MEZEI KITTI*

A MODERN TECHNOLÓGIÁK KIHÍVÁSAI A BÜNTETŐJOGBAN, KÜLÖNÖS TEKINTETTEL A KIBERBŰNÖZÉSRE**

Jelen tanulmány célja, hogy – a teljesség igénye nélkül – vizsgáljon egyes aktuális büntetőjogi kérdéseket a modern technológiákkal kapcsolatban, különös tekintettel a kiberbűnözésre. Napjainkra az innovációknak köszönhetően az információs társadalomban felgyorsult a technológiai fejlődés, amely a bűnözés természetére egyaránt lényeges és maradandó hatást gyakorol. Új típusú bűncselekmények jelennek meg, illetve a hagyományos deliktumok átalakulnak. Ma már az elkövetés eszközeként akár egy algoritmusnak vagy egy autonóm járműnek is szerep juthat. Az új informatikai eszközök – mint például az Internet of Things (IoT) – is könnyedén válhatnak a hackertámadások célpontjaivá. Az online közösségi oldalakon nagy mennyiségű személyes adatot osztanak meg nap mint nap. A kriptovalutákkal összefüggésben elkövetett bűncselekmények egyre nagyobb számban jelennek meg. Mindez a büntetőjog számára is kihívást jelent, ezért a tanulmány az ezekkel kapcsolatos visszaéléseket kívánja bemutatni.

BEVEZETÉS

Nem túlzás azt állítani, hogy a technológiai innováció mindannyiunk életét érinti. Ez a dinamikus fejlődés a jogrendszert is folyamatos kihívások elé állítja, ezért szükséges, hogy az új technikai újításokkal kapcsolatban felmerülő jogi kérdésekre, problémákra reflektálni tudjunk. Mindez azért is különösen fontos, mert az egyes társadalmi és gazdasági folyamatok egyre inkább függenek az információs rendszerektől, valamint meghatározhatják a gazdasági szereplők versenyképességét.[1] Az információs társadalom egyik jellemzőjévé vált az infokommunikációs eszközök számának, sokféleségének a növekedése és használatuk széles körű elterjedése.[2]

A gyors ütemű informatikai fejlődés nyilvánvaló előnyei mellett (például széles körű kommunikációs lehetőséget nyújt, illetve az információkhoz könnyű és azonnali hozzáférést biztosít stb.) megvannak a maga veszélyei is, hiszen lehetőséget

* PhD, tudományos munkatárs, Társadalomtudományi Kutatóközpont Jogtudományi Intézet, 1097 Budapest, Tóth Kálmán u. 4.; egyetemi adjunktus, Budapest Műszaki és Gazdaságtudományi Egyetem, Gazdaság- és Társadalomtudományi Kar, Üzleti Jog Tanszék, 1117 Budapest, Magyar tudósok körútja 2. E-mail: *mezei.kitti@tk.mta.hu.*

** Jelen tanulmány a 129018. számú, „A jogrendszer reagálóképessége 2010–2018" című NKFIH pályázat keretében készült; a Mesterséges Intelligencia Nemzeti Laboratórium támogatásával jelent meg.

1 Pintér Róbert: „Információ- és hálózatgazdasági alapok" in Nemeslaki András (szerk.): Információs társadalom (Budapest: Dialog Campus 2018) 17–19.

2 Kincsei Attila: „Technológia és társadalom az információ korában" in Balogh Gábor (szerk.): Az információs társadalom (Budapest: Gondolat 2007) 47.

teremt a bűnözés eddig ismeretlen formái számára. Éppen ezért a kiberbűnözés jelenti napjaink egyik legnagyobb kihívását. Az új technológiák megjelenése (például mobilinformatikai és okoseszközök, Internet of Things[3], mesterséges intelligencia), a megvalósítható funkciók bővülése, illetve az információs hálózatok használatának elterjedése magukkal hozzák az újabb elkövetési módokat, illetve büntetendő cselekmények körét.[4] A tisztán informatikai bűncselekményeken kívül, amelyek kizárólag a digitális környezetben követhetők el (például hacking, adatmanipuláció, számítógépes vírusok), ma már szinte bármelyik hagyományos bűncselekmény (például csalás, zsarolás, pénzmosás) is elkövethető az információs rendszerek használatával, a hálózatra csatlakozva. Mindez kihívások elő állítja mind a jogalkotást – a büntetőjogi szabályozást tekintve –, mind a jogalkalmazást a büntetendő magatartások minősítéseinek kérdésében.

Az internetnek számos olyan jellemzője van, amelyek egyben a használatával összefüggő visszaélések térnyerésére, illetve a bűncselekmények hatékonyabb elkövetésére is lehetőséget teremtenek. A hálózatra csatlakozott eszközök és felhasználók száma évről évre növekvő tendenciát mutat.[5] Mivel egy egész világra kiterjedő hálózatról van szó, amely azonnali és valós idejű kapcsolatteremtést tesz lehetővé, a kiterjedt online jelenlét miatt tömeges informatikai támadás történhet. Mindennek lényege az elektronikus formában megjelenő nagy mennyiségű adat („Big Data" jelenség)[6]. Az internet ennélfogva speciális, de egymással összefüggő tulajdonságokkal rendelkezik, amelyek egyúttal megkönnyíthetik a különféle bűncselekmények elkövetését, azonban már egy új színtéren.

Az internet globális jellege a határon átívelő bűnözést segíti. Az elkövetők a világ bármely pontján kereshetnek célpontokat, illetve sebezhetőségeket, és ehhez még arra sincs szükségük, hogy az elkövetéskor fizikailag akár egy országon belül tartózkodjanak; bűnözői infrastruktúrájukat is különböző államokból irányíthatják. Ez pedig olyan összetett joghatósági és illetékességi kérdéseket vet fel a büntető eljárásjogban, amelyek a mai napig megválaszolatlanok.

Az interneten egyben lehetséges decentralizált és rugalmas hálózatok létrehozásais, amelyek az elkövetők laza szerveződését segítik elő, például egymás között megoszthatják a szakmai tudásukat és jártasságukat, valamint az általuk kifejlesztett technikai eszközöket. Az internet egyben kommunikációs csatorna is, amely a

[3] Az „Internet of Things", vagy rövidítve „IoT", mellyel a mindennapjainkban használt – gyakran „okos" elnevezésű – eszközök az interneten keresztül is elérhetők, és képesek egymással akár önállóan is kommunikálni. Ennek a kommunikációnak a motorja az ún. M2M (machine-to-machine) technológia, ami olyan adatáramlást jelent, amely emberi közreműködés nélkül, gépek között zajlik. A kommunikáció minden olyan gép között létrejöhet, amely a megfelelő technológiával (érzékelőkkel, hálózati csatolókkal) van ellátva ahhoz, hogy csatlakozzon a rendszerhez.

[4] Nagy Zoltán András: *Bűncselekmények számítógépes környezetben* (Budapest: Ad Librum 2009) 23–24.

