részt vevő rendszerek tulajdonosainak sokszor nincs arról tudomásuk, hogy a gépük vírusfertőzés áldozata, a támadással érintett információs rendszer tekintetében az akadályozási szándék esetükben tehát egyértelműen kizárható. A szándék általában a mestergép tulajdonosa, a *botherder* oldalán jelenik meg, az ő cselekménye szándékos és egyben célzatos. Az elkövető ebben az esetben nemcsak a túlterheléses támadással célzott információs rendszer működését akadályozza, hanem az összes olyan információs rendszer működését is, amelyet megfertőzött és távoli hozzáféréssel támadásra utasított. A hacktivistákat saját erőforrásaival támogató önkéntesek ellenben

[35] Nagy–Mezei (2017): i. m. 164.

[36] Mezei Kitti: A DDoS-támadások büntetőjogi szabályozása az Egyesült Államokban, Európában és Magyarországon. *Pro Futuro,* 8. (2018), 1. 70.

[37] Karsai Krisztina (szerk.): *Kommentár a Büntető Törvénykönyvről szóló 2012. évi C. törvényhez.* Budapest, Wolters Kluwer, 2017.

maguk is lehetnek tettesek, amennyiben tudatuk átfogta azt, hogy számítógépüket DDoS-támadások elkövetésére használták fel, és ehhez kifejezetten hozzájárultak.

Az információs rendszerben tárolt adatok jogosulatlan megváltoztatása és törlése

A 423. § (2) bekezdésének b) pontjában található az elkövetési magatartások II. köre, amely elektronikus adatok bevitelét, megváltoztatását, törlését és hozzáférhetetlenné tételét rendeli büntetni. Elkövető ebben az esetben bárki lehet, még az is, aki a rendszerbe jogosultan lép be, ám a fent megnevezett műveleteket már jogosulatlanul végzi. A tényállás szövegében a jogosulatlan jelző az eredményre utal, így elkövetheti a bűncselekményt az is, aki egyébként jogosult a rendszerbe belépni, ott az adatokon műveleteket végrehajtani, jogosultsága azonban nem terjed ki a rendszer működésének akadályozására. Adat törlése kapcsán az elkövető tudattartalma lényeges, megvalósul ugyanis a törlés akkor is, ha az adatokat csak különleges szakértelemmel lehet visszaállítani. A törlés megvalósulhat a törlés funkcióval vagy a mágnesszalagok elektromágneses úton való törlésével, hozzáférhetetlenné tételen pedig az adatok elrejtését értjük például egy olyan fájlban, amely jelszóval védett, vagy kódolt, de idetartozik az adathordozó elrejtése is.

A cselekmény az adatok megváltoztatásán túl megvalósítható új, valótlan adatok rögzítésével is. Ezekben az esetekben az adatbevitel más bűncselekményt is megvalósíthat (például sikkasztás), de az is előfordulhat, hogy az elkövető az adatbevitelt vagy -módosítást más jogellenes cselekmény leplezésére használja fel.

A doxing vagy az információ kiszivárogtatása a magyar büntetőjogban

A magyar büntetőjog rendszerében más szabályok vonatkoznak a személyes adatokkal való visszaélésre, valamint a minősített adatokra.

A visszaélés a személyes adatokkal a Btk. 219. §-ában szabályozott deliktum. A Btk. keretjogszabály, amelyet tartalommal a 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.) és a GDPR[38] töltenek ki. A bűncselekmény jogi tárgya a személyes adat megismeréséhez és biztonságos kezeléséhez, őrzéséhez való jog. A személyes adat lehet az egyénnel összefüggésbe hozható bármely információ. A GDPR 4. cikk 1. pontja példálózó jelleggel fel is sorolja a legjellemzőbb személyes adatokat, amelyek: „név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai,

[38] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet). L 119/1 (2016. május 4.).

genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó ismeret".[39] A Btk. személyes adattal való visszaélést büntetni rendelő szakaszában általános alanyt használ a törvényhozó, vagyis az elkövető – szemben a magántitok megsértésével – bárki lehet. A törvény négyféle elkövetési magatartást szabályoz. Az első két alapeset szerint megvalósítható a bűncselekmény jogosulatlan vagy céltól eltérő adatkezeléssel. Adatkezelésnek minősül az adatokon végzett bármilyen művelet, vagy a műveletek összessége, például gyűjtése, törlése, megváltoztatása, nyilvánosságra hozatala. Jogosulatlannak minősül az az adatkezelés, amely a GDPR 6. cikk (1), illetve az Infotv. 5. § (1) bekezdéseiben felsorolt jogalapok hiányában történik. Jogosulatlan az adatkezelés például akkor, ha ahhoz az érintett nem járult hozzá, vagy azt nem jogszabály rendelte el. A céltól eltérő adatkezelés akkor is tényállásszerű, ha az adatkezelésre egyébként megfelelő jogalappal került sor, mivel a célhozkötöttség olyan általános elv, amelynek az adatkezelés teljes folyamatát át kell hatnia. Az 1/2012. Büntető Jogegységi Határozat kimondta, hogy az első fordulatba ütköző bűncselekményt bárki elkövetheti, nem csak az, aki adatkezelőnek minősül. Ezt erősítette meg a BH2012. 87., amikor kimondta, hogy alanyi oldalon nem feltétel az Infotv. szerinti adatkezelői minőség. Éppen ezért személyes adattal visszaélés könnyen megvalósulhat azáltal, hogy a sértettről annak hozzájárulása nélkül osztanak meg valamilyen személyes adatot, az online környezetben igen gyakran képet vagy videófelvételt. Lényeges fordulata ennek a szakasznak, hogy az a) és b) pontban leírt elkövetési magatartások tanúsításával még nem valósul meg bűncselekmény, annak szükséges eleme az is, hogy az elkövetés jogtalan haszonszerzési célból vagy jelentős érdeksérelmet okozva valósuljon meg. A jelentős érdeksérelem tehát minden esetben valamilyen negatív eredmény, többnyire a sértett társadalmi megítélésének, megbecsültségének csorbulása. A jelentős érdeksérelem, mint eredmény vonatkozásában a bírósági gyakorlat azt mutatja, hogy bekövetkeztének megállapítása nem a sértett szubjektív és elfogult álláspontján alapul, hanem bírói mérlegelésen, amelyben fontos szerepet tölt be a sértett egyéni tulajdonságainak, élethelyzetének és a társadalmi felfogásnak a vizsgálata. Az egyén társadalmi megítélésének csorbulása esetében lényeges annak vizsgálata, hogy a nyilvánosságra került információról hogyan vélekedik általában a társadalom, és melyek azok a tényezők, amelyek a közfelfogást negatív irányban befolyásolhatják. Személyes adattal visszaélés kísérlete miatt ítélték el azt a politikust, aki egyes megyei vadásztársaságok által szervezett ingyenes vadászatokról hozott nyilvánosságra információkat (vadászati naplók, trófeabírálati lapok, számlák). A terhelt védekezésében előadta, hogy az ingyenes vadászatok, amelyeken zömében magas rangú politikusok vettek részt, a közvagyont károsították, ezért államtitkári minőségét kihasználva, de hatáskörét túllépve kért be személyes adatokat is tartalmazó információkat a vadásztársaságoktól, földügyi hatóságoktól. A bíróság szerint ugyanakkor az érintetteknek nem származott jelentős hátránya az információk nyilvánosságra hozatalából, amely

[39] GDPR 4. cikk 1. pont.

a köztudatban inkább politikai jellegű lejáratásként jelent meg, így a cselekmény kísérleti szakban maradt (28.B.436/2011/56.).

A Btk. 265. §-a rendeli büntetni a minősített adattal való visszaélést. A minősített adatok körét a minősített adat védelméről szóló 2009. évi CLV. törvény (Mavtv.) határozza meg, és idesorolja azokat a szigorúan titkos, titkos, bizalmas, illetve korlátozott terjesztésű nemzeti vagy külföldi minősített adatokat, amelyekről a „minősítő a minősítési eljárás során megállapította, hogy az érvényességi időn belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele a minősítéssel védhető közérdekek közül bármelyiket közvetlenül sérti vagy veszélyezteti, és tartalmára tekintettel annak nyilvánosságát és megismerhetőségét a minősítés keretében korlátozza".[40] A cselekmény elkövetési magatartásai a minősített adat jogosulatlan megszerzése, felhasználása, jogosulatlan személy részére történő hozzáférhetővé, illetve jogosult személy részére hozzáférhetetlenné tétele. A hacktivisták módszereibe leginkább a második és harmadik elkövetési magatartások, vagyis a minősített adatok jogosulatlan felhasználása és hozzáférhetővé tétele illeszkedik. A bírósági gyakorlat alapján a hozzáférhetővé tételnek fontos feltétele, hogy az csak akkor valósul meg, ha konkrétan áll fenn annak a veszélye, hogy a titok ténylegesen illetéktelen személy számára hozzáférhetővé válik, a titok megismerhetőségének absztrakt veszélye, amit mondjuk a kezelő mulasztása okozott, még nem eredményez tényállásszerűséget.[41]