[5] Lásd a statisztikát ehhez az Európai Unióban: *https://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_households_and_individuals.*

[6] A „Big Data" kifejezés az interneten megjelenő hatalmas mennyiségű adatmennyiségre utal, amely új társadalmi jelenségként a jogalkotást és a jogalkalmazást is kihívások elé állítja. Ződi Zsolt: „Jog és jogtudomány a Big Data korában" *Állam- és Jogtudomány* 2017/1. 95., valamint ehhez részletesen lásd még Ződi Zsolt: *Platformok, robotok és a jog* (Budapest: Gondolat Kiadó 2018) 221–240.

különböző bűncselekmények elkövetésében is fontos szerepet tölthet be. A kiberbűnözés ennek következtében napjainkra profitorientált, szolgáltatásalapú üzleti modellé nőtte ki magát, amelynek motorját az online feketegazdaság adja (például Darknet fórumok),[7] ahol a különböző kibertámadásokat elősegítő eszközök és egyéb illegális szolgáltatások is elérhetők. Emellett az internet relatív névtelenséget biztosít, és ezt a bűnelkövetők fokozhatják a különböző titkosítást és anonimitást biztosító technológiák használatával, amelyek alkalmasak a személyazonosság elrejtésére. Ezért a szervezett bűnözés,[8] de a terrorizmus képviselői is előszeretettel használják az internetet, legyen szó illegális online kereskedelemről vagy propagandaterjesztésről, emellett kibertámadásokkal is bővült az eszköztáruk.[9]

Azzal, hogy a sértettekkel távoli kapcsolatfelvételt garantál, az internet megszünteti azokat a szociális akadályokat is, amelyekkel az elkövetőknek a valóságban, akár személyes találkozáskor kellene szembenézniük. Az ilyen típusú bűnözésre magas látencia jellemző, mert a gyanútlan felhasználók sokszor nem is észlelik, hogy bűncselekmény áldozatává váltak, és nem jelentik az esetet a hatóságoknak (például bankkártya-visszaélések, pénzintézetek ellen intézett támadások), amely tovább nehezíti a felderítést.

Az információs rendszerek segítségével könnyedén lehet végrehajtani adat- vagy programmanipulációt minimális költségek mellett, mert az információ elektronikus megjelenítésének köszönhetően lehetőség van az adatok másolására minőségi veszteség nélkül, valamint módosítására anélkül, hogy annak látható nyoma lenne.

Az online környezet lehetővé teszi az automatizált műveleteket, amelyek rendkívül gyorsan, jelentős kárt tudnak okozni, mivel egy rosszindulatú program képes sokszorosítani önmagát, és akár több millió rendszert megfertőzni egyidejűleg (lásd WannaCry zsarolóvírus), vagy egy botnet-hálózat[10] segítségével az elkövetők nagy-

[7] A Darknet elosztott, anonimitást biztosító, titkosított hálózat a Deep Weben belül, ami kizárólag speciális szoftverek használatával érhető el, mint például a The Onion Routerrel (TOR), I2P-vel vagy Freenettel, amelyeket magasfokú titkosítással láttak el. A bűnelkövetők kihasználják ezeket, mert a használatuk révén könnyedén el tudják rejteni a személyazonosságukat, az internetes forgalmukat és a szerverük helyét. A digitális feketegazdaság középpontját a Darknet-fórumok jelentik, amelyek a különböző illegális termékek és szolgáltatások színteréül szolgálnak (pl. crimeware, kábítószer, gyermekpornográf tartalmak stb.). Lásd Mezei Kitti: „A szervezett bűnözés az interneten" in Mezei Kitti (szerk.): A bűnügyi tudományok és az informatika. (Budapest–Pécs: PTE ÁJK–MTA Társadalomtudományi Kutatóközpont 2019) 137–143.

[8] Lásd a kiberbűnözés és a szervezett bűnözés kapcsolatáról bővebben Simon Béla – Gyaraki Réka: „Kiberbűnözés" in Kiss Tibor (szerk.): Kibervédelem a bűnügyi tudományokban (Budapest: Dialog Campus 2020) 95–119.

[9] A szakirodalom is részletesen foglalkozik már a kiberterrorizmus kérdéseivel: Neparáczki Anna Viktória: „A kiberterrorizmus büntető anyagi jogi megítélése" *Ügyészek Lapja* 2020/1. 71–85., Dornfeld László: „Kiberterrorizmus – A jövő terrorizmusa?" in Mezei Kitti (szerk.): A bűnügyi tudományok és az informatika (Budapest–Pécs: PTE ÁJK–MTA Társadalomtudományi Kutatóközpont 2019) 46–63.; illetve Szabó Imre: „Az informatikai terrorizmus veszélyei" *Belügyi Szemle* 2011/2. 5–20.

[10] A felhasználó tudta nélkül megfertőzött információs rendszereket, amelyek távolról irányíthatók, zombinak nevezik. Másik elnevezésük a robot és network szavak összevonásából eredő „botnet", amely a több bot összekapcsolásával keletkezett hálózatot jelenti. A botnet-hálózat tagjait a fertőzött zombieszközök alkotják. Ez a hálózat pedig alkalmas arra, hogy az eszközök számítási kapacitását és sávszélességet kihasználva például DDoS-támadást, avagy túlterheléses támadást indít-

szabású támadásokat tudnak végrehajtani, amely akár az adott rendszer teljes leállásához is vezethet.[11]

A kiberbűnözés által okozott kár 2017-ben 600 milliárd dollár volt a különböző sértetti köröknél (pl. vállalatok, pénzintézetek, kormányzati szervek stb.), és a szakértők szerint ez 2021-re meg duplázódik.[12] Úgy gondolom, mindez rávilágít arra, hogy mekkora lehetőség rejlik a modern technológiák által nyújtott előnyök bűnelkövetési célú felhasználásában, ugyanakkor mekkora veszélyt és kockázatot hordoz a felhasználókra nézve.

A KIBERBŰNÖZÉS FOGALMI MEGHATÁROZÁSA

A kibertér (cyberspace) kifejezést William Gibson amerikai író alkotta meg az 1982-ben megjelent „Burning Chrome" című novellájában, amely később a *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 Számítástechnikai bűnözésről szóló egyezmény[13] (a továbbiakban: Budapesti egyezmény) is ezt alkalmazza (Convention on Cybercrime). Tanulmányomban az informatikai bűnözést és kiberbűnözést mint szinonim fogalmakat használom, mert ezek a szakirodalomban elfogadottak. Fontos azonban megjegyezni, hogy a kiberbűnözésnek még nincs általánosan elfogadott és egységes jogi definíciója.

A recens nemzetközi szakirodalomban több szerző is, így Jonathan Clough,[14] Peter Grabosky[15] és Susan W. Brenner[16] is a kiberbűnözésre mintegy gyűjtőfogalomként tekint, amelynek két fő kategóriája különböztethető meg: az egyik azon deliktumok csoportja, amelyek kizárólag információs rendszerekkel (például számítógépekkel, azok hálózatával vagy egyéb információs és kommunikációs technológiák – IKT – használatával) követhetők el. Jellemzően az ilyen bűncselekmény tárgya az információs rendszer. Ez a tisztán informatikai bűncselekmény vagy kiberbűncselekmény, az ún. cyber-dependent crime (például számítógépes vírusok használata, hacking stb.). A második, tágabb kategóriába tartoznak azok a hagyományos bűncselekmé-

sanak. Gyányi Sándor: „A botnetek, a túlterheléses támadások eszközei" *Magyar Rendészet* 2013. Különszám 24.

[11] Bert-Jaap Koops: „The Internet and its Opportunities for Cybercrime" *Tilburg School Legal Studies Paper Series* No. 2011/9. 740–741.

[12] McAfee: „Economics Impact of Cybercrime – No Slowing Down" *Report* February 2018. *www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf.*

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

[14] Jonathan Clough: Principles of cybercrime (Cambridge University Press 2014) 10–11.

[15] Peter Grabosky: *Cybercrime* (London: Oxford University Press 2016) 8–9.

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

nyek, amelyeket az információs rendszerek felhasználásával követnek el, mint például a csalás, zsarolás, gyermekpornográfia, szerzői jogi jogsértések, zaklatás és még sorolhatnánk. Ez az ún. cyber-enabled crime esetköre, amikor az információs rendszer a bűncselekmény elkövetésének az eszköze.[17]

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. E meghatározást használja a hazai szakirodalom is.[18]

A MODERN TECHNOLÓGIÁK LEGNAGYOBB VESZÉLYE: A KIBERTÁMADÁS

A hálózati összekapcsoltság a termékek és szolgáltatások egyre növekvő számának a központi elemévé vált. Ez a jellemző megkérdőjelezi a biztonság hagyományos koncepcióját, mivel a hálózati összekapcsoltság közvetlenül veszélyeztetheti a termék biztonságát, és közvetett veszélyt is magában hordozhat, amennyiben feltörhető, ami további biztonsági kiberfenyegetésekhez vezet, és ez érinti már a felhasználók biztonságát is.[19] Éppen ezért az elkövetők a különböző IoT-eszközök sebezhetőségét keresik[20], például routereket, biztonsági kamerákat vagy akár az okostelevíziókat és egészségügyi berendezéseket veszik célba egy-egy kibertámadás során. A „meghackelt" IoT-eszközöket pedig jogsértő cselekményekhez használják fel, mert álta-

[17] Clough (15. lj.) 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, illetve Council of Europe: Explanatory Report to the Convention on Cybercrime. *European Treaty Series* – No. 185. 2001. 79. cikk.; Éves jelentéseiben *(Internet Organised Crime Threat Assessment)* az Europol is azonos jelentéstartalommal használja ezeket a fogalmakat, de részben eltérő elnevezéssel, így a *cyber-dependent crime*-ot, valamint a *cyber-facilitated crime*-ot.

[18] Lásd erről bővebben: Nagy Zoltán: „A számítógépes környezetben elkövetett bűncselekmények kodifikációjáról de lege lata – de lege ferenda" *Belügyi Szemle* 1999/11. 16–27.; Szathmáry Zoltán: *Bűnözés az információs társadalomban – Alkotmányos büntetőjogi dilemmák az információs társadalomban* (Pécs: PTE ÁJK 2012) 79–80.; valamint Parti Katalin – Kiss Tibor: „Az informatikai bűnözés" in Borbíró Andrea – Gönczöl Katalin – Kerezsi Klára – Lévay Miklós (szerk.): Kriminológia (Budapest: Wolters Kluwer 2017) 491–493.; Szabó Imre: „Informatikai bűncselekmények" in Dósa Imre (szerk.): Az informatikai jog nagy kézikönyve (Budapest: Complex 2008) 547.; valamint Varga Árpád: „Az informatikai bűnözés fogalmi meghatározása, csoportosítása és helye a hazai jogfejlődésben" *In Medias Res* 2019/1. 145–167.

[19] Erre figyelmeztet többek között az Európai Bizottság által elfogadott Fehér könyv is a mesterséges intelligenciáról, amely az új technológiák esetén a kockázatalapú szabályozási rendszer kialakítását hangsúlyozza.

[20] Lásd bővebben: Sara Sun Beale – Peter Berris: „Hacking the Internet of Things: Vulnerabilities, dangers, legal responses" *Duke Law & Technology Review*, Vol. 16, No. 1. 162–204.

luk könnyedén lehet szenzitív adatokat gyűjteni a felhasználókról (pl. mikor tartózkodik otthon az illető). Gondoljunk csak egy okosotthonra, amelyet ugyanúgy érhet támadás, mint bármely más informatikai eszközt, és ennek következében az elkövető át tudja venni az irányítást felette, különböző parancsokat továbbíthat, ezáltal alkalmas lehet a sértett megfigyelésére vagy akár az otthonába történő bezárására vagy a kizárására.[21] Sőt, az autonóm járművek is könnyedén válhatnak majd a hackertámadások célpontjaivá.[22] Nem kell azonban az autonóm járművekre várnunk, hiszen az autólopás már napjainkra is új szintre lépett a technológiai újításoknak köszönhetően, mert az sem példa nélküli, hogy nagy értékű gépkocsikat lopnak el úgy, hogy a kulcs nélküli indítórendszerüknek a védelmét jeltovábbító eszközökkel kijátsszák, vagy szoftveresen feltörik.[23]

Az egyes hacking-jellegű cselekmények mögött leggyakrabban a következő motivációk húzódnak: hozzáférés az információhoz, az adat megváltoztatása, illetve törlése, valamint az információs rendszer használata.[24] A jogosulatlan belépés további büntetendő magatartásokat segíthet elő, például az „ellopott" szenzitív adatokkal a sértetteket zsarolhatják. Más esetekben az adatokat további csalás jellegű magatartásokhoz használják fel, többek között adathalászathoz vagy arra, hogy a versenytársak bizalmas információkhoz férjenek hozzá. Az esetek többségében személyes, pénzügyi és egészségügyi adatokat szereznek meg (pl. név és születési idő, telefonszámok, e-mail-címek, felhasználói adatok, jelszavak és bankkártyaadatok). Az elkövetők ezeket gyakran nem saját maguknak szerzik meg, hanem azért, hogy később a Darknet-fórumokon értékesítsék.

A hatályos 2012. évi C. törvény a Büntető Törvénykönyvről (a továbbiakban: Btk.) a kiberbűncselekmények esetében a védelem középpontjába az információs rendszert helyezi. Ennek definícióját pedig az értelmező rendelkezések között határozza meg a 459. § 15. pontjában, amely szerint „információs rendszer minden olyan berendezés – vagy egymással kapcsolatban lévő ilyen berendezések összessége –, amely automatikusan végez adatfeldolgozást, azaz adatok bevitelét, kezelését, tárolását, továbbítását látja el."[25] Ebbe minden informatikai eszköz beletartozik a laptoptól kezdve a drónokig.

[21] Stein Schjolberg: *The history of cybercrime 1976–2014* (Cybercrime Research Institute 2014) 148–149.

[22] Ambrus István: „Az autonóm járművek és a büntetőjogi felelősségre vonás akadályai" in Mezei Kitti (szerk.): A bűnügyi tudományok és az informatika. (Budapest–Pécs: PTE ÁJK–MTA Társadalomtudományi Kutatóközpont 2019) 10–11., valamint Frank Douma – Sarah Aue Palodichuk: „Criminal liability issues created by autonomous vehicles" *Santa Clara Law Review* Vol. 52. No. 4. 1164–1165.

[23] Legyen szó akár önvezető vagy hagyományos autóról, ha az elkövető a jármű információs rendszerének átprogramozásával iktatja ki a védelmet és lopja el azt, akkor az információs rendszer vagy adat megsértése bűncselekmény, és a lopás bűncselekménye valóságos anyagi halmazatot képez. Abban az esetben, ha a jármű eltulajdonításának megakadályozására szolgáló eszközt teszik a lopás elleni védelemre alkalmatlanná, mindezt anélkül, hogy az információs rendszerbe jogosulatlanul belépnének, akkor a halmazat kizárt, és csak a dolog elleni erőszakkal elkövetett lopás, azaz a vagyoni bűncselekmény minősített esete állapítható meg. Lásd Sinku Pál: „Ellentmondások a gazdasági bűncselekmények megítélésében" in Belovics Ervin – Tamási Erzsébet – Varga Zoltán (szerk.): Örökség és büntetőjog – Emlékkönyv Békés Imre tiszteletére (Budapest: PPKE JÁK 2011) 71–72.

[24] Clough (9. lj.) 33.