Konklúzió

A növekvő társadalmi támogatottság ellenére hiba lenne úgy tekinteni a hacktivistákra, mint a kibertér Robin Hoodjaira. Szemben az ártalmatlan kiberaktivisták eszköztárával, a hacktivisták eszközei jogsértőek. Akár számítógépes rendszerekbe való jogosulatlan belépésről, akár DDoS-támadások megindításáról, akár minősített adatok kiszivárogtatásáról beszélünk, olyan magatartásokról van szó, amelyeket a magyar büntetőjog pönalizál.

Noha e cselekmények jogsértő jellege nem kérdéses, a hacktivistáknak mégsem kell különösebben tartaniuk a felelősségre vonástól, hiszen a hackercsoportokhoz köthető személyek felderítése nem egyszerű és igencsak erőforrás-igényes feladat. Tipikusan olyan cselekményekről beszélünk, ahol igen magas a látencia, az igazán nagy kárt okozó cselekményeken túli magatartások nem is feltétlenül kerülnek fel a nyomozó hatóságok radarjára. Mivel a hacktivista csoportok nem feltétlenül kötődnek adott országokhoz, a csoport tagjainak felderítése kiterjedt nemzetközi együttműködést igényel, a kibertér által biztosított anonimitás miatt pedig magas

[40] 2009. évi CLV. törvény a minősített adat védelméről (Mavtv.) 3. § 1. pont.
[41] BH2016. 138.

fokú műszaki-technikai ismeretek is szükségesek az eredményes munkához. Noha mind az Interpol, mind az Europol igyekszik összehangolni a nemzeti nyomozó hatóságok munkáját, az Europol által évente közzétett internetes szervezett bűnözésről szóló jelentés még 2021-ben is az egyik kezelendő problémaként azonosította a nemzetközi együttműködés nehézkességét.[42]

Felhasznált irodalom

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

Az Anonymous átírta az alaptörvényt. *Index,* 2012. március 4. Online: https://index.hu/tech/2012/03/04/az_anonymous_atirta_az_alaptorvenyt

Az Anonymous azt állítja, meghackelték az orosz kémműholdakat. *HVG.hu,* 2022. március 3. Online: https://hvg.hu/tudomany/20220305_oroszorszag_kemmuhold_anonymous_hackerek_hackertamadas_network_battalion_65_roszkozmosz

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet). L 119/1 (2016. május 4.)

Az Európai Parlament és a Tanács 2013/40/EU irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról. L 218/8 (2013. augusztus 4.)

Beyer, Jessica L.: The Emergence of a Freedom of Information Movement: Anonymous, WikiLeaks, the Pirate Party, and Iceland. *Journal of Computer-Mediated Communication,* 19. (2014), 2. 141–154. Online: https://doi.org/10.1111/jcc4.12050

Burgess, Matt: Ukraine's Volunteer 'IT Army' Is Hacking in Uncharted Territory. *Wired,* 2022. február 27. Online: www.wired.com/story/ukraine-it-army-russia-war-cyberattacks-ddos/

Denning, Dorothy E.: Activism, Hacktivism, and Cyberterrorism: The Internet As a Tool for Influencing Foreign Policy. In John Arquilla – David Ronfeldt (szerk.): *Networks and Netwars. The Future of Terror, Crime, and Militancy.* Santa Monica, RAND Corporation, 2001. 239–288. Online: https://doi.org/10.7249/MR1382

Dornfeld László: Kiberterrorizmus – a jövő terrorizmusa? In Mezei Kitti (szerk.): *A bűnügyi tudományok és az informatika.* Pécs–Budapest, Pécsi Tudományegyetem Állam- és Jogtudományi Kar – MTA Társadalomtudományi Kutatóközpont, 2019. 46–63.

Európai Gazdasági és Szociális Bizottság: Az Európai Gazdasági és Szociális Bizottság véleménye – Kiberaktivisták és civil társadalmi szervezetek (saját kezdeményezésű vélemény). C 13/116 (2016. január 15.). Online: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv%3AOJ.C_.2016.013.01.0116.01.HUN&toc=OJ%3AC%3A2016%3A013%3ATOC

Europol: *Internet Organised Crime Threat Assessment (IOCTA) 2021.* Luxembourg, Publications Office of the European Union, 2021. Online: www.europol.europa.eu/publications-events/main-reports/iocta-report

[42] Europol: Internet Organised Crime Threat Assessment (IOCTA) 2021. Luxembourg, Publications Office of the European Union, 2021. 40.