[25] Btk. 459. § (1) bekezdés 15. pont

A hackinget, avagy a jogosulatlan belépést a Btk. 423. § (1) bekezdése, a tisztán informatikai bűncselekménynek minősülő információs rendszer vagy adat megsértésének tényállása szabályozza. Ennek értelmében 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. A bűncselekménynek a jogi tárgya az információs rendszerek megfelelő működéséhez és a bennük tárolt, feldolgozott, továbbított adatok megbízhatóságához, hitelességéhez, valamint a titokban maradásához fűződő társadalmi-gazdasági érdek.[26]

A bűncselekmény megállapításához szükséges, hogy az információs rendszer technikai intézkedéssel biztosított védelemmel legyen ellátva, és ez a védelem aktív legyen, azaz rendelkezzen például felhasználói azonosítóval és jelszóval vagy egyéb védelemmel. Tehát nem tekinthető jogosulatlannak a belépés abban az esetben, ha az információs rendszer nem védett, illetve a védelem nincs aktiválva, mert ezek konjunktív feltételek a bűncselekmény megállapíthatóságához.[27] Továbbá az elkövetési mód meghatározása szerint a bűncselekmény megvalósul, ha a belépés a védelmi intézkedés megsértésével vagy kijátszásával történik, például a biztonsági rendszer hiányosságait kihasználva lépnek be jogosulatlanul vagy a jogosult jelszavával, belépési kódjával, amelynek megszerzési módja azonban közömbös (például történhet megtévesztéssel, kifürkészéssel, kódtörő programmal, social engineering, vagyis pszichológiai manipulációval, vagy elképzelhető, hogy a felhasználó hanyagsága folytán jut hozzá az elkövető).

A bűncselekmény nem célzatos, ezért az elkövetésnek nem feltétele az sem, hogy haszonszerzési, károkozási vagy egyéb hasonló célzattal történjen. Az sem követelmény továbbá, hogy az információs rendszerben tárolt adaton az elkövető később bármilyen műveletet végezzen, vagy akár a rendszer működését akadályozza. Önmagában tehát a jogosulatlan belépés is büntetendő (mere hacking). Amennyiben ezt további jogosulatlan műveletek követik – például adatok törlése, hozzáférhetetlenné tétele –, akkor már a következő bekezdések egyik fordulata valósul meg, és

[26] Karsai Krisztina: „XLIII. fejezet Tiltott adatszerzés és az információs rendszer elleni bűncselekmények" in Karsai Krisztina (szerk.): Kommentár a Büntető Törvénykönyvhöz (Budapest: Complex 2013) 898.

[27] Nagy Zoltán András: „XLIII. fejezet tiltott adatszerzés és az információs rendszer elleni bűncselekmények" in Tóth Mihály – Nagy Zoltán András (szerk.): Magyar Büntetőjog: Különös rész (Budapest: Osiris 2014) 594–595., valamint lásd BH 2017.12.392.: A Kúria kimondta, hogy a büntetőjog alapelveivel összhangban a jogosultság keretein való túllépés is akkor minősül bűncselekménynek, ha az egyben a rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával történik (pl. más jelszavának a felhasználásával), ugyanis akkor, ha valakinek van jogosultsága az információs rendszerbe történő belépéshez, akkor pusztán e jogosultság kereteinek túllépése nem éri el azt a veszélyességi szintet, mint amit az első fordulat megkíván. Tehát önmagában a jogosultság kereteinek túllépésével való belépés vagy bennmaradás nem büntetendő, amennyiben nem valamely biztonsági intézkedés megsértésével valósul meg, vagy nem kapcsolódik össze további tisztességtelen célzattal – pl. jelentős érdeksérelemmel, jogtalan károkozási, haszonszerzési célú adatszerzéssel vagy manipulálással, vagy a rendszer megzavarásának a szándékával, illetve eredményével –, mert ennek hiányában a magatartás társadalomra veszélyessége csekély.

beleolvad, a súlyosabb jogtárgysértésre figyelemmel [Btk. 423. § (2) bekezdés a) és b) pont].[28]

AZ INFORMÁCIÓS RENDSZER FELHASZNÁLÁSÁVAL ELKÖVETETT ZSAROLÁS ESETEI

Az információs rendszer felhasználásával elkövetett zsarolás egy hagyományos bűncselekmény modern változata, amely során gyakran az elkövetők az online térben fenyegetik a sértettet, hogy valamilyen formában kárt okoznak neki, amennyiben a követelésüknek nem tesz eleget. Előfordulhat ugyanis, hogy az elkövetők jogosulatlanul belépnek a sértett számítógépébe a biztonsági intézkedések kijátszásával, például malware aktiválásával – gondoljunk csak a zsarolóvírusokra[29] – szerzik meg vagy éppen titkosítják az azon tárolt bizalmas, személyes adatokat, értékes gazdasági vagy üzleti titkokat, esetleg kompromittáló képeket. A virtuális betörést követően hozzáférhetnek a beépített webkamerához, illetve mikrofonhoz, és saját maguk készíthetnek olyan kép-, videó- és hangfelvételeket, amelyek a zsarolás alapját képezhetik. Ezután a zsarolási fázis következik, amikor az elkövető azzal fenyeget, hogy például az interneten (pl. közösségi oldalakon, fórumokon) megosztja az adatokat, vagy a család, barátok részére elküldi a felvételt, amennyiben a sértett nem fizet neki egy meghatározott pénzösszeget.

Emellett a zsarolásnak egy új formája is megjelent, amely során az elkövetők Darknet-fórumokon szereznek meg olyan adatbázisokat, amelyek nagyszámban tartalmaznak személyes adatokat, így például e-mail-címeket, és ezekre elküldik azt az üzenetet, hogy kompromittáló kép- vagy videófelvétel van a birtokukban az érintett felhasználóról, és amennyiben nem fizet, közzéteszik a felvételt. Az sem példa nélküli, hogy zsarolási céllal használják fel a DDoS-támadásokat.[30]

[28] Szathmáry Zoltán: „A számítástechnikai bűncselekmények és rendszertani elhelyezésük" *Jogtudományi Közlöny* 2012/4. 173–174.

[29] A legnagyobb veszélyt az elmúlt években a zsarolóvírusok (ransomware vagy cryptoware) jelentették, mely kártékony programok úgy működnek, hogy a megfertőzött információs rendszeren tárolt fájlokat, akár a teljes adatállományt titkosítják, ezáltal a sértett számára elérhetetlenné teszik azokat, majd rendkívül magas, akár milliós nagyságrendű váltságdíjat követelnek a helyreállító, titkosítást feloldó kódért cserébe. A szoftver fizetési határidőt is szabhat, amelynek lejárta után akár végérvényesen elérhetetlenné teszik az adatokat. Az elkövetők kiléténekmegismerése szinte lehetetlen, mert általában a váltságdíjat a nehezen lenyomozható ún. kriptovalutában – például bitcoinban – kérik. Lásd erről bővebben: Bart Custers – Jan-Jaap Oerlemans – Ronald Pool: „Laundering the profits of ransomware: Money laundering methods for vouchers and cryptocurrencies" *European Journal of Crime, Criminal Law and Criminal Justice* 2020. 121–152.

[30] 2016-ban az Europol sikeres akciót hajtott végre és letartóztatták a zsarolásokban élen járó DD4BC (Distributed Denial of Service for Bitcoin) Team hacker csoportnak a kulcstagjait, akik számos DDoS-támadást indítottak európai cégekkel szemben. Az elkövetők elsősorban olyan vállalkozások oldalait választják ki, amelyek folyamatos és zavartalan működést követelnek meg (pl. webáruházak, online szerencsejáték oldalak, energia- és pénzügyi szféra szolgáltatói). Az általuk alkalmazott zsaroló séma a következőképpen néz ki: felmérik a célpont hálózati sérülékenységét, majd kisebb erősségű DDoS-támadásokat indítanak a céggel szemben, ezt követően a további támadások indításának elkerülése érdekében bitcoin formájában fizetséget kérnek a cégtől. Abban az eset-

A Btk. 367. § (1) bekezdése szerint, aki jogtalan haszonszerzés végett mást erőszakkal vagy fenyegetéssel arra kényszerít, hogy valamit tegyen, ne tegyen vagy eltűrjön, és ezzel vagyoni hátrányt okoz, az a zsarolás tényállását valósítja meg. A zsarolás olyan fenyegetéssel is elkövethető, amely csak hajlítja a sértett akaratát, annak cselekvési szabadságát csak kisebb-nagyobb mértékben befolyásolja. Ezzel mintegy lehetőséget nyújt számára, hogy az erőszak vagy fenyegetés erejét, komolyságát összevesse az őt fenyegető hátránnyal, amely lehet vagyoni jellegű, de érinthet akár egzisztenciát, becsületet, családi együttélést. Jelen esetben a zsarolást fenyegetéssel követik el, amely a súlyos hátrány kilátásba helyezésével alkalmas arra, hogy a megfenyegetettben komoly félelmet keltsen. A zsarolás célzatos bűncselekmény, és eredménye a vagyoni hátrány. Ha a fenyegetés alkalmazása megtörtént, de az eredmény még nem következett be, akkor a zsarolás kísérlete valósul meg.[31]

Ezek alapján a jogosulatlan, engedély nélküli informatikai műveletek végzése az információs rendszer és adat elleni bűncselekménynek az elkövetési magatartásait valósítják meg, és a zsarolással halmazatban megállapítható e bűncselekmény.

A SZEMÉLYES ADATTAL VISSZAÉLÉS

Az Európai Parlament és Tanács 2013/40/EU irányelve az információs rendszerek elleni támadásokról[32] először hívta fel a figyelmet arra, hogy a kiberbűnözésre alkalmazott integrált megközelítés egy másik fontos eleme a hatékony fellépés a személyazonosság-lopás és a személyazonossághoz kapcsolódó egyéb bűncselekmények ellen. Ez különösen indokolt, mert a felhasználók sokszor nincsenek tisztában az online jelenléttel járó veszélyekkel, a megosztott információkkal és képekkel járó fenyegetésekkel. Ennek eredményeképpen a szenzitív adatokat az erre illetéktelen személyek már egyre könnyebben tudják megszerezni (pl. gondoljunk csak az erre a célra kifejlesztett malware, phishing és egyéb módszerekre).[33]

Egyebek mellett Bert-Jaap Koops és Ronald Leenes tettek kísérletet a témakör szempontjából releváns fogalmak meghatározására és ezek egymástól való elhatárolására.[34] Álláspontjuk szerint gyűjtőfogalomnak a személyazonossághoz kapcsolódó bűncselekmények (identity-related crimes) tekinthetők. Ezen büntetendő magatartásoknak az elkövetési tárgya vagy eszköze a személyazonossághoz köt-

ben, ha az áldozat ennek a követelésnek nem tesz eleget, akkor további, erőteljesebb támadásokat indítanak a cég oldalával szemben, amely annak akár a teljes elérhetetlenségéhez is vezethet. *www.cardschat.com/news/pokerstars-ddos-attackers-arrested-by-Europol-extortion-group-also-alleged-to-have-targeted-betfair-neteller-18629*, valamint *www.neih.gov.hu/zsarolo-ddos.*

31 Akácz József: „XXXV. A vagyon elleni erőszakos bűncselekmények" in Kónya István (szerk): Magyar büntetőjog I–III. – Kommentár a gyakorlat számára (Budapest: HVG-ORAC 2017).

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. HL L 218/8. 2013.8.14.

33 OECD: *Policy Guidance on Online Identity Theft* (Seoul: 2008) 3.

34 Bert-Jaap Koops – Ronald Leenes: „ID Theft, ID Fraud and/or ID-related Crime. Definitions matter" *Datenschutz und Datensickerheit* 2006 (9) 556.

hető. A személyazonosság-csalás (identity fraud) pedig a csalásnak egy olyan speciális formája, amelynek az elkövetési tárgya vagy eszköze a személyazonossággal összefügg. A személyazonosság-lopás (identity theft) olyan speciális csalás vagy egyéb büntetendő magatartás, amelynek az elkövetési tárgya vagy eszköze más létező személynek a személyazonosságához kapcsolódik, valamint az érintett személy beleegyezése nélkül történik.[35]

A személyazonosság-lopás azért veszélyes különösen, mert az elkövető általában megszerzi valakinek az adatait, és mások előtt ennek a személynek adja ki magát, majd olyan magatartást tanúsít, amelynek negatív következményei a sértettnél realizálódnak.[36] Érdemes megjegyezni ugyanakkor, hogy a személyazonosság-lopást általában nem önálló deliktumként kezelik, hanem ezt az elnevezést a különböző büntetendő magatartások körének gyűjtőfogalmaként használják.[37] Jellemzően az egyes országok büntető törvénykönyveiben a következő magatartásokat rendelik büntetni: másnak a személyazonosságával összefüggő információinak jogosulatlan megszerzését, valamint az ezekkel való kereskedést, vagy a személyazonosságra vonatkozó hamis információk létrehozását, illetve ennek elősegítését.[38]

Fontos vizsgálni továbbá a teljesség igénye nélkül, csak példálózó jelleggel, hogy a szakirodalom szerint mely információk alkalmasak az adott személy azonosítására. Vannak olyan információk, amelyekkel születésünknél fogva rendelkezünk, így például a név, születési hely és idő (attributed identity), emellett az egyedi azonosítást lehetővé tevő biometrikus jellemzők, mint az ujjlenyomat, DNS-profil vagy írisz (biometric identity). Ezenkívül azok is idetartoznak, amelyek különböző életeseményünkhöz köthetők, példaként említhetők a végzettségek, munkahelyek, házasságkötés, vezetői engedély, személyazonosító igazolvány, társadalombiztosítási azonosító jel, bankkártya- és bankszámlaadatok (biographical identity), végül az általunk választottak is, így a felhasználónevek, jelszavak és egyebek is (chosen identity).[39]

Az Európai Unióban, a 2018. május 25-étől alkalmazandó, Általános Adatvédelmi Rendelet (a továbbiakban: GDPR)[40] nyújt segítséget, ugyanis meghatározza a személyes adat fogalmát, amely a természetes, élő személyek azonosítást teszi lehetővé. A GDPR 4. cikk 1. pontja szerint: „személyes adat: azonosított vagy azonosítható természetes személyre („érintett") vonatkozó bármely információ; azonosítható

[35] Koops –Leenes (35. lj.) 556.

[36] Korinek László: „Tendenciák korunk bűnözésében, bűnüldözésében" MTA székfoglaló előadás (Budapest: 2013) 44.

[37] A személyazonosság-lopással kapcsolatban az Egyesült Nemzetetek Szervezete kézikönyvet adott ki. Lásd United Nations Office on Drugs and Crime: *Handbook on Indentity-related crime* (Vienna 2011).

[38] Clough (9. lj.) 241.

[39] Bert-Jaap Koops – Ronald Leenes – Martin Meints – Nicole Van Der Meulen – David-Olivier Jaquet-Chiffelle: „A typology of identity-related crime. Conceptual, technical and legal issues" *Information, Communication & Society* Vol. 12. No. 1. February 2009 3–4.