Fehér Katalin: *Digitalizáció és új média.* Budapest, Akadémiai Kiadó, 2017. Online: https://doi.org/10.1556/9789630597432

Gelányi Anikó – Csepely-Knorr Tamás: A jogosulatlan wifi használat minősítése, avagy ha nyitva van az ajtó, akkor bemehetek? *Infokommunikáció és Jog*, 6. (2009), 34. 201–207. Online: https://infojog.hu/wp-content/uploads/pdf/200934_GelanyiAniko_CsepelyKnorrTamas.pdf

Görgényi Ilona – Gula József – Horváth Tibor – Jacsó Judit – Lévay Miklós – Sántha Ferenc – Váradi Erika: *Magyar büntetőjog különös rész.* Budapest, Wolters Kluwer, 2020.

Hancu [Hanula Zsolt]: Az oroszok visszabombázzák Észtországot az online kőkorszakba. *Index,* 2007. május 31. Online: https://index.hu/tech/net/eszt290507/

Illig, Andrew T.: Computer Age Protesting: Why Hacktivism is a Viable Option for Modern Social Activists. *Dickinson Law Review,* 119. (2015), 4. 1033–1057. Online: https://ideas.dickinsonlaw.psu.edu/cgi/viewcontent.cgi?article=4107&context=dlra

Ireland, Leanna: We are all (not) Anonymous: Individual- and Country-Level Correlates of Support for and Opposition to Hacktivism. *New Media & Society,* (2022). Online: https://doi.org/10.1177/14614448221122252

Karsai Krisztina (szerk.): *Kommentár a Büntető Törvénykönyvről szóló 2012. évi C. törvényhez.* Budapest, Wolters Kluwer, 2017.

Mezei Kitti: A DDoS-támadások büntetőjogi szabályozása az Egyesült Államokban, Európában és Magyarországon. *Pro Futuro,* 8. (2018), 1. 66–83. Online: https://doi.org/10.26521/Profuturo/2018/1/4674

Mezei Kitti: A jogosulatlan belépés, avagy a hacking szabályozása a büntetőjogban. *Rendőrségi Tanulmányok,* 3. (2020), 2. 23–43.

Nagy Zoltán András – Mezei Kitti: A zsarolóvírus és a botnet vírus mint napjaink két legveszélyesebb számítógépes vírusa. In Gaál Gyula – Hautzinger Zoltán (szerk.): *Szent Lászlótól a modernkori magyar rendészettudományig.* Pécs, Magyar Hadtudományi Társaság, Határőr Szakosztály, Pécsi Szakcsoport, 2017. 163–168.

Nagy Zoltán András: A számítógépes bűnözés története. In Dobák Imre – Hautzinger Zoltán (szerk.): *Szakmaiság, szerénység, szorgalom. Ünnepi kötet a 65 éves Boda József tiszteletére.* Budapest, Dialóg Campus Kiadó, 2018. 471–480.

ORFK: ketten tettek feljelentést a WannaCry vírus támadása miatt. *HVG,* 2017. június 16. Online: https://hvg.hu/tudomany/20170616_wannacry_zsarolovirus_orfk_magyar_feljelentesek

Szathmáry Zoltán: Etikus és nem etikus hacking – a kéretlen sérülékenységvizsgálat büntetőjogi kérdései. *Magyar Jog,* 67. (2020), 6. 340–346.

Takács Petra: A Google Maps-en több ezer „értékeléssel" figyelmeztetik az orosz népet. *Liner.hu,* 2022. március 4. Online: https://liner.hu/google-maps-orosz-ukran-haboru-2/

Travaglino, Giovanni A.: Support for Anonymous as Vicarious Dissent: Testing the Social Banditry Framework. *Group Processes & Intergroup Relations,* 22. (2019), 2. 163–181. Online: https://doi.org/10.1177/1368430217722037

Varga Balázs: Informatikai bűncselekmények. *Jogi Fórum,* 2003. december 19. Online: www.jogi-forum.hu/publikaciok/127.

Varga Zoltán (szerk.): *Nagykommentár a Büntető törvénykönyvről szóló 1978. évi IV. törvényhez.* Budapest, KJK-Kerszöv, 2004.