[40] Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete 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) HL L 119/1. 2016.5.4.

az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható."[41] Ezt a fogalom-meghatározást emelték be a hazai információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.). értelmező rendelkezéseibe is.[42] Konkrét példa a személyes adatra: a vezetéknév és keresztnév, a lakcím, illetve a személyazonosító igazolvány száma. Megjegyzendő, hogy a személyes adatok köre azonban folyamatosan bővül, változik, hiszen függ a technológia fejlődésétől. Személyes adatnak minősülnek az érintettek által használt készülékek, alkalmazások, eszközök és protokollok által rendelkezésre bocsátott online azonosítók (például IP-címek és cookie-azonosítók), valamint az egyéb azonosítók széles köre is (például rádiófrekvenciás azonosító címkék).[43]

A személyazonosság-lopást a hazai Btk. sem önálló bűncselekményként szabályozza, de ez nem jelenti azt, hogy büntetlenül maradna ez a magatartás, mert a személyes adatokkal való visszaélést és az egyéb csalásjellegű magatartásokat is szankcióval fenyegeti a törvény.[44]

A személyes adatok hazai büntetőjogi védelmét a személyes adattal való visszaélés (Btk. 219. §) deliktuma hivatott elsősorban biztosítani, ezért indokoltnak tartom e speciális bűncselekménynek a részletes elemzését és a kapcsolódó fogalmak tisztázását. E tényállás a szabályozási struktúráját tekintve a keretdiszpozíciók közé tartozik, azaz olyan büntető rendelkezés, amely a büntetendő magatartások körét más jogszabályban meghatározott magatartási normára történő utalással határozza meg.[45] Jelen esetben az irányadó adatvédelmi szabályozás – vagyis a GDPR és az Infotv. – tölti meg tartalommal.

A bűncselekmény jogi tárgya a személyes adatok megismeréséhez és kezeléséhez fűződő jog[46], ezen keresztül pedig közvetve a személyes adatok védelméhez fűződő általános társadalmi érdek. Az Alaptörvény VI. cikkének (2) bekezdése szerint mindenkit megillet a személyes adatok védelméhez való jog.

A bűncselekmény elkövetési tárgya maga a személyes adat, míg az adat által azonosított vagy azonosítható természetes személy a bűncselekmény sértettjének

[41] Az amerikai szabályozás is hasonlóan határozza meg a személyazonosító információ fogalmát [15 U.S.C. 1681a. § (q)(3) (a)-(b)], amely magában foglalja az adott személy azonosítására – önállóan vagy más információval együtt – használható bármely nevet vagy számot. Ezt követően exemplifikatív felsorolást alkalmaz, amely például érinti az elektronikus és telekommunikációs azonosításra szolgáló információkat is.

[42] Infotv. 3. § 1–3. pont

[43] Péterfi Attila – Révész Balázs – Buzás Péter (szerk.): *Magyarázat a GDPR-ról* (Budapest: Wolters Kluwer, 2018) 64.

[44] Korinek (37 lj.) 44.

[45] Hollán Miklós: „A nemzeti büntetőjog kerettényállásai és az uniós jog" *Miskolci Jogi Szemle* 2018/2. 19–20.

[46] Belovics Ervin: „Az emberi méltóság és az egyes alapvető jogok elleni bűncselekmények – Btk. XXI. fejezet" in Belovics Ervin – Molnár Gábor Miklós – Sinku Pál (szerk.): Büntetőjog II. – Különös rész (Budapest: HVG-Orac 2018) 271.

tekinthető.[47] A személyes adat mint elkövetési tárgy azonban nemcsak a személyes adattal való visszaéléskor, hanem más bűncselekményekkel kapcsolatban is előfordulhat, így jellemzően a hivatali visszaélés (Btk. 305. §) és a tiltott adatszerzés (Btk. 422. §) esetén. A személyes adattal visszaélés bűncselekmény minősített esete valósul meg, ha az elkövetési tárgy különleges adat vagy bűnügyi személyes adat,[48] valamint a másik esetkör valósul meg, amennyiben hivatalos személyként vagy közmegbízatás felhasználásával követik el.

A törvény csak a kirívóan súlyos jogsértéseket kívánja szankcionálni, ezért a személyes adat jogosulatlan vagy a céltól eltérő kezelése csak akkor tényállásszerű, ha jelentős érdeksérelem okozásával vagy haszonszerzési célból követik el.[49] Az első esetben a jelentős érdeksérelemnek a sértetti oldalon kell beállnia, és annak objektíve be is kell következnie. Az elkövetési magatartás és az eredmény között okozati összefüggésnek kell fennállnia. Az eredmény bekövetkeztével válik befejezetté a bűncselekmény. A jelentős érdeksérelem fogalmát sem a Btk., sem más jogszabály nem határozza meg, így a jogalkalmazóknak az eset összes körülményeire tekintettel kell megítélniük.[50] A jelentős érdeksérelem objektív jellegű fogalom, vagyis a passzív alany szubjektív értékítéletének nincs jelentősége az eredmény megállapításának szempontjából. Megítélésénél figyelembe kell venni az érdeksérelem irányát, jellegét, minőségét, társadalmi jelentőségét, fokának, súlyának következményeit. Megvalósulhat személyi (erkölcsi) sérelem formájában (pl. nagymértékben negatívan befolyásolja a passzív alany szakmai tekintélyét, családi életét, erkölcsi megbecsülését),[51] de anyagi vonzata is lehet.[52]

[47] Gellér Balázs és Ambrus István az elkövetési tárgy új fogalmát határozza meg, amely szerint nem csupán személy vagy dolog lehet, hanem egy harmadik kategóriaként más speciális tárgy is. Ez a kitétel alá tartoznak a nem kézzelfogható, virtuális tárgyak, mint amilyen a személyes adat vagy az információs rendszeren tárolt adat. Az új, kiterjesztett elkövetési tárgy-fogalom alapján, tehát elkövetési tárgynak tekinthetők. Lásd Gellér Balázs – Ambrus István: *A magyar büntetőjog általános tanai I.* (Budapest: ELTE Eötvös 2019) 204–206. Ezzel ellentétes álláspontot képvisel Szomora Zsolt, aki szerint a személyes adat eszmei jellegére tekintettel elkövetési tárgynak nem tekinthető. Szomora Zsolt: „Btk. XXI. fejezet." in Karsai Krisztina (szerk.): Kommentár a Büntető Törvénykönyvhöz (Budapest: Complex 2013) 459.

[48] Infotv. 3. § 3. pont szerint „különleges adat: a) a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdekképviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat, b) az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat." 3. § 4. pont értelmében „bűnügyi személyes adat: a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat."

[49] Lásd a Btk. 219. §-hoz fűzött részletes miniszteri indokolását. A tényállás annyiban módosult, hogy a haszonszerzési célzat keretében a törvény már nem utal annak jogosulatlan jellegére.

[50] 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) 409.

[51] Belovics (47. lj.) 273. o.

[52] Horváth Tibor – Kereszti Béla – Maráz Vilmosné – Nagy Ferenc – Vida Mihály: *A magyar büntetőjog különös része* (Budapest: Korona 1999) 135.

A Kúria elvi éllel mondta ki, hogy a jelentős érdeksérelem okozásával elkövetett személyes adattal visszaélés elkövetője nemcsak az adatvédelmi jogszabályok fogalommeghatározásának megfelelő adatkezelő,[53] hanem bárki lehet.[54]

A Nemzeti Adatvédelmi és Információszabadság Hatóság kapcsolódó gyakorlata alapján különösen a bűncselekmény gyanúját keltő ügyeknek tekinthetők az olyan esetek, amikor ismeretlen személyek a felhasználó nevében és fényképei felhasználásával a közösségi oldalon álprofilt hoznak létre. E profilon keresztül a valódi ismerőseit jelöli be az elkövető, a nevében pedig üzeneteket, bejegyzéseket tesz közzé. A cél sok esetben az érintett lejáratása, hírnevének rontása mások előtt, és ez jelentős érdeksérelemmel járhat, [55] de előfordul az is, hogy mások személyes adatait használják fel bűncselekmények elkövetéséhez (például álprofilon vagy e-kereskedelmi platformon keresztül meghatározott pénzösszeget vagy bankkártyaadatot csalnak ki más gyanútlan felhasználóktól).

Ezzel összefüggésben érdemes rávilágítani például az IoT-eszközökkel kapcsolatban felmerülő veszélyekre is, hiszen ezek már sok esetben természetes személyekhez kötődnek, ami miatt a magánszféra érintettsége is megjelenik a használatukkor. Ha ezekhez a tárgyakhoz köthető információk egyszersmind az érintettekkel is kapcsolatba hozhatók, akkor máris személyes adatnak minősülnek. A rendszer felépítésében pedig általában több szereplő vesz részt, így a gyártók, alkalmazásfejlesztők, az adatok dolgozásában résztvevők, valamint az adatelemzők. Éppen ezért az adatalany számára az adatok útja könnyen teljesen követhetetlen az IoT-rendszerben, valamint minél több tárgy kapcsolódik a hálózatba, annál több adat gyűjthető az adott személyről, amely alapján akár részletes személyiségprofil is alkotható.[56]

A személyes adattal való visszaélés tényállásával kapcsolatban egyes szerzők szintén kritikaként fogalmazták meg, hogy nem nyújt megfelelő védelmet például a tömeges, valamint az érintett teljes személyiségét érintő profilozással szemben, a kiskorúak számára és végül az ún. deepfake-jelenség esetén.[57]

[53] Infotv. 3. § 9. pontja szerint „adatkezelő: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely – törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között – önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja."

[54] 1/2012. számú BJE-határozat.

[55] Péterfalvi – Eszteri (51. lj.) 411. o.

[56] Szabó Endre Győző: „II. fejezet: Adatvédelem és technológia" in Klein Tamás – Tóth András (szerk.): Technológia jog, robotjog, cyberjog (Budapest: Wolters Kluwer 2018) 33.

[57] A „deepfake" elkövetési forma esetében algoritmus segítségével képesek az adott személyről készült videófelvételben kicserélni az arcképet egy másik személy arcképére, amely bárki számára megtévesztő lehet. Lásd Miskolczi Barna – Szathmáry Zoltán: *Büntetőjogi kérdések az információk korában* (Budapest: HVG-ORAC 2019) 140–141.

A KRIPTOVALUTÁK HASZNÁLATÁNAK BÜNTETŐJOGI KIHÍVÁSAI

A blockchain technológia[58] megjelenésével párhuzamosan terjedt el a virtuális fizetési és értékképzési rendszerként működő kriptovaluták[59] használata. A kriptovaluták rendszere decentralizált. Továbbá közvetítő közbeiktatása nélkül működik, ami azt jelenti, hogy az utalásokat a felhasználók közvetlenül egymás között tudják lebonyolítani (Peer-to-Peer rendszer). Független, mert nem áll mögötte egyetlen ország, azok jegybankjai vagy más szervezet sem, hanem a felhasználók közös megegyezésén, bizalmán alapul a működése. A bitcoin tranzakciók például nyilvánosan nyomon követhetők – a blokklánc működéséből adódóan –, vagyis rögzíti a feladó és címzett felekhez tartozó ún. Bitcoin-címeket és a tranzakciók összegét a blokkcsatornán, azonban ezek nem köthetők konkrét személyekhez. Ezek ezért ún. pszeudoanonim tranzakciók.[60] Elérhetők azonban már olyan kriptovaluták (például Monero, Zcash és Dash) is, amelyek a bitcoinhoz képest is magasabb fokú titkosítást képesek biztosítani, és a technológiai korlátok miatt potenciálisan lehetetlenné válik egy-egy tranzakció mögött álló személy azonosítása, valamint az illegális értékmozgás nyomon követése, ami növelheti a bűnelkövetési célú felhasználást.[61] Ezt kihasználva például a Darknet-fórumokon is előszeretettel használják a kriptovalutákat fizetőeszközként. A legnagyobb kihívást a kriptovalutákkal elkövetett bűncselekmények felderítésében az jelenti, hogy a tranzakciók nem köthetők konkrét személyekhez, mert ezen utalásokhoz nincs szükség személyazonosításra vagy hitelesítésre. A decentralizáltságnak köszönhetően a virtuális fizetési rendszerek nem rendelkeznek központi felügyeleti szervvel, vagyis a büntetőeljárás során az eljáró hatóságok nem tudnak kihez fordulni a szükséges információkért, mint pél-

[58] Az elosztott főkönyvi technológiának (distributed ledger technology, avagy DLT) a leggyakrabban előforduló formája a blockchain (blokklánc). A DLT a tulajdonjog nyilvántartására szolgál – legyen szó pénzeszköz vagy más eszköz, vagyonelem tulajdonjogáról. Jelenleg a bankok ügyleteiket – vagyis azon műveleteiket, amelyek keretében pénz- vagy egyéb pénzügyi eszközük tulajdonjoga gazdát cserél – centralizált rendszereken keresztül bonyolítják le, amelyeket gyakran központi bankok üzemeltetnek. Az elosztott főkönyv ezzel szemben olyan tranzakciós adatbázis, amely több számítógépből álló hálózaton oszlik el, nem pedig központi helyen tárolják. A blokklánc esetén a tranzakciók csoportonként, azaz blokkonként időrendi sorrendben egymáshoz kapcsolva láncot alkotnak. A teljes láncot összetett matematikai algoritmusok védik, ezek gondoskodnak az adatok sértetlenségéről, biztonságáról. A lánc képezi az adatbázisban szereplő összes ügylet (pl. tranzakciók) átfogó nyilvántartását, ami a hálózat minden tagja számára elérhető.
Lásd: *www.ecb.europa.eu/explainers/tell-me-more/html/distributed_ledger_technology.hu.html.*

[59] A kriptovaluta ökoszisztéma részletesebb megismeréséhez lásd: Györfi András – Léderer András – Paluska Ferenc – Pataki Gábor – Trinh Anh Tuan: *Kriptopénz ABC* (Budapest: HVG Könyvek 2019).

[60] Székely Iván meghatározása szerint a *pszeudoanonimitás* azt jelenti, hogy *„van alanya az adatoknak, de az alany valós kilétét nem ismerjük; egy valós adatalanynak több fedőneve, profilja, virtuális személyisége is lehet”*. Az *anonimitás* lényege, hogy *„az adatokat, illetve az adatok kezelésével járó eseményeket, cselekvéseket nem tudjuk egy meghatározott személlyel kapcsolatba hozni”*. Székely Iván: „Privát szférát erősítő technológiák” *Információs Társadalom* 2008/1. 25.

[61] Lásd bővebben Robby Houben – Alexander Snyers: *Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion* (European Union 2018) 46–49.

dául a pénzintézetek esetén, amikor egyszerű banki megkeresés révén a pénzmozgás könnyen és egyszerűen nyomon követhető, valamint a pénzt küldő és fogadó személyek kiléte kideríthető.

A kriptovaluták megvásárlására általában vagy egy másik ilyen eszközzel rendelkező felhasználótól, vagy egy erre szakosodott kriptotőzsdén (például Coinbase) keresztül van lehetőség. Az előbbi esetet kihasználva jelent meg olyan csalásmódszer is, amely alapján az elkövetők bitcoin értékesítését ígérik a sértetteknek, azonban a megbízásokat végül nem teljesítik. A nyomozó hatóságok erre következtetnek abból, hogy megfigyelhető a banki ügyfeleknél az, hogy a fizetési számláikra jóváírások érkeznek, amelyek közleményei virtuális fizetőeszköz kereskedelemre utalnak. Ezt követően azonban a fizetési számlán csalásjellegű tevékenység miatt az átutalások törlését és az összegek visszautalását kérték.[62]

Megállapítandó – ahogy ezt Eszteri Dániel is szemlélteti egy hazai esetet bemutatva[63] –, hogy a kriptovalutával összefüggésben elkövetett vagyon elleni bűncselekmény minősítése a Btk. 373. §-ban szabályozott, hagyományos értelemben vett csalásnak felel meg. Ezzel kapcsolatban fontos a kárnak – mint tényállási elemnek – a fogalmával is részletesen foglalkozni. A büntetőjog a kár fogalmának tartalmi elemeit a polgári jogtól eltérően határozza meg. A vagyon fogalmát pedig sem a Btk., sem a Ptk. nem határozza meg. A Btk. 76. § értelmező rendelkezése azonban érinti, mert a vagyon fogalma alá vonja a vagyon hasznát, a vagyoni értékű jogot, a követelést, továbbá bármely pénzben kifejezhető értékkel bíró előnyt is. Az 1/2008. BJE határozat indokolása szerint a vagyon a pénzben kifejezhető értékkel bíró javakat és azok hasznát foglalja magában. Ezt figyelembe véve úgy gondolom, hogy a kriptovalutára is mint vagyonelemre tekinthetünk, és ezért a vagyonelkobzás tárgyát képezheti. A vagyonnal pedig azért kellett foglalkozni, mert a kár fogalmánál is megjelenik, mivel a Btk. 459. § (1) bekezdésének 16. pontja szerint a bűncselekménnyel a vagyonban okozott értékcsökkenést jelenti, ami kiegészül a csalás esetében a 373. § (7) bekezdéssel, amelynek értelmében kárnak kell tekinteni az igénybe vett szolgáltatás meg nem fizetett ellenértékét is. A kár pénzben kifejezhető, összegszerűen meghatározható anyagi értéknagyság.[64] Ezzel összefüggésben fontos megállapítani, hogy a virtuális fizetőeszközök a piaci viszonyok között konkrétan – egy adott időpontra vonatkozóan – kiszámítható, valódi pénzben kifejezhető értékkel rendelkeznek, így a kár – és a vagyoni hátrány – megállapításánál értékelhetők.[65]

A pénzmosás kihívás elé állítja a jogalkotókat, különösen a virtuális fizetőeszközök korában, ami a korábbiaknál sokkal kifinomultabb, nehezebben követhető módot nyújt az illegálisan szerzett jövedelmek tisztára mosására. A kriptovaluták használata pénzmosási és terrorizmusfinanszírozási kockázatokat hordoz magában, ami a decentralizált infrastruktúrának és a pszeudoanonim tranzakcióknak az eredmé-

[62] Nemzeti Adó- és Vámhivatal Központi Irányítása Pénzmosás és Terrorizmusfinanszírozás Elleni Iroda: *Éves jelentés – 2017. év* 11.

[63] Eszteri Dániel: „Egy Bitcoinnal elkövetett vagyon elleni bűncselekmény és az ahhoz kapcsolódó egyes jogi kérdések" *Infokommunikáció és Jog* 2017/1.

[64] Molnár Gábor: *Gazdasági bűncselekmények* (Budapest: HVG-ORAC 2009) 702.

[65] Eszteri (64. lj.) i. m. 30.

nye. Ezeknek a jellemzőknek a kihasználásával egyúttal a kriptovaluták új lehetőséget – mint adóparadicsomot – jelenthetnek az adófizetés kikerülésére is, mert segítségükkel az adócsalók könnyebben tudják a elrejteni azon jövedelmeket és bevételeket, amelyek után nem kívánnak adózni. Az adócsalást egyszerűbbé teszi az is, hogy általában a kriptovaluta-felhasználóknak nincs jelentési kötelezettségük.[66]

A tranzakciók szolgálhatják a legális üzleti műveletek elszámolását, de az illegális tevékenységekét is. A bűncselekményből származó pénzek kriptovalutákra történő átváltása, majd különböző címekre való tovább utalása alkalmas ezek tisztára mosására. A pénzmosás valamennyi fázisa a virtuális fizetőeszközök használata során is megvalósulhat a fiat pénzekhez hasonló módon.

Uniós szinten azonban a kriptováltó szolgáltatóknak ez idáig nem volt kötelezettségük arra, hogy a gyanús tevékenységeket azonosítsák, így a bűnelkövetők – és akár a terrorista csoportok is – pénzt utalhattak az uniós pénzügyi rendszerbe vagy a virtuális fizetőeszköz rendszereken belül azáltal, hogy elrejtik az átutalások, valamint magas fokú anonimitást élveznek ezeken a platformokon.

Az Európai Bizottság javaslatára 2018. május 30-án az Európai Parlament és Tanács az ötödik pénzmosás elleni irányelvet fogadta el, amelynek nóvuma, hogy először határozta meg a virtuális fizetőeszköz fogalmát. További jelentős lépésnek számít, hogy a hatályát kiterjesztették további kötelezett szolgáltatókra is, akik a virtuális fizetőeszközök és a rendeleti pénzek közötti átváltásával foglalkoznak, valamint a letétkezelő pénztárca-szolgáltatókra. Utóbbi fogalmát a 3. cikk 19. pontja határozza meg, amely alapján: „olyan szervezet, amely ügyfelei nevében virtuális fizetőeszközök tartására, tárolására és átutalására szolgáló kriptográfiai magánkulcsok megőrzésével kapcsolatos szolgáltatást nyújt".

Az ötödik pénzmosás elleni irányelv kötelezett szolgáltatókkal szemben az ún. „ismerd meg az ügyfeled" (Know Your Customer avagy KYC) követelményt támasztja, ami a meghatározott ügyfél-átvilágítási eljárás segítségével elősegíti a pénzmosási és a terrorizmusfinanszírozási kockázat csökkentését az ügyfelek azonosítása és kilétének ellenőrzése révén.

Az irányelv 47. cikkének (1) bekezdése értelmében a tagállamok kötelezettsége, hogy biztosítsák a virtuális fizetőeszközök és rendeleti pénzek közötti átváltási szolgáltatásokat nyújtó szolgáltatók, valamint a letétkezelő pénztárca-szolgáltatók nyilvántartásba vételét. Kétségkívül megállapítható, hogy a kriptovaluták a technológiai ismérveik folytán alkalmasak a pénzmosásra, mindezek ellenére fontos felhívni a figyelmet a hazai szabályozás egyik hiányosságára. A Btk. ugyanis a „dolgot" határozza meg a pénzmosás elkövetési tárgyaként, amelynek fogalmát a Btk. 402. § (1) bekezdése kiterjeszti a vagyoni jogosultságot megtestesítő okiratra és dematerializált értékpapírra is. Problematikus azonban, hogy a hatályos szabályozás értelmében nem tartozik az elkövetési tárgy fogalmi körébe a számlapénz és az elektronikus pénz, valamint a kriptovaluta sem. A pénzmosás – 2021. január 1-jétől hatályba lépő – új tényállása azonban a nemzetközi egyezmények szóhasz-

[66] U. S. Department of Justice: Report of the Attorney General's Cyber Digital Task Force (Washington: 2018) 55.

nálatát követi. A jogalkalmazói igényre figyelemmel felváltja a „dolog" fogalmát a „vagyon", amely szélesebb körű, a dolgokat és a testetlen vagyonelemeket egyaránt magában foglaló, általánosabb fogalom.

ÖSSZEGZÉS

A modern technológiák használata új veszélyeket hordoz magában. Valamennyi, a számítógépes hálózatra csatlakoztatott eszköz könnyedén válhat különböző kibertámadás célpontjává. A felhasználók részéről fokozott figyelmet és körültekintést igényel mindez. Az elkövetői oldalról pedig az online tér és az új innovatív megoldások megkönnyítik mind az új típusú bűncselekmények, mind a hagyományos deliktumok elkövetését. Ez a büntetőjogot kihívás elé állítja, hiszen a büntetendő magatartások minősítése esetenként kérdésessé válhat, valamint az újonnan megjelenő technológiákkal a jogalkotásnak is lépést kell tartania. Erre jó példa a kriptovaluták esete, amelyek a mai napig jogi szürke zónát képez, azonban bűnelkövetési célú használatuk vitathatatlan